Séminaires & Congrès
12, 2005, p. 119–178

INDÉPENDANCE ALGÉBRIQUE DE VALEURS DE SÉRIES D'EISENSTEIN (THÉORÈME DE NESTERENKO)

par

Vincent Bosser

Résumé. — Ce texte est consacré au théorème de Nesterenko sur l'indépendance algébrique de valeurs de séries d'Eisenstein. Après en avoir rappelé l'énoncé et les principaux corollaires, on en présente la preuve, en mettant plus particulièrement l'accent sur le lemme de multiplicité utilisé. La preuve de ce lemme repose sur des résultats d'algèbre commutative (théorie de l'élimination) et de géométrie diophantienne qui sont expliqués en détail. Le texte se termine par un bref aperçu de différentes variantes de la preuve du théorème de Nesterenko, et notamment des méthodes permettant d'obtenir des versions quantitatives du théorème.

***Abstract* (Algebraic independence of values of Eisenstein series).** — This text is devoted to Nesterenko's theorem on the algebraic independence of values of Eisenstein series. After recalling its statement and its main corollaries, we present its proof, stressing particularly the multiplicity estimate used. The proof of this estimate rests on results from commutative algebra (elimination theory) and diophantine geometry which are explained in detail. The text ends with a brief overview of different variants of the proof of Nesterenko's theorem, and especially of the methods providing quantitative versions of the theorem.

Introduction

Soient P, Q et R les fonctions de Ramanujan : ces fonctions sont reliées aux séries d'Eisenstein E_2, E_4, E_6 de poids 2, 4, et 6 par les relations $P(e^{2\pi i\tau}) = E_2(\tau)$, $Q(e^{2\pi i\tau}) = E_4(\tau)$ et $R(e^{2\pi i\tau}) = E_6(\tau)$ (où $\tau \in \mathbb{C}$ est tel que $\Im m\, \tau > 0$). En 1996, Nesterenko a démontré le résultat remarquable suivant : si q est un nombre complexe non nul tel que $|q| < 1$, alors au moins trois nombres parmi q, $P(q)$, $Q(q)$, et $R(q)$ sont algébriquement indépendants sur $\mathbb{Q}$.

Les conséquences de ce théorème sont nombreuses. Par exemple, il implique l'indépendance algébrique sur $\mathbb{Q}$ des nombres π, e^{π} et $\Gamma(1/4)$, ou bien le théorème stéphanois

***Classification mathématique par sujets* (2000).** — 11J85, 11G, 11G35, 11G50.
Mots clefs. — Indépendance algébrique, séries d'Eisenstein, lemme de multiplicité, lemme de zéro, théorie de l'élimination, géométrie diophantienne, théorème de Bézout.

(anciennement *conjecture de Mahler*), ou bien encore la transcendance des nombres $\sum_{n\geqslant 0} q^{n^2}$ pour q algébrique vérifiant $0 < |q| < 1$ (nombres qui furent considérés tout d'abord par Liouville avec $q^{-1} \in \mathbb{Z}$, et dont il n'avait pu démontrer que l'irrationalité).

La démonstration de ce résultat suit dans ses grandes lignes le schéma classique d'une preuve de transcendance : construction d'une fonction auxiliaire F à forte multiplicité en zéro à l'aide d'un lemme de Siegel, existence et minoration d'une dérivée non nulle de F au point q d'ordre pas trop grand à l'aide d'une formule d'interpolation, majoration analytique au moyen des inégalités de Cauchy, application d'un lemme de multiplicité, et enfin application d'un critère d'indépendance algébrique.

En fait, l'apport de Nesterenko réside ici dans l'établissement du lemme de multiplicité, qui constitue le point crucial et difficile de la preuve. Ce lemme de multiplicité se démontre à l'aide des techniques de théorie de l'élimination et des outils de géométrie diophantienne qui ont été développés essentiellement par Nesterenko et Philippon au cours de ces 25 dernières années. L'objet de ces notes est d'expliquer comment on peut établir le théorème de Nesterenko, et plus particulièrement le lemme de multiplicité.

Après avoir rappelé, au § 1, l'énoncé et les principales conséquences du théorème, on présentera tout d'abord rapidement (§ 2) la démonstration initiale de Nesterenko, en admettant le lemme de multiplicité. On reviendra ensuite en détail sur la preuve de ce lemme : il s'agit ici d'une majoration de la multiplicité en 0 d'un polynôme non nul en les fonctions z, $P(z)$, $Q(z)$ et $R(z)$. Bien que la preuve proposée s'inspire du travail de Nesterenko, on adoptera ici une présentation différente sur plusieurs points. Tout d'abord, on utilisera le formalisme, les définitions et les résultats de Philippon (formes résultantes, cycles...) plutôt que le point de vue de Nesterenko. Ensuite, de nombreux arguments de la preuve originale ont été modifiés et certains points ont été (me semble-t-il) simplifiés et clarifiés. Cette preuve du lemme de multiplicité fait l'objet du § 4. Comme on l'a dit, elle repose sur des outils d'algèbre commutative et de géométrie diophantienne. Ceux-ci seront présentés au § 3 : théorie de l'élimination, théorie des hauteurs des variétés projectives, distance d'un point à une variété, théorèmes de Bézout arithmétique et métrique... Enfin, dans un dernier paragraphe (§ 5), on donnera un bref aperçu des différentes variantes de la preuve du théorème de Nesterenko, et notamment des méthodes permettant d'obtenir des versions quantitatives du théorème (le plus souvent sans démonstration).

Notations générales. — Dans tout ce texte, on note $\mathbb{N}$ (resp. $\mathbb{N}^*$) l'ensemble des entiers $\geqslant 0$ (resp. $\geqslant 1$). Si F est un polynôme en plusieurs indéterminées $z_1, \ldots, z_n$, on note $\deg F$ son degré total, et $\deg_{z_i} F$ son degré partiel par rapport à z_i. De façon analogue, si z^i désigne un groupe d'indéterminées $z_{i_1}, \ldots, z_{i_k}$, on note $\deg_{z^i} F$ le degré de F par rapport au groupe d'indéterminées z^i. Lorsque $\alpha = (\alpha_1, \ldots, \alpha_N)$ est un N-uplet d'éléments de $\mathbb{N}$ (où $N \in \mathbb{N}^*$), on note $|\alpha| = \alpha_1 + \cdots + \alpha_N$. Enfin, si K est un corps, on note $\overline{K}$ une clôture algébrique de K.

1. Énoncé du théorème et corollaires

Notons $\mathcal{H} = \{\tau \in \mathbb{C} \mid \Im m\,\tau > 0\}$. Pour tout $k \geqslant 2$, notons E_{2k} la série d'Eisenstein de poids k normalisée par

$$E_{2k}(\tau) = \frac{1}{2\zeta(2k)} \sum_{\substack{(m,n)\in\mathbb{Z}^2 \\ (m,n)\neq 0}} \frac{1}{(m\tau+n)^{2k}} \qquad (\tau \in \mathcal{H}).$$

Notons encore E_2 la fonction analytique dans $\mathcal{H}$ définie de façon analogue par

$$E_2(\tau) = \frac{1}{2\zeta(2)} \left[2\sum_{n\geqslant 1} \frac{1}{n^2} + 2\sum_{m\geqslant 1}\sum_{n\in\mathbb{Z}} \frac{1}{(m\tau+n)^2} \right].$$

On sait ([**Sch74**, pages 55 et 63] ou [**Lan76**, Chap. X]), que si $q = e^{2\pi i\tau}$ $(\tau \in \mathcal{H})$, les fonctions E_2, E_4, E_6 admettent le développement en série de Fourier suivant :

$$E_2(\tau) = 1 - 24 \sum_{n\geqslant 1} \sigma_1(n) q^n \tag{1}$$

$$E_4(\tau) = 1 + 240 \sum_{n\geqslant 1} \sigma_3(n) q^n \tag{2}$$

$$E_6(\tau) = 1 - 504 \sum_{n\geqslant 1} \sigma_5(n) q^n \tag{3}$$

où $\sigma_k(n) = \sum_{d|n} d^k$. On notera dans la suite P, Q et R les fonctions définies par $P(q) = E_2(\tau)$, $Q(q) = E_4(\tau)$ et $R(q) = E_6(\tau)$ (notations de Ramanujan). Les fonctions P, Q, R sont définies et analytiques dans le disque ouvert $\{q \in \mathbb{C} \mid |q| < 1\}$. De plus, elles vérifient le système différentiel suivant (voir [**Lan76**], Chap. X, theorem 5.3) :

$$(S_0) \qquad \begin{cases} \mathscr{D}P = \frac{1}{12}(P^2 - Q) \\ \mathscr{D}Q = \frac{1}{3}(PQ - R) \\ \mathscr{D}R = \frac{1}{2}(PR - Q^2) \end{cases}$$

où $\mathscr{D} = q\frac{d}{dq}$.

Comme on l'a dit dans l'introduction, le théorème que nous allons étudier dans ces notes est le suivant [**Nes96**] :

Théorème 1.1. — *Soit $q\in\mathbb{C}$ tel que $0<|q|<1$. Alors l'ensemble $\{q, P(q), Q(q), R(q)\}$ contient au moins trois nombres algébriquement indépendants sur $\mathbb{Q}$.*

Ce théorème fournit de nombreux résultats de transcendance ou d'indépendance algébrique. Nous ne donnerons ici à titre d'exemple que cinq corollaires. On pourra consulter [**Nes96**], [**NP01**, chap. 3] et [**Wal97**] pour d'autres résultats.

Selon les notations usuelles, on notera dans ce qui suit j l'invariant modulaire, et J la fonction définie dans le disque épointé $\{q \in \mathbb{C} \mid 0 < |q| < 1\}$ par $J(e^{2\pi i\tau}) = j(\tau)$ ($\tau \in \mathcal{H}$). Le premier corollaire que nous énoncerons est le suivant :

Corollaire 1.2

(i) *Soit $\tau \in \mathcal{H}$ qui ne soit congru ni à i ni à $\rho = e^{2\pi i/3}$ modulo $\mathrm{SL}_2(\mathbb{Z})$, et soit $q = e^{2\pi i\tau}$. Alors on a*

$$\operatorname{degtr}_{\mathbb{Q}} \mathbb{Q}(q, J(q), J'(q), J''(q)) \geqslant 3.$$

(ii) *En particulier, pour tout $q \in \mathbb{C}$ algébrique tel que $0 < |q| < 1$, les nombres $J(q)$, $J'(q)$ et $J''(q)$ sont algébriquement indépendants sur $\mathbb{Q}$.*

Démonstration. — En utilisant la relation bien connue [**Lan76**, chap. 1, § 3]

$$J = 1728 \frac{Q^3}{Q^3 - R^2}$$

et le système différentiel (S_0), on vérifie que l'on a les formules :

$$P = 6\frac{\mathscr{D}^2 J}{\mathscr{D} J} - 4\frac{\mathscr{D} J}{J} - 3\frac{\mathscr{D} J}{J - 1728}, \ Q = \frac{(\mathscr{D} J)^2}{J(J-1728)}, \ R = -\frac{(\mathscr{D} J)^3}{J^2(J-1728)}.$$

Ces formules sont valables lorsque $\mathscr{D} J(q) \neq 0$, $J(q) \neq 0$ et $J(q) \neq 1728$, *i.e.* lorsque τ n'est congru ni à i ni à ρ modulo $\mathrm{SL}_2(\mathbb{Z})$. Il en résulte que dans ce cas les corps $\mathbb{Q}(q, J(q), J'(q), J''(q))$ et $\mathbb{Q}(q, P(q), Q(q), R(q))$ sont égaux. Ceci démontre (i).

Pour démontrer (ii), il suffit de constater que si $q = e^{2\pi i\tau}$ est algébrique, alors τ ne peut pas être algébrique irrationnel d'après le théorème de Gelfond-Schneider (car $2\pi i$ est un logarithme de 1)[(1)]. Donc τ vérifie les hypothèses de (i). □

On remarquera que la partie (ii) du corollaire entraîne en particulier le théorème stéphanois (conjecture de Mahler).

Les deux corollaires suivants concernent les fonctions elliptiques et généralisent des résultats antérieurs de Chudnovsky [**Chu84**].

Corollaire 1.3. — *Soient $\wp$ une fonction elliptique de Weierstrass d'invariants g_2, g_3 algébriques, (ω_1, ω_2) une base du réseau des périodes de $\wp$ telle que $\Im m(\omega_2/\omega_1) > 0$, η_1 la quasi-période correspondant à ω_1, et $\tau = \omega_2/\omega_1$. Alors les nombres $e^{2\pi i\tau}$, ω_1/π et η_1/π sont algébriquement indépendants sur $\mathbb{Q}$.*

Démonstration. — D'après des formules classiques (voir [**Lan87**], chap. 4, formules (5) et (6) p. 44 et chap. 18, formule (2) p. 249), on a, en notant $q = e^{2\pi i\tau}$:

$$P(q) = 3\frac{\omega_1}{\pi}\frac{\eta_1}{\pi}, \quad Q(q) = \frac{3}{4}\Big(\frac{\omega_1}{\pi}\Big)^4 g_2, \quad R(q) = \frac{27}{8}\Big(\frac{\omega_1}{\pi}\Big)^6 g_3.$$

[(1)] Théorème de Gelfond-Schneider [**Wal00**] : soient $\alpha \in \overline{\mathbb{Q}}$, $\alpha \neq 0$, et $\beta \in \overline{\mathbb{Q}} \smallsetminus \mathbb{Q}$. Alors, pour toute détermination $\ell \neq 0$ du logarithme de α (*i.e.* pour tout $\ell \in \mathbb{C}$, $\ell \neq 0$, tel que $e^{\ell} = \alpha$), le nombre $\alpha^{\beta} := e^{\beta\ell}$ est transcendant.

On en déduit $\mathbb{Q}(q, P(q), Q(q), R(q)) \subset \mathbb{Q}(q, g_2, g_3, \omega_1/\pi, \eta_1/\pi) \subset \overline{\mathbb{Q}}(q, \omega_1/\pi, \eta_1/\pi)$, d'où le corollaire. □

Corollaire 1.4

(i) *Soit $\wp$ une fonction elliptique de Weierstrass d'invariants g_2, g_3 algébriques, correspondant à une courbe elliptique à multiplications complexes par le corps quadratique K. Alors, si ω est une période non nulle de $\wp$ et $\tau \in K$ est tel que $\Im m\,\tau \neq 0$, les trois nombres π, ω et $e^{2\pi i\tau}$ sont algébriquement indépendants sur $\mathbb{Q}$.*

(ii) *En particulier, les nombres π, e^{π} et $\Gamma(1/4)$ (resp. π, $e^{\pi\sqrt{3}}$ et $\Gamma(1/3)$) sont algébriquement indépendants sur $\mathbb{Q}$.*

Démonstration

(i) Il n'y a pas de restriction à supposer la période $\omega = \omega_1$ primitive (*i.e.* multiple d'aucune autre période). Soit alors ω_2 telle que (ω_1, ω_2) soit une base du réseau des périodes de $\wp$ et telle que $\omega_2/\omega_1 \in \mathcal{H}$. Notons η_1, η_2 les quasi-périodes correspondant à ω_1 et ω_2. On peut supposer sans perte de généralité que $\tau = \omega_2/\omega_1$ (car ω_2/ω_1 est dans $K = \mathbb{Q}(\tau)$, donc de la forme $a + b\tau$, $a, b \in \mathbb{Q}$, $b \neq 0$). Maintenant, d'après [**Mas75**, Chap. 3, Lemma 3.1], il existe $\kappa \in \overline{\mathbb{Q}}$ et des entiers A, B, C avec $C \neq 0$ tels que

$$A + B\tau + C\tau^2 = 0 \qquad \text{et} \qquad A\eta_1 - C\tau\eta_2 = \kappa\tau\omega_1. \tag{4}$$

D'autre part, on dispose de la relation de Legendre :

$$\tau\omega_1\eta_1 - \omega_1\eta_2 = 2\pi i. \tag{5}$$

On déduit aisément de (4) et (5) que $\eta_1 \in \overline{\mathbb{Q}}(\pi, \omega_1)$, d'où $\overline{\mathbb{Q}}(e^{2\pi i\tau}, \omega_1/\pi, \eta_1/\pi) \subset \overline{\mathbb{Q}}(e^{2\pi i\tau}, \pi, \omega_1)$. Le corollaire 1.3 donne alors immédiatement le résultat.

(ii) On applique (i) à la courbe elliptique d'équation $y^2 = 4x^3 - 4x$, pour laquelle on a $K = \mathbb{Q}(i)$. On prend alors $\tau = i$ et pour ω la période fondamentale réelle $\omega = 2\int_1^\infty \frac{dt}{\sqrt{4t^3-4t}} = \frac{1}{2}B(1/4, 1/2) = \frac{\Gamma(1/4)^2}{\sqrt{8\pi}}$, où B désigne la fonction bêta d'Euler. On procède de façon analogue pour les nombres π, $e^{\pi\sqrt{3}}$ et $\Gamma(1/3)$ avec la courbe elliptique d'équation $y^2 = 4x^3 - 4$. Voir [**Nes96**, Corollary 5] pour les détails. □

Une conséquence remarquable du corollaire 1.4 est la suivante.

Corollaire 1.5. — *Pour tout entier $d \geqslant 1$, les nombres π et $e^{\pi\sqrt{d}}$ sont algébriquement indépendants sur $\mathbb{Q}$.*

Démonstration. — Pour tout corps quadratique imaginaire $K = \mathbb{Q}(\sqrt{-d})$, il existe une fonction $\wp$ de Weierstrass d'invariants g_2, g_3 algébriques et définissant une courbe elliptique CM dont le corps des multiplications complexes est K. Il suffit alors d'appliquer le corollaire 1.4 (i) avec $\tau = i\sqrt{d}$. □

Le dernier corollaire que nous citerons concerne les fonctions thêta de Jacobi. Pour $q \in \mathbb{C}$ tel que $|q| < 1$, notons

$$\theta_2(q) = 2q^{1/4} \sum_{n \geqslant 0} q^{n(n+1)}, \qquad \theta_3(q) = 1 + 2 \sum_{n \geqslant 1} q^{n^2}, \qquad \theta_4(q) = \theta_3(-q).$$

On a alors :

Corollaire 1.6. — *Soit $i \in \{2,3,4\}$. Alors, pour tout $q \in \mathbb{C}$ algébrique tel que $0 < |q| < 1$, les trois nombres $\theta_i(q)$, $\theta_i'(q)$ et $\theta_i''(q)$ sont algébriquement indépendants sur $\mathbb{Q}$.*

Démonstration du corollaire 1.6. — L'assertion provient de l'existence de relations algébriques liant les nombres $P(q^2)$, $Q(q^2)$, $R(q^2)$ aux nombres $\theta_i(q)$, $\mathscr{D}\theta_i(q)$ et $\mathscr{D}^2\theta_i(q)$ (où $\mathscr{D} = q\frac{d}{dq}$). Voir [**Ber97**]. $\square$

Les nombres $\sum_{n \geqslant 0} q^{-n^2}$ avec $q \in \mathbb{N}$ et $q > 1$ avaient déjà été considérés par Liouville en 1851, mais la méthode qui lui avait permis de trouver les premiers exemples de nombres transcendants ne lui avait donné ici que des résultats d'irrationalité. La question de la transcendance de ces nombres était ouverte depuis cette date.

2. Preuve du théorème

2.1. Schéma de la preuve. — Dans tout ce paragraphe 2, on utilisera la notation suivante. Si A est un polynôme à coefficients dans $\mathbb{C}$ (en une ou plusieurs indéterminées), on note $H(A)$ le maximum des modules de ses coefficients (« hauteur » du polynôme A).

Pour démontrer l'indépendance algébrique de nombres, on dispose de critères d'indépendance algébrique généraux. L'idée est ici d'appliquer le critère suivant, qui est un cas particulier du résultat principal de [**Phi86**] :

Théorème 2.1. — *Soient $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ et $k \geqslant 0$ un entier. Soient encore $\tau, \lambda : \mathbb{N} \to \mathbb{R}$ des fonctions croissantes telles que λ/τ^{k+1} soit croissante, et telles que*

$$\lim_{N \to +\infty} \tau(N) = \lim_{N \to +\infty} \lambda(N) = +\infty, \qquad \lim_{N \to +\infty} \frac{\lambda(N+1)}{\lambda(N)} = 1,$$

et

$$\lim_{N \to +\infty} \frac{\lambda(N)}{\tau(N)^{k+1}} = +\infty.$$

Supposons qu'il existe une suite de polynômes $B_N \in \mathbb{Z}[X_1, \ldots, X_n]$ ($N \in \mathbb{N}$) telle que

$$\deg B_N \leqslant \tau(N), \qquad \log H(B_N) \leqslant \tau(N)$$

et

$$e^{-\gamma_2 \lambda(N)} \leqslant |B_N(\alpha_1, \ldots, \alpha_n)| \leqslant e^{-\gamma_1 \lambda(N)},$$

où γ_1, γ_2 sont des réels positifs ne dépendant que de k, n et $\alpha_1, \ldots, \alpha_n$. Alors on a

$$\operatorname{degtr}_{\mathbb{Q}} \mathbb{Q}(\alpha_1, \ldots, \alpha_n) \geqslant k+1.$$

Démonstration. — Reprenant les notations de [**Phi86**], on vérifie que les polynômes B_N de l'énoncé n'ont pas de zéro dans la boule fermée $B(\theta, e^{-\gamma_2\lambda(N)-c_1\tau(N)})$ et que $\overline{\mathbf{h}}(B_N) \leqslant c_2\tau(N)$, où c_1 et c_2 sont des réels positifs dépendant de n et $\alpha_1, \dots, \alpha_n$. On applique alors [**Phi86**, théorème 2.11] en prenant $K = \mathbb{Q}$, $\theta = (\alpha_1, \dots, \alpha_n)$, $\delta(N) = \tau(N)$, $\sigma(N) = c_2\tau(N)$, $S(N) = \gamma_1\lambda(N)$, $R(N) = \gamma_2\lambda(N) + c_2\tau(N)$, et en prenant pour la suite d'idéaux $(I_N)_{N\geqslant 0}$ la suite $(B_N)_{N\geqslant 0}$. $\square$

Dans notre cas, on a $n = 4$ et $(\alpha_1, \dots, \alpha_4) = (q, P(q), Q(q), R(q))$. On veut donc construire une suite de polynômes B_N de degrés et hauteurs contrôlés (ne croissant pas trop vite), et obtenir une minoration et une majoration du nombre $|B_N(q, P(q), Q(q), R(q))|$, de sorte que les hypothèses du critère 2.1 soient satisfaites.

Comme on l'a dit, la construction suit un schéma classique en transcendance. En fait, celle-ci va être rendue possible essentiellement grâce aux trois propriétés suivantes :

– Les fonctions P, Q, R ont des coefficients de Taylor entiers qui ne croissent pas trop vite ;
– Elles satisfont le système d'équations différentielles (S_0) ;
– On dispose du « lemme de multiplicité » 2.9.

Le schéma de la preuve est le suivant. On commence par se fixer un entier N suffisamment grand. À l'aide d'un lemme de Siegel, on construit alors un polynôme $A = A_N \in \mathbb{Z}[Z, X_1, X_2, X_3]$, de degré et hauteur contrôlés en fonction de N, et tel que la fonction $F = F_N$ définie par $F(z) = A(z, P(z), Q(z), R(z))$ soit non nulle et ait un zéro en $z = 0$ avec une multiplicité M élevée (à savoir $M \geqslant N^4/2$) (première étape). Lors d'une seconde étape, on montre, à l'aide d'une formule d'interpolation, qu'il existe une dérivée $F^{(T)}(q)$ non nulle avec un ordre de dérivation T pas trop grand, et on minore $|F^{(T)}(q)|$ en fonction du paramètre M. Lors d'une troisième étape, on majore, par des arguments analytiques (inégalités de Cauchy), le nombre $|F^{(T)}(q)|$ en fonction de N et M. Comme les fonctions P, Q, R vérifient le système (S_0), on vérifie alors que la fonction $(12z)^T F^{(T)}(z)$ est de la forme $B(z, P(z), Q(z), R(z))$, où $B = B_N \in \mathbb{Z}[Z, X_1, X_2, X_3]$. La dernière étape consiste à vérifier que ce polynôme vérifie bien les hypothèses du critère d'indépendance algébrique 2.1. Pour ce faire, on majore $\deg B$ et $H(B)$ grâce aux majorations de $\deg A$, $H(A)$ et T obtenues dans les étapes 1 et 2, et on estime $|B(q, P(q), Q(q), R(q))|$ au moyen des estimations de $|F^{(T)}(q)|$ obtenues dans les étapes 2 et 3. Toutes ces estimations dépendent de N, mais aussi de M. Pour pouvoir appliquer le critère 2.1, il faut donc encore éliminer le paramètre M. Cette suppression du paramètre M repose sur la minoration $M \geqslant N^4/2$, ainsi que sur un lemme de multiplicité (lemme 2.9), qui donne une majoration de M en fonction de N.

2.2. Première étape : construction d'une fonction auxiliaire. — Soit donc $q \in \mathbb{C}$ tel que $0 < |q| < 1$. On se fixe N un entier, suffisamment grand pour pouvoir satisfaire aux différentes inégalités qui interviendront par la suite. Cet entier est désormais fixé jusqu'à la fin du paragraphe 2.5. En particulier, la fonction F et les polynômes A et B construits ci-après dépendent de N (même si pour alléger les notations on ne fera pas figurer l'indice N). On appellera dans la suite « constantes » des nombres réels ne dépendant que de q.

La première étape de la démonstration consiste à construire un polynôme auxiliaire non nul $A = A_N \in \mathbb{Z}[Z, X_1, X_2, X_3]$, de degré et de hauteur petits, et tel que la fonction définie par $F(z) = A(z, P(z), Q(z), R(z))$ ait un ordre élevé en $z = 0$. De façon précise, on démontre :

Proposition 2.2. — *Il existe un polynôme $A = A_N \in \mathbb{Z}[Z, X_1, X_2, X_3]$, $A \neq 0$, tel que*

$$\deg_Z A \leqslant N, \quad \deg_{X_i} A \leqslant N \ (1 \leqslant i \leqslant 3), \quad \log H(A) \leqslant 61 N \log N, \tag{6}$$

et tel que si on pose $F(z) = A(z, P(z), Q(z), R(z))$, alors on ait

$$\mathrm{ord}_0 F(z) \geqslant \frac{1}{2} N^4. \tag{7}$$

La démonstration de ce résultat va se faire de façon classique à l'aide d'un lemme de Siegel. Le lemme de Siegel que nous utiliserons est le suivant. Il s'agit d'un résultat assurant l'existence d'une solution en nombres entiers non triviale et pas trop grande, pour un système d'équations linéaires homogènes à coefficients entiers.

Lemme 2.3. — *Soient ν, μ des entiers $\geqslant 1$ tels que $\mu > \nu$ et $d_{ij} \in \mathbb{Z}$, $1 \leqslant i \leqslant \nu$, $1 \leqslant j \leqslant \mu$. Soit encore B un réel tel que $B \geqslant 1$ et $B \geqslant \max_{\substack{1 \leqslant i \leqslant \nu \\ 1 \leqslant j \leqslant \mu}} |d_{ij}|$. Alors il existe $x = (x_1, \ldots, x_\mu) \in \mathbb{Z}^\mu \smallsetminus \{0\}$ vérifiant*

$$\sum_{1 \leqslant j \leqslant \mu} d_{ij} x_j = 0, \qquad 1 \leqslant i \leqslant \nu,$$

et

$$\max_{1 \leqslant j \leqslant \mu} |x_j| \leqslant (\mu B)^{\nu/(\mu - \nu)}.$$

Démonstration. — Voir [**Wal74**, page 32]. La démonstration repose sur le principe des tiroirs. □

Démonstration de la proposition 2.2. — Écrivons $A = \sum_{\alpha \in \mathcal{A}} a_\alpha Z^{\alpha_0} X_1^{\alpha_1} X_2^{\alpha_2} X_3^{\alpha_3}$, où $a_\alpha \in \mathbb{Z}$, $\alpha = (\alpha_0, \alpha_1, \alpha_2, \alpha_3) \in \mathbb{N}^4$, et $\mathcal{A} = \{\alpha \in \mathbb{N}^4 \mid 0 \leqslant \alpha_i \leqslant N, 0 \leqslant i \leqslant 3\}$. Il suffit de vérifier $\mathrm{ord}_0 F(z) \geqslant \big[\frac{(N+1)^4}{2}\big]$. Écrivons, pour $\alpha \in \mathcal{A}$ et $|z| < 1$,

$$z^{\alpha_0} P(z)^{\alpha_1} Q(z)^{\alpha_2} R(z)^{\alpha_3} = \sum_{n \geqslant 0} d_{\alpha n} z^n \qquad (d_{\alpha n} \in \mathbb{Z}).$$

On a alors

$$F(z) = \sum_{n \geqslant 0} \Big(\sum_{\alpha \in \mathcal{A}} a_\alpha d_{\alpha n} \Big) z^n,$$

et la condition cherchée s'écrit

$$\sum_{\alpha \in \mathcal{A}} d_{\alpha n} a_\alpha = 0, \qquad 0 \leqslant n \leqslant \Big[\frac{(N+1)^4}{2}\Big] - 1. \tag{8}$$

Pour trouver une solution de ce système en nombres entiers petite et non triviale, on applique le lemme de Siegel 2.3. De la majoration évidente $|\sigma_k(n)| \leqslant n^{k+1}$ pour $n \geqslant 1$ et de la définition de $d_{\alpha n}$ on déduit facilement l'estimation suivante pour les coefficients du système, valable pour $\alpha \in \mathcal{A}$ et $n \geqslant 1$:

$$\begin{aligned} |d_{\alpha n}| &\leqslant 504^{\alpha_1+\alpha_2+\alpha_3} n^{2\alpha_1+4\alpha_2+6\alpha_3} \#\{k \in \mathbb{N}^{\alpha_1+\alpha_2+\alpha_3} \mid |k| = n - \alpha_0\} \\ &\leqslant 504^{3N} n^{12N} (n+1)^{3N} \leqslant (2\cdot 504)^{3N} n^{15N}. \end{aligned} \tag{9}$$

On obtient donc la majoration, pour $\alpha \in \mathcal{A}$ et $0 \leqslant n \leqslant \left[\frac{(N+1)^4}{2}\right] - 1$:

$$|d_{\alpha n}| \leqslant (2\cdot 504)^{3N} \left(\frac{(N+1)^4}{2}\right)^{15N}.$$

Le nombre d'équations est ici $\nu = \left[\frac{(N+1)^4}{2}\right] < (N+1)^4$ et le nombre d'inconnues est $\mu = \operatorname{card} \mathcal{A} = (N+1)^4$. On a de plus $\frac{\nu}{\mu-\nu} \leqslant 1$, donc par le lemme 2.3 il existe des entiers a_α non tous nuls satisfaisant à (8) et tels que

$$\max_{\alpha\in\mathcal{A}} |a_\alpha| \leqslant (N+1)^4 (2\cdot 504)^{3N} \left(\frac{(N+1)^4}{2}\right)^{15N} \leqslant N^{61N}.$$

Ceci démontre la proposition 2.2. □

2.3. Deuxième étape : interpolation. — On note ici et dans tout le paragraphe 2, $M = \operatorname{ord}_{z=0} F$ (où F est la fonction de la proposition 2.2). On a $M < \infty$ car les fonctions z, $P(z)$, $Q(z)$ et $R(z)$ sont algébriquement indépendantes sur $\mathbb{C}$ en vertu d'un résultat de Mahler [**Mah69**][(2)]. De plus, on notera pour la suite que la minoration (7) implique que M tend vers l'infini avec N. Dorénavant, toutes les estimations rencontrées seront uniquement fonctions de ces deux paramètres N et M.

On définit encore des constantes r et γ par

$$r = \min\{\frac{1+|q|}{2}, 2|q|\} \qquad \text{et} \qquad \gamma = 36 \left(\log \frac{r}{|q|}\right)^{-1}. \tag{10}$$

On a $0 < |q| < r < 1$ et $\gamma > 1$.

Le but de la deuxième étape est d'établir la proposition suivante :

Proposition 2.4. — *Il existe un entier T tel que $0 \leqslant T \leqslant \gamma N \log M$ et pour lequel on a*

$$|F^{(T)}(q)| \geqslant \left(\frac{|q|}{2}\right)^{2M}. \tag{11}$$

La preuve de ce résultat repose sur une formule d'interpolation, outil classique en transcendance. Le lemme qui nous est ici utile est le suivant :

(2) Ce résultat est aussi une conséquence du lemme de multiplicité énoncé au § 2.5, mais la preuve de ce lemme de multiplicité utilise le résultat de Mahler !

Lemme 2.5. — *Soient M et L des entiers $\geqslant 0$, $r \in \mathbb{R}$ et $q \in \mathbb{C}$ tels que $0 < |q| \leqslant r$. Soit F une fonction analytique dans un ouvert contenant le disque $\{z \in \mathbb{C} \mid |z| \leqslant r\}$ et telle que* $\operatorname{ord}_0 F(z) \geqslant M$. *Alors on a*

$$\frac{r^M}{M!}|F^{(M)}(0)| \leqslant \Big(\frac{r}{|q|}\Big)^{-L}|F|_r + 2^{M+L}\Big(\frac{r}{|q|}\Big)^M \sum_{\ell=0}^{L-1}\Big(\frac{|q|}{2}\Big)^\ell \frac{|F^{(\ell)}(q)|}{\ell!},$$

où on a noté $|F|_r = \sup\{|F(z)|,\, |z| = r\} = \sup\{|F(z)|,\, |z| \leqslant r\}$.

Démonstration. — Voir [**Nes96**], preuve du lemme 2.3 (voir aussi [**Wal97**, lemme 3]). □

Nous allons appliquer ce lemme à notre fonction F construite au paragraphe précédent. Nous avons besoin pour cela d'estimer la quantité $|F|_r$ en fonction de nos paramètres M et N. Cette estimation va résulter du lemme facile suivant :

Lemme 2.6. — *Si r est défini comme en (10), F est la fonction de la proposition 2.2 et $M = \operatorname{ord}_0 F$, alors on a, pour tout $z \in \mathbb{C}$ tel que $|z| \leqslant r$,*

$$|F(z)| \leqslant |z|^M M^{35N}.$$

Démonstration. — On procède comme dans [**NP01**, chap. 3]. Écrivons $F(z) = \sum_{n\geqslant M} f_n z^n$. Avec les notations de la preuve de la proposition 2.2, on a, en utilisant l'estimation (9) et puisque N est choisi suffisamment grand :

$$|f_n| = \Big|\sum_{\alpha\in\mathcal{A}} a_\alpha d_{\alpha n}\Big| \leqslant (N+1)^4 \cdot \max_\alpha |d_{\alpha n}| \cdot H(A) \leqslant n^{15N} N^{62N} \quad (n \geqslant M).$$

Pour $|z| \leqslant r$, on a maintenant :

$$\begin{aligned}|F(z)| &\leqslant |z|^M N^{62N} \sum_{n\geqslant 0}(n+M)^{15N}|z|^n \\ &\leqslant |z|^M N^{62N}(1+M)^{15N}\big(1 + \sum_{n\geqslant 1} n^{15N} r^n\big) \\ &\leqslant |z|^M N^{62N}(1+M)^{15N}\frac{(15N)!}{(1-r)^{15N+1}} \\ &\leqslant |z|^M M^{35N}\end{aligned}$$

en utilisant (7) et en notant que r est une constante. □

Démonstration de la proposition 2.4. — Définissons $L = [\gamma N \log M] + 1$ et posons $U = \max_{0\leqslant \ell\leqslant L-1} |F^{(\ell)}(q)|$. En appliquant le lemme 2.5 et en remarquant que $F^{(M)}(0)/M! \in \mathbb{Z} \smallsetminus \{0\}$, on obtient :

$$r^M \leqslant \frac{r^M}{M!}|F^{(M)}(0)| \leqslant \Big(\frac{r}{|q|}\Big)^{-L}|F|_r + 2^{M+L}U\Big(\frac{r}{|q|}\Big)^M \sum_{\ell=0}^{L-1}\Big(\frac{|q|}{2}\Big)^\ell \cdot \frac{1}{\ell!},$$

d'où, puisque $|q| \leqslant 2$ et $|F|_r \leqslant r^M M^{35N}$ d'après le lemme 2.6 :

$$\Big(\frac{r}{|q|}\Big)^L \leqslant M^{35N} + U\Big(\frac{r}{|q|}\Big)^L\Big(\frac{2}{|q|}\Big)^M 2^L e.$$

Maintenant, l'inégalité $\gamma N \log M \leqslant L$ et la définition de γ donnent $M^{35N} \leqslant \frac{1}{M^N}\big(\frac{r}{|q|}\big)^L \leqslant \frac{1}{2}\big(\frac{r}{|q|}\big)^L$, d'où, pour $N \gg 0$, la minoration

$$U\Big(\frac{r}{|q|}\Big)^L\Big(\frac{2}{|q|}\Big)^M 2^L e \geqslant \frac{1}{2}\Big(\frac{r}{|q|}\Big)^L.$$

On en déduit facilement $U \geqslant \big(\frac{|q|}{2}\big)^{2M}$ grâce à (7), d'où la proposition. □

2.4. Troisième étape : majoration de $|F^{(T)}(q)|$. — Il s'agit de prouver ici la proposition 2.7. Là encore, l'argument est classique en transcendance et repose sur les inégalités de Cauchy.

Proposition 2.7. — *On a pour le nombre $|F^{(T)}(q)|$ la majoration suivante :*

$$|F^{(T)}(q)| \leqslant r^{M/2}.$$

Démonstration. — On applique les inégalités de Cauchy à la fonction F et au cercle $\{z \in \mathbb{C} \mid |z-q| = R\} \subset \{z \in \mathbb{C} \mid |z| \leqslant r\}$, où $R = r - |q|$. On obtient

$$|F^{(T)}(q)| \leqslant \frac{T!}{R^T}\sup_{|z-q|=R}|F(z)| \leqslant \frac{T^T}{R^T} r^M M^{35N},$$

en utilisant le lemme 2.6. Il suffit maintenant de remarquer que l'on a $0 < r < 1$, $N \leqslant (2M)^{1/4}$ et $T \leqslant \gamma N \log M \leqslant \gamma (2M)^{1/4}\log M$ pour conclure. □

2.5. Quatrième étape : conclusion. — Pour vérifier les hypothèses du critère d'indépendance algébrique il nous faut trouver un polynôme $B = B_N$ adéquat. Or, il est facile de voir que puisque les fonctions P, Q, R satisfont le système différentiel (S_0), la fonction $z^T F^{(T)}(z)$ est un polynôme en les fonctions z, $P(z)$, $Q(z)$, $R(z)$. C'est ce polynôme (après multiplication par un dénominateur pour le rendre à coefficients entiers) qui sera notre polynôme B.

Plus précisément, soit $D : \mathbb{C}(Z, X_1, X_2, X_3) \to \mathbb{C}(Z, X_1, X_2, X_3)$ l'opérateur différentiel associé au système (S_0), c'est-à-dire défini par

$$(12)\quad D = Z\frac{\partial}{\partial Z} + \frac{1}{12}(X_1^2 - X_2)\frac{\partial}{\partial X_1} + \frac{1}{3}(X_1X_2 - X_3)\frac{\partial}{\partial X_2} + \frac{1}{2}(X_1X_3 - X_2^2)\frac{\partial}{\partial X_3}.$$

Alors, pour tout $E \in \mathbb{C}(Z, X_1, X_2, X_3)$, on a, en notant $f(z) = E(z, P(z), Q(z), R(z))$,

$$zf'(z) = DE\,(z, P(z), Q(z), R(z)).$$

On va tout d'abord montrer (le polynôme A étant celui défini dans la proposition 2.2 et l'entier T celui de la proposition 2.4) :

Proposition 2.8. — *Soit B la fraction rationnelle définie par $B(Z,X_1,X_2,X_3) = (12Z)^T(Z^{-1}D)^T(A)$. Alors B est un polynôme de $\mathbb{Z}[Z,X_1,X_2,X_3]$ vérifiant*

$$\deg_Z B \leqslant N, \quad \deg_{X_i} B \leqslant 3\gamma N \log M \ (1 \leqslant i \leqslant 3), \quad \log H(B) \leqslant \gamma N(\log M)^2, \tag{13}$$

et

$$e^{-\kappa_2 M} \leqslant |B(q,P(q),Q(q),R(q))| \leqslant e^{-\kappa_1 M}, \tag{14}$$

où $\kappa_1 = \frac{1}{3}\log\frac{1}{r}$ et $\kappa_2 = 3\log\frac{2}{|q|}$.

Démonstration. — On vérifie aisément par récurrence que pour tout entier $n \geqslant 1$ on a

$$(12Z)^n(Z^{-1}D)^n = \prod_{0\leqslant k\leqslant n-1}(12(D-k)). \tag{15}$$

Le fait que B soit un polynôme de $\mathbb{Z}[Z,X_1,X_2,X_3]$ s'en déduit immédiatement. On a de plus $B(z,P(z),Q(z),R(z)) = (12z)^T F^{(T)}(z)$. Les deuxième et troisième étapes (propositions 2.4 et 2.7) donnent alors respectivement, pour $N \gg 0$ (et compte tenu de $T \leqslant \gamma N \log M \leqslant \gamma(2M)^{1/4}\log M$ d'après (7)),

$$|B(q,P(q),Q(q),R(q))| \geqslant (12|q|)^T\Big(\frac{|q|}{2}\Big)^{2M} \geqslant \Big(\frac{|q|}{2}\Big)^{3M}$$

et

$$|B(q,P(q),Q(q),R(q))| \leqslant (12|q|)^T r^{M/2} \leqslant r^{M/3},$$

c'est-à-dire (14). Maintenant, les formules (12) et (15) donnent sans peine $\deg_Z B \leqslant \deg_Z A$ et $\deg_{X_i} B \leqslant \deg_{X_i} A + 2T$ $(1 \leqslant i \leqslant 3)$, d'où les estimations de $\deg_Z B$ et $\deg_{X_i} B$ en utilisant (6). Pour estimer $H(B)$, on remarque que pour tout polynôme non nul $E \in \mathbb{C}[Z,X_1,X_2,X_3]$, on a

$$\begin{aligned} H(12DE) &\leqslant H(12Z\partial E/\partial Z) + H((X_1^2 - X_2)\partial E/\partial X_1) \\ &\quad + H(4(X_1X_2 - X_3)\partial E/\partial X_2) + H(6(X_1X_3 - X_2^2)\partial E/\partial X_3) \\ &\leqslant H(E)(12\deg_Z E + 2\deg_{X_1} E + 8\deg_{X_2} E + 12\deg_{X_3} E) \\ &\leqslant 34H(E)\max\{\deg_Z E, \deg_{X_1} E, \deg_{X_2} E, \deg_{X_3} E\}. \end{aligned}$$

Ainsi, pour tout k, $0 \leqslant k \leqslant T-1$, on a

$$H(12(D-k)E) \leqslant (34\max\{\deg_Z E, \deg_{X_1} E, \deg_{X_2} E, \deg_{X_3} E\} + 12k)H(E).$$

On en déduit, par récurrence avec la formule (15), l'estimation

$$\begin{aligned} \log H(B) &\leqslant \sum_{0\leqslant k\leqslant T-1} \log\big(34(N+2k)+12k\big) + \log H(A) \\ &\leqslant T\log(34N + 80T) + \log H(A) \\ &\leqslant \gamma N(\log M)\log(81\gamma N\log M) + 61N\log N \\ &\leqslant \gamma N(\log M)^2 \end{aligned}$$

puisque $N \leqslant (2M)^{1/4}$ et N est suffisamment grand. □

Pour pouvoir conclure à l'aide du théorème 2.1, il nous faut encore obtenir des estimations dépendant de N uniquement. Pour cela, on a besoin d'une majoration de la multiplicité M en fonction de N (rappelons que la proposition 2.2 donne la minoration $M \geqslant N^4/2$). Une telle majoration est fournie par le lemme de multiplicité suivant.

***Théorème 2.9* (lemme de multiplicité)**. — *Soient L_1, L_2 des entiers $\geqslant 1$. Alors, pour tout polynôme $E \in \mathbb{C}[Z, X_1, X_2, X_3]$, $E \neq 0$, tel que* $\deg_Z E \leqslant L_1$ *et* $\deg_{X_i} E \leqslant L_2$ *($i = 1, 2, 3$), on a :*

$$\mathrm{ord}_0\, E(z, P(z), Q(z), R(z)) \leqslant cL_1L_2^3,$$

où $c > 0$ est une constante absolue.

Remarque. — D'après [**Nes96**, Theorem 3], la valeur $c = 10^{46}$ convient.

Ce lemme de multiplicité constitue le point crucial et difficile de la preuve de [**Nes96**]. Sa démonstration fera l'objet du paragraphe 4 (voir § 4.6, corollaire 4.24). Elle repose sur des résultats d'algèbre commutative et de géométrie diophantienne (exposés au paragraphe suivant), ainsi que sur l'étude des idéaux premiers $\mathfrak{p} \subset \mathbb{C}[Z, X_1, X_2, X_3]$ stables par l'opérateur différentiel D.

Fin de la démonstration du théorème 1.1. — En admettant le théorème 2.9, la preuve du théorème 1.1 est maintenant immédiate. En effet, ce théorème appliqué avec $E = A_N$ donne $M \leqslant cN^4$. Cette majoration de M, combinée avec la minoration $M \geqslant N^4/2$ (proposition 2.2), permet d'exprimer les estimations de la proposition 2.8 en fonction de N uniquement. On vérifie ainsi que le polynôme $B = B_N$ satisfait

$$\deg B_N \leqslant \gamma_0 N \log N, \qquad \log H(B_N) \leqslant \gamma_0 N (\log N)^2$$

et

$$e^{-\gamma_2 N^4} \leqslant |B_N(q, P(q), Q(q), R(q))| \leqslant e^{-\gamma_1 N^4},$$

où γ_0, γ_1, γ_2 sont des réels > 0 ne dépendant que de q. Les hypothèses du critère 2.1 sont donc satisfaites avec $n = 4$, $k = 2$, $\tau(N) = \gamma_0 N(\log N)^2$ et $\lambda(N) = N^4$, ce qui achève de démontrer le théorème 1.1. □

Remarque 2.10. — La démonstration ci-dessus montre que pour pouvoir obtenir un degré de transcendance 3, il est crucial d'avoir des estimations de $\deg B_N$ et $\log H(B_N)$ « petites » devant N^4 (à savoir $\lim_{N\to\infty}(\max\{\deg B_N, \log H(B_N)\})^3/N^4 = 0$ si l'on utilise le critère 2.1). D'après la preuve de la proposition 2.8, les estimations pour $\deg B_N$ et $\log H(B_N)$ proviennent des estimations de $\deg A_N$, $\log H(A_N)$ et T (on a $\deg B_N \ll \deg A_N + T$ et $\log H(B_N) \ll \log H(A_N) + T \log(N + T)$). Il importe donc d'avoir des estimations de $\log H(A_N)$ et T « petites » ($\deg A_N$ étant par construction majoré par $4N$) : des majorations en N^2 par exemple ne permettraient pas de conclure. En reprenant la preuve des propositions 2.2 et 2.4, on voit que les majorations obtenues pour $\log H(A_N)$ et T dépendent de la croissance des coefficients de Taylor des fonctions

P, Q et R. Le fait que ces coefficients ne croissent pas trop vite (*i.e.* croissent au plus polynomialement) est donc un facteur déterminant dans le succès de la démonstration du théorème 1.1.

3. Géométrie diophantienne

On présente ici les outils importants utilisés dans la preuve du lemme de multiplicité 2.9. Ces outils jouent également un rôle essentiel dans la démonstration des résultats mentionnés au § 5. Ils ont été essentiellement développés et introduits en transcendance par Nesterenko et Philippon ([**Nes77**], [**Nes85a**], [**Nes85b**], [**Phi86**], [**Phi91**], [**Phi94**], [**Phi95**]...).

Il est important de noter que les approches de Nesterenko et Philippon, bien que très voisines, ne sont pas tout à fait les mêmes. Les notations, définitions et énoncés ne sont donc pas toujours identiques. Nous adopterons ici essentiellement le point de vue de Philippon.

Signalons que l'on ne trouvera que très peu de démonstrations dans ce § 3. En revanche, on donnera des références précises pour les assertions non démontrées ici.

3.1. Notations. — Dans tout ce paragraphe 3, on note K un corps de caractéristique zéro (certains résultats ne subsisteraient plus en caractéristique p), $m \geqslant 0$ un entier, $X_0, \ldots, X_m$ des indéterminées, et $R = K[X_0, \ldots, X_m]$. On désignera parfois la collection des indéterminées $X_0, \ldots, X_m$ simplement par X, de sorte que l'on écrira par exemple $R = K[X]$. On notera encore $\mathfrak{M}$ l'idéal $(X_0, \ldots, X_m)$, et si $\alpha = (\alpha_0, \ldots, \alpha_m) \in \mathbb{N}^{m+1}$, on pose $X^\alpha = X_0^{\alpha_0} \cdots X_m^{\alpha_m}$ et, conformément aux notations générales de la page 120, $|\alpha| = \alpha_0 + \cdots + \alpha_m$.

Si I est un idéal propre d'un anneau noethérien, on désigne par $\mathrm{ht}(I)$ sa hauteur (algébrique), c'est-à-dire la longueur maximale des chaînes d'idéaux premiers arrivant en I si I est premier, et $\inf_{\mathfrak{p} \supset I} \mathrm{ht}(\mathfrak{p})$ sinon (où $\mathfrak{p}$ parcourt les idéaux premiers contenant I). On prendra garde de ne pas confondre cette notation avec la notation $h(I)$ introduite ci-après (paragraphe 3.4), qui désignera quant à elle une hauteur *arithmétique* de l'idéal I.

Si V est une partie de $\mathbb{P}_m(\overline{K})$, on note $\mathscr{I}(V) \subset K[X]$ l'idéal engendré par les polynômes homogènes nuls sur V. En sens inverse, si I est un idéal homogène de $R = K[X]$, on notera $\mathscr{Z}(I) \subset \mathbb{P}_m(\overline{K})$ l'ensemble des zéros de l'idéal I. Les parties non vides $V \subset \mathbb{P}_m(\overline{K})$ de la forme $V = \mathscr{Z}(\mathfrak{p})$ pour $\mathfrak{p}$ idéal premier homogène de $K[X]$ seront appelées variétés sur K.[(3)]

On utilisera aussi la notion de cycle sur K. Par définition, on appellera cycle (positif) sur K toute combinaison linéaire formelle de variétés $\mathsf{Z} = \sum_{1 \leqslant i \leqslant s} \ell_i [V_i]$, où $s \geqslant 0$, $\ell_1, \ldots, \ell_s \in \mathbb{N}^*$ et $V_1, \ldots, V_s \subset \mathbb{P}_m(\overline{K})$ sont des variétés sur K ayant toutes même

[(3)] Une variété sur K est donc K-irréductible, mais pas nécessairement $\overline{K}$-irréductible.

dimension. Si $s = 0$, on obtient le cycle nul. La dimension commune des variétés V_i est la dimension du cycle et est notée $\dim \mathsf{Z}$ (elle est bien définie uniquement lorsque le cycle Z n'est pas nul). Lorsque $\mathsf{Z} = 0$, on posera par convention $\dim \mathsf{Z} = -1$ (ce qui permettra de conserver la validité des énoncés pour le cycle nul). Si V est une variété sur K, on identifiera souvent V au cycle $[V]$ qu'elle définit, de sorte que l'on écrira par exemple $\mathsf{Z} = V$. Enfin, comme on ne considérera que des variétés et des cycles positifs sur K, on dira souvent plus simplement « variété » et « cycle » dans la suite.

À tout idéal homogène propre I de $K[X]$ on associe de façon naturelle un cycle de dimension $\dim \mathscr{Z}(I) = m - \mathrm{ht}(I)$, que nous noterons $\mathsf{Z}(I)$ et qui est défini de la façon suivante. Si $\mathrm{ht}(I) = m+1$, alors $\mathsf{Z}(I) = 0$. Sinon, soient $Q_1, \ldots, Q_s$ les composantes primaires isolées de I de hauteur $\mathrm{ht}(I)$ (dans une décomposition primaire réduite de I), et notons, pour chaque i, $1 \leqslant i \leqslant s$, $\mathfrak{p}_i = \sqrt{Q_i}$ et ℓ_i la longueur de l'idéal primaire Q_i.(4) Alors le cycle associé à I est $\mathsf{Z}(I) = \sum_{1 \leqslant i \leqslant s} \ell_i [\mathscr{Z}(\mathfrak{p}_i)]$. Si $I = K[X]$, on conviendra encore de poser $\mathsf{Z}(I) = 0$. Enfin, si $F \in K[X]$ est un polynôme homogène, on notera $\mathsf{Z}(F)$ le cycle associé à l'idéal (F). Si $F \neq 0$ on a $\mathsf{Z}(F) = \sum_{1 \leqslant i \leqslant s} \ell_i [\mathscr{Z}(F_i)]$, où $F = \prod_{1 \leqslant i \leqslant s} F_i^{\ell_i}$ est la décomposition de F en produit de facteurs irréductibles.

3.2. Formes éliminantes et résultantes

3.2.1. Introduction. — Étant donné un idéal homogène I de $K[X]$ (ou une variété de $\mathbb{P}_m$, ou plus généralement un cycle), il est très utile en approximation diophantienne de pouvoir définir, comme on sait le faire pour un polynôme de $K[X]$, les notions de degré, hauteur, et valeur absolue en un point pour cet idéal I (ou, de façon analogue, les notions de degré, hauteur et distance d'un point à la variété ou au cycle). Pour ce faire, l'idée est d'associer à l'idéal I un certain polynôme f (qui sera en fait déterminé seulement à un facteur de K^* près), et de définir les notions en question au moyen de f. Ce polynôme f sera obtenu par la théorie de l'élimination (formes de Chow).

En fait, il y a deux façons naturelles d'associer un tel polynôme f à un idéal ou un cycle : on peut en effet associer ou bien une forme éliminante, ou bien une forme résultante. Les deux notions peuvent être vues comme une généralisation de la théorie classique du résultant de polynômes. L'objet de ce paragraphe est d'exposer les résultats dont nous aurons besoin.(5)

Considérons pour commencer le cas du résultant de deux polynômes homogènes U, V de $R = K[X_0, X_1]$, de degrés d et e respectivement. Écrivons $U = u_0 X_1^d + \cdots + u_d X_0^d$ et $V = v_0 X_1^e + \cdots + v_e X_0^e$. Si f désigne le résultant de U et V, on sait que f est un polynôme en les coefficients $u_0, \ldots, u_d, v_0, \ldots, v_e$ de U et V, homogène de degré e par

(4) Rappel : si Q est $\mathfrak{p}$-primaire, la longueur de Q est le plus grand entier $\ell \geqslant 1$ tel qu'il existe une suite strictement croissante d'idéaux $\mathfrak{p}$-primaires $q_1 = Q \subset q_2 \subset \cdots \subset q_\ell = \mathfrak{p}$, *cf.* [**ZS58**]. C'est aussi la longueur $\ell_{K[X]_\mathfrak{p}}((K[X]/Q)_\mathfrak{p})$ du $K[X]_\mathfrak{p}$-module $(K[X]/Q)_\mathfrak{p}$.

(5) L'ordre adopté ici pour présenter ces résultats ne suit pas toujours l'ordre logique dans lequel ils se démontrent.

rapport au groupe de variables u, homogène de degré d par rapport au groupe de variables v, et satisfaisant la condition, pour tous $u_0, \ldots, u_d, v_0, \ldots, v_e \in \overline{K}$:

$$U \text{ et } V \text{ ont un zéro commun distinct de } (0,0) \Longleftrightarrow f(u_0, \ldots, u_d, v_0, \ldots, v_e) = 0.$$

Cette condition se réécrit encore, en introduisant les zéros $\mathscr{Z}(U) \subset \mathbb{P}_1(\overline{K})$, $\mathscr{Z}(V) \subset \mathbb{P}_1(\overline{K})$ des polynômes U et V :

$$\mathscr{Z}(U) \cap \mathscr{Z}(V) \neq \varnothing \Longleftrightarrow f(u_0, \ldots, u_d, v_0, \ldots, v_e) = 0. \tag{16}$$

Les formes éliminantes et résultantes que l'on va définir maintenant auront des propriétés tout à fait analogues à celles-ci (voir théorèmes 3.4 et 3.12 ci-dessous), le cas classique du résultant de deux (ou de $m+1$) polynômes correspondant au cas $I = (0)$.

3.2.2. Formes éliminantes. — Soit I un idéal homogène de $R = K[X_0, \ldots, X_m]$, distinct de R. Notons r l'entier de $\{0, \ldots, m\}$ défini par $r = m + 1 - \mathrm{ht}(I)$, et soit $d = (d_1, \ldots, d_r)$ un élément de $(\mathbb{N}^*)^r$. On introduit de nouvelles indéterminées u_α^i, où $1 \leqslant i \leqslant r$ et $\alpha \in \mathbb{N}^{m+1}$, $|\alpha| = d_i$, et on pose

$$U_i = \sum_{\substack{\alpha \in \mathbb{N}^{m+1} \\ |\alpha| = d_i}} u_\alpha^i X^\alpha.$$

Les indéterminées u_α^i sont donc les coefficients du polynôme homogène générique U_i de degré d_i. Comme pour les variables X on notera parfois plus simplement u l'ensemble des variables u_α^i, et de même, si i est fixé, on écrira u^i pour l'ensemble des variables $\{u_\alpha^i \mid |\alpha| = d_i\}$. Si $r = 0$ on convient de poser $d = \varnothing$. Dans ce cas il n'y a pas de variables u et on a donc, par exemple, $K[u] = K$, $R[u] = R$.

Ces notations étant posées, on a :

Définition 3.1. — On appelle *idéal éliminant d'indice* d de I l'idéal de $K[u]$ suivant :

$$\mathfrak{E}_d(I) = \{f \in K[u] \mid \exists\, k \geqslant 0,\, \forall\, i \in \{0, \ldots, m\},\, fX_i^k \in (I, U_1, \ldots, U_r)\},$$

où $(I, U_1, \ldots, U_r)$ est l'idéal de $K[X, u]$ engendré par I et $U_1, \ldots, U_r$.

On se restreindra dans la suite pour simplifier au cas des idéaux « équidimensionnels » (c'est-à-dire dont tous les premiers associés ont même hauteur[(6)]).

On a la propriété suivante :

Lemme 3.2. — *Soient $I \subsetneqq K[X]$ un idéal homogène équidimensionnel, $r = m+1-\mathrm{ht}(I)$, et $d \in (\mathbb{N}^*)^r$. Alors $\mathfrak{E}_d(I)$ est un idéal homogène principal non nul.*

Démonstration. — Le lemme résulte de [**Phi86**], prop. (1.3) (i), lemme (1.8) et prop. (1.5) (ii) (ou de [**NP01**], chap. 5, lemme 2.4 et § 2.3). Voir aussi [**Nes77**], Lemma 5 et prop. 2. □

On peut maintenant définir :

(6) « Unmixed ideal » en anglais.

Définition 3.3

(i) Soient $I \subsetneq K[X]$ un idéal homogène équidimensionnel et $d \in (\mathbb{N}^*)^r$, où $r = m + 1 - \mathrm{ht}(I)$. On appelle *forme éliminante d'indice d de I* tout générateur de l'idéal principal $\mathfrak{E}_d(I) \subset K[u]$.

(ii) Soient $\mathsf{Z} = \sum_{1 \leqslant i \leqslant s} \ell_i [V_i]$ un cycle de $\mathbb{P}_m$, $r = \dim \mathsf{Z} + 1$, et $d \in (\mathbb{N}^*)^r$. On appelle *forme éliminante d'indice d de Z* tout polynôme f de la forme $f = \lambda f_1^{\ell_1} \cdots f_s^{\ell_s}$, où $\lambda \in K^*$ et f_i est une forme éliminante d'indice d de $\mathfrak{p}_i = \mathscr{I}(V_i)$ $(1 \leqslant i \leqslant s)$. On appelle *forme de Chow* de Z toute forme éliminante d'indice $(1, \ldots, 1)$ (r fois) de Z.

On notera qu'une forme éliminante est un polynôme homogène qui n'est jamais nul. De plus, deux formes éliminantes sont égales à un facteur de K^* près.

Les formes éliminantes que l'on vient de définir peuvent être vues comme une généralisation de la théorie du résultant en vertu du résultat suivant, tout à fait analogue à la propriété (16).

***Théorème 3.4* (théorème de l'élimination)**. — *Soient $I \subsetneq K[X_0, \ldots, X_m]$ un idéal homogène équidimensionnel, $r = m + 1 - \mathrm{ht}(I)$, $d \in (\mathbb{N}^*)^r$, et f une forme éliminante d'indice d de I. Soient encore L une extension de K et $\rho : K[u] \to L$ un morphisme de K-algèbres (que l'on étend en un morphisme $\rho : K[X, u] \to L[X]$ en posant $\rho(X_i) = X_i$ pour tout i). Alors les assertions suivantes sont équivalentes :*

(i) $\rho(f) = 0$

(ii) *Il existe un zéro non trivial $x = (x_0, \ldots, x_m) \in \overline{L}^{m+1} \smallsetminus \{0\}$ de l'idéal $\rho(I, U_1, \ldots, U_r) \subset L[X]$.*

Dans cet énoncé, ρ est donc une spécialisation des variables u (par exemple à valeurs dans $\overline{K}$), et (i) signifie que la spécialisation $\rho(u)$ de ces variables est un zéro du polynôme f. Quant à l'assertion (ii), elle signifie qu'il existe un élément $x \in \overline{L}^{m+1} \smallsetminus \{0\}$ tel que pour tout polynôme $P \in I$ on ait $P(x) = \rho(U_1)(x) = \cdots = \rho(U_r)(x) = 0$, c'est-à-dire encore

$$\mathscr{Z}(I) \cap H_1 \cap \cdots \cap H_r \neq \varnothing \qquad \text{dans } \mathbb{P}_m(\overline{L}),$$

où on a noté $H_i = \mathscr{Z}(\rho(U_i)) \subset \mathbb{P}_m(\overline{L})$ $(1 \leqslant i \leqslant r)$ l'hypersurface définie par l'équation $\rho(U_i) = 0$.

Démonstration. — Voir [**Phi86**, prop (1.4)] ou [**NP01**, chap. 5, théorème 2.2] (voir aussi [**Nes77**, Lemma 4]). □

On a également le résultat suivant (on rappelle que $\mathfrak{M}$ désigne l'idéal $(X_0, \ldots, X_m)$ de $K[X]$) :

Théorème 3.5. — *Soient $I \subsetneq K[X]$ un idéal homogène équidimensionnel, $r = m + 1 - \mathrm{ht}(I)$, et $d \in (\mathbb{N}^*)^r$.*

(i) *On a $\sqrt{I} = \mathfrak{M}$ si et seulement si $f = 1$ est une forme éliminante d'indice d de I.*

(ii) *Si I est premier et $I \neq \mathfrak{M}$, alors toute forme éliminante d'indice d de I est irréductible dans $K[u]$.*

(iii) *Soient $Q_1, \ldots, Q_s$ les composantes primaires de I, $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ les idéaux premiers associés correspondants, et notons, pour chaque i ($1 \leqslant i \leqslant s$), e_i l'exposant de l'idéal primaire Q_i.*[(7)] *Alors, si f_i est une forme éliminante d'indice d de $\mathfrak{p}_i$, le produit $\prod_{1\leqslant i\leqslant s} f_i^{e_i}$ est une forme éliminante d'indice d de I.*

Démonstration. — Pour (i) et (ii) voir [**NP01**, chap. 5, lemme 2.4] ou [**Phi86**, prop. (1.3)]. L'assertion (iii) résulte de [**Nes77**, corollary page 251] (voir aussi [**Phi86**], remarque page 11 suivant la preuve de la proposition (1.3)). □

On trouvera d'autres propriétés utiles des formes éliminantes dans [**Nes77**], [**Phi86**] et [**NP01**, chap. 5]. Nous donnons pour conclure deux exemples.

Exemple 3.6. — Prenons $K = \mathbb{Q}$ et $I = (0)$. L'idéal I est premier de hauteur nulle, donc $r = m + 1$. Si $f \in \mathbb{Q}[X]$ est une forme éliminante d'indice d de I normalisée de sorte que les coefficients de f soient dans $\mathbb{Z}$ et premiers entre eux, alors f est, au signe près, le résultant des $m + 1$ polynômes homogènes $U_1, \ldots, U_{m+1}$. En effet, la forme f et le résultant sont deux polynômes irréductibles de $\mathbb{Z}[u]$ qui ont les mêmes zéros d'après le théorème de l'élimination (voir [**Mac94**]).

Exemple 3.7. — Soit $V = \{x\}$ une variété réduite à un point $x = (x_0, \ldots, x_m) \in \mathbb{P}_m(K)$. On a ici $r = \dim V + 1 = 1$. Alors, pour tout $d \in \mathbb{N}^*$, une forme éliminante d'indice d de V est

$$f(u) = \sum_{\substack{\alpha\in\mathbb{N}^{m+1}\\ |\alpha|=d}} u_\alpha^1 x^\alpha = U_1(x).$$

En effet, la forme $U_1(x)$ est irréductible dans $K[u]$ et a les mêmes zéros que toute forme éliminante d'indice d de V puisqu'elle vérifie, pour tout morphisme de K-algèbres $\rho : K[u] \to \overline{K}$, l'équivalence :

$$\rho(U_1)(x) = 0 \Longleftrightarrow V \cap \mathscr{Z}(\rho(U_1)) \neq \varnothing.$$

3.2.3. Formes résultantes. — Nous introduisons ici la notion de forme résultante, voisine de celle de forme éliminante.

Soit $I \subset K[X]$ un idéal homogène distinct de $K[X]$, et notons $r = m + 1 - \mathrm{ht}(I)$. On fixe comme précédemment $d = (d_1, \ldots, d_r)$ un élément de $(\mathbb{N}^*)^r$, et on définit les variables u_α^i et les polynômes U_i comme au § 3.2.2.

Si maintenant T est un $K[u]$-module de torsion de type fini, alors pour tout idéal premier $\mathfrak{p}$ de $k[u]$ de hauteur 1, la longueur $\ell_{K[u]_\mathfrak{p}}(T_\mathfrak{p})$ du $K[u]_\mathfrak{p}$-module $T_\mathfrak{p}$ est finie

[(7)] Rappel : si Q est $\mathfrak{p}$-primaire, l'exposant de Q est le plus petit entier $e \geqslant 1$ tel que $\mathfrak{p}^e \subset Q$.

et égale à zéro pour presque tout $\mathfrak{p}$ (*i.e.* pour tout $\mathfrak{p} \in \operatorname{Spec} K[u]$ de hauteur 1 sauf un nombre fini). Pour un tel module on note alors $\chi(T)$ l'idéal de $K[u]$ suivant :

$$\chi(T) = \prod_{\substack{\mathfrak{p} \in \operatorname{Spec} K[u] \\ \operatorname{ht} \mathfrak{p}=1}} \mathfrak{p}^{\ell_{\mathfrak{p}}},$$

où $\ell_{\mathfrak{p}} = \ell_{K[u]_{\mathfrak{p}}}(T_{\mathfrak{p}})$. Le diviseur correspondant à l'idéal $\chi(T)$ n'est autre que le *contenu* de T au sens de [**Bou85**, chap. VII, § 4, n°5, def. 4].

Ceci étant, soit $M = K[u][X]/(I, U_1, \ldots, U_r)$: c'est un $K[u][X]$-module gradué (par les X_i). Pour $\ell \geqslant 0$, on note alors M_ℓ le $K[u]$-module des éléments homogènes de degré ℓ. On a :

Lemme 3.8. — *Il existe un entier $\ell_0 \geqslant 0$ vérifiant la propriété suivante : pour tout $\ell \geqslant \ell_0$, M_ℓ est un $K[u]$-module de torsion de type fini et $\chi(M_\ell) = \chi(M_{\ell_0})$.*

Démonstration. — Voir [**NP01**, chap. 5, § 3.2]. □

On notera dans la suite $\mathfrak{R}_d(I)$ l'idéal $\chi(M_{\ell_0})$ du lemme 3.8. Comme l'anneau $K[u]$ est noethérien et factoriel, ses idéaux premiers de hauteur 1 sont principaux. En particulier, l'idéal $\mathfrak{R}_d(I)$ est principal. On pose alors :

Définition 3.9

(i) Soient $I \subsetneqq K[X_0, \ldots, X_m]$ un idéal homogène et $d \in (\mathbb{N}^*)^r$, où $r = m + 1 - \operatorname{ht}(I)$. On appelle *forme résultante d'indice d de I* tout générateur de l'idéal principal $\mathfrak{R}_d(I) \subset K[u]$.

(ii) Soient $\mathsf{Z} = \sum_{1 \leqslant i \leqslant s} \ell_i [V_i]$ un cycle de $\mathbb{P}_m$, $r = \dim \mathsf{Z} + 1$, et $d \in (\mathbb{N}^*)^r$. On appelle *forme résultante d'indice d de Z* tout polynôme f de la forme $f = \lambda f_1^{\ell_1} \cdots f_s^{\ell_s}$, où $\lambda \in K^*$ et f_i est une forme résultante d'indice d de $\mathfrak{p}_i = \mathscr{I}(V_i)$ $(1 \leqslant i \leqslant s)$.

Comme on l'a déjà dit, formes éliminantes et formes résultantes sont étroitement liées :

Théorème 3.10. — *Si $\mathfrak{p} \subset K[X]$ est un idéal homogène premier, alors les notions de forme éliminante et résultante coïncident. Il en résulte que les deux notions coïncident pour les cycles sur K.*

Démonstration. — Le théorème résulte facilement des résultats de [**NP01**, chap. 5] et de [**Phi86**]. Soit f (resp. g) une forme éliminante (resp. résultante) d'indice d de $\mathfrak{p}$. D'après [**NP01**, chap. 5, § 3.2], on a $\sqrt{(f)} = \sqrt{(g)}$. Comme $f \in K[u]$ est ou bien irréductible ou bien un élément de K^* (théorème 3.5 (i) et (ii)), on a donc $g = \lambda f^\nu$, où $\nu \in \mathbb{N}^*$ et $\lambda \in K^*$. Mais d'après [**NP01**, chap. 5, prop. 3.4] et [**Phi86**, remarque 1 page 15], g et f ont même degré. Donc $\nu = 1$, d'où le théorème. □

Pour un idéal quelconque, formes éliminantes et formes résultantes ne coïncident plus, comme le montre le théorème suivant.

Théorème 3.11. — *Soient $I \subsetneq K[X]$ un idéal homogène, $r = m + 1 - \mathrm{ht}(I)$, et $d \in (\mathbb{N}^*)^r$. Soient encore $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ les idéaux premiers associés de I de hauteur $\mathrm{ht}(I)$, $Q_1, \ldots, Q_s$ les composantes primaires correspondantes, et notons, pour chaque i ($1 \leqslant i \leqslant s$), ℓ_i la longueur de l'idéal primaire Q_i. Alors, si f_i est une forme résultante d'indice d de $\mathfrak{p}_i$, le produit $\prod_{1 \leqslant i \leqslant s} f_i^{\ell_i}$ est une forme résultante d'indice d de I.*

Démonstration. — Voir [**NP01**, chap. 5, théorème 3.3]. Noter que dans le cas $r = 0$ l'énoncé s'applique et donne la forme résultante $f = 1$. $\square$

Le théorème 3.11 montre que toute forme résultante d'indice d d'un idéal I est aussi une forme résultante du cycle associé $\mathsf{Z}(I)$, alors que ce n'est plus vrai en général pour les formes éliminantes, comme le montre le théorème 3.5 (iii) (en effet, on a $e_i \leqslant \ell_i$ pour tout i (voir [**BM80**, lemma 1]), l'inégalité pouvant être stricte). De ce point de vue, les formes résultantes sont plus adaptées que les formes éliminantes. Comme on le verra, elles se comportent également mieux vis-à-vis des intersections (voir § 3.6), et du degré des idéaux (voir théorème 3.12 ci-après). C'est pourquoi nous utiliserons la notion de forme résultante dans ce qui suit. Il est à noter toutefois que Nesterenko, lui, utilise les formes éliminantes.

3.3. Degré. — Commençons par quelques rappels. Si $I \subsetneq R = K[X_0, \ldots, X_m]$ est un idéal homogène tel que $\sqrt{I} \neq \mathfrak{M}$, on définit son degré $d(I)$ comme étant l'entier tel que $\frac{d(I)}{(r-1)!} Y^{r-1}$ soit le terme de plus haut degré du polynôme de Hilbert $P_{R/I}(Y)$ du R-module R/I, où $r = m + 1 - \mathrm{ht}(I) = \dim \mathscr{Z}(I) + 1$. Autrement dit, on a $d(I) = \lim_{\ell \to +\infty} \frac{(r-1)!}{\ell^{r-1}} \dim_K(R/I)_\ell$ ([**Eis95**, § 1.9] ou [**Har77**, Chap. I, § 7]). On étend la définition au cas $\sqrt{I} = \mathfrak{M}$ en posant $d(I) = 0$. On montre facilement ([**NP01**, chap. 5, page 63] ou [**NP01**, chap. 11, § 2.2]) que si $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ sont les idéaux premiers associés de I de hauteur $\mathrm{ht}(I)$, et si ℓ_i est la longueur de la composante $\mathfrak{p}_i$-primaire de I ($1 \leqslant i \leqslant s$), alors $d(I) = \sum_{1 \leqslant i \leqslant s} \ell_i d(\mathfrak{p}_i)$. Si $V \subset \mathbb{P}_m$ est une variété sur K, on notera encore $d(V) = d(\mathscr{I}(V))$ son degré : c'est aussi le nombre de points d'intersection de V avec $r = \dim V + 1$ hyperplans $H_1, \ldots, H_r$ de $\mathbb{P}_m$ en position « suffisamment générale » (l'intersection $V \cap H_1 \cap \cdots \cap H_r$ étant alors de cardinal fini). Enfin, pour un cycle $\mathsf{Z} = \sum_{1 \leqslant i \leqslant s} \ell_i [V_i]$, on étend la définition par linéarité, *i.e.* on pose $d(\mathsf{Z}) = \sum_{1 \leqslant i \leqslant s} \ell_i d(V_i)$. On a ainsi, pour tout idéal homogène $I \subsetneq K[X_0, \ldots, X_m]$, $d(I) = d(\mathsf{Z}(I))$.

Ce degré est en fait donné par celui des formes résultantes :

Théorème 3.12. — *Soient $I \subsetneq K[X_0, \ldots, X_m]$ un idéal homogène, $r = m + 1 - \mathrm{ht}(I)$, $d \in (\mathbb{N}^*)^r$, et f une forme résultante d'indice d de I. Alors f est un polynôme non nul de $K[u]$ qui est, pour chaque entier $i \in \{1, \ldots, r\}$, homogène par rapport au groupe de variables $u^i = \{u^i_\alpha \mid |\alpha| = d_i\}$, et de degré $\deg_{u^i} f = d(I) \prod_{j \neq i} d_j$.*

Démonstration. — Voir [**NP01**, chap. 5, prop. 3.4]. $\square$

En particulier, si f est une forme de Chow d'une variété V (resp. d'un cycle Z, ou d'un cycle de la forme $\mathsf{Z}(I)$), alors on a $d(V) = \deg_{u^i} f$ (resp. $d(\mathsf{Z}) = \deg_{u^i} f$, $d(I) = \deg_{u^i} f$) pour tout i, $1 \leqslant i \leqslant r$.

3.4. Hauteur. — À partir de maintenant, K désigne pour simplifier ou bien un corps de nombres, ou bien le corps des fractions rationnelles $\mathbb{C}(Z)$. On pourrait généraliser à des corps plus généraux les résultats ci-après (voir par ex. [**Nes97**, § 1] et [**NP01**, chap. 3, § 4]).

Soit V (resp. Z, I) une variété sur K (resp. un cycle, un idéal homogène de $K[X]$). On souhaite définir ici une hauteur *arithmétique* de V (resp. de Z, de I). On va définir cette hauteur comme la hauteur d'une forme de Chow de V (resp. de Z, de $\mathsf{Z}(I)$). Il nous faut pour cela définir la hauteur $h(f)$ d'un polynôme $f \in K[u]$. Dans le cas où K est un corps de nombres, on trouve couramment différentes définitions dans la littérature. Nous adopterons ici les mêmes choix que dans [**Phi95**, § 2], [**NP01**, chap. 6, § 3] et [**NP01**, chap. 7, § 2]. On en trouvera d'autres dans [**Phi86**] et [**Phi91**], ainsi que dans [**Nes97**]. Il faut toutefois noter que toutes ces hauteurs sont comparables entre elles et qu'un autre choix que celui adopté ici conduirait à des énoncés semblables (voir remarques 3.13 et 3.14 ci-après).

À K on associe un ensemble $\mathcal{M}$ de places de K, et pour chaque $v \in \mathcal{M}$, une valeur absolue (dite v-adique) $|\ |_v$ correspondante, de la façon suivante.

Dans le cas où K est un corps de nombres, on prend pour $\mathcal{M}$ l'ensemble de toutes les places non triviales de K. Si v est ultramétrique, alors v correspond à un ensemble de valeurs absolues équivalentes au-dessus d'un nombre premier p, et l'on choisit $|\ |_v$ telle que $|p|_v = p^{-1}$. Si v est archimédienne, alors v définit un plongement $\sigma_v : K \hookrightarrow \mathbb{C}$, et l'on pose $|\alpha|_v = |\sigma_v(\alpha)|$ (valeur absolue usuelle de $\mathbb{C}$) pour tout $\alpha \in K$.

Dans le cas $K = \mathbb{C}(Z)$, on prend $\mathcal{M} = \mathbb{C} \cup \{\infty\}$. On pose, pour $f \in \mathbb{C}(Z)$, $|f|_\alpha = e^{-\operatorname{ord}_\alpha f}$ si $\alpha \in \mathbb{C}$, et $|f|_\infty = e^{\deg f}$ (on a identifié les éléments de $\mathbb{C} \cup \{\infty\}$ et les places qu'ils déterminent).

Dans tous les cas, on notera S l'ensemble des places archimédiennes de $\mathcal{M}$ (donc $S = \varnothing$ si $K = \mathbb{C}(Z)$). Si $x = (x_1, \dots, x_N)$ est un N-uplet d'éléments de K, on notera encore

$$\|x\|_v = \begin{cases} \max_{1\leqslant i\leqslant N} |x_i|_v & \text{si } v \notin S \\ \sqrt{\sum_{1\leqslant i\leqslant N} |x_i|_v^2} & \text{si } v \in S. \end{cases}$$

Soit maintenant F un polynôme d'un anneau $K[z^1, \dots, z^p]$, où z^i représente un groupe d'indéterminées $(z_1^i, \dots, z_{N_i}^i)$ ($N_i \in \mathbb{N}^*$, $1 \leqslant i \leqslant p$). On suppose F homogène par rapport à chacun des groupes d'indéterminées z^i ($1 \leqslant i \leqslant p$). Pour tout $v \in \mathcal{M}$, on définit alors $|F|_v$ comme suit. Si $v \notin S$, alors $|F|_v$ est le maximum des valeurs absolues v-adiques des coefficients de F. Si $v \in S$, on pose $|F|_v = 0$ si $F = 0$, et sinon

$$(17)\quad \log|F|_v = \int_{S_{N_1}\times\cdots\times S_{N_p}} \log|\sigma_v(F)|\sigma_{N_1}\wedge\cdots\wedge\sigma_{N_p} + \sum_{1\leqslant i\leqslant p} \deg_{z^i} F \sum_{1\leqslant j\leqslant N_i-1} \frac{1}{2j},$$

où, pour tout i ($1 \leqslant i \leqslant p$), S_i est la sphère unité de $\mathbb{C}^i \simeq \mathbb{R}^{2i}$ et σ_i la mesure invariante de masse totale 1 sur S_i. Ces définitions s'appliquent en particulier à des polynômes homogènes de $K[X]$ (*i.e.* $p = 1$, $z^1 = X$, $N_1 = m + 1$), ou bien à des formes résultantes d'indice d ($p = r$, $z^i = u^i$, $N_i = \binom{d_i+m}{m}$), ou bien encore aux formes $\mathfrak{d}_x f$ qui interviendront au paragraphe 3.5 (où on aura $p = r$ et $z^i = s^i$). On a $|FG|_v = |F|_v|G|_v$ pour tous F, G.

On définit encore, pour tout $v \in \mathcal{M}$, $n_v = 1$ si $K = \mathbb{C}(Z)$ et $n_v = \frac{[K_v:\mathbb{Q}_v]}{[K:\mathbb{Q}]}$ si K est un corps de nombres (où, selon les notations usuelles, $\mathbb{Q}_v$ et K_v sont les complétés respectifs de $\mathbb{Q}$ et K en la place v). On définit alors la hauteur de $F \neq 0$ par la formule

$$h(F) = \sum_{v\in\mathcal{M}} n_v \log |F|_v. \tag{18}$$

On démontre que $h(F) \geqslant 0$ (voir remarque 3.13) et que $h(FG) = h(F) + h(G)$ pour tous polynômes F et G non nuls. De plus, la formule du produit dans K implique $h(\lambda) = 0$ dès que $\lambda \in K^*$. On a donc aussi $h(\lambda F) = h(F)$ pour tout $\lambda \in K^*$ et tout $F \neq 0$.

Remarque 3.13. — Soit F un polynôme comme ci-dessus, et supposons que K soit un corps de nombres. Dans [**Phi86**] et [**Phi91**], la hauteur de F est définie par la formule (18), mais en prenant cette fois comme définition de $\log |F|_v$ pour $v \in S$ la mesure de Mahler (logarithmique) $m(\sigma_v(F))$ du polynôme $\sigma_v(F)$ (au lieu de la formule (17)). Il résulte de [**Lel92**, théorème 2] ou [**Lel94**, théorème 4] que l'on a les inégalités suivantes (pour $v \in S$) :

$$m(\sigma_v(F)) \leqslant \log |F|_v \leqslant m(\sigma_v(F)) + \sum_{1\leqslant i\leqslant p} \deg_{z^i} F \sum_{1\leqslant j\leqslant N_i-1} \frac{1}{2j}\cdot$$

Si $h_{\mathrm{Ma}}(F)$ désigne la hauteur de [**Phi86**], on a donc :

$$h_{\mathrm{Ma}}(F) \leqslant h(F) \leqslant h_{\mathrm{Ma}}(F) + \sum_{1\leqslant i\leqslant p} \deg_{z^i} F \sum_{1\leqslant j\leqslant N_i-1} \frac{1}{2j}\cdot \tag{19}$$

Comme $h_{\mathrm{Ma}}(F) \geqslant 0$ (voir par exemple [**Phi86**]), il en résulte en particulier que $h(F) \geqslant 0$. Sans le terme correctif $\sum_{1\leqslant i\leqslant p} \deg_{z^i} F \sum_{1\leqslant j\leqslant N_i-1} \frac{1}{2j}$ dans la formule (17), $h(F)$ pourrait être négatif.

Remarque 3.14. — Soit $F \in K[z^1, \ldots, z^p]$ comme précédemment, et supposons encore que K soit un corps de nombres. Pour $v \in S$, notons $\|F\|_{v,\max}$ le maximum des valeurs absolues v-adiques des coefficients de F. La hauteur de F définie par Nesterenko dans [**Nes97**] ou [**NP01**, Chap. 3, § 4, Example 2] est

$$h_{\mathrm{Ne}}(F) = [K:\mathbb{Q}] \left(\sum_{v\notin S} n_v \log |F|_v + \sum_{v\in S} n_v \log \|F\|_{v,\max} \right).$$

Il est facile de comparer cette hauteur avec la hauteur h_{Ma} définie dans la remarque précédente. En effet, on vérifie facilement que l'on a, en notant comme ci-dessus

$m(\sigma_v(F))$ la mesure de Mahler de $\sigma_v(F)$:

$$\begin{aligned} m(\sigma_v(F)) &\leqslant \log\|F\|_{v,\max} + \sum_{1\leqslant i\leqslant p} \log\binom{N_i - 1 + \deg_{z^i} F}{N_i - 1} \\ &\leqslant \log\|F\|_{v,\max} + \sum_{1\leqslant i\leqslant p} \deg_{z^i} F \;\log N_i. \end{aligned}$$

Dans l'autre sens, on a (en procédant par exemple comme dans la preuve du lemme 1.13 de [**Phi86**])

$$\log\|F\|_{v,\max} \leqslant m(\sigma_v(F)) + \sum_{1\leqslant i\leqslant p} \deg_{z^i} F \;\log N_i.$$

On en déduit :

$$|h_{\mathrm{Ma}}(F) - \frac{1}{[K:\mathbb{Q}]} h_{\mathrm{Ne}}(F)| \leqslant \sum_{1\leqslant i\leqslant p} \deg_{z^i} F \;\log N_i.$$

Cette estimation, jointe aux inégalités (19), permet de comparer la hauteur $h(F)$ avec celle de Nesterenko.

Remarque 3.15. — Nous utiliserons au paragraphe 4 le cas $K = \mathbb{C}(Z)$. Dans ce cas, il est facile de vérifier que pour tout polynôme non nul $F \in \mathbb{C}[Z][X]$, homogène en X et primitif (*i.e.* dont les coefficients sont premiers entre eux dans $\mathbb{C}[Z]$), on a $h(F) = \deg_Z F$ (en effet, on a alors $|F|_v = 1$ pour tout $v \neq \infty$). Il en résulte aisément que pour un polynôme non nul quelconque $F \in \mathbb{C}[Z][X]$, homogène en X, on a toujours $h(F) \leqslant \deg_Z F$.

Ayant défini la hauteur d'un polynôme, on peut maintenant définir la hauteur d'un cycle et celle d'un idéal homogène :

Définition 3.16

(i) Soit Z un cycle sur K (par exemple une variété V). On définit la hauteur $h(\mathsf{Z})$ de Z par $h(\mathsf{Z}) = h(f)$, où f est une forme de Chow de Z.

(ii) Soit $I \subsetneq K[X]$ un idéal homogène. On définit la hauteur de I, notée $h(I)$, par $h(I) = h(\mathsf{Z}(I))$, où $\mathsf{Z}(I)$ est le cycle associé à I.

On vérifie immédiatement que cette définition est indépendante de la forme de Chow choisie.

Remarque 3.17. — Dans les travaux de Nesterenko (notamment dans [**Nes97**]), la hauteur $h_{\mathrm{Ne}}(I)$ d'un idéal homogène I est définie comme la hauteur $h_{\mathrm{Ne}}(g)$ d'une forme *éliminante* g d'indice $(1,\dots,1)$ de I, et non comme la hauteur $h(f)$ d'une forme *résultante* f de I, comme c'est en fait le cas ici (*cf.* théorème 3.10 et commentaire suivant le théorème 3.11). Si l'on souhaite comparer $h(I)$ et $h_{\mathrm{Ne}}(I)$, on pourra donc le faire facilement lorsque I est premier (à l'aide par exemple de la remarque 3.14 ci-dessus), puisque alors $f = g$ (théorème 3.10). Mais dans le cas général on aura seulement $h(g) \leqslant h(f)$, ce qui ne fournit, en comparant $h_{\mathrm{Ne}}(g)$ et $h(g)$, qu'une *majoration* de $h_{\mathrm{Ne}}(I)$ en fonction de $h(I)$.

Exemple 3.18. — Soit $V = \{x\}$ une variété sur K réduite à un point. Alors la hauteur $h(V)$, notée $h(x)$, est donnée par

$$h(V) = h(x) = \sum_{v \in \mathcal{M}} n_v \log \|x\|_v.$$

Cela résulte immédiatement de l'exemple 3.7 et des définitions. Lorsque K est un corps de nombres, cette hauteur n'est rien d'autre que le degré d'Arakelov normalisé $\widehat{\deg}_n x^* \overline{\mathcal{O}(1)}$ défini dans [**Gra**, § 2.3].

Dans le cas d'un cycle de la forme $\mathsf{Z}(F)$ on a le résultat suivant :

Proposition 3.19. — *Soit $F \in K[X]$ un polynôme homogène non nul. Alors*

$$h(\mathsf{Z}(F)) = \begin{cases} h(F) + (\deg F) \sum_{1 \leqslant i \leqslant m-1} \sum_{1 \leqslant j \leqslant i} \dfrac{1}{2j} & \text{si } K \text{ est un corps de nombres} \\ h(F) & \text{si } K = \mathbb{C}(Z). \end{cases}$$

Démonstration. — Voir [**NP01**, chap. 7, théorème 3.4] pour la première égalité. La seconde se démontre de façon analogue et est même plus simple. Voir aussi la proposition 1.3 de [**Nes97**]. □

3.5. Distances. — Un autre ingrédient important dans la preuve de Nesterenko, et en approximation diophantienne en général, est la notion de distance. On garde les hypothèses et notations du paragraphe précédent. On fixe de plus v une place de $\mathcal{M}$, et on note $\mathcal{K}_v$ le complété d'une clôture algébrique de K_v (la valeur absolue $|\ |_v$ se prolongeant de façon unique à $\overline{K_v}$). La place v étant maintenant fixée, on omettra l'indice v et on écrira plus simplement $|\ | = |\ |_v$, $\|\ \| = \|\ \|_v$ et $\mathcal{K} = \mathcal{K}_v$.

Soit $x = (x_0, \ldots, x_m)$ un point de $\mathbb{P}_m(\mathcal{K})$. Étant donnée une variété V de $\mathbb{P}_m$ sur K (ou plus généralement un cycle Z), on aimerait définir une quantité $\operatorname{Dist}(x, V)$ représentant la distance du point x à la variété V. Comme précédemment cette distance sera définie au moyen des formes de Chow. La notion correspondante pour un idéal représentera la « valeur absolue de I au point x ».

Soient donc $V \subset \mathbb{P}_m$ une variété sur K, $r = \dim V + 1$, et f une forme de Chow de V. Les variables u seront ici notées u_j^i ($0 \leqslant j \leqslant m$, $1 \leqslant i \leqslant r$), de sorte que $U_i = \sum_{0 \leqslant j \leqslant m} u_j^i X_j$. On introduit de nouvelles indéterminées s_{jk}^i, $1 \leqslant i \leqslant r$, $0 \leqslant j < k \leqslant m$, et l'on pose $s_{jk}^i = -s_{kj}^i$ si $j > k$ et $s_{jj}^i = 0$. On définit alors un morphisme de $\mathcal{K}$-algèbres $\mathfrak{d}_x : \mathcal{K}[u] \to \mathcal{K}[s]$ en posant

$$\mathfrak{d}_x(u_j^i) = \sum_{0 \leqslant k \leqslant m} s_{jk}^i x_k$$

(noter que ce morphisme dépend des coordonnées homogènes choisies pour le point x). On vérifie aussitôt que ce morphisme (prolongé en $\mathfrak{d}_x : \mathcal{K}[X, u] \to \mathcal{K}[X, s]$ par

$\mathfrak{d}_x(X_i) = X_i$ pour tout i) est tel que $(\mathfrak{d}_x U_i)(x) = 0$, $1 \leqslant i \leqslant r$. On en déduit facilement, d'après le théorème de l'élimination 3.4, que

$$x \in V \Longrightarrow \mathfrak{d}_x(f) = 0.$$

En fait, cette implication est une équivalence, comme il résulte par exemple de [**Nes77**, Lemma 11]. Cette équivalence justifie la définition suivante :

Définition 3.20. — Soit $x = (x_0, \dots, x_m)$ un point de $\mathbb{P}_m(\mathcal{K})$.

(i) Si Z est un cycle sur K, on définit

$$\operatorname{Dist}(x, \mathsf{Z}) = \frac{|\mathfrak{d}_x f|}{|f| \, \|x\|^{\deg f}}, \tag{20}$$

où f est une forme de Chow de Z.

(ii) Si $I \subsetneq K[X]$ est un idéal homogène, on définit la valeur absolue de I au point x par

$$|I(x)| = \operatorname{Dist}(x, \mathsf{Z}(I)).$$

On vérifie immédiatement que la définition (i) de dépend ni du représentant de x choisi dans $\mathcal{K}^{m+1}$, ni de la forme de Chow choisie. D'autre part, si $\mathsf{Z} = \sum_{1\leqslant i\leqslant s} \ell_i [V_i]$ est un cycle, on vérifie que l'on a

$$\operatorname{Dist}(x, \mathsf{Z}) = \prod_{1\leqslant i\leqslant s} \operatorname{Dist}(x, V_i)^{\ell_i}.$$

On démontre (voir [**NP01**, chap. 7, prop. 4.1]) que $0 \leqslant \operatorname{Dist}(x, \mathsf{Z}) \leqslant 1$ pour tout x et tout cycle Z.

Comme au paragraphe précédent (remarque 3.17), on se gardera de confondre la notation $|I(x)|$ introduite ici avec celle de Nesterenko [**Nes97**] (qui utilise une forme éliminante de I ainsi que des définitions différentes pour les valeurs absolues archimédiennes). Pour un idéal premier ou pour un idéal principal, et si $v \notin S$, les deux définitions coïncident néanmoins.

Dans le cas d'un idéal principal on a le résultat suivant :

Proposition 3.21. — *Si $I = (F)$ est principal, alors*

$$|I(x)| = \frac{|F(x)|}{|F| \, \|x\|^{\deg F}}.$$

Démonstration. — On trouvera une preuve de ce résultat dans [**Jad96**, proposition 3.6 page 64]. □

Cette formule justifie la notation $|I(x)|$ pour un idéal.

Dans le cas maintenant où la variété V est réduite à un point, on a la

Proposition 3.22. — *Si $V=\{y\}$ est réduite à un point, alors*

$$\mathrm{Dist}(x,V)=\begin{cases}\dfrac{\sqrt{\sum_{0\leqslant i<j\leqslant m}|x_jy_i-x_iy_j|^2}}{\|x\|\,\|y\|} & si\ v\in S\\[2mm] \dfrac{\max_{0\leqslant i<j\leqslant m}|x_jy_i-x_iy_j|}{\|x\|\,\|y\|} & sinon.\end{cases}\tag{21}$$

Démonstration. — L'exemple 3.7 donne explicitement une forme de Chow de $V=\{y\}$ en fonction des coordonnées homogènes de y. Les formules résultent alors d'un calcul direct (voir [**Lau92**, § 5, prop. 5] pour le cas $v\in S$). Voir aussi un énoncé analogue dans [**Nes97**, prop. 1.3]. □

On notera plus simplement $\mathrm{Dist}(x,y)$ au lieu de $\mathrm{Dist}(x,\{y\})$. On étend la notation $\mathrm{Dist}(x,y)$ à $y\in\mathbb{P}_m(\mathcal{K})$ quelconque par les formules (21). On démontre que l'on définit ainsi une distance (ultramétrique si $v\notin S$) sur $\mathbb{P}_m(\mathcal{K})$ [**Jad96**].

Ayant défini une distance $\mathrm{Dist}(x,y)$ entre points, il est naturel de définir une autre distance de x à V, à savoir :

Définition 3.23. — Soit $V\subset\mathbb{P}_m$ une variété sur K. On pose

$$d(x,V)=\min_{y\in V(\mathcal{K})}\mathrm{Dist}(x,y).\tag{22}$$

Cette distance interviendra au § 4. Les quantités $d(x,V)$ et $\mathrm{Dist}(x,V)$ sont comparables au sens suivant (on convient bien entendu que $\log 0=-\infty$) :

Proposition 3.24. — *Soient $V\subset\mathbb{P}_m$ une variété sur K, et x un point de $\mathbb{P}_m(\mathcal{K})$. Alors on a*

$$\log\mathrm{Dist}(x,V)\leqslant C_1d(V)+\log d(x,V)$$

et

$$\log d(x,V)\leqslant\frac{1}{d(V)}\log\mathrm{Dist}(x,V)+C_2,$$

où $C_1=C_1(m)$ et $C_2=C_2(m)$ sont des constantes $\geqslant 0$ ne dépendant que de m. Si $v\notin S$, on peut de plus prendre $C_1=C_2=0$.

Démonstration. — La première inégalité résulte immédiatement de [**Nes97**, Corollary 2]. La seconde est établie dans le cas $v\in S$ dans [**NP01**, chap. 6, § 5] (« closest point property »). Le cas $v\notin S$, plus simple, se démontre de manière analogue. □

Nous terminons ce paragraphe par la proposition suivante, que nous utiliserons aux §§ 4 et 5.

Proposition 3.25. — *Soient $\mathfrak{p}\subset K[X]$ un idéal homogène premier, $V=\mathscr{Z}(\mathfrak{p})\subset\mathbb{P}_m$, $F\in\mathfrak{p}$ un polynôme homogène, et $x\in\mathbb{P}_m(\mathcal{K})$. Alors*

$$\mathrm{Dist}(x,\mathsf{Z}(F))\leqslant d(x,V)e^{C_3\deg F},$$

où $C_3=C_3(m)\geqslant 0$ ne dépend que de m. De plus, si $v\notin S$, on peut prendre $C_3=0$.

Démonstration. — La proposition résulte de [**Nes97**, Corollary 1] (prendre $\overline{\omega} = x$ et $\overline{\xi} \in V(\mathcal{K})$). Noter que du fait des définitions légèrement différentes adoptées dans cette référence, la constante qui y figure est différente de notre constante C_3 lorsque $v \in S$. ☐

3.6. Théorèmes de Bézout. — Il est fréquent en approximation diophantienne, lorsque l'on souhaite démontrer une propriété pour une variété V, de se ramener à un problème en dimension $\dim V - 1$ en intersectant avec une hypersurface H convenablement choisie. Il est alors important de pouvoir majorer le degré, la hauteur et la distance de $V \cap H$ en fonction des quantités correspondantes pour V et H. Un tel résultat s'appelle un théorème de Bézout. En fait, on peut établir de tels théorèmes pour une intersection de variétés $V \cap W$, où W est une variété qui n'est plus nécessairement une hypersurface, mais la situation est beaucoup plus compliquée dans ce cadre (voir par ex. [**Phi95**]). Nous ne considérerons pas ce cas ici.

Soient donc $V \subset \mathbb{P}_m$ une variété sur K, et $\mathfrak{p} = \mathscr{I}(V) \subsetneq K[X]$ l'idéal premier homogène correspondant. Soit encore F un polynôme homogène non nul de $K[X]$ tel que $F \notin \mathfrak{p}$ (*i.e.* $V \not\subset \mathscr{Z}(F)$), et notons $J = (\mathfrak{p}, F)$ l'idéal de $K[X]$ engendré par $\mathfrak{p}$ et F. On se fixe enfin une valeur absolue $|\,| = |\,|_v$, $v \in \mathcal{M}$, nous permettant de définir les fonctions $\mathrm{Dist}(\,,\,)$ et $d(\,,\,)$ comme au paragraphe 3.5. Alors on a :

Théorème 3.26. — *Avec les notations précédentes, on a :*

(i) $d(\mathsf{Z}(J)) \leqslant d(V) \deg F$, *avec égalité si* $\mathsf{Z}(J) \neq 0$.

(ii) $h(\mathsf{Z}(J)) \leqslant h(V) \deg F + h(F) d(V) + C_3 d(V) \deg F$, *avec* $C_3 = 0$ *si* $K = \mathbb{C}(Z)$ *et* $C_3 = \frac{1}{2}\log(m+1)$ *sinon.*

(iii) *Soit* $x \in \mathbb{P}_m(\mathcal{K})$. *Posons* $\Delta = [K : \mathbb{Q}]$ *si* K *est un corps de nombres, et* $\Delta = 1$ *si* $K = \mathbb{C}(Z)$. *Alors :*

$$\frac{1}{\Delta} \log \mathrm{Dist}(x, \mathsf{Z}(J)) \leqslant \frac{1}{\Delta} \log \rho + h(F) d(V) + h(V) \deg F + C_4 d(V)\, \deg F,$$

où $C_4 = C_4(m) \geqslant 0$ *est une constante ne dépendant que de* m, *et où*

$$\rho = \begin{cases} \mathrm{Dist}(x, V) & \textit{si } \mathrm{Dist}(x, \mathsf{Z}(F)) \leqslant d(x, V) \\ \mathrm{Dist}(x, \mathsf{Z}(F)) & \textit{si } \mathrm{Dist}(x, \mathsf{Z}(F)) > d(x, V). \end{cases}$$

On peut de plus prendre $C_4 = 0$ *si* v *est ultramétrique.*

Démonstration. — L'assertion (i) est le théorème de Bézout classique (voir par ex. [**Har77**, chap. 1, th. 7.7] ou [**NP01**, chap. 5, lemme 2.11]). L'assertion (ii) résulte dans le cas d'un corps de nombres de [**NP01**, chap. 6, § 4]. Dans le cas $K = \mathbb{C}(Z)$ elle se démontre de façon analogue (*cf.* théorème 3.4 et corollaire 3.6 de [**NP01**, chap. 7]). L'énoncé (ii) est également démontré dans [**Nes97**, prop. 1.4]. L'assertion (iii) enfin figure dans [**Nes97**, prop. 1.4], ainsi que (si $v \in S$) dans [**NP01**, chap. 6, §§ 7 et 8] (« premier » et « second » théorème de Bézout métrique) (noter que les constantes de ces références sont *a priori* différentes de notre C_4, compte tenu des autres définitions qui sont adoptées dans ces textes). $\square$

Les énoncés (i), (ii) et (iii) seront appelés respectivement théorèmes de Bézout géométrique, arithmétique et métrique.

Il est facile de déduire du théorème 3.26 et des résultats de [**NP01**, chap. 5] une version plus générale des théorèmes de Bézout géométrique et arithmétique (nous en aurons besoin au § 4). On a en effet :

Corollaire 3.27. — *Soient $I \subset K[X]$ un idéal homogène de hauteur $\leqslant m$, et F un polynôme homogène de $K[X]$ qui ne soit pas diviseur de zéro dans $K[X]/I$. Alors, en notant $J = (I, F)$, on a :*

(i) *$d(\mathsf{Z}(J)) \leqslant d(\mathsf{Z}(I)) \deg F$, avec égalité si $\mathsf{Z}(J) \neq 0$.*

(ii) *$h(\mathsf{Z}(J)) \leqslant h(\mathsf{Z}(I)) \deg F + h(F)\, d(\mathsf{Z}(I)) + C_3\, d(\mathsf{Z}(I)) \deg F$, où C_3 est la constante du théorème 3.26.*

Démonstration. — Notons $\delta = \deg F$. On peut supposer $\delta \geqslant 1$, car le résultat est évident si F est constant (alors $\mathsf{Z}(J) = 0$). Soient $r = m+1-\mathrm{ht}(I)$, $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ les idéaux premiers associés de I de hauteur $\mathrm{ht}(I)$, ℓ_i la longueur de la composante $\mathfrak{p}_i$-primaire de I $(1 \leqslant i \leqslant s)$, $f_i \in K[u^1, \dots, u^r]$ une forme résultante d'indice $d = (1, \dots, 1, \delta) \in (\mathbb{N}^*)^r$ de $\mathfrak{p}_i$ $(1 \leqslant i \leqslant s)$, et $f = \prod_{1 \leqslant i \leqslant s} f_i^{\ell_i}$. Alors f est une forme résultante d'indice d de I et de $\mathsf{Z}(I)$ (*cf.* théorème 3.11 et définition 3.9 (ii)). Écrivons $F = \sum_\alpha a_\alpha X^\alpha$ (où $\alpha \in \mathbb{N}^{m+1}$, $|\alpha| = \delta$) et notons $\rho : K[u^1, \dots, u^r] \to K[u^1, \dots, u^{r-1}]$ le morphisme de $K[u^1, \dots, u^{r-1}]$-algèbres défini par $\rho(u^r_\alpha) = a_\alpha$ pour tout α. D'après la proposition 3.6 de [**NP01**, chap. 5], $\rho(f)$ (resp. $\rho(f_i)$) est une forme de Chow de J (resp. de $(\mathfrak{p}_i, F)$). On en déduit, par le théorème 3.12 et le théorème de Bézout géométrique 3.26 (i) :

$$
\begin{aligned}
d(\mathsf{Z}(J)) &= \deg_{u^1} \rho(f) = \deg_{u^1}\Big(\prod_{1\leqslant i\leqslant s} (\rho(f_i))^{\ell_i}\Big) = \sum_{1\leqslant i\leqslant s} \ell_i \deg_{u^1}(\rho(f_i)) \\
&= \sum_{1\leqslant i\leqslant s} \ell_i d\big(\mathsf{Z}((\mathfrak{p}_i, F))\big) \leqslant \Big(\sum_{1\leqslant i\leqslant s} \ell_i d(\mathsf{Z}(\mathfrak{p}_i))\Big) \deg F = d(\mathsf{Z}(I)) \deg F,
\end{aligned}
$$

l'inégalité ci-dessus étant une égalité si $\mathsf{Z}(J) \neq 0$, puisque alors $\mathrm{ht}(J) = \mathrm{ht}((\mathfrak{p}_i, F)) \leqslant m$ et donc $\mathsf{Z}((\mathfrak{p}_i, F)) \neq 0$ pour tout i. On a de même pour la hauteur :

$$
\begin{aligned}
h(\mathsf{Z}(J)) = h(\rho(f)) &= \sum_{1\leqslant i\leqslant s} \ell_i h(\rho(f_i)) = \sum_{1\leqslant i\leqslant s} \ell_i h\big(\mathsf{Z}((\mathfrak{p}_i, F))\big) \\
&\leqslant \Big(\sum_{1\leqslant i\leqslant s} \ell_i h(\mathsf{Z}(\mathfrak{p}_i))\Big) \deg F + h(F)\Big(\sum_{1\leqslant i\leqslant s} \ell_i d(\mathsf{Z}(\mathfrak{p}_i))\Big) \\
&\qquad\qquad + C_3\Big(\sum_{1\leqslant i\leqslant s} \ell_i d(\mathsf{Z}(\mathfrak{p}_i))\Big) \deg F \\
&= h(\mathsf{Z}(I)) \deg F + h(F)\, d(\mathsf{Z}(I)) + C_3\, d(\mathsf{Z}(I)) \deg F.
\end{aligned}
$$

$\square$

4. Lemme de multiplicité

Comme on l'a vu, le point clef de la preuve présentée au § 2 est le lemme de multiplicité 2.9. Celui-ci est en fait un corollaire d'un lemme de multiplicité plus général pour des fonctions $f_1, \ldots, f_m$, analytiques en zéro, et qui sont solutions de certains systèmes différentiels. Le but de cette partie est d'exposer ces résultats. En un premier temps, nous énoncerons ce lemme de multiplicité plus général et en expliquerons la preuve (paragraphes 4.1 à 4.5). Il restera alors à voir, en un deuxième temps, pourquoi ce lemme de multiplicité s'applique aux fonctions de Ramanujan P, Q, R et au système différentiel (S_0) : ceci sera fait au § 4.6.

4.1. Énoncé d'un lemme de multiplicité général. — Soient $A_0, \ldots, A_m$ des polynômes de $\mathbb{C}[Z, X_1, \ldots, X_m]$ tels que $A_0 \neq 0$, et considérons le système d'équations différentielles

$$(S) \qquad A_0(z, y_1, \ldots, y_m) y_j' = A_j(z, y_1, \ldots, y_m), \quad 1 \leqslant j \leqslant m.$$

Notons encore $D : \mathbb{C}[Z, X_1, \ldots, X_m] \to \mathbb{C}[Z, X_1, \ldots, X_m]$ l'opérateur différentiel associé au système (S), *i.e.*

$$D = A_0 \frac{\partial}{\partial z} + \sum_{1 \leqslant j \leqslant m} A_j \frac{\partial}{\partial X_j}. \tag{23}$$

Supposons maintenant qu'il existe des fonctions $f_1, \ldots, f_m$, analytiques au voisinage de zéro,[8] qui soient solutions du système (S). Nous noterons $f = (f_1, \ldots, f_m)$ dans la suite. Soit alors $A \in \mathbb{C}[Z, X_1, \ldots, X_m]$ un polynôme tel que la fonction $F(z) = A(z, f_1(z), \ldots, f_m(z))$ ne soit pas identiquement nulle. Le but du lemme de multiplicité que l'on va établir est de donner une majoration, en fonction des degrés $\deg_Z A$ et $\deg_X A$, de l'ordre en $z = 0$ de la fonction F. On ne pourra établir une telle majoration que si le couple (D, f) possède une propriété spéciale, que nous appellerons la « propriété $\mathscr{D}$ ». Avant d'expliquer de quoi il s'agit, énonçons tout de suite le lemme de multiplicité de Nesterenko :

Théorème 4.1. — *Soient $f_1, \ldots, f_m$ des fonctions analytiques au voisinage de zéro, formant une solution du système différentiel (S), et telles que le couple (D, f) vérifie la propriété $\mathscr{D}$. Alors il existe un réel $c_0 > 0$ (dépendant des fonctions $f_1, \ldots, f_m$ et des polynômes $A_0, \ldots, A_m$), tel que pour tout polynôme non nul $A \in \mathbb{C}[Z, X_1, \ldots, X_m]$, on ait :*

$$\operatorname{ord}_0 A(z, f_1(z), \ldots, f_m(z)) \leqslant c_0 (\deg_Z A + 1)(\deg_X A + 1)^m.$$

Nous verrons ci-après (§ 4.2) que ce théorème est un cas particulier d'un résultat plus général, le théorème 4.8. Nous verrons également (corollaire 4.23) que les fonctions

[8] Si l'on souhaite avoir un résultat au voisinage d'un point quelconque $\xi \in \mathbb{C}$, on se ramène immédiatement en zéro par translation.

de Ramanujan P, Q, R vérifient les hypothèses du théorème 4.1 avec le système (S_0). Le théorème 2.9 est donc un simple corollaire de ce théorème.

Passons maintenant à la définition de la propriété $\mathscr{D}$. Soient donc D l'opérateur différentiel défini par (23) , et $f = (f_1, \ldots, f_m)$ un m-uplet de fonctions analytiques au voisinage de zéro (non nécessairement solutions de (S)). Définissons alors, pour tout idéal premier $\mathfrak{p} \subset \mathbb{C}[Z, X_1, \ldots, X_m]$,

$$c_{\mathfrak{p}} = c_{\mathfrak{p},f} = \min_{E \in \mathfrak{p}} \operatorname{ord}_0 E(z, f_1(z), \ldots, f_m(z)) \in \mathbb{N} \cup \{+\infty\}.$$

En suivant une démarche analogue à celle de Nesterenko [**NP01**, chap. 10], on pose alors :

Définition 4.2. — On dira que le couple (D, f) vérifie la propriété $\mathscr{D}$ s'il existe un réel $c > 0$ (dépendant de D et f) tel que, pour tout idéal premier $\mathfrak{p} \neq 0$ de $\mathbb{C}[Z, X_1, \ldots, X_m]$, stable par D (*i.e.* tel que $D\mathfrak{p} \subset \mathfrak{p}$), et tel que $\mathfrak{p} \cap \mathbb{C}[Z] = (0)$, on ait $c_{\mathfrak{p}} \leqslant c$.

Remarque 4.3. — De façon équivalente, dire que (D, f) vérifie la propriété $\mathscr{D}$ signifie qu'il existe un réel $c > 0$ tel que tout idéal premier $\mathfrak{p} \neq 0$ stable par D et tel que $\mathfrak{p} \cap \mathbb{C}[Z] = (0)$ contienne un polynôme $E \neq 0$ vérifiant $\operatorname{ord}_0 E(z, f_1(z), \ldots, f_m(z)) \leqslant c$.

Remarque 4.4. — Il est facile de voir que si (D, f) vérifie la propriété $\mathscr{D}$ et si $(f_1, \ldots, f_m)$ est une solution de (S), alors les fonctions $f_1, \ldots, f_m$ sont algébriquement indépendantes sur $\mathbb{C}(z)$. Voir [**NP01**, chap. 10, § 1].

Remarque 4.5. — Une condition suffisante pour que (D, f) vérifie la propriété $\mathscr{D}$ est que $f_1, \ldots, f_m$ soient algébriquement indépendantes sur $\mathbb{C}(z)$ et que

$$\bigcap_{\substack{\mathfrak{p} \neq 0, D\mathfrak{p} \subset \mathfrak{p} \\ \mathfrak{p} \cap \mathbb{C}[Z] = (0) \\ (0, f_1(0), \ldots, f_m(0)) \in \mathscr{Z}(\mathfrak{p})}} \mathfrak{p} \neq 0,$$

l'intersection portant sur tous les idéaux premiers non nuls $\mathfrak{p}$ de $\mathbb{C}[Z, X_1, \ldots, X_m]$ stables par D, tels que $\mathfrak{p} \cap \mathbb{C}[Z] = (0)$, et ayant le point $(0, f_1(0), \ldots, f_m(0))$ comme zéro (on convient que $\cap_{\varnothing} \mathfrak{p} = \mathbb{C}[Z, X_1, \ldots, X_m]$). En effet, il suffit alors de choisir $E \neq 0$ dans l'intersection, et de prendre $c = \operatorname{ord}_0 E(z, f_1(z), \ldots, f_m(z))$ (noter que si $(0, f_1(0), \ldots, f_m(0)) \notin \mathscr{Z}(\mathfrak{p})$, alors $c_{\mathfrak{p}} = 0$). C'est en fait cette condition que l'on vérifiera au paragraphe 4.6 pour les fonctions P, Q, R (voir théorème 4.25).

Remarque 4.6. — La propriété $\mathscr{D}$ est automatiquement vérifiée si $f_1, \ldots, f_m$ sont algébriquement indépendantes sur $\mathbb{C}(z)$, si $(f_1, \ldots, f_m)$ est une solution de (S), et si $A_0(0, f_1(0), \ldots, f_m(0)) \neq 0$. Voir [**NP01**, chap. 10, § 1, Example 1]. Ainsi, les seuls problèmes pour vérifier cette propriété apparaissent lorsque le point $(0, f_1(0), \ldots, f_m(0))$ est un point singulier du système différentiel (S). C'est en particulier le cas pour les fonctions de Ramanujan, où la vérification de cette propriété n'est pas triviale.

Remarque 4.7. — Dans le cas où le système (S) est de la forme

$$a_0(z)y_j' = \sum_{1\leqslant i\leqslant m} a_{ij}(z)y_i, \quad 1\leqslant j\leqslant m, \quad a_0, a_{ij}\in\mathbb{C}[Z],$$

et où $f_1,\dots,f_m$ sont algébriquement indépendantes sur $\mathbb{C}(z)$ et forment une solution de (S), alors la propriété $\mathscr{D}$ est toujours vérifiée [**Nes74**].

4.2. Lien avec une minoration de la distance d'un point à un cycle. — La preuve du théorème 4.1 repose sur les résultats de géométrie diophantienne exposés au § 3, dont nous conservons les notations. On travaillera ici avec le corps $K=\mathbb{C}(Z)$.

Pour voir comment apparaissent les notions du § 3, introduisons la valeur absolue $|\,|_0$ sur K définie par $|f|_0 = e^{-\operatorname{ord}_0 f}$. Cette valeur absolue restera fixée jusqu'à la fin de ce § 4, et nous noterons donc plus simplement $|\,| = |\,|_0$ et $\|\,\| = \|\,\|_0$. Comme au § 3.5, on notera $\mathcal{K}=\mathcal{K}_0$ le complété d'une clôture algébrique de $K_0=\mathbb{C}((Z))$. On dispose alors d'une fonction Dist relative à ce choix de la valeur absolue. Comme les fonctions $f_1,\dots,f_m$ du théorème 4.1 sont analytiques en zéro, elles définissent des éléments de $\mathbb{C}[[Z]]\subset\mathcal{K}$, que nous noterons encore $f_1,\dots,f_m$. Avec ces notations, la conclusion du théorème 4.1 s'écrit alors

$$\log|A(Z,f_1,\dots,f_m)| \geqslant -c_0(\deg_Z A+1)(\deg_X A+1)^m. \tag{24}$$

Maintenant, si l'on note $x=(1,f_1,\dots,f_m)\in\mathbb{P}_m(\mathcal{K})$ et $\widetilde{A}(X_0,\dots,X_m) = X_0^{\deg_X A}A(Z,X_1/X_0,\dots,X_m/X_0)\in K[X]$ l'homogénéisé de A (vu comme polynôme à coefficients dans K), on a $\|x\|=1$ et $\widetilde{A}(x)=A(Z,f_1,\dots,f_m)$, d'où

$$\log\operatorname{Dist}(x,\mathsf{Z}(\widetilde{A})) = \log\frac{|A(Z,f_1,\dots,f_m)|}{|\widetilde{A}|}.$$

Ainsi, la conclusion (24) s'écrit encore :

$$\log\operatorname{Dist}(x,\mathsf{Z}(\widetilde{A})) \geqslant -c_0(\deg_Z\widetilde{A}+1)(\deg_X\widetilde{A}+1)^m - \log|\widetilde{A}|.$$

La conclusion du lemme de multiplicité 4.1 n'est donc rien d'autre qu'une minoration de la distance du point x à un cycle de dimension $m-1$. Ce lemme de multiplicité va ainsi être un cas particulier du théorème suivant, qui donne une minoration de la distance $\log\operatorname{Dist}(x,\mathsf{Z})$ pour un cycle Z de dimension quelconque, en fonction du degré et de la hauteur du cycle.

Théorème 4.8. — *Soient $f_1,\dots,f_m$ des fonctions analytiques au voisinage de zéro, formant une solution du système différentiel (S), et telles que le couple (D,f) vérifie la propriété $\mathscr{D}$. Notons x le point de $\mathbb{P}_m(\mathcal{K})$ défini par $x=(1,f_1,\dots,f_m)$. Alors il existe un réel $\tau>0$ tel que pour tout cycle Z de $\mathbb{P}_m$ de dimension $r-1<m$, on ait :*

$$\log\operatorname{Dist}(x,\mathsf{Z}) \geqslant -\tau^{mr}\big(h(\mathsf{Z})d(\mathsf{Z})^{r/(m+1-r)} + d(\mathsf{Z})^{m/(m+1-r)}\big). \tag{25}$$

Démonstration du théorème 4.1 à partir du théorème 4.8. — On peut supposer $\deg_X A \geqslant 1$, car sinon on a trivialement $\operatorname{ord}_0 A(z, f_1(z), \dots, f_m(z)) \leqslant \deg_Z A$. Soit alors $\widetilde{A} = X_0^{\deg_X A} A(Z, X_1/X_0, \dots, X_m/X_0) \in K[X]$ l'homogénéisé de A, et appliquons le théorème 4.8 au cycle $\mathsf{Z}(\widetilde{A})$. On a $r = m$ (car $\widetilde{A} \notin K$), $\log \operatorname{Dist}(x, \mathsf{Z}(\widetilde{A})) = -\operatorname{ord}_0 A(z, f_1(z), \dots, f_m(z)) - \log|\widetilde{A}|$, $h(\mathsf{Z}(\widetilde{A})) = h(\widetilde{A}) \leqslant \deg_Z A$ (d'après la proposition 3.19 et la remarque 3.15), et $d(\mathsf{Z}(\widetilde{A})) = \deg_X \widetilde{A} = \deg_X A$ (voir § 3.3). On obtient :

$$\begin{aligned}\operatorname{ord}_0 A(z, f_1(z), \dots, f_m(z)) &\leqslant \tau^{m^2}((\deg_Z A)(\deg_X A)^m + (\deg_X A)^m) - \log|\widetilde{A}| \\ &\leqslant \tau^{m^2}(\deg_Z A + 1)(\deg_X A)^m + \deg_Z A \\ &\leqslant (\tau^{m^2} + 1)(\deg_Z A + 1)(\deg_X A)^m. \qquad \square\end{aligned}$$

Pour démontrer le théorème 4.8, nous allons travailler dans l'anneau $R = K[X_0, \dots, X_m] = K[X]$ et avec des idéaux homogènes. Or, la propriété $\mathscr{D}$ est une propriété « inhomogène ». Nous aurons besoin d'une version homogène de cette propriété $\mathscr{D}$ que nous définissons maintenant.

Soit $x \in \mathbb{P}_m(\mathcal{K})$ un point projectif. Pour tout idéal premier homogène $\mathfrak{p} \subset K[X]$, on note

$$c'_{\mathfrak{p}} = c'_{\mathfrak{p},x} = \inf_{\substack{E \in \mathfrak{p} \\ E \text{ homogène}}} \{-\log \operatorname{Dist}(x, \mathsf{Z}(E))\} \in \mathbb{R}_{\geqslant 0} \cup \{+\infty\}.$$

La version homogène de la propriété $\mathscr{D}$ que nous considérerons est la suivante :

Définition 4.9. — Soient $\mathcal{D} : K[X] \to K[X]$ un opérateur différentiel et $x \in \mathbb{P}_m(\mathcal{K})$ un point. On dira que le couple $(\mathcal{D}, x)$ vérifie la propriété $\mathscr{D}'$ s'il existe un réel $c' > 0$ (dépendant de $\mathcal{D}$ et x) tel que, pour tout idéal homogène premier non nul $\mathfrak{p} \subset K[X]$ stable par $\mathcal{D}$, on ait $c'_{\mathfrak{p}} \leqslant c'$.

Le lien entre les propriétés $\mathscr{D}$ et $\mathscr{D}'$ est le suivant. Reprenons les polynômes $A_0, \dots, A_m$ précédents, ainsi que $D : \mathbb{C}[Z, X_1, \dots, X_m] \to \mathbb{C}[Z, X_1, \dots, X_m]$ l'opérateur différentiel qu'ils définissent (*cf.* (23)). Notons $d = \max_{0 \leqslant j \leqslant m} \deg_X A_j$ et, pour $0 \leqslant j \leqslant m$, soit $B_j(Z, X_0, \dots, X_m) = X_0^d A_j(Z, X_1/X_0, \dots, X_m/X_0)$. Le polynôme $B_j \in K[X]$ est homogène de degré d pour tout j. Notons encore $\mathcal{D} : K[X] \to K[X]$ l'homogénéisé de l'opérateur différentiel D, défini par

$$\mathcal{D} = B_0 \frac{\partial}{\partial Z} + \sum_{1 \leqslant j \leqslant m} X_0 B_j \frac{\partial}{\partial X_j}. \tag{26}$$

Soient enfin $f_1, \dots, f_m$ des fonctions analytiques au voisinage de 0, $f = (f_1, \dots, f_m)$, et $x = (1, f_1, \dots, f_m) \in \mathbb{P}_m(\mathcal{K})$ le point qu'elles définissent. On a :

Proposition 4.10. — *Avec les notations précédentes, les assertions suivantes sont équivalentes :*

(i) *Le couple (D, f) vérifie la propriété $\mathscr{D}$.*
(ii) *Le couple $(\mathcal{D}, x)$ vérifie la propriété $\mathscr{D}'$.*

Démonstration (esquisse). — Notons, pour tout $A \in \mathbb{C}[Z, X_0, \ldots, X_m]$ et tout $B \in \mathbb{C}[Z, X_1, \ldots, X_m]$,

$$\mathring{A} = A(Z, 1, X_1, \ldots, X_m) \quad \text{et} \quad \widetilde{B} = X_0^{\deg_X B} B(Z, X_1/X_0, \ldots, X_m/X_0).$$

Pour montrer que (i) entraîne (ii), on considère $\mathfrak{p} \subset K[X]$ un idéal homogène premier non nul stable par $\mathcal{D}$, et l'on définit $\mathfrak{q} = \{\mathring{A} \mid A \in \mathfrak{p} \cap \mathbb{C}[Z, X_0, \ldots, X_m]\}$. Si $X_0 \in \mathfrak{p}$, alors $c'_{\mathfrak{p}} \leqslant -\log \operatorname{Dist}(x, \mathsf{Z}(X_0)) = 0$. Sinon, $\mathfrak{q} \subset \mathbb{C}[Z, X_1, \ldots, X_m]$ est un idéal premier non nul, stable par D, et tel que $\mathfrak{q} \cap \mathbb{C}[Z] = (0)$. Par la propriété $\mathscr{D}$, on a donc $c_{\mathfrak{q}} \leqslant c$. Mais en utilisant le fait que pour tout polynôme homogène (en X) $A \in \mathbb{C}[Z, X_0, \ldots, X_m]$ tel que $Z \nmid A$, on a $-\log \operatorname{Dist}(x, \mathsf{Z}(A)) = \operatorname{ord}_0 \mathring{A}(z, f_1(z), \ldots, f_m(z))$, on montre aisément que $c_{\mathfrak{q}} = c'_{\mathfrak{p}}$, d'où (i). On raisonne de façon analogue pour déduire (i) à partir de (ii). Partant cette fois d'un idéal $\mathfrak{q} \subset \mathbb{C}[Z, X_1, \ldots, X_m]$, premier, non nul, stable par D, et tel que $\mathfrak{q} \cap \mathbb{C}[Z] = (0)$, on définit $\mathfrak{p}$ l'idéal homogène de $K[X]$ engendré par les polynômes $\widetilde{B}$, $B \in \mathfrak{q}$. On vérifie que $\mathfrak{p}$ est un idéal homogène premier non nul de $K[X]$ stable par $\mathcal{D}$, et que $c_{\mathfrak{q}} = c'_{\mathfrak{p}}$, d'où l'implication $(ii) \Rightarrow (i)$. Les détails sont laissés au lecteur. □

Terminons ce paragraphe en expliquant le principe général de la preuve du théorème 4.8. On souhaite donc obtenir une minoration de $\log \operatorname{Dist}(x, \mathsf{Z})$ en fonction de $d(\mathsf{Z})$ et $h(\mathsf{Z})$, disons $\log \operatorname{Dist}(x, \mathsf{Z}) \geqslant M(d(\mathsf{Z}), h(\mathsf{Z}))$. Pour cela, on procède par récurrence sur la dimension du cycle (donc sur r). Si $r = 0$, c'est trivial. Pour passer de r à $r+1$, on se donne un cycle Z de dimension r et, raisonnant par contradiction, on suppose que $\log \operatorname{Dist}(x, \mathsf{Z}) < M(d(\mathsf{Z}), h(\mathsf{Z}))$. On voit facilement que l'on peut supposer que $\mathsf{Z} = V = \mathscr{Z}(\mathfrak{p})$ est une variété. Pour appliquer l'hypothèse de récurrence et obtenir une contradiction, il nous faut construire un cycle Z' de dimension $\leqslant r-1$ tel que $\log \operatorname{Dist}(x, \mathsf{Z}')$ soit inférieur à $M(d(\mathsf{Z}'), h(\mathsf{Z}'))$. Pour cela, on va prendre Z' de dimension $r-1$ et de la forme $\mathsf{Z}' = \mathsf{Z}((\mathfrak{p}, F))$, où $F \in K[X]$ est un polynôme homogène bien choisi tel que $F \notin \mathfrak{p}$. La majoration de $\log \operatorname{Dist}(x, \mathsf{Z}')$ sera fournie par le théorème de Bézout métrique.

On voit donc qu'il nous faudra trouver un polynôme $F \notin \mathfrak{p}$ dont les quantités $\deg F$, $h(F)$ et $\log \operatorname{Dist}(x, \mathsf{Z}(F))$ sont contrôlées (le plus finement possible) en fonction des données $d(V)$, $h(V)$, et $\log \operatorname{Dist}(x, V)$. Or, ce qui est précisément relativement facile de faire, c'est de choisir un tel polynôme *dans* $\mathfrak{p}$. Pour trouver F, on va donc partir d'un polynôme $E \in \mathfrak{p}$ tel que $d(E)$, $h(E)$ et $\log \operatorname{Dist}(x, \mathsf{Z}(E))$ soient « contrôlés », puis construire F à partir de E. C'est ici que l'opérateur différentiel $\mathcal{D}$ va intervenir, car il fournit un moyen naturel de construire un nouveau polynôme à partir du polynôme donné E (à savoir $\mathcal{D}E$), dont les paramètres degré, hauteur et distance sont en outre du même ordre de grandeur que les paramètres correspondants pour E. On va donc être amené à considérer les itérés $\mathcal{D}^n E$ ($n \geqslant 1$), en espérant que pour un $n \geqslant 1$ on aura $\mathcal{D}^n E \notin \mathfrak{p}$. Comme on le verra, c'est le fait que le couple $(\mathcal{D}, x)$ satisfasse la propriété $\mathscr{D}'$ qui garantira l'existence d'un tel entier n. Il suffira alors de prendre $F = \mathcal{D}^N E$, où $N \geqslant 1$ est le plus petit de ces entiers (en fait pour des raisons techniques il faudra prendre $F = (\mathcal{D}^N E)^2$). La difficulté ici consiste alors à *majorer* N en fonction des données (pour pouvoir contrôler $\deg F$ et $h(F)$).

La démonstration du théorème 4.8 fait l'objet des trois paragraphes suivants et va donc s'opérer en trois étapes. Lors d'une première étape, on construit le polynôme E puis, en supposant l'existence d'un entier n tel que $\mathcal{D}^n E \notin \mathfrak{p}$, on majore degré et hauteur de $A = \mathcal{D}^N E$ (N défini comme précédemment). Dans une seconde étape, utilisant la propriété $\mathscr{D}'$, on démontre l'existence de l'entier n et on majore $\log \mathrm{Dist}(x, \mathsf{Z}(A))$. En posant $F = A^2$ on a alors trouvé notre polynôme $F \notin \mathfrak{p}$. On peut alors enfin, lors de la troisième étape, procéder à la récurrence selon le schéma décrit ci-dessus, et achever ainsi la preuve du théorème 4.8.

4.3. Première étape : majoration de $\deg_X(\mathcal{D}^N E)$ et de $h(\mathcal{D}^N E)$. — Ce paragraphe est consacré à la première des trois étapes qui seront nécessaires pour démontrer le théorème 4.8. On se donne donc des polynômes $A_0, \ldots, A_m$ de $\mathbb{C}[Z, X_1, \ldots, X_m]$ comme précédemment, qui définissent des polynômes homogènes $B_0, \ldots, B_m$ de $K[X]$ et un opérateur différentiel homogène $\mathcal{D}$. Le but de cette première étape est d'établir la proposition 4.11 ci-après. Il est ici intéressant de noter que dans tout ce paragraphe les fonctions $f_1, \ldots, f_m$ du théorème 4.8 n'interviennent pas, et que la proposition 4.11 est en réalité valable plus généralement pour toute dérivation $\mathcal{D}$ de l'anneau $K[X]$ de la forme $\mathcal{D} = C_0 \frac{\partial}{\partial Z} + \sum_{1 \leqslant j \leqslant m} C_j \frac{\partial}{\partial X_j}$, où $C_0 \in \mathbb{C}[Z, X_0, \ldots, X_m]$ est un polynôme homogène en X de degré d, et $C_1, \ldots, C_m \in \mathbb{C}[Z, X_0, \ldots, X_m]$ sont des polynômes homogènes en X de même degré $d+1$.

Proposition 4.11. — *Il existe un nombre réel $\lambda \geqslant 1$ (ne dépendant que de m et $\mathcal{D}$) vérifiant la propriété suivante. Soit $\mathfrak{p} \subset K[X_0, \ldots, X_m]$ un idéal homogène premier non nul de hauteur $\leqslant m$ tel que $X_0 \notin \mathfrak{p}$, et soit $r = m+1-\mathrm{ht}(\mathfrak{p})$. Soit E un polynôme homogène non nul de $\mathfrak{p} \cap \mathbb{C}[Z, X_0, \ldots, X_m]$ tel que la quantité*

$$h^+(\mathfrak{p}) \deg_X E + d(\mathfrak{p}) \deg_Z E \tag{27}$$

soit minimale, où $h^+(\mathfrak{p}) = \max\{1, h(\mathfrak{p})\}$. On suppose en outre que l'hypothèse suivante est vérifiée :

$$\text{Il existe un entier } n \geqslant 1 \text{ tel que } \mathcal{D}^n E \notin \mathfrak{p}. \tag{H}$$

Alors, si N désigne le plus petit entier tel que $\mathcal{D}^N E \notin \mathfrak{p}$, le polynôme $A = \mathcal{D}^N E$ vérifie :

$$\begin{aligned} \deg_X A &\leqslant \lambda^{2^{m+1}} d(\mathfrak{p})^{1/(m+1-r)} \quad \textit{et} \\ h(A) \leqslant \deg_Z A &\leqslant \lambda^{2^{m+1}} \big(h(\mathfrak{p}) d(\mathfrak{p})^{-(m-r)/(m+1-r)} + 1\big). \end{aligned} \tag{28}$$

Pour démontrer cette proposition, nous aurons besoin tout d'abord du lemme suivant, qui montre *grosso modo* que dans tout idéal homogène premier non nul $\mathfrak{p}$ de $K[X]$ on peut trouver des polynômes $E \in \mathfrak{p} \cap \mathbb{C}[Z, X]$ de degrés en Z et en X contrôlés en fonction de $d(\mathfrak{p})$ et $h(\mathfrak{p})$.

Lemme 4.12. — *Il existe un nombre réel* $\gamma = \gamma(m) \geqslant 1$ *(ne dépendant que de* m*) vérifiant la propriété suivante. Soit* $\mathfrak{p} \subset K[X]$ *un idéal homogène premier non nul tel que* $\mathrm{ht}(\mathfrak{p}) \leqslant m$*, et soit* $r = m + 1 - \mathrm{ht}(\mathfrak{p})$*. Soient encore* μ, ν *des entiers* $\geqslant 0$ *vérifiant*

$$\nu^{m-r+1} \geqslant \gamma d(\mathfrak{p}) \quad et \quad (\mu+1)\nu^{m-r} \geqslant \gamma h(\mathfrak{p}). \tag{29}$$

Alors il existe un polynôme $P \in \mathfrak{p} \cap \mathbb{C}[Z, X]$*, homogène en* X*, et tel que* $\deg_X P = \nu$*,* $\deg_Z P \leqslant \mu$*.*

Remarque. — On peut prendre $\gamma = 2m(m!)$.

Démonstration. — La démonstration repose sur une majoration d'une certaine « fonction de Hilbert géométrique ». Définissons, pour μ, $\nu \in \mathbb{N}$,

$$\mathcal{L}_{\mu,\nu} = \{P \in \mathbb{C}[Z, X] \mid P \text{ homogène en } X,\ P \neq 0,\ \deg_X P = \nu,\ \deg_Z P \leqslant \mu\} \cup \{0\}.$$

La conclusion du lemme signifie $\mathfrak{p} \cap \mathcal{L}_{\mu,\nu} \neq \{0\}$, *i.e.*

$$\dim_{\mathbb{C}}\big(\mathcal{L}_{\mu,\nu}/\mathfrak{p} \cap \mathcal{L}_{\mu,\nu}\big) < \dim_{\mathbb{C}} \mathcal{L}_{\mu,\nu}. \tag{30}$$

Or, on a d'une part $\dim_{\mathbb{C}} \mathcal{L}_{\mu,\nu} = (\mu+1)\binom{\nu+m}{m}$, et d'autre part, on a la majoration suivante, pour $\mu \geqslant 0$ et $\nu \geqslant 1$ (voir [**NP01**, chap. 9]) :

$$\dim_{\mathbb{C}}\big(\mathcal{L}_{\mu,\nu}/\mathfrak{p} \cap \mathcal{L}_{\mu,\nu}\big) \leqslant \gamma_0((\mu+1)\nu^{r-1}d(\mathfrak{p}) + \nu^r h(\mathfrak{p})),$$

où $\gamma_0 = \gamma_0(m)$ (on peut prendre $\gamma_0 = m$ d'après [**NP01**, chap. 9]). En prenant $\gamma = 2(m!)\gamma_0$, on en déduit aisément, compte tenu de (29), l'inégalité (30) et donc le lemme 4.12. □

Soient maintenant E, $\mathfrak{p}$ et N comme dans l'énoncé de la proposition 4.11. On se fixe encore un réel λ, ne dépendant que de m et $\mathcal{D}$, mais suffisamment grand pour pouvoir satisfaire les différentes inégalités qui interviendront dans la suite (ce réel λ est celui de la proposition 4.11). On pose encore $L = \deg_X E$ et $M = \max\{1, h(E)\}$. On notera que E, vu comme polynôme à coefficients dans $\mathbb{C}[Z]$, est automatiquement primitif (*i.e.* ses coefficients sont premiers entre eux), et donc $h(E) = \deg_Z E$ (*cf.* remarque 3.15). Le lemme 4.12 implique le résultat suivant :

Corollaire 4.13. — *On a les majorations :*

$$L = \deg_X E \leqslant 3\lambda d(\mathfrak{p})^{1/(m-r+1)} \quad et \quad \deg_Z E \leqslant 3\lambda h^+(\mathfrak{p}) d(\mathfrak{p})^{-(m-r)/(m-r+1)}.$$

Démonstration. — Définissons

$$\mu = [\gamma h(\mathfrak{p}) d(\mathfrak{p})^{-(m-r)/(m-r+1)}] \quad \text{et} \quad \nu = 1 + [\gamma d(\mathfrak{p})^{1/(m-r+1)}].$$

On vérifie immédiatement que μ et ν satisfont aux inégalités (29). Il existe donc un polynôme $P \in \mathfrak{p} \cap \mathbb{C}[Z, X]$, homogène en X, et tel que $\deg_X P = \nu$, $\deg_Z P \leqslant \mu$. Par minimalité de la quantité (27), on déduit

$$Lh^+(\mathfrak{p}) + d(\mathfrak{p}) \deg_Z E \leqslant \nu h^+(\mathfrak{p}) + \mu d(\mathfrak{p}) \leqslant 3\lambda h^+(\mathfrak{p}) d(\mathfrak{p})^{1/(m-r+1)},$$

d'où les majorations du corollaire. □

Notre tâche principale va être maintenant de majorer N. Pour cela, on introduit, pour chaque entier $n \geqslant 0$, l'idéal $J_n = (E, \dots, \mathcal{D}^n E) = (\mathcal{D}^i E)_{0 \leqslant i \leqslant n}$. On a $J_n \subset J_{n+1}$ pour tout n, et N est le plus petit entier n tel que $J_n \not\subset \mathfrak{p}$.

Nous allons ci-après exclusivement travailler dans l'idéal $\mathfrak{p}$. Ainsi, on ne tiendra pas compte par exemple des composantes primaires ou des premiers associés des idéaux qui interviendront, dès lors que ceux-ci ne sont pas inclus dans $\mathfrak{p}$. Autrement dit, on travaillera dans l'anneau localisé $R_{\mathfrak{p}}$ (rappelons que $R = K[X]$). Si I est un idéal de R, on notera $IR_{\mathfrak{p}}$ l'idéal de $R_{\mathfrak{p}}$ engendré par I. On posera également $h = \mathrm{ht}(J_{N-1}R_{\mathfrak{p}})$.

Définissons alors les entiers $0 \leqslant n_1 < \cdots < n_h < n_{h+1} = N$ et $\delta_1, \dots, \delta_h \geqslant 0$ de la façon suivante. Pour $1 \leqslant i \leqslant h$, n_i est le plus petit entier tel que $\mathrm{ht}(J_{n_i}R_{\mathfrak{p}}) = i$, et δ_i est le plus grand entier $\geqslant 0$ tel que $\mathrm{ht}(J_{n_i}R_{\mathfrak{p}}) = \cdots = \mathrm{ht}(J_{n_i+\delta_i}R_{\mathfrak{p}})$. Comme $J_0 = (E)$ est principal, on a $\mathrm{ht}(J_0 R_{\mathfrak{p}}) = 1$ et $n_1 = 0$. De plus, puisque $\mathrm{ht}(J_{n+1}R_{\mathfrak{p}}) \leqslant \mathrm{ht}(J_n R_{\mathfrak{p}}) + 1$ et $J_N R_{\mathfrak{p}} = R_{\mathfrak{p}}$, les entiers n_i et δ_i sont bien définis. On notera aussi que, par définition, $n_{i+1} = n_i + \delta_i + 1$ $(1 \leqslant i \leqslant h)$.

Avec ces notations, on a :

Lemme 4.14. — *Il existe des polynômes $E_1, \dots, E_h \in \mathbb{C}[Z, X]$, homogènes en X, vérifiant $E_1 = E$ et pour tout i, $1 \leqslant i \leqslant h$, les conditions :*

(i) $E_i \in J_{n_i}$

(ii) $\mathrm{ht}((E_1, \dots, E_i)R_{\mathfrak{p}}) = i$

(iii) $\deg_X E_i \leqslant L + n_i d$ *et* $\deg_Z E_i \leqslant M + n_i d'$, *où* $d = \max_{0 \leqslant j \leqslant m} \deg_X B_j$ *et* $d' = \max_{0 \leqslant j \leqslant m} \deg_Z B_j$.

Démonstration. — On procède par récurrence sur i. Si $i = 1$, $E_1 = E$ vérifie bien les conditions (i), (ii) et (iii). Soit maintenant $i > 1$ et supposons construits $E_1, \dots, E_{i-1}$. Notons $\mathfrak{q}_1, \dots, \mathfrak{q}_s$ les premiers associés $\mathfrak{q}$ de $(E_1, \dots, E_{i-1})$ tels que $\mathfrak{q} \subset \mathfrak{p}$ et $\mathrm{ht}(\mathfrak{q}R_{\mathfrak{p}}) = i - 1$. Pour tout $j \in \{1, \dots, s\}$, il existe $m_j \in \{0, \dots, n_i\}$ tel que $\mathcal{D}^{m_j}E \notin \mathfrak{q}_j$ (car sinon $J_{n_i} \subset \mathfrak{q}_j \subset \mathfrak{p}$, d'où $i = \mathrm{ht}(J_{n_i}R_{\mathfrak{p}}) \leqslant \mathrm{ht}(\mathfrak{q}_j R_{\mathfrak{p}}) = i - 1$). Puisque $X_0 \notin \mathfrak{p}$ il existe alors (voir par exemple [**Eis95**, exercise 3.19 (a) page 114]) des entiers $t_j \in \mathbb{N}$ et des nombres complexes λ_j $(0 \leqslant j \leqslant n_i)$ tels que le polynôme $E_i = \sum_{0 \leqslant j \leqslant n_i} \lambda_j X_0^{t_j} \mathcal{D}^j E$ soit homogène en X et satisfasse $E_i \notin \mathfrak{q}_1 \cup \cdots \cup \mathfrak{q}_s$. On peut de plus évidemment choisir $t_j = 0$ pour au moins un indice j. Alors (i), (ii) et (iii) sont vérifiés. □

Dans la suite, on notera $\mathfrak{A}_i$ l'idéal $\mathfrak{A}_i = (E_1, \dots, E_i)R_{\mathfrak{p}} \cap R$. L'idéal $\mathfrak{A}_i$ est donc l'intersection des composantes primaires de l'idéal $(E_1, \dots, E_i)$ contenues dans $\mathfrak{p}$. De plus, l'idéal $\mathfrak{A}_i$ est équidimensionnel. En effet, l'idéal $(E_1, \dots, E_i)R_{\mathfrak{p}}$ est équidimensionnel puisque $R_{\mathfrak{p}}$ est un anneau de Cohen-Macaulay et que $(E_1, \dots, E_i)R_{\mathfrak{p}}$ est de hauteur i engendré par i éléments ([**Mat96**, théorèmes 17.6 et 17.7]). Il en est donc de même de $\mathfrak{A}_i$, puisque les idéaux premiers associés de $\mathfrak{A}_i$ correspondent à ceux de $(E_1, \dots, E_i)R_{\mathfrak{p}}$ via l'application canonique $R \to R_{\mathfrak{p}}$, les hauteurs étant conservées.

Nous aurons également besoin de la majoration suivante de δ_i :

Lemme 4.15. — *Soit $i \in \{1, \ldots, h\}$, et soit $\mathfrak{q} \supset J_{n_i+\delta_i}$ un premier associé minimal de hauteur i tel que $\mathfrak{q} \subset \mathfrak{p}$ (alors c'est aussi un premier associé minimal de $\mathfrak{A}_i$). Soit Q la composante $\mathfrak{q}$-primaire de $\mathfrak{A}_i$, et ℓ_Q sa longueur. Alors on a $\delta_i + 1 \leqslant \ell_Q$.*

Démonstration. — La suite d'inclusions $(E_1, \ldots, E_i) \subset J_{n_i} \subset \cdots \subset J_{n_i+\delta_i} \subset \mathfrak{q}$ donne la chaîne d'idéaux $\mathfrak{q}$-primaires

$$Q \subset Q_{n_i} \subset \cdots \subset Q_{n_i+\delta_i} \subset \mathfrak{q}, \tag{31}$$

où $Q = (E_1, \ldots, E_i)R_{\mathfrak{q}} \cap R = \mathfrak{A}_i R_{\mathfrak{q}} \cap R$ et $Q_j = J_j R_{\mathfrak{q}} \cap R$. Maintenant, on a des inclusions strictes $Q_j \subsetneqq Q_{j+1}$ $(n_i \leqslant j < n_i + \delta_i)$, car une égalité $Q_j = Q_{j+1}$ impliquerait $\mathcal{D}(Q_j) = \mathcal{D}(J_j R_{\mathfrak{q}} \cap R) \subset \mathcal{D}(J_j)R_{\mathfrak{q}} \cap R \subset J_{j+1}R_{\mathfrak{q}} \cap R = Q_{j+1} = Q_j$, d'où $\mathcal{D}^n Q_j \subset Q_j$ pour tout $n \geqslant 0$, et donc en particulier on aurait $\mathcal{D}^n E \in \mathfrak{p}$ pour tout $n \geqslant 0$, contrairement à l'hypothèse faite dans la proposition 4.11. La majoration $\delta_i + 1 \leqslant \ell_Q$ résulte alors immédiatement de (31). □

Pour majorer N, nous allons majorer n_i par récurrence sur i $(2 \leqslant i \leqslant h+1)$. Pour ce faire, on va utiliser les théorèmes de Bézout géométrique et arithmétique, mais ceux-ci ne seront pas directement applicables tels quels. Nous aurons besoin de la remarque facile suivante pour pouvoir les appliquer :

Lemme 4.16. — *Soient $I, J \subset K[X_0, \ldots, X_m]$ deux idéaux homogènes tels que $\mathrm{ht}(J) = \mathrm{ht}(I) + 1$. Soit encore $F \in K[X_0, \ldots, K_m]$ un polynôme homogène qui n'est contenu dans aucun idéal premier associé de I (i.e. qui n'est pas diviseur de zéro dans $K[X_0, \ldots, X_m]/I$), et tel que $(I, F) \subset J$. Alors on a :*

$$d(\mathsf{Z}(J)) \leqslant d(\mathsf{Z}(I,F)) \quad \textit{et} \quad h(\mathsf{Z}(J)) \leqslant h(\mathsf{Z}(I,F)).$$

Démonstration. — Notons $r = m + 1 - \mathrm{ht}(J)$, $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ les premiers associés de J de hauteur $\mathrm{ht}(J)$ et, pour $i \in \{1, \ldots, s\}$, désignons par ℓ_i la longueur de la composante $\mathfrak{p}_i$-primaire de J. Soient encore $f_1, \ldots, f_s$ des formes de Chow de $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ respectivement. Alors $f = \prod_{1 \leqslant i \leqslant s} f_i^{\ell_i}$ est une forme de Chow du cycle $\mathsf{Z}(J)$. Maintenant, $\mathfrak{p}_i$ $(1 \leqslant i \leqslant s)$ est aussi un premier associé minimal de (I, F) de hauteur $\mathrm{ht}((I,F))$ (puisque $\mathrm{ht}(\mathfrak{p}_i) = \mathrm{ht}(I) + 1 = \mathrm{ht}((I,F))$). Notons ℓ'_i la longueur de la composante $\mathfrak{p}_i$-primaire de (I,F). Le cycle $\mathsf{Z}((I,F))$ admet une forme de Chow de la forme $g = g_1 \prod_{1 \leqslant i \leqslant s} f_i^{\ell'_i}$. Or, de l'inclusion $(I,F) \subset J$ on déduit facilement que l'on a $\ell_i \leqslant \ell'_i$. On voit donc que f divise g dans $K[X_0, \ldots, X_m]$, d'où l'on déduit $\deg_{u^1} f \leqslant \deg_{u^1} g$ et $h(f) \leqslant h(g)$. Autrement dit, on a $d(\mathsf{Z}(J)) \leqslant d(\mathsf{Z}(I,F))$ et $h(\mathsf{Z}(J)) \leqslant h(\mathsf{Z}(I,F))$. □

Nous sommes maintenant enfin en mesure de majorer l'entier N :

Lemme 4.17. — *On a pour N la majoration $N \leqslant \lambda^{2^{m+1}-2}$.*

Démonstration. — Comme on l'a dit, on va majorer n_i par récurrence $(2 \leqslant i \leqslant h+1)$, et en déduire ainsi la majoration pour N puisque $N = n_{h+1}$. De façon plus précise, définissons, pour tout entier $i \geqslant 1$, les constantes suivantes :

$$a_i = \lambda^{2^{i+1}-4}, \quad b_i = \lambda^{2^i-1}, \quad c_i = \lambda^{2^i-2}.$$

On va montrer par récurrence que l'on a, pour tout $i \in \{1, \ldots, h\}$:

(i) $\deg_X E_i \leqslant b_i L$
(ii) $h(E_i) \leqslant b_i M$
(iii) $d(\mathfrak{A}_i) \leqslant a_i L^i$
(iv) $h(\mathfrak{A}_i) \leqslant a_i M L^{i-1}$
(v) $n_{i+1} \leqslant c_i + 2^i \lambda a_i \leqslant c_{i+1}$.

Notons d'abord que l'inégalité $c_i + 2^i\lambda a_i \leqslant c_{i+1}$ est immédiate puisque λ est choisi suffisamment grand (et i est majoré par $h \leqslant m$). Remarquons aussi que pour $i = 1$ les inégalités (i) à (iv) sont triviales puisque dans ce cas $d(\mathfrak{A}_i) = \deg_X E$ et $h(\mathfrak{A}_i) = h(E)$. Démontrons (v). Si $J_1 \not\subset \mathfrak{p}$, alors $N = n_2 = 1$ et l'inégalité est vraie. Si en revanche $J_1 \subset \mathfrak{p}$, on a $\mathrm{ht}(J_1 R_\mathfrak{p}) = 2$ puisque $\mathcal{D}E \notin (E)$ (sinon on aurait $\mathcal{D}^n E \in \mathfrak{p}$ pour tout n). On a donc encore $n_2 = 1$ et l'inégalité (v) est claire.

Supposons maintenant avoir démontré les inégalités (i) à (v) pour l'entier i, et cherchons à les démontrer pour $i+1$ $(1 \leqslant i \leqslant h-1)$. Les inégalités (i) et (ii) résultent immédiatement de la partie (iii) du lemme 4.14. En effet, on a

$$\deg_X E_{i+1} \leqslant L + n_{i+1} d \leqslant n_{i+1} \lambda L \leqslant b_{i+1} L$$

en utilisant (v) (pour l'indice i) et le fait que $L \geqslant 1$ (puisque $E \notin K^*$). L'estimation est analogue pour $h(E_{i+1})$ (noter simplement que $h(E_{i+1}) \leqslant \deg_Z E_{i+1}$).

Pour démontrer (iii) et (iv), on remarque que $(\mathfrak{A}_i, E_{i+1}) \subset \mathfrak{A}_{i+1}$ et $\mathrm{ht}(\mathfrak{A}_{i+1}) = \mathrm{ht}(\mathfrak{A}_i) + 1$. Comme l'idéal $\mathfrak{A}_i$ est équidimensionnel, il résulte en particulier de la dernière égalité que le polynôme E_{i+1} n'appartient à aucun idéal premier associé de $\mathfrak{A}_i$. On peut ainsi appliquer le lemme 4.16, ce qui donne, en utilisant en outre les théorèmes de Bézout géométrique et arithmétique (corollaire 3.27),

$$d(\mathfrak{A}_{i+1}) \leqslant d(\mathfrak{A}_i) \deg_X E_{i+1} \leqslant a_i L^i b_{i+1} L \leqslant a_{i+1} L^{i+1}$$

et

$$h(\mathfrak{A}_{i+1}) \leqslant h(\mathfrak{A}_i) \deg_X E_{i+1} + h(E_{i+1}) d(\mathfrak{A}_i) \leqslant 2 a_i b_{i+1} M L^i \leqslant a_{i+1} M L^i.$$

Reste à établir (v) au rang $i+1$. Il s'agit donc de montrer $n_{i+2} = n_{i+1} + \delta_{i+1} + 1 \leqslant c_{i+1} + 2^{i+1}\lambda a_{i+1}$. Puisque $n_{i+1} \leqslant c_{i+1}$ par hypothèse de récurrence, il suffit donc de montrer $\delta_{i+1} + 1 \leqslant 2^{i+1}\lambda a_{i+1}$. Pour cela, considérons $\mathfrak{q} \supset J_{n_{i+1}+\delta_{i+1}}$ un premier associé minimal tel que $\mathfrak{q} \subset \mathfrak{p}$ et $\mathrm{ht}(\mathfrak{q}) = i+1$. Alors, par le lemme 4.15, on a $\delta_{i+1} + 1 \leqslant \ell$, où ℓ est la longueur de la composante $\mathfrak{q}$-primaire de $\mathfrak{A}_{i+1}$. Il suffit donc de montrer $\ell \leqslant 2^{i+1}\lambda a_{i+1}$. Raisonnons par l'absurde et supposons $\ell > 2^{i+1}\lambda a_{i+1}$. Alors, puisque $\ell d(\mathfrak{q}) \leqslant d(\mathfrak{A}_{i+1})$ (voir le paragraphe 3.3) et en utilisant l'inégalité (iii) déjà prouvée, on obtient :

$$\lambda d(\mathfrak{q}) \leqslant \frac{\lambda}{\ell} d(\mathfrak{A}_{i+1}) \leqslant \frac{\lambda a_{i+1} L^{i+1}}{2^{i+1}\lambda a_{i+1}} = \Big(\frac{L}{2}\Big)^{i+1}.$$

En particulier, puisque λ est grand, on a $L \geqslant 2$ et la majoration ci-dessus donne $\lambda d(\mathfrak{q}) \leqslant (L-1)^{i+1}$. De la même façon, on trouve

$$\lambda h(\mathfrak{q}) \leqslant \frac{\lambda}{\ell} h(\mathfrak{A}_{i+1}) \leqslant \frac{ML^i}{2^{i+1}} \leqslant M\Big(\frac{L}{2}\Big)^i \leqslant (\deg_Z E + 1)(L-1)^i.$$

Utilisant alors le lemme 4.12, on en déduit qu'il existe un polynôme $P \in \mathfrak{q} \cap \mathbb{C}[Z, X]$, homogène en X, et tel que $\deg_X P = L - 1$, $\deg_Z P \leqslant \deg_Z E$. Or, ceci contredit la minimalité de la quantité (27). La contradiction obtenue achève de démontrer (v) et par suite le lemme, en faisant $i = h$. □

La preuve de la proposition 4.11 est maintenant immédiate :

Démonstration de la proposition 4.11. — Le lemme 4.17 et le corollaire 4.13 donnent

$$\deg_X \mathcal{D}^N E \leqslant \deg_X E + Nd \leqslant L + \lambda^{2^{m+1}-1} \leqslant \lambda^{2^{m+1}} d(\mathfrak{p})^{1/(m-r+1)}$$

et

$$\begin{aligned} h(\mathcal{D}^N E) \leqslant \deg_Z \mathcal{D}^N E \leqslant \deg_Z E + Nd' &\leqslant \deg_Z E + \lambda^{2^{m+1}-1} \\ &\leqslant \lambda^{2^{m+1}}\big(h(\mathfrak{p})d(\mathfrak{p})^{-(m-r)/(m-r+1)} + 1\big). \quad \square \end{aligned}$$

4.4. Deuxième étape : construction du polynôme F. — On reprend les notations et hypothèses du théorème 4.8. Le but de cette partie est de démontrer la proposition suivante :

Proposition 4.18. — *Il existe un nombre réel $\lambda \geqslant 1$ (dépendant de m, D et de $f_1, \dots, f_m$) vérifiant la propriété suivante. Soient $\mathfrak{p} \subset K[X_0, \dots, X_m]$ un idéal homogène premier non nul de hauteur $\leqslant m$, $V = \mathscr{Z}(\mathfrak{p})$, et $r = \dim V + 1$. Supposons que l'on ait*

$$\log \operatorname{Dist}(x, V) \leqslant -4\lambda^{2^{m+1}}\big(h(V)d(V)^{1/(m+1-r)} + d(V)\big). \tag{32}$$

Alors il existe un polynôme $F \in \mathbb{C}[Z, X_0, \dots, X_m]$, homogène en X, tel que $F \notin \mathfrak{p}$, et vérifiant

(i) $\deg_X F \leqslant 2\lambda^{2^{m+1}} d(V)^{1/(m+1-r)}$,
(ii) $h(F) \leqslant \deg_Z F \leqslant 2\lambda^{2^{m+1}}\big(h(V)d(V)^{-(m-r)/(m+1-r)} + 1\big)$,
(iii) $\operatorname{Dist}(x, \mathsf{Z}(F)) \leqslant d(x, V)$.

Pour démontrer la proposition 4.18, nous allons utiliser la proposition 4.11, et devrons donc vérifier que l'hypothèse (H) de cette proposition est satisfaite. Pour ce faire, nous aurons besoin de la remarque suivante, qui relie l'hypothèse (H) à une hypothèse concernant les idéaux premiers $\mathcal{D}$-stables de $K[X]$, ce qui nous permettra d'utiliser la propriété $\mathscr{D}'$.

Lemme 4.19. — *Soit $\mathfrak{p} \subset K[X]$ un idéal premier homogène non nul. Alors les deux conditions suivantes sont équivalentes :*

(i) *Il existe un polynôme homogène non nul $E \in \mathfrak{p}$ tel que $(\mathcal{D}^n E)_{n \geqslant 0} \subset \mathfrak{p}$.*
(ii) *Il existe un idéal premier homogène non nul $\mathfrak{q} \subset \mathfrak{p}$ tel que $\mathcal{D}\mathfrak{q} \subset \mathfrak{q}$.*

Démonstration. — L'implication $(ii) \Rightarrow (i)$ est claire. Car si $\mathfrak{q} \subset \mathfrak{p}$ est un idéal premier homogène non nul $\mathcal{D}$-stable, alors on a, pour tout polynôme $E \in \mathfrak{q}$ homogène et non nul, $(\mathcal{D}^n E)_{n \geqslant 0} \subset \mathfrak{p}$. Prouvons donc $(i) \Rightarrow (ii)$. Soit $E \in \mathfrak{p}$ un polynôme homogène non nul tel que $(\mathcal{D}^n E)_{n \geqslant 0} \subset \mathfrak{p}$. Notons $\mathcal{A} = (\mathcal{D}^n E)_{n \geqslant 0}$, et soit $\mathfrak{q}$ un idéal premier associé minimal de $\mathcal{A}$ tel que $\mathfrak{q} \subset \mathfrak{p}$ (alors $\mathfrak{q}$ est homogène). On va montrer $\mathcal{D}\mathfrak{q} \subset \mathfrak{q}$. Soit donc $a \in \mathfrak{q}$. Soit encore $\mathcal{A} = Q_1 \cap \cdots \cap Q_s$ une décomposition primaire réduite de $\mathcal{A}$ telle que $\sqrt{Q_1} = \mathfrak{q}$. Comme $\cap_{i \neq 1} \sqrt{Q_i} \not\subset \mathfrak{q}$ par minimalité de $\mathfrak{q}$, on a $\cap_{i \neq 1} Q_i \not\subset \mathfrak{q}$, et par suite il existe $b \notin \mathfrak{q}$ tel que $b \in Q_i$ pour tout $i \neq 1$. Soit alors $e \geqslant 1$ tel que $\mathfrak{q}^e \subset Q_1$. On a $a^e b \in \mathcal{A}$, donc $\mathcal{D}^e(a^e b) \in \mathcal{D}^e \mathcal{A} \subset \mathcal{A} \subset \mathfrak{q}$. Maintenant, la formule de Leibniz montre que $\mathcal{D}^e(a^e b) = e!(\mathcal{D}a)^e b + ab'$, où $b' \in K[X]$. On en déduit $(\mathcal{D}a)^e b \in \mathfrak{q}$, d'où $\mathcal{D}a \in \mathfrak{q}$ car $b \notin \mathfrak{q}$. Ainsi, $\mathcal{D}\mathfrak{q} \subset \mathfrak{q}$, ce qui achève de démontrer $(i) \Rightarrow (ii)$. □

Le lemme suivant, joint au lemme précédent, montre que l'hypothèse (H) de la proposition 4.11 est vérifiée dès que la distance $\log \operatorname{Dist}(x, \mathsf{Z}(\mathfrak{p}))$ est petite.

Lemme 4.20. — *Soit $\mathfrak{p}$ un idéal homogène premier non nul de $K[X]$ vérifiant* $\operatorname{ht}(\mathfrak{p}) \leqslant m$ *et* $\log \operatorname{Dist}(x, \mathsf{Z}(\mathfrak{p})) < -c' d(\mathfrak{p})$*, où c' est le réel de la propriété $\mathscr{D}'$. Alors $X_0 \notin \mathfrak{p}$, et $\mathfrak{p}$ ne contient pas d'idéal homogène premier non nul $\mathcal{D}$-stable.*

Démonstration. — Pour tout polynôme homogène $E \in \mathfrak{p}$ on a, d'après les propositions 3.24 et 3.25 et en notant $V = \mathscr{Z}(\mathfrak{p})$,

$$d(V) \log \operatorname{Dist}(x, \mathsf{Z}(E)) \leqslant d(V) \log d(x, V) \leqslant \log \operatorname{Dist}(x, V) < -c' d(V). \tag{33}$$

On a donc $X_0 \notin \mathfrak{p}$, car sinon en prenant $E = X_0$ dans (33) on obtiendrait $0 = d(V) \log \operatorname{Dist}(x, \mathsf{Z}(X_0)) < 0$, ce qui est absurde. Pour prouver la seconde assertion du lemme, commençons par remarquer que l'infimum définissant $c'_{\mathfrak{p}}$ est ici un minimum : en effet, puisque $x = (1, f_1, \ldots, f_m)$ avec $f_1, \ldots, f_m$ analytiques au voisinage de zéro, on vérifie immédiatement que $-\log \operatorname{Dist}(x, \mathsf{Z}(E)) \in \mathbb{N} \cup \{+\infty\}$ pour tout polynôme homogène $E \in \mathfrak{p}$. Choisissant alors E tel que $c'_{\mathfrak{p}} = -\log \operatorname{Dist}(x, \mathsf{Z}(E))$, les inégalités (33) donnent $c' < c'_{\mathfrak{p}}$. Si donc $\mathfrak{q} \subset \mathfrak{p}$ est un idéal homogène premier non nul, on a $c' < c'_{\mathfrak{p}} \leqslant c'_{\mathfrak{q}}$, ce qui implique $\mathcal{D}\mathfrak{q} \not\subset \mathfrak{q}$ d'après la propriété $\mathscr{D}'$. Le lemme est démontré. □

Remarque 4.21. — C'est uniquement dans la preuve de ce lemme 4.20 qu'intervient la propriété $\mathscr{D}'$, le seul rôle de ce lemme étant à son tour de garantir, grâce au lemme 4.19, que l'hypothèse (H) de la proposition 4.11 est vérifiée. On voit donc qu'en fait la condition sur les idéaux stables dans la propriété $\mathscr{D}'$ n'est pas celle qui apparaît naturellement, la condition naturelle faisant plutôt intervenir les idéaux de la forme $\mathcal{A} = (\mathcal{D}^n E)_{n \geqslant 0}$ pour un certain polynôme homogène $E \in \mathbb{C}[Z, X_0, \ldots, X_m]$. Plus précisément, appelons *idéal $\mathcal{D}$-monogène* tout idéal de $\mathbb{C}[Z, X_0, \ldots, X_m]$ de cette forme. La condition naturelle que l'on obtient en voulant assurer l'hypothèse (H) (en utilisant la même méthode que dans la preuve du lemme 4.20) est alors que le couple $(\mathcal{D}, x)$ vérifie la propriété $\mathscr{D}''$ suivante : il existe un réel $c' > 0$ tel que, pour tout idéal homogène premier $\mathfrak{p}$ contenant un idéal $\mathcal{D}$-monogène non nul, on ait $c'_{\mathfrak{p}} \leqslant c'$. Le lemme 4.19 montre que le couple $(\mathcal{D}, x)$ vérifie $\mathscr{D}''$ si et seulement s'il vérifie $\mathscr{D}'$ (avec le même réel c').

Démonstration de la proposition 4.18. — On prend λ supérieur à la constante c' de la propriété $\mathscr{D}'$ et au réel λ de la proposition 4.11. Alors, d'après (32), les hypothèses du lemme 4.20 sont vérifiées, donc $X_0 \notin \mathfrak{p}$ et $\mathfrak{p}$ ne contient pas d'idéal premier homogène non nul $\mathcal{D}$-stable. Le lemme 4.19 montre alors que l'hypothèse (H) de la proposition 4.11 est satisfaite (en fait pour tout polynôme homogène non nul E). Soit alors $A = \mathcal{D}^N E$ le polynôme fourni par cette proposition, et notons $B = \mathcal{D}^{N-1}E$. Nous allons majorer $\log \mathrm{Dist}(x, \mathsf{Z}(A))$.

Tout d'abord, puisque $(f_1, \dots, f_m)$ est une solution du système (S), il résulte de la définition de $\mathcal{D}$ que pour tout polynôme $P \in \mathbb{C}[Z, X_0, \dots, X_m]$, on a

$$A_0(z, f_1(z), \dots, f_m(z)) \frac{d}{dz} P(z, 1, f_1(z), \dots, f_m(z)) = \mathcal{D}P(z, 1, f_1(z), \dots, f_m(z)).$$

On a donc en particulier

$$\begin{aligned} \mathrm{ord}_0(\mathcal{D}B(z, 1, f_1(z), \dots, f_m(z))) &\geqslant \mathrm{ord}_0 \frac{d}{dz} B(z, 1, f_1(z), \dots, f_m(z)) \\ &\geqslant \mathrm{ord}_0 B(z, 1, f_1(z), \dots, f_m(z)) - 1, \end{aligned}$$

i.e. $-\log |A(x)| \geqslant -\log |B(x)| - 1$. On en déduit, puisque $-\log |A| \leqslant \deg_Z A$,

$$\begin{aligned} \log \mathrm{Dist}(x, \mathsf{Z}(A)) &= \log |A(x)| - \log |A| \\ &\leqslant \log |B(x)| + \deg_Z A + 1 \\ &\leqslant \log |B(x)| - \log |B| + \deg_Z A + 1 \\ &\leqslant \log \mathrm{Dist}(x, \mathsf{Z}(B)) + \deg_Z A + 1. \end{aligned} \tag{34}$$

Maintenant, on remarque que

$$1 + \deg_Z A \leqslant -\frac{1}{2} \log \mathrm{Dist}(x, \mathsf{Z}(B)). \tag{35}$$

En effet, par les propositions 3.24 et 3.25, les estimations (28) et l'hypothèse (32), on a :

$$\begin{aligned} d(V)\big(1 + &\deg_Z A + \frac{1}{2} \log \mathrm{Dist}(x, \mathsf{Z}(B))\big) \\ &\leqslant d(V)(1 + \deg_Z A) + \frac{1}{2} d(V) \log d(x, V) \\ &\leqslant (1 + \lambda^{2^{m+1}}) d(V) + \lambda^{2^{m+1}} h(V) d(V)^{1/(m+1-r)} + \frac{1}{2} \log \mathrm{Dist}(x, V) \\ &\leqslant (1 - \lambda^{2^{m+1}}) d(V) - \lambda^{2^{m+1}} h(V) d(V)^{1/(m+1-r)} \leqslant 0. \end{aligned}$$

Les inégalités (34) et (35) donnent $\log \mathrm{Dist}(x, \mathsf{Z}(A)) \leqslant \frac{1}{2} \log \mathrm{Dist}(x, \mathsf{Z}(B))$, soit encore $\log \mathrm{Dist}(x, \mathsf{Z}(A^2)) \leqslant \log \mathrm{Dist}(x, \mathsf{Z}(B))$. En prenant $F = A^2 \notin \mathfrak{p}$, on obtient donc $\log \mathrm{Dist}(x, \mathsf{Z}(F)) \leqslant \log d(x, V)$, c'est-à-dire (iii). Les assertions (i) et (ii) résultent quant à elles immédiatement de (28). $\square$

4.5. Fin de la preuve du théorème 4.8. — Les préparatifs ayant été faits, on peut maintenant démontrer le théorème 4.8. Soit λ un réel comme dans la proposition 4.18 (ne dépendant donc que de m, D et de $f_1, \dots, f_m$), mais choisi suffisamment grand pour que les inégalités ci-dessous soient satisfaites. On pose $\tau = \lambda^{2^{m+2}}$. Nous allons démontrer le théorème 4.8 par récurrence sur r.

Pour $r = 0$ l'inégalité à démontrer est triviale, puisque alors $\log \mathrm{Dist}(x, \mathsf{Z}) = h(\mathsf{Z}) = d(\mathsf{Z}) = 0$. Soit donc $r \geqslant 1$ tel que $r \leqslant m$, et supposons que la minoration du théorème soit vraie pour tous les cycles de dimension $r-2$. Il s'agit de démontrer qu'elle est vraie pour tout cycle Z de dimension $r-1$. On voit facilement qu'il suffit de démontrer la minoration (25) lorsque $\mathsf{Z} = V$ est une variété. En effet, si l'inégalité (25) est vraie pour les variétés, alors on a, pour un cycle $\mathsf{Z} = \sum_{1\leqslant i\leqslant s} \ell_i [V_i]$ de dimension $r-1$:

$$\begin{aligned}
-\log \mathrm{Dist}(x, \mathsf{Z}) &= -\sum_{1\leqslant i\leqslant s} \ell_i \log \mathrm{Dist}(x, V_i) \\
&\leqslant \tau^{mr} \sum_{1\leqslant i\leqslant s} \ell_i h(V_i) d(V_i)^{r/(m+1-r)} + \tau^{mr} \sum_{1\leqslant i\leqslant s} \ell_i d(V_i)^{m/(m+1-r)} \\
&\leqslant \tau^{mr} d(\mathsf{Z})^{r/(m+1-r)} \Big(\sum_{1\leqslant i\leqslant s} \ell_i h(V_i) \Big) + \tau^{mr} \Big(\sum_{1\leqslant i\leqslant s} \ell_i d(V_i) \Big)^{m/(m+1-r)} \\
&\leqslant \tau^{mr} h(\mathsf{Z}) d(\mathsf{Z})^{r/(m+1-r)} + \tau^{mr} d(\mathsf{Z})^{m/(m+1-r)}.
\end{aligned}$$

Soit donc $V = \mathscr{Z}(\mathfrak{p})$ une variété. Raisonnons par l'absurde et supposons que l'inégalité (25) soit fausse, *i.e.*

$$\log \mathrm{Dist}(x, V) < -\tau^{mr} \big(h(V) d(V)^{r/(m+1-r)} + d(V)^{m/(m+1-r)} \big). \tag{36}$$

Alors l'inégalité (32) est en particulier satisfaite, et l'on peut appliquer la proposition 4.18, qui nous fournit un certain polynôme homogène $F \in \mathbb{C}[Z, X_0, \dots, X_m]$. Les théorèmes de Bézout géométrique et arithmétique (théorème 3.26 (i) et (ii)) donnent alors, en notant $J = (\mathfrak{p}, F)$ et en tenant compte des estimations de $h(F)$ et $\deg_X F$ données par la proposition 4.18 :

$$d(\mathsf{Z}(J)) \leqslant 2\lambda^{2^{m+1}} d(V)^{(m+2-r)/(m+1-r)}$$

et

$$h(\mathsf{Z}(J)) \leqslant 2\lambda^{2^{m+1}} (2h(V) d(V)^{\frac{1}{(m+1-r)}} + d(V)).$$

On déduit de ces majorations et de l'hypothèse de récurrence :

$$\begin{aligned}
-\log \mathrm{Dist}(x, \mathsf{Z}(J)) &\leqslant \tau^{m(r-1)} \big(h(\mathsf{Z}(J)) d(\mathsf{Z}(J))^{(r-1)/(m+2-r)} + d(\mathsf{Z}(J))^{m/(m+2-r)} \big) \\
&\leqslant 2\tau^{m(r-1)} \big(2\lambda^{2^{m+1}} \big)^{(m+1)/(m+2-r)} \Big(h(V) d(V)^{r/(m+1-r)} + d(V)^{m/(m+1-r)} \Big) \\
&\leqslant 2\tau^{m(r-1)} \big(2\lambda^{2^{m+1}} \big)^{m} \Big(h(V) d(V)^{r/(m+1-r)} + d(V)^{m/(m+1-r)} \Big).
\end{aligned} \tag{37}$$

Mais par ailleurs, le théorème de Bézout métrique 3.26 (iii) donne, compte tenu de l'hypothèse (36) (noter que le théorème 3.26 (iii) s'applique ici avec $\rho = \mathrm{Dist}(x, V)$

grâce à l'inégalité (iii) de la proposition 4.18) :

$$\begin{aligned}\log \operatorname{Dist}(x, \mathsf{Z}(J)) &\leqslant \log \operatorname{Dist}(x, V) + h(F)d(V) + h(V)\deg_X F \\ &\leqslant (4\lambda^{2^{m+1}} - \tau^{mr})\big(h(V)d(V)^{r/(m+1-r)} + d(V)^{m/(m+1-r)}\big).\end{aligned}$$

Cette dernière inégalité étant contradictoire avec l'inégalité (37) (puisque l'on a $2\tau^{m(r-1)}\big(2\lambda^{2^{m+1}}\big)^m = 2^{m+1}\tau^{mr-m/2} < \tau^{mr} - 4\sqrt{\tau} = \tau^{mr} - 4\lambda^{2^{m+1}}$ par choix de τ), on voit que l'hypothèse (36) était donc fausse. Ainsi, on a bien la minoration (25) pour les cycles de dimension $r-1$, ce qui achève de démontrer le théorème par récurrence. $\square$

4.6. Propriété $\mathscr{D}$ pour les fonctions de Ramanujan. — On a vu au § 1 que les fonctions de Ramanujan P, Q, R sont solutions du système différentiel (S_0), l'opérateur différentiel D associé à ce système étant défini par (12) (§ 2.5). Afin de pouvoir appliquer le théorème 4.1 au triplet $f = (P, Q, R)$ et à l'opérateur D, il nous faut vérifier que le couple (D, f) vérifie la propriété $\mathscr{D}$. Ceci résulte du théorème suivant [**Nes96**][9] :

Théorème 4.22. — *Soit $D : \mathbb{C}[Z, X_1, X_2, X_3] \to \mathbb{C}[Z, X_1, X_2, X_3]$ l'opérateur différentiel défini par*

$$D = Z\frac{\partial}{\partial Z} + \frac{1}{12}(X_1^2 - X_2)\frac{\partial}{\partial X_1} + \frac{1}{3}(X_1X_2 - X_3)\frac{\partial}{\partial X_2} + \frac{1}{2}(X_1X_3 - X_2^2)\frac{\partial}{\partial X_3}. \tag{38}$$

Soit encore $f = (f_1, f_2, f_3)$ un triplet de fonctions analytiques au voisinage de zéro, algébriquement indépendantes sur $\mathbb{C}(z)$, et telles que $f_1(0) = f_2(0) = f_3(0) = 1$. Alors le couple (D, f) vérifie la propriété $\mathscr{D}$.

Corollaire 4.23. — *Soit $D : \mathbb{C}[Z, X_1, X_2, X_3] \to \mathbb{C}[Z, X_1, X_2, X_3]$ l'opérateur différentiel défini par (38), et soit $f = (P, Q, R)$. Alors le couple (D, f) vérifie la propriété $\mathscr{D}$.*

Démonstration. — Les fonctions de Ramanujan sont algébriquement indépendantes sur $\mathbb{C}(z)$ d'après [**Mah69**], analytiques au voisinage de zéro, et vérifient de plus $P(0) = Q(0) = R(0) = 1$ (voir formules (1), (2) et (3) page 121). $\square$

Ce corollaire, joint au théorème 4.1, donne alors immédiatement le lemme de multiplicité utilisé au paragraphe 2.5 (théorème 2.9) :

Corollaire 4.24. — *Soient L_1, L_2 des entiers $\geqslant 1$. Alors, pour tout polynôme $E \in \mathbb{C}[Z, X_1, X_2, X_3]$, $E \neq 0$, tel que $\deg_Z E \leqslant L_1$ et $\deg_{X_i} E \leqslant L_2$ ($i = 1, 2, 3$), on a :*

$$\operatorname{ord}_0 E(z, P(z), Q(z), R(z)) \leqslant cL_1L_2^3,$$

où $c > 0$ est une constante absolue.

[9] Pellarin [**Pel05**] a tout récemment obtenu une autre démonstration de ce résultat. Voir à ce sujet la remarque 4.30.

Pour démontrer le théorème 4.22, Nesterenko démontre en fait le résultat plus fort suivant :

Théorème 4.25. — *Soit $D : \mathbb{C}[Z, X_1, X_2, X_3] \to \mathbb{C}[Z, X_1, X_2, X_3]$ l'opérateur différentiel défini par (38), et soit $\Delta = X_2^3 - X_3^2$. Alors on a*

$$\Delta \in \bigcap_{\substack{\mathfrak{p} \neq 0, D\mathfrak{p} \subset \mathfrak{p} \\ \mathfrak{p} \cap \mathbb{C}[Z] = (0) \\ (0,1,1,1) \in \mathscr{Z}(\mathfrak{p})}} \mathfrak{p}.$$

Il est clair que le théorème 4.25 entraîne le théorème 4.22 grâce à la remarque 4.5. La fin de ce paragraphe est consacrée à sa démonstration. La preuve utilise trois lemmes, dont nous ne donnerons que l'esquisse de la démonstration pour les deux premiers, renvoyant à l'article [**Nes96**] ou au chapitre 10 de [**NP01**] pour davantage de détails. On conserve les notations du théorème 4.25.

Lemme 4.26. — *Il n'y a que deux idéaux premiers principaux non nuls de l'anneau $\mathbb{C}[Z, X_1, X_2, X_3]$ stables par D, à savoir $\mathfrak{p}_1 = (Z)$ et $\mathfrak{p}_2 = (\Delta)$.*

Démonstration (esquisse). — Soit $\mathfrak{p} = (A)$ un idéal premier principal non nul stable par D. En comparant les poids[(10)] des polynômes A et DA, puis le degré partiel par rapport à Z, on montre tout d'abord que l'on a $DA = (aX_1 + b)A$, avec $a, b \in \mathbb{C}$. En utilisant la propriété $\frac{\mathrm{d}}{\mathrm{d}z}(A(z, P(z), Q(z), R(z))) = DA(z, P(z), Q(z), R(z))$, on montre ensuite que $b \in \mathbb{N}$, $a \in \mathbb{Z}$. On constate alors, en posant $S = A\Delta^{-a}Z^{-b}$ (et en étendant la dérivation D en une dérivation $D : \mathbb{C}(Z, X_1, X_2, X_3) \to \mathbb{C}(Z, X_1, X_2, X_3)$), que l'on a $DS = 0$, donc la fonction $S(z, P(z), Q(z), R(z))$ est constante. Comme les fonctions z, $P(z)$, $Q(z)$ et $R(z)$ sont algébriquement indépendantes sur $\mathbb{C}$ d'après [**Mah69**], on en déduit que S est constant, d'où $A = c\Delta^a Z^b$ avec $c \in \mathbb{C}^*$, $a, b \in \mathbb{N}$. Le fait que A soit irréductible implique enfin $A = c\Delta$ ou $A = cZ$. Voir [**Nes96**, Lemma 4.1] ou [**NP01**, chap. 10, Lemma 5.2] pour les détails. □

Pour pouvoir énoncer le lemme qui suit, nous aurons besoin de la notion de *fonction algébrique au voisinage d'un point* $\xi \in \mathbb{C}$ que nous définissons maintenant. Soit $\xi \in \mathbb{C}$ un nombre complexe. D'après un théorème de Puiseux ([**Eis95**, cor. 13.15], [**Iwa93**, th. 2.5 et th. 2.6], ou [**Eic66**, chap. III, § 1.6]), le corps des séries (formelles) de Puiseux $\Omega = \bigcup_{e \geqslant 1} \mathbb{C}\big(\big((X - \xi)^{1/e}\big)\big)$ est une extension algébriquement close de $\mathbb{C}(X - \xi) = \mathbb{C}(X)$, et tout polynôme non constant $F(Y) \in \mathbb{C}(X)[Y]$ se décompose en facteurs linéaires dans Ω. On appellera *fonction algébrique au voisinage de* ξ toute racine dans Ω d'un polynôme non constant $F(Y)$ à coefficients dans $\mathbb{C}(X)$. Autrement dit,

(10) Le poids d'un monôme $\lambda Z^{\alpha_0} X_1^{\alpha_1} X_2^{\alpha_2} X_3^{\alpha_3}$ $(\lambda \neq 0)$ est ici défini comme étant $\alpha_1 + 2\alpha_2 + 3\alpha_3$, et le poids d'un polynôme quelconque F est le maximum des poids des monômes apparaissant dans F.

une fonction algébrique au voisinage de ξ est une série formelle

$$f = f(X) = \sum_{n \geqslant n_0} a_n (X-\xi)^{n/e} \tag{39}$$

avec $e \in \mathbb{N}^*$, $n_0 \in \mathbb{Z}$, $a_n \in \mathbb{C}$, telle que l'on ait identiquement $A(X, f(X)) = 0$ pour un certain polynôme non nul A de $\mathbb{C}[X,Y]$. On démontre [**Eic66**, chap. III, § 1.6], mais nous n'en aurons pas besoin ici, que le rayon de convergence de la série $\sum_{n \geqslant 0} a_n t^n$ est alors non nul. Dans la suite, si l'on peut prendre $n_0 \geqslant 0$ dans (39), on dira que la fonction algébrique est *entière*[11], et on notera dans ce cas $f(\xi) := a_0$. Enfin, si f est une fonction algébrique donnée par (39), on définit f' de façon naturelle par $f' = \sum_{n \geqslant n_0} \frac{n}{e} a_n (X-\xi)^{(n-e)/e}$.

On peut alors énoncer :

Lemme 4.27. — *Le système d'équations différentielles*

$$(\Sigma) \qquad \begin{cases} (x^2-f)f' = 4(xf-g) \\ (x^2-f)g' = 6(xg-f^2) \end{cases}$$

a une unique solution avec f, g fonctions algébriques entières au voisinage de 1 *telles que $f(1) = g(1) = 1$, à savoir $f = X^2$ et $g = X^3$.*

Démonstration [**Nes96**, Lemma 4.3] *ou* [**NP01**, chap. 10, Lemma 5.3]

Supposons qu'il existe $f, g \in \mathbb{C}[[(X-1)^{1/e}]]$ vérifiant (Σ) et telles que $f(1) = g(1) = 1$, $f \neq X^2$. En posant[12] $u = X^2 - f = (X-1)^2 + 2(X-1) + 1 - f$ et $v = X^3 - g = (X-1)^3 + 3(X-1)^2 + 3(X-1) + 1 - g$, on obtient des fonctions algébriques entières $u, v \in \mathbb{C}[[(X-1)^{1/e}]]$ telles que $u(1) = v(1) = 0$, $u \neq 0$, et vérifiant le système

$$(\Sigma') \qquad \begin{cases} uu' = 6Xu - 4v \\ 2v' = 12u - 3Xu'. \end{cases}$$

On vérifie alors que $v \neq 0$ ($v = 0$ impliquerait $u' = 6X$ d'après la première équation, d'où $u = 3X^2/2$ d'après la seconde, ce qui est contradictoire), et l'on peut écrire

$$u = \sum_{n \geqslant \lambda} a_n (X-1)^{n/e}, \qquad v = \sum_{n \geqslant \mu} b_n (X-1)^{n/e}, \tag{40}$$

où $\lambda \geqslant 1$, $\mu \geqslant 1$, $a_\lambda \neq 0$, $b_\mu \neq 0$, et où $e \geqslant 1$ est choisi minimal. On remplace ensuite dans (Σ') u et v par leurs expressions (40). En comparant les termes de plus petit exposant, on trouve alors $\lambda = \mu = e$, $a_e = 12$, $b_e = -18$.

[11] On démontre que les éléments de Ω ayant un développement de Puiseux (39) avec $n_0 \geqslant 0$ sont exactement les éléments entiers sur $\mathbb{C}[[X-\xi]]$ ([**Eic66**, chap. III, §§ 1.4 et 1.5] ou [**Eis95**, cor. 13.15]). Le mot *entier* est donc à prendre dans son sens algébrique, et non analytique (une série (39) avec $n_0 \geqslant 0$ ne définit pas une fonction entière au sens de l'analyse complexe en général).

[12] Nesterenko choisit $u = X^2 - f$ et $v = Xf - g$. Le choix adopté ici nous semble plus naturel.

La seconde étape consiste à montrer que $e = 1$. On suppose donc $e \geqslant 2$. On voit facilement qu'il existe alors un plus petit entier $r \geqslant e$ tel que $a_r \neq 0$ et $e \nmid r$ (par minimalité de e). La comparaison des coefficients de $(X-1)^{r/e}$ (resp. de $(X-1)^{\frac{r}{e}-1}$) dans chaque membre de la première (resp. seconde) équation du système (Σ') donne alors $ra_r = 0$, ce qui est contradictoire. Ainsi, on a $e = 1$, c'est-à-dire $u, v \in \mathbb{C}[[X-1]]$.[13]

L'étape suivante de la démonstration consiste à démontrer qu'il existe un seul couple de séries formelles $(u, v) \in \mathbb{C}[[X-1]] \times \mathbb{C}[[X-1]]$ vérifiant (Σ') et satisfaisant aux conditions $u(1) = v(1) = 0$, $u'(1) = 12$, $v'(1) = -18$. Ceci s'obtient facilement en montrant par récurrence, à l'aide des équations du système (Σ'), que $u^{(k)}(1)$ et $v^{(k)}(1)$ sont déterminés de façon unique à partir de $u(1), \ldots, u^{(k-1)}(1)$ pour tout $k \geqslant 2$ (on dérive k fois la première équation de (Σ'), $(k-1)$ fois la seconde, et on évalue en 1).

Pour terminer la démonstration, on remarque que la fonction de Ramanujan P est inversible au voisinage de zéro puisque $P'(0) = -24 \neq 0$ (voir formule (1) page 1), et définit ainsi une fonction P^{-1} analytique au voisinage de 1. En posant alors $F(z) = Q(P^{-1}(z))$ et $G(z) = R(P^{-1}(z))$, et en tenant compte du fait que les fonctions P, Q, R satisfont le système (S_0), on vérifie que F, G sont solutions du système (Σ) et que de plus $F(1) = G(1) = 1$. Les fonctions $U(z) = z^2 - F(z)$ et $V(z) = z^3 - G(z)$ vérifient alors (Σ'), ainsi que $U(1) = V(1) = 0$, $U'(1) = 12$ et $V'(1) = -18$, comme on le calcule aisément à partir des formules (1), (2) et (3). Maintenant, les fonctions U et V étant analytiques au voisinage de 1, elles admettent chacune un développement en série entière, et ces développements en série coïncident avec ceux de u et v d'après l'unicité démontrée à l'étape précédente. Ainsi, les fonctions U et V, et donc F et G, sont des fonctions algébriques. La fonction F vérifie donc identiquement au voisinage de 1 une relation $A(z, F(z)) = 0$, où $A \in \mathbb{C}[X, Y]$ est un polynôme non nul. Ceci entraîne $A(P(z), Q(z)) = 0$ dans un voisinage de zéro, mais ceci est impossible puisque les fonctions P et Q sont algébriquement indépendantes sur $\mathbb{C}$ [**Mah69**]. La contradiction obtenue achève de démontrer le lemme. $\square$

Avant d'énoncer le lemme 4.28, rappelons le résultat classique suivant de la théorie des fonctions algébriques [**Eic66**, chap. III, § 1.5] : si $F \in \mathbb{C}[X_1, X_2]$ est un polynôme irréductible et a, b deux nombres complexes tels que $F(a, b) = 0$, alors il existe au moins une fonction algébrique au voisinage de a, soit $y = y(X)$, entière, vérifiant $y(a) = b$, et telle que l'on ait identiquement $F(X, y(X)) = 0$. Le lemme dont nous aurons besoin est un analogue de ce théorème mais en trois variables. Il résulte en fait de la théorie des courbes algébriques, mais on en donnera ci-après une preuve « élémentaire » n'y faisant pas appel, utilisant le résultat en deux variables ci-dessus, et qui m'a été fournie par D. Masser.

[13] Les fonctions algébriques u et v sont donc en fait des fonctions analytiques au voisinage de 1, puisque le rayon de convergence des séries est non nul d'après une remarque précédente.

Lemme 4.28. — *Soit* $\mathfrak{q} \subset \mathbb{C}[X_1, X_2, X_3]$ *un idéal premier de hauteur* 2 *tel que* $\mathfrak{q} \cap \mathbb{C}[X_1] = (0)$ *et tel que* $(1,1,1)$ *soit un zéro de l'idéal* $\mathfrak{q}$. *Alors il existe des fonctions algébriques au voisinage de* 1, *soit* $y = y(X)$ *et* $z = z(X)$, *entières, vérifiant* $y(1) = z(1) = 1$, *et telles que l'on ait identiquement* $F(X, y(X), z(X)) = 0$ *pour tout polynôme* $F \in \mathfrak{q}$.

Démonstration. — Par translation on se ramène immédiatement au voisinage de zéro. Autrement dit, on supposera dans ce qui suit que $(0,0,0)$ est un zéro de $\mathfrak{q}$. Il s'agit alors de prouver qu'il existe des séries de Puiseux $y, z \in \mathbb{C}[[X^{1/e}]]$ (pour un certain entier $e \geqslant 1$), vérifiant $y(0) = z(0) = 0$ et $F(X, y(X), z(X)) = 0$ pour tout polynôme $F \in \mathfrak{q}$. Notons x_1, x_2 et x_3 les images de X_1, X_2 et X_3 par la surjection canonique $\mathbb{C}[X_1, X_2, X_3] \to \mathbb{C}[X_1, X_2, X_3]/\mathfrak{q}$. Puisque l'anneau $\mathbb{C}[x_1, x_2, x_3] = \mathbb{C}[X_1, X_2, X_3]/\mathfrak{q}$ est de dimension 1, son corps des fractions est de degré de transcendance 1 sur $\mathbb{C}$. Comme en outre $\mathfrak{q} \cap \mathbb{C}[X_1] = (0)$, x_1 est transcendant sur $\mathbb{C}$ et x_2, x_3 sont algébriques sur $\mathbb{C}(x_1)$, donc $\mathbb{C}(x_1)[x_2, x_3]$ est une extension finie de $\mathbb{C}(x_1)$. Notons d le degré de cette extension. Notons encore $\Omega = \bigcup_{e \geqslant 1} \mathbb{C}\big(\big(X^{1/e}\big)\big)$, où X est une indéterminée : c'est une extension algébriquement close du corps $\mathbb{C}(X)$. Le $\mathbb{C}$-isomorphisme $\iota : \mathbb{C}(x_1) \to \mathbb{C}(X)$ envoyant x_1 sur X admet alors exactement d prolongements $\mathbb{C}(x_1)[x_2, x_3] \to \Omega$, que nous noterons $\varphi_1, \dots, \varphi_d$. Posons $y_j = \varphi_j(x_2)$ et $z_j = \varphi_j(x_3)$ $(1 \leqslant j \leqslant d)$. Pour tout $\lambda \in \mathbb{C}$, il existe un polynôme irréductible $P_\lambda(X, T) \in \mathbb{C}[X][T]$ tel que $P_\lambda(x_1, x_2 + \lambda x_3) = 0$. Alors $P_\lambda(X_1, X_2 + \lambda X_3) \in \mathfrak{q}$, et donc en particulier $P_\lambda(0,0) = 0$. De plus, les éléments $t_{j\lambda} = \varphi_j(x_2 + \lambda x_3) = y_j + \lambda z_j$ $(1 \leqslant j \leqslant d)$ sont les racines dans Ω de l'équation $P_\lambda(X, t) = 0$. D'après le résultat en deux variables rappelé ci-dessus, il existe au moins un indice $j = j_\lambda$ tel que la fonction algébrique $t_{j\lambda}$ soit entière avec $t_{j\lambda}(0) = 0$. Comme il n'y a qu'un nombre fini d'indices j, il existe, par le principe des tiroirs, $\lambda, \mu \in \mathbb{C}$ avec $\lambda \neq \mu$ tels que $j_\lambda = j_\mu$. Notons $j = j_\lambda = j_\mu$. Alors pour cet indice j les fonctions algébriques y_j et z_j sont entières et telles que $y_j(0) = z_j(0) = 0$. De plus, on a $F(X, y_j(X), z_j(X)) = \varphi_j(F(x_1, x_2, x_3)) = 0$ pour tout $F \in \mathfrak{q}$. $\square$

Remarque 4.29. — On peut aussi démontrer le lemme 4.28 différemment en considérant la courbe $\mathscr{C}$ correspondant à $\mathfrak{q}$: il suffit de paramétrer (*via* la normalisée $\widetilde{\mathscr{C}}$ de $\mathscr{C}$) une des branches de $\mathscr{C}$ au point $(1,1,1)$ à l'aide d'un paramètre local. Voir l'exemple page 134 de [**Sha77**], où le cas d'une courbe plane est traité.

Démonstration du théorème 4.25. — Rappelons tout d'abord le résultat suivant, que nous utiliserons à plusieurs reprises au cours de la preuve : si A est un anneau noethérien intègre et $\mathfrak{p}$ un idéal premier de l'anneau de polynômes $A[X_1, \dots, X_n]$, alors $\mathrm{ht}(\mathfrak{p}) \leqslant \mathrm{ht}(\mathfrak{p} \cap A) + n$ ([**Mat96**, § 15, th. 15.5]).

Soit maintenant $\mathfrak{p} \subset \mathbb{C}[Z, X_1, X_2, X_3]$ un idéal premier non nul stable par D, ayant $(0,1,1,1)$ comme zéro, et tel que $\mathfrak{p} \cap \mathbb{C}[Z] = (0)$. Notons $\mathfrak{q} = \mathfrak{p} \cap \mathbb{C}[X_1, X_2, X_3]$. Alors $\mathfrak{q}$ est premier, et la formule (38) montre que l'on a $D\mathfrak{q} \subset \mathfrak{q}$. On distingue alors quatre cas, selon la valeur de la hauteur (algébrique) de $\mathfrak{q}$.

Premier cas : $\mathrm{ht}(\mathfrak{q}) = 0$, *i.e.* $\mathfrak{q} = (0)$. Alors $\mathrm{ht}(\mathfrak{p}) \leqslant \mathrm{ht}(\mathfrak{q}) + 1 = 1$ d'après le rappel ci-dessus, donc $\mathfrak{p}$ est principal ([**Mat96**, th. 20.1]). Le lemme 4.26 donne alors $\mathfrak{p} = (Z)$ ou $\mathfrak{p} = (\Delta)$. Or, le cas $\mathfrak{p} = (Z)$ est exclu car $\mathfrak{p} \cap \mathbb{C}[Z] = (0)$, et le cas $\mathfrak{p} = (\Delta)$ l'est également puisque $\mathfrak{q} = (0)$. Le cas $\mathrm{ht}(\mathfrak{q}) = 0$ est donc impossible.

Deuxième cas : $\mathrm{ht}(\mathfrak{q}) = 1$. Alors $\mathfrak{q}$ est principal, engendré par un polynôme irréductible non nul A. L'idéal (A) de l'anneau $\mathbb{C}[Z, X_1, X_2, X_3]$ est alors principal, non nul et stable, d'où $(A) = (\Delta)$ par le lemme 4.26 (le cas $(A) = (Z)$ étant à nouveau exclu puisque $\mathfrak{p} \cap \mathbb{C}[Z] = (0)$). On a donc bien $\Delta \in \mathfrak{p}$.

Troisième cas : $\mathrm{ht}(\mathfrak{q}) = 3$. Dans ce cas, $\mathfrak{q}$ est un idéal maximal de $\mathbb{C}[X_1, X_2, X_3]$ donc il existe $a, b, c \in \mathbb{C}$ tels que $\mathfrak{q} = (X_1 - a, X_2 - b, X_3 - c)$. Mais $(1,1,1)$ est un zéro de $\mathfrak{q}$, donc $1 - a = 1 - b = 1 - c = 0$, $\mathfrak{q} = (X_1 - 1, X_2 - 1, X_3 - 1)$, et par suite $X_2^3 - X_3^2 \equiv 1 - 1 \equiv 0 \pmod{\mathfrak{q}}$. On a ici encore $\Delta \in \mathfrak{p}$.

Dernier cas : $\mathrm{ht}(\mathfrak{q}) = 2$. Ce cas est un peu plus délicat que les précédents. La première étape consiste à remarquer que nécessairement $\mathfrak{q} \cap \mathbb{C}[X_1] = (0)$. En effet, supposons $\mathfrak{q} \cap \mathbb{C}[X_1] \neq (0)$. Alors $\mathfrak{q} \cap \mathbb{C}[X_1]$ est un idéal maximal de $\mathbb{C}[X_1]$, donc $\mathfrak{q} \cap \mathbb{C}[X_1] = (X_1 - c)$ pour un $c \in \mathbb{C}$. Comme précédemment, le fait que $(1,1,1)$ soit un zéro de $\mathfrak{q}$ implique $c = 1$, d'où $X_1 - 1 \in \mathfrak{q}$. Alors $D(X_1 - 1) \in \mathfrak{q}$, ce qui donne, avec (38), $\frac{1}{12}(X_1^2 - X_2) \equiv 0 \pmod{\mathfrak{q}}$. On en déduit $X_2 \equiv X_1^2 \equiv 1 \pmod{\mathfrak{q}}$, puis $D(X_2 - 1) = \frac{1}{3}(X_1X_2 - X_3) \equiv 0 \pmod{\mathfrak{q}}$, d'où $X_3 \equiv X_1X_2 \equiv 1 \pmod{\mathfrak{q}}$. On obtient ainsi $(X_1 - 1, X_2 - 1, X_3 - 1) \subset \mathfrak{q}$, ce qui est impossible puisque $\mathrm{ht}(\mathfrak{q}) = 2$.

On a donc $\mathfrak{q} \cap \mathbb{C}[X_1] = (0)$. Puisque $\mathrm{ht}(\mathfrak{q}) = 2$, on a aussi, en vertu du rappel préliminaire, $\mathfrak{q} \cap \mathbb{C}[X_1, X_2] \neq (0)$ et $\mathfrak{q} \cap \mathbb{C}[X_1, X_3] \neq (0)$. Soient alors $A \in \mathfrak{q} \cap \mathbb{C}[X_1, X_2]$ et $B \in \mathfrak{q} \cap \mathbb{C}[X_1, X_3]$, choisis irréductibles. Soient encore $y(X)$ et $z(X)$ les fonctions algébriques fournies par le lemme 4.28. On a donc identiquement $A(X, y(X)) = 0$, ainsi que $DA(X, y(X), z(X)) = 0$ puisque $DA \in \mathfrak{q}$. Ceci donne les relations :

$$\frac{\partial A}{\partial X_1}(X, y(X)) + y'(X)\frac{\partial A}{\partial X_2}(X, y(X)) = 0, \tag{41}$$

$$\tfrac{1}{12}(X^2 - y(X))\frac{\partial A}{\partial X_1}(X, y(X)) + \frac{1}{3}(Xy(X) - z(X))\frac{\partial A}{\partial X_2}(X, y(X)) = 0. \tag{42}$$

Comme $\frac{\partial A}{\partial X_2}(X, y(X)) \neq 0$ (car y est une racine, nécessairement simple, du polynôme irréductible $A(X, Y) \in \mathbb{C}(X)[Y]$), on tire de (41) et (42) l'équation $(X^2 - y(X))y'(X) = 4(Xy(X) - z(X))$. En raisonnant de façon analogue avec le polynôme B, on obtient l'équation $(X^2 - y(X))z'(X) = 6(Xz(X) - y^2(X))$. Appliquant maintenant le lemme 4.27, on en déduit $y(X) = X^2$ et $z(X) = X^3$. Ainsi, on a $A(X, X^2) = 0$ et $B(X, X^3) = 0$, et par suite $A = \lambda(X_2 - X_1^2)$ et $B = \mu(X_3 - X_1^3)$, où $\lambda, \mu \in \mathbb{C}^*$. On obtient donc $X_2 - X_1^2 \in \mathfrak{q}$ et $X_3 - X_1^3 \in \mathfrak{q}$, d'où l'on déduit finalement $\Delta = X_2^3 - X_3^2 \equiv (X_1^2)^3 - (X_1^3)^2 \equiv 0 \pmod{\mathfrak{q}}$. □

Remarque 4.30. — Alors que ce texte était quasiment achevé, Pellarin [**Pel05**] a obtenu une démonstration astucieuse beaucoup plus simple du théorème 4.25, et même un résultat un peu plus général : il montre en effet que tout idéal premier non nul

$\mathfrak{p} \subset \mathbb{C}[Z, X_1, X_2, X_3]$ tel que $\mathfrak{p} \cap \mathbb{C}[Z] = (0)$ et $D\mathfrak{p} \subset \mathfrak{p}$ contient le polynôme Δ (l'hypothèse $(0,1,1,1) \in \mathscr{Z}(\mathfrak{p})$ est donc supprimée). Le principe de sa méthode est le suivant. Comme dans la démonstration ci-dessus, dont on reprend les notations, on discute suivant la valeur de $\mathrm{ht}(\mathfrak{q})$. Si $\mathrm{ht}(\mathfrak{q}) = 0$ ou $\mathrm{ht}(\mathfrak{q}) = 1$, on procède comme précédemment (on utilise le lemme 4.26). La simplification concerne le cas $\mathrm{ht}(\mathfrak{q}) \geqslant 2$ et consiste à se ramener au cas d'un idéal *isobare*, qui se traite par des arguments algébriques élémentaires (on appelle idéal isobare un idéal de $\mathbb{C}[X_1, X_2, X_3]$ engendré par des polynômes isobares, les indéterminées X_1, X_2, X_3 ayant les poids 1, 2 et 3 respectivement). Plus précisément, notons $\widetilde{\mathfrak{q}} \subset \mathfrak{q}$ l'idéal de $\mathbb{C}[X_1, X_2, X_3]$ engendré par les polynômes isobares de $\mathfrak{q}$. L'idéal $\widetilde{\mathfrak{q}}$ est premier, stable par D, et de plus on montre facilement (argument à l'aide d'un résultant) que $\widetilde{\mathfrak{q}} \neq (0)$. On a alors les différents cas suivants. Si $\widetilde{\mathfrak{q}} \cap \mathbb{C}[X_2] \neq (0)$, alors $X_2 \in \widetilde{\mathfrak{q}}$, donc $DX_2 \in \widetilde{\mathfrak{q}}$, et par suite $\Delta = 3X_3\,DX_2 - 2X_2\,DX_3 \in \widetilde{\mathfrak{q}}$. Si $\widetilde{\mathfrak{q}} \cap \mathbb{C}[X_2] = (0)$ et $\widetilde{\mathfrak{q}} \cap \mathbb{C}[X_2, X_3] = (0)$, alors $\mathrm{ht}(\widetilde{\mathfrak{q}}) = 1$, et donc $\Delta \in \widetilde{\mathfrak{q}}$ par le lemme 4.26. Enfin, si $\widetilde{\mathfrak{q}} \cap \mathbb{C}[X_2] = (0)$ et $\widetilde{\mathfrak{q}} \cap \mathbb{C}[X_2, X_3] \neq (0)$, on commence par choisir $A \in \widetilde{\mathfrak{q}} \cap \mathbb{C}[X_2, X_3]$ non nul et isobare tel que $\deg_{X_3} A$ soit minimal. Un calcul simple montre alors que le crochet de Rankin $[A, X_2]$ (voir [**Pel05**]), qui est élément de $\widetilde{\mathfrak{q}}$, est égal à $\Delta\frac{\partial A}{\partial X_3}$. Puisque $\frac{\partial A}{\partial X_3} \notin \widetilde{\mathfrak{q}}$ par minimalité de $\deg_{X_3} A$, on obtient ici encore $\Delta \in \widetilde{\mathfrak{q}}$. Il est intéressant de noter que cette méthode peut être appliquée à d'autres systèmes différentiels (un exemple figure dans [**Pel04**]).

5. Autres preuves du théorème de Nesterenko et versions quantitatives

La preuve du théorème 1.1 présentée au § 2 a consisté à construire, au moyen d'outils et d'arguments classiques de transcendance (lemme de Siegel, extrapolation, lemme de multiplicité), une suite de polynômes qui vérifient les hypothèses d'un critère d'indépendance algébrique, à savoir le théorème 2.1. L'utilisation de ce critère d'indépendance algébrique pour conclure ne donne qu'un résultat qualitatif. Il est en fait possible de remplacer l'utilisation de ce critère par d'autres critères, plus généraux, qui fournissent une version quantitative du théorème 1.1. Il est également possible d'éviter le recours à un critère d'indépendance algébrique. L'objectif de ce dernier paragraphe est de présenter brièvement ces variantes(14) de la démonstration du théorème et de donner un aperçu du type de résultats qu'on peut établir. On ne cherchera pas ici à énoncer les résultats les plus précis possibles, renvoyant pour cela aux articles cités en bibliographie.

Nous commencerons au § 5.1 par démontrer une version quantitative du théorème 1.1 (théorème 5.1) en suivant la méthode de [**Nes96**]. Cette méthode est en fait très semblable (à quelques détails près) à celle utilisée dans la démonstration du critère

(14) Il y a aussi des variantes pour la partie transcendante : par exemple dans [**Phi97**], l'auteur utilise les déterminants d'interpolation au lieu d'un lemme de Siegel.

d'indépendance algébrique de [**Phi86**] (dont le théorème 2.1 est un corollaire), et peut être généralisée pour obtenir des critères d'indépendance algébrique fournissant directement un résultat quantitatif (« critères pour les mesures d'indépendance algébrique »). Nous donnerons un exemple simplifié d'un tel critère au § 5.2, et verrons comment il s'utilise. Enfin, au § 5.3, on expliquera comment on peut démontrer le théorème de Nesterenko par une approche différente due à Philippon, reposant sur des « propriétés d'approximation ».

Dans tout ce paragraphe, si A est un polynôme à coefficients dans $\mathbb{C}$, on note, comme au § 2.1, $H(A)$ le maximum des modules des coefficients de A. Pour tout réel t, on note de plus $\log^+ t = \log \max\{t, e\}$.

5.1. Version quantitative du théorème de Nesterenko d'après [Nes96]

Comme on l'a dit, nous allons expliquer ici comment on peut obtenir une version quantitative du théorème 1.1 sans utiliser le critère d'indépendance algébrique 2.1 pour conclure, en suivant la méthode utilisée dans [**Nes96**]. On va utiliser pour cela la théorie du paragraphe 3 dans le cas $K = \mathbb{Q}$. On ne donnera ici qu'une rapide esquisse de la preuve des résultats, renvoyant à [**Nes96**] ou à [**NP01**, Chap. 3] pour les détails.

Dans ce qui suit, on fixe $q \in \mathbb{C}$ tel que $q \neq 0$ et $|q| < 1$. On travaillera dans $\mathbb{P}_4$ et avec $K = \mathbb{Q}$. On pose $x = (1, q, P(q), Q(q), R(q)) \in \mathbb{P}_4(\mathbb{C})$. On notera encore $|\cdot|$ la valeur absolue usuelle de $\mathbb{C}$: avec les notations des §§ 3.4 et 3.5, on a donc $|\cdot| = |\cdot|_v$, où v est l'unique place archimédienne de $\mathbb{Q}$, et $\mathcal{K} = \mathcal{K}_v = \mathbb{C}$. Avec ce choix de valeur absolue, on peut définir (voir §§ 3.4 et 3.5) la norme $\|\alpha\|$ d'un élément $\alpha \in \mathbb{C}^5$, la valeur absolue $|\cdot|$ d'un polynôme multihomogène à coefficients dans $\mathbb{Q}$, ainsi qu'une fonction distance, notée $\mathrm{Dist}(\cdot,\cdot)$. Pour tout cycle Z sur $\mathbb{Q}$, on pose $t(\mathsf{Z}) = d(\mathsf{Z}) + h(\mathsf{Z})$. On a $t(\mathsf{Z}) \geqslant 1$ si $\mathsf{Z} \neq 0$ et $t(\mathsf{Z}) = 0$ si Z est le cycle nul.

Dans [**Nes96**], Nesterenko démontre le résultat quantitatif suivant qui, comme on va le voir dans un instant, contient le théorème 1.1 :

Théorème 5.1. — *Soit $q \in \mathbb{C}^*$ tel que $|q| < 1$. Pour tout r, $0 \leqslant r \leqslant 3$, il existe un réel $\mu_r > 0$ (dépendant de r et de q) vérifiant la condition suivante. Pour tout cycle Z sur $\mathbb{Q}$ de dimension $r-1$, on a*

$$\log \mathrm{Dist}(x, \mathsf{Z}) \geqslant -\mu_r t(\mathsf{Z})^{4/(4-r)} \big(\log^+ t(\mathsf{Z})\big)^{8r/(4-r)}, \tag{43}$$

où $x = (1, q, P(q), Q(q), R(q)) \in \mathbb{P}_4(\mathbb{C})$.

Remarque 5.2. — Cet énoncé peut être amélioré, notamment en ce qui concerne la dépendance en $\log^+ t(\mathsf{Z})$ ([**Phi98**], [**Nes97**]).

Le théorème 5.1 implique en particulier $\mathrm{Dist}(x, \mathsf{Z}) > 0$, puisque le membre de droite de l'inégalité (43) est fini. Ceci permet d'en déduire immédiatement le théorème 1.1 de la façon suivante. Désignons par $\mathfrak{p}$ l'idéal de $\mathbb{Q}[X_0, \ldots, X_4]$ engendré par les polynômes homogènes s'annulant en x, et notons $V = \mathscr{Z}(\mathfrak{p})$ et $r = \dim V + 1$. On a $x \in V$ donc

$\mathrm{Dist}(x, V) = 0$. Le théorème 5.1 implique alors $r \geqslant 4$, d'où l'on déduit immédiatement $\mathrm{degtr}_{\mathbb{Q}}\, \mathbb{Q}(q, P(q), Q(q), R(q)) = \dim V \geqslant 3$.

Esquisse de démonstration du théorème 5.1. — Nous allons déduire le théorème 5.1 de la construction de transcendance du § 2. Rappelons qu'on a démontré à la fin de ce paragraphe (voir la proposition 2.8 et la fin de la démonstration du théorème 1.1 page 131) que pour tout entier N suffisamment grand, il existe un polynôme non nul $B_N \in \mathbb{Z}[X_1, \ldots, X_4]$ vérifiant

$$\deg B_N \leqslant \gamma_0 N (\log N)^2, \qquad \log H(B_N) \leqslant \gamma_0 N (\log N)^2$$

et

$$-\gamma_2 N^4 \leqslant \log |B_N(q, P(q), Q(q), R(q))| \leqslant -\gamma_1 N^4, \tag{44}$$

où γ_0, γ_1 et γ_2 sont des constantes strictement positives ne dépendant que de q. Nous allons démontrer le théorème 5.1 par récurrence sur r en utilisant ce résultat, par une méthode analogue à celle utilisée pour démontrer le théorème 4.8 (§ 4.5).

Pour $r = 0$ l'énoncé est trivial (avec $\mu_0 = 1$ par exemple), car le seul cycle de dimension -1 est le cycle nul qui vérifie $\mathrm{Dist}(x, 0) = 1$. Soit maintenant r, $1 \leqslant r \leqslant 3$, et supposons que l'énoncé soit vrai pour $r - 1$. On désigne dans ce qui suit par $c_1, c_2, \ldots, c_6$ des « constantes », c'est-à-dire des réels > 0 ne dépendant que de q et r, effectivement calculables. Ces nombres réels étant déterminés, on fixe alors C_0 une autre constante, elle aussi effectivement calculable, et choisie suffisamment grande pour pouvoir satisfaire aux différentes inégalités qui interviendront. On va montrer que pour tout cycle Z de dimension $r - 1$, on a l'inégalité (43) avec la valeur $\mu_r = C_0^8$. Supposons que ce ne soit pas le cas. Alors il existe une variété V pour laquelle (43) est fausse (on vérifie en effet facilement, grâce à l'additivité des fonctions $t(\cdot)$ et $\log \mathrm{Dist}(x, \cdot)$, que si l'inégalité (43) est vraie lorsque Z est une variété, alors elle est vraie pour tous les cycles). Notons $\mathfrak{p} = \mathscr{I}(V) \subset \mathbb{Q}[X_0, \ldots, X_4]$ l'idéal premier correspondant à V. On pose

$$U = C_0^8 t(V)^{4/(4-r)} \big(\log^+ t(V)\big)^{8r/(4-r)} \tag{45}$$

et

$$N = \min\bigg\{ \big[U^{1/4}\big], \bigg[\Big(\frac{-\log d(x, V)}{2\gamma_2}\Big)^{1/4}\bigg] \bigg\}, \tag{46}$$

où $[\cdot]$ désigne la partie entière (et où γ_2 est la constante figurant dans (44)). Avec ces notations on a donc $\log \mathrm{Dist}(x, V) < -U$. On vérifie sans peine que $U \geqslant C_0^8$ puis, grâce à la seconde inégalité de la proposition 3.24, que $N \geqslant C_0$. Les paramètres U et N sont donc plus grands que toute constante arbitraire (fixée avant C_0). Posons $B = B_N$, et notons $F \in \mathbb{Q}[X_0, X_1, X_2, X_3, X_4]$ l'homogénéisé de B. Nous allons appliquer le théorème de Bézout métrique 3.26 (iii) à l'idéal $J = (\mathfrak{p}, F^m) \subset \mathbb{Q}[X_0, \ldots, X_4]$, où m est l'entier défini par $m = \big[\frac{8\gamma_2}{\gamma_1}\big] + 1$, et obtenir ainsi une majoration de $\log \mathrm{Dist}(x, \mathsf{Z}(J))$, contradictoire avec la minoration donnée par l'hypothèse de récurrence. Il nous faut tout d'abord vérifier que $F^m \notin \mathfrak{p}$, c'est-à-dire encore $F \notin \mathfrak{p}$. Pour cela, raisonnant par l'absurde, on vérifie à l'aide de la proposition 3.25 que l'hypothèse $F \in \mathfrak{p}$ entraîne

$$\begin{aligned}\log|B(q, P(q), Q(q), R(q))| &= \log \operatorname{Dist}(x, \mathsf{Z}(F)) + \log|F| + \|x\|(\deg F)\\ &\leqslant \log d(x, V) + c_1 \deg F + \log|F|\\ &\leqslant -2\gamma_2 N^4 + c_2 N(\log N)^2 < -\gamma_2 N^4\end{aligned}$$

puisque $N \geqslant C_0$ avec C_0 choisi suffisamment grand (on a aussi utilisé le fait que $\log|F| \leqslant \log H(F) + c_3 \deg F$, ce qui résulte des remarques 3.13 et 3.14). Cette inégalité contredisant la première inégalité de (44), on a bien $F \notin \mathfrak{p}$. Appliquons maintenant le théorème de Bézout métrique 3.26 (iii). On est amené à distinguer deux cas.

Premier cas : $d(x, V) < \operatorname{Dist}(x, \mathsf{Z}(F^m))$. Dans ce cas il est facile de voir que $N = \left[U^{1/4}\right]$. En effet, un calcul analogue à celui esquissé ci-dessus pour prouver $F \notin \mathfrak{p}$ montre que

$$\log \operatorname{Dist}(x, \mathsf{Z}(F)) \leqslant -\gamma_1 N^4 + c_4 N(\log N)^2 \leqslant -\gamma_1 N^4/2. \tag{47}$$

Si maintenant on avait $N = \left[\left(-\log d(x, V)/2\gamma_2\right)^{1/4}\right]$, alors on aurait

$$4\gamma_2 N^4 \geqslant -\log d(x, V) \geqslant -\log \operatorname{Dist}(x, \mathsf{Z}(F^m)) = -m \log \operatorname{Dist}(x, \mathsf{Z}(F)),$$

ce qui contredit (47) par choix de m. On a donc bien $N = \left[U^{1/4}\right]$ comme annoncé. On en déduit en particulier

$$\frac{1}{2} U^{1/4} \leqslant N \leqslant U^{1/4}. \tag{48}$$

Par ailleurs, on vérifie que

$$h(F^m) d(V) + h(V) \deg F^m + C_4 d(V) \deg F^m \leqslant c_5 t(V) N (\log N)^2, \tag{49}$$

C_4 étant le réel du théorème 3.26 (iii). Ce dernier théorème, ainsi que (47), (49), (48) et (45) donnent alors :

$$\begin{aligned}\log \operatorname{Dist}(x, \mathsf{Z}(J)) \leqslant -\frac{m\gamma_1}{32} C_0^8\, t(V)^{4/(4-r)} \left(\log^+ t(V)\right)^{8r/(4-r)}&\\ + C_0^3 t(V)^{1+1/(4-r)} \left(\log^+ t(V)\right)^{2+2r/(4-r)}&\\ < -C_0^7\, t(V)^{4/(4-r)} \left(\log^+ t(V)\right)^{8r/(4-r)}.&\end{aligned} \tag{50}$$

Pour voir que cette majoration contredit la minoration donnée par l'hypothèse de récurrence, on utilise les théorèmes de Bézout géométrique et arithmétique, qui donnent

$$t(\mathsf{Z}(J)) \leqslant c_6 t(V) N (\log N)^2 \leqslant C_0^3\, t(V)^{(5-r)/(4-r)} \left(\log^+ t(V)\right)^{8/(4-r)}.$$

Grâce à cette estimation, l'hypothèse de récurrence implique alors la minoration

$$\begin{aligned}\log \operatorname{Dist}(x, \mathsf{Z}(J)) &\geqslant -\mu_{r-1} t(\mathsf{Z}(J))^{4/(5-r)} \left(\log^+ t(\mathsf{Z}(J))\right)^{(8r-8)/(5-r)}\\ &\geqslant -C_0^7\, t(V)^{4/(4-r)} \left(\log^+ t(V)\right)^{8r/(4-r)}.\end{aligned}$$

On a donc bien obtenu une contradiction avec (50).

Deuxième cas : $d(x,V) \geqslant \mathrm{Dist}(x, \mathsf{Z}(F^m))$. Dans ce cas le théorème de Bézout 3.26 (iii) donne, en utilisant l'hypothèse $\log \mathrm{Dist}(x,V) < -U$ ainsi que (49), (45) et l'inégalité $N \leqslant U^{1/4}$:

$$\log \mathrm{Dist}(x, \mathsf{Z}(J)) \leqslant -C_0^8\, t(V)^{4/(4-r)} \big(\log^+ t(V)\big)^{8r/(4-r)} + C_0^3 t(V)^{1+1/(4-r)} \big(\log^+ t(V)\big)^{2+2r/(4-r)},$$

et l'on a donc encore la majoration (50) dans ce cas. Les mêmes calculs que précédemment conduisent de nouveau à une contradiction, ce qui achève de démontrer le théorème 5.1. □

Lorsque $\mathrm{degtr}_{\mathbb{Q}}\, \mathbb{Q}(q, P(q), Q(q), R(q)) = 3$, il est possible de déduire du théorème 5.1 une mesure d'indépendance algébrique d'une base de transcendance quelconque $(\alpha_1, \alpha_2, \alpha_3)$ du corps $\mathbb{Q}(q, P(q), Q(q), R(q))$. De façon précise :

Corollaire 5.3. — *Soit* $q \in \mathbb{C}^*$ *tel que* $|q| < 1$ *et* $\mathrm{degtr}_{\mathbb{Q}}\, \mathbb{Q}(q, P(q), Q(q), R(q)) = 3$*, et soit* $(\alpha_1, \alpha_2, \alpha_3)$ *une base de transcendance du corps* $\mathbb{Q}(q, P(q), Q(q), R(q))$*. Il existe un réel* $\mu > 0$ *(dépendant de* q*,* α_1*,* α_2*,* α_3*) tel que pour tout polynôme non nul* $A \in \mathbb{Z}[X_1, X_2, X_3]$*, on ait*

$$\log |A(\alpha_1, \alpha_2, \alpha_3)| \geqslant -\mu\, t(A)^4 \big(\log^+ t(A)\big)^{24},$$

où $t(A) = \deg A + \log H(A)$*.*

Esquisse de la démonstration. — On consultera [**Nes97**], [**Phi98**] et [**Nes96**, Theorem 2] pour des résultats plus précis. Nous suivrons ici [**Nes96**] auquel on renvoie pour davantage de détails. On note ci-après $c_1, \ldots, c_6$ des réels > 0 ne dépendant que de q et $\alpha_1, \alpha_2, \alpha_3$. Soit $\mathfrak{p}$ l'idéal homogène engendré par les polynômes homogènes de $\mathbb{Q}[X_0, \ldots, X_4]$ s'annulant en $x = (1, q, P(q), Q(q), R(q))$, et posons $V = \mathscr{Z}(\mathfrak{p})$. Comme $\mathrm{degtr}_{\mathbb{Q}}\, \mathbb{Q}(q, P(q), Q(q), R(q)) = 3$ on a $\dim V = 3$. Soit maintenant $D \in \mathbb{Z}[X_1, X_2, X_3, X_4]$ tel que $d = D(q, P(q), Q(q), R(q)) \neq 0$ et $d\alpha_i \in \mathbb{Z}[q, P(q), Q(q), R(q)]$ pour tout $i \in \{1, 2, 3\}$. Alors, si A est un polynôme non nul quelconque de $\mathbb{Z}[X_1, X_2, X_3]$, il existe un polynôme non nul $B \in \mathbb{Z}[X_1, X_2, X_3, X_4]$ tel que $d^{\deg A} A(\alpha_1, \alpha_2, \alpha_3) = B(q, P(q), Q(q), R(q))$ et $t(B) \leqslant c_1\, t(A)$. Soit F l'homogénéisé de B dans $\mathbb{Z}[X_0, X_1, X_2, X_3, X_4]$. Puisque $F \notin \mathfrak{p}$ on peut appliquer le théorème de Bézout métrique du § 3.6, ce qui donne, en notant $J = (\mathfrak{p}, F)$ et en remarquant que $d(x, V) = 0$:

$$\begin{aligned}\log \mathrm{Dist}(x, \mathsf{Z}(J)) &\leqslant \log \mathrm{Dist}(x, \mathsf{Z}(F)) + c_2\, t(B) \\ &\leqslant \log |B(q, P(q), Q(q), R(q))| + c_3\, t(B).\end{aligned}$$

D'autre part, les théorèmes de Bézout géométrique et arithmétique (théorème 3.26 (i) et (ii)) impliquent $t(\mathsf{Z}(J)) \leqslant c_4\, t(B)$, et donc le théorème 5.1 (avec $\mathsf{Z} = \mathsf{Z}(J)$ et $r = 3$)

fournit $\log \operatorname{Dist}(x, \mathsf{Z}(J)) \geqslant -c_5\, t(B)^4 \big(\log^+ t(B)\big)^{24}$. Grâce à la majoration précédente on obtient ainsi

$$\log |B(q, P(q), Q(q), R(q))| \geqslant -c_6\, t(B)^4 \big(\log^+ t(B)\big)^{24},$$

d'où la minoration du corollaire puisque $t(B) \leqslant c_1\, t(A)$. □

5.2. Utilisation d'un critère pour les mesures d'indépendance algébrique

La méthode employée pour démontrer le théorème 5.1 est, tout comme au § 4.5, une méthode de « descente ». Le principe en est le suivant (comparer avec le schéma de démonstration de la fin du § 4.2). On suppose que l'on dispose d'une majoration de $\log \operatorname{Dist}(x, \mathsf{Z})$ en fonction de $t(\mathsf{Z})$, où Z est un cycle. On en déduit aussitôt qu'il existe une variété V (une composante du cycle) pour laquelle on a une majoration analogue de $\log \operatorname{Dist}(x, V)$ en fonction de $t(V)$. On construit alors (par la méthode de transcendance du § 2) un polynôme F tel que $F \notin \mathfrak{p}$, où $\mathfrak{p}$ est l'idéal de V, et on applique le théorème de Bézout métrique pour obtenir une majoration de $\log \operatorname{Dist}(x, \mathsf{Z}(J))$, où $J = (F, \mathfrak{p})$, le cycle $\mathsf{Z}(J)$ étant de dimension $\dim V - 1$. L'utilisation des théorèmes de Bézout géométrique et arithmétique permet alors d'obtenir une majoration en fonction de $t(\mathsf{Z}(J))$. On descend ainsi jusqu'à la dimension -1, pour laquelle la majoration est trivialement fausse, ce qui donne finalement une *minoration* de $\log \operatorname{Dist}(x, \mathsf{Z})$.

Ce type d'argument était déjà utilisé dans la démonstration du théorème principal de [**Phi86**], dont le critère d'indépendance algébrique du § 2 (théorème 2.1) est un corollaire. On peut en fait obtenir par cette méthode des critères d'indépendance algébrique généraux dont la conclusion est quantitative, c'est-à-dire dont la conclusion fournit une minoration de la distance du point considéré à un cycle. Ces critères, appelés dans [**Phi98**] « critères pour les mesures d'indépendance algébrique », permettent d'obtenir presque immédiatement le théorème 5.1 (à partir de la construction de transcendance du § 2 comme au paragraphe précédent) et donc le corollaire 5.3. De tels critères ont été obtenus notamment par Jabbouri [**Jab92**] et Jadot [**Jad96**]. On consultera également [**NP01**, chap. 8] et [**Abl92**]. À titre d'illustration, nous citerons l'énoncé très simplifié suivant, qui résulte du critère principal de [**NP01**, chap. 8], et que nous appliquerons ensuite pour retrouver le théorème 5.1. Notons encore qu'un tel critère pour les mesures d'indépendance algébrique permet aussi de déduire un énoncé qualitatif du type de celui énoncé au § 2.1 (théorème 2.1) (voir [**Jad96**] ou [**NP01**, chap. 8]).

Théorème 5.4. — *Soient $n \geqslant 1$ un entier, $\alpha_1, \dots, \alpha_n \in \mathbb{C}$, et $x = (1, \alpha_1, \dots, \alpha_n) \in \mathbb{P}_n(\mathbb{C})$. Il existe des réels strictement positifs c et γ, ne dépendant que de n et $\alpha_1, \dots, \alpha_n$, vérifiant la condition suivante. Soient U, τ et σ des réels tels que $1 \leqslant \sigma^{n+1} < \tau < U$. On suppose que pour tout réel s tel que $\tau < s \leqslant U$, il existe un polynôme $Q_s \in \mathbb{Z}[X_1, \dots, X_n]$ tel que*

$$\deg Q_s \leqslant \tau, \qquad \log H(Q_s) \leqslant \tau \tag{51}$$

et

$$-\sigma\gamma s \leqslant \log|Q_s(\alpha_1,\dots,\alpha_n)| \leqslant -\gamma s. \tag{52}$$

Alors, pour toute variété $V \subset \mathbb{P}_n$ *sur* $\mathbb{Q}$ *de dimension* d *et vérifiant*

$$c\,t(V)\sigma^{d+1}\tau^{d+1} < U, \tag{53}$$

on a

$$\log \operatorname{Dist}(x,V) \geqslant -c\,U.$$

Démonstration (à partir de [**NP01**, chap. 8]*).* — Nous allons déduire cet énoncé du critère principal de [**NP01**, chap. 8], dont nous reprenons les notations. Soient $n \geqslant 1$ et $\alpha_1,\dots,\alpha_n \in \mathbb{C}$. Il est facile de vérifier qu'il existe un réel $c_1 > 0$, ne dépendant que de n et $\alpha_1,\dots,\alpha_n$ et que l'on choisira tel que $c_1 \geqslant (n+1)(n+2+3\log(n+1))$, tel que pour tout polynôme homogène $F \in \mathbb{Z}[X_0,\dots,X_n]$, on ait (voir remarques 3.13 et 3.14 et [**NP01**, chap. 6, § 4, p. 87])

$$\log\frac{\|F(x)\|}{\|F\|} \leqslant c_1 \deg F + \log|F(x)| \tag{54}$$

et

$$h_1(F) \leqslant c_1 \deg F + \log H(F). \tag{55}$$

De plus, si δ est un réel > 0 tel que $\log|F(x)| \geqslant -\delta$, on démontre, par une méthode analogue à celle utilisée dans [**Jad96**, page 127] ou bien en utilisant la proposition 3.25, que F n'a pas de zéro dans la boule $B(x, e^{-\delta - c_1\max\{\deg F, \log H(F)\}})$ de $\mathbb{P}_n(\mathbb{C})$. On choisit alors $c_2 \geqslant c_1 + 1$ tel que $2c_1 + c_2 \leqslant c_2^{(n+2)/(n+1)}$, puis on pose $\gamma = c_1 + c_2$ et $c = c_1 c_2^{n+1}$. Nous allons voir que ces réels γ et c satisfont aux conditions du théorème 5.4. On se donne donc des réels U, τ, σ, et une variété V de dimension d comme dans l'énoncé. Afin d'appliquer le critère de [**NP01**, Chap. 8], on pose $U' = c_2 U$, $\tau' = \delta' = c_2\tau$, $\sigma' = c_2^{1/(n+1)}\sigma$, et $k = d$. On vérifie immédiatement que $\delta' \geqslant 1$ et $1 \leqslant {\sigma'}^{k+1} < \tau' < U'$. Définissons, pour tout réel S tel que $\tau'/{\sigma'}^{k+1} < S \leqslant U'/{\sigma'}^{k+1}$, le polynôme $Q'_S \in \mathbb{Z}[X_0,\dots,X_n]$ comme l'homogénéisé du polynôme Q_s, où $s = S{\sigma'}^{k+1}/c_2$ (s vérifie $\tau < s \leqslant U$). La forme Q'_S vérifie l'hypothèse (1) du critère principal de [**NP01**, chap. 8] d'après (55). Elle en vérifie également l'hypothèse (2) d'après (54), la seconde inégalité de (52), l'inégalité $\tau < s$ et le choix de γ. De plus, d'après la remarque ci-dessus, Q'_S n'a pas de zéro dans la boule de centre x et de rayon

$$e^{-\sigma\gamma s - c_1\tau} \geqslant e^{-(2c_1+c_2)\sigma s} \geqslant e^{-c_2^{(n+2)/(n+1)}\sigma s} = e^{-S{\sigma'}^{k+2}},$$

et donc l'hypothèse (3) est aussi vérifiée. Enfin, on a

$$\begin{aligned}(k+1)\big(\delta' h(V) + (k+1)\tau' d(V) + 3\delta'\log(n+1)d(V)\big){\sigma'}^{k+1}{\delta'}^{k}\\ \leqslant c_1 t(V){\sigma'}^{k+1}{\tau'}^{k+1} \leqslant c c_2 \sigma^{k+1}\tau^{k+1} t(V) < U',\end{aligned}$$

et la condition (4) de [**NP01**, chap. 8] est satisfaite. L'application du critère principal de cette dernière référence donne alors immédiatement le résultat. $\square$

L'utilisation du théorème 5.4 au lieu du théorème 2.1 au § 2.5 permet d'obtenir directement le théorème 5.1 :

Démonstration du théorème 5.1 à partir du théorème 5.4. — Soient $q \in \mathbb{C}^*$ tel que $|q| < 1$ et r un entier tel que $0 \leqslant r \leqslant 3$. Comme au § 5.1 on peut supposer que $r \geqslant 1$, et de plus il suffit de démontrer la minoration (43) pour les variétés. Soit donc V une variété sur $\mathbb{Q}$ de dimension $r-1$. On a vu à la fin du paragraphe 2.5 que pour tout entier N suffisamment grand, il existe un polynôme non nul $B_N \in \mathbb{Z}[X_1, \ldots, X_4]$ tel que $\deg B_N \leqslant \gamma_0 N(\log N)^2$, $\log H(B_N) \leqslant \gamma_0 N(\log N)^2$, et $-\gamma_2 N^4 \leqslant \log |B_N(q, P(q), Q(q), R(q))| \leqslant -\gamma_1 N^4$, où γ_0, γ_1 et γ_2 sont des constantes strictement positives ne dépendant que de q. Ce résultat étant acquis, on désigne alors par $C_0 > 0$ un réel ne dépendant que de q et r, choisi suffisamment grand pour que les inégalités ci-dessous soient satisfaites. On pose

$$\sigma = 2^4 \frac{\gamma_2}{\gamma_1}, \qquad U = C_0^{16} t(V)^{4/(4-r)} \big(\log^+ t(V)\big)^{8r/(4-r)},$$

et

$$\tau = C_0^5 t(V)^{1/(4-r)} \big(\log^+ t(V)\big)^{8/(4-r)}.$$

On a $1 \leqslant \sigma^5 < \tau < U$. Pour tout réel s tel que $\tau < s \leqslant U$, posons encore $N = \big[(\sigma\gamma s/\gamma_2)^{1/4}\big]$ et $Q_s = B_N$ (noter que $s > \tau \geqslant C_0^5$ donc N est suffisamment grand et par suite B_N bien défini). On vérifie immédiatement, en utilisant l'encadrement $N \leqslant (\sigma\gamma s/\gamma_2)^{1/4} \leqslant 2N$, que Q_s satisfait à l'hypothèse (52) du théorème 5.4 (avec $n = 4$ et $(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = (q, P(q), Q(q), R(q))$). D'autre part, puisque C_0 est choisi assez grand, on vérifie facilement que l'on a

$$\gamma_0 N(\log N)^2 \leqslant C_0^5 t(V)^{1/(4-r)} \big(\log^+ t(V)\big)^{2+2r/(4-r)} = \tau,$$

donc Q_s satisfait aussi à l'hypothèse (51). Enfin, on vérifie sans peine que la condition (53) est également satisfaite. L'application du théorème 5.4 fournit alors immédiatement la minoration souhaitée pour $\log \mathrm{Dist}(x, V)$. $\square$

5.3. Utilisation de propriétés d'approximation. — Les démonstrations du théorème de Nesterenko exposées aux paragraphes 2.5, 5.1 et 5.2 ne sont en fait que des présentations différentes de la même méthode. On utilise en effet dans les trois cas la méthode de transcendance du § 2 pour construire certains polynômes (notés précédemment B_N), ce qui permet ensuite d'effectuer une descente jusqu'à la dimension -1 par adjonction successive de ces polynômes. Au § 5.1, cette descente a été décrite explicitement, aux § 2.5 et 5.2 elle est contenue dans la démonstration des critères d'indépendance algébrique utilisés.

Une approche sensiblement différente pour l'indépendance algébrique a été proposée par Philippon dans [**Phi97**] et [**Phi00**], qui n'utilise pas de critère d'indépendance algébrique, mais s'appuie sur des « propriétés d'approximation » générales, indépendantes de la construction de transcendance. Ces propriétés d'approximation sont actuellement des conjectures, dont on trouvera les énoncés précis dans [**Phi97**] et [**NP01**, chap. 4, § 4]. Toutefois, elles ont été démontrées en petites dimensions par Philippon, ce qui permet de retrouver autrement le théorème de Nesterenko (théorème 1.1). Renvoyant aux articles susmentionnés pour les démonstrations, on se contentera ici de donner, sans preuve, des versions très simplifiées des résultats de Philippon.

Une version simplifiée de la première propriété d'approximation que démontre Philippon est la suivante :

Théorème 5.5. — *Soit $n \geqslant 1$ un entier. Il existe des réels $\gamma_n \geqslant 1$ et $c_n > 0$ vérifiant la propriété suivante. Soient $x \in \mathbb{P}_n(\mathbb{C})$ et $d \in \{n, n-1, n-2, n-3\}$ avec $d \geqslant 0$. Alors, pour tout réel $T \geqslant 1$, il existe une variété $V \subset \mathbb{P}_n$ sur $\mathbb{Q}$, de dimension d, telle que $t(V) \leqslant \gamma_n T^{n-d}$ et satisfaisant à*

$$\log \mathrm{Dist}(x, V) \leqslant -c_n\, t(V) T^{d+1}.$$

Cet énoncé résulte de [**Phi97**, prop. 9] ou de l'énoncé plus précis [**Phi00**, théorème 1], et se démontre également par une méthode de descente. On conjecture qu'il reste vrai pour tout d, $0 \leqslant d \leqslant n$. On notera encore que les constantes γ_n et c_n sont calculées dans [**Phi00**].

Philippon déduit du théorème 5.5 la propriété d'approximation suivante pour les points [**Phi00**, théorème 2]. Pour tout point $\alpha \in \mathbb{P}_n(\overline{\mathbb{Q}})$, on note $d(\alpha) = [\mathbb{Q}(\alpha) : \mathbb{Q}]$ son degré et $h(\alpha)$ sa hauteur (*cf.* exemple 3.18).

Théorème 5.6. — *Soit $n \in \{1, 2\}$. Il existe des réels $\gamma'_n \geqslant 1$ et $c'_n \geqslant 1$ vérifiant la propriété suivante. Pour tout $x \in \mathbb{P}_n(\mathbb{C})$ et tout réel $T \geqslant 1$, il existe un point $\alpha \in \mathbb{P}_n(\overline{\mathbb{Q}})$ vérifiant $d(\alpha) \leqslant \gamma'_n T^n$, $d(\alpha)h(\alpha) \leqslant \gamma'_n T^n$ et*

$$\log \mathrm{Dist}(x, \alpha) \leqslant -c'_n\, d(\alpha)(h(\alpha) + 1)T.$$

On conjecture que le théorème 5.6 est vrai pour tout entier $n \geqslant 1$. Utilisé conjointement avec la méthode de transcendance du § 2, le théorème 5.6 permet de retrouver le théorème 1.1. On montre en effet par la méthode transcendante [**NP01**, chap. 4, proposition 4.1] que si $q \in \mathbb{C}^*$ est tel que $|q| < 1$ et si $(x_1, \ldots, x_n)$ est une base de transcendance du corps $\mathbb{Q}(q, P(q), Q(q), R(q))$, alors il existe un réel $c > 0$ tel que pour tout $\alpha \in \mathbb{P}_n(\overline{\mathbb{Q}})$, on ait

$$\log \mathrm{Dist}(x, \alpha) \geqslant -c\left(d(\alpha)t(\alpha)\right)^{4/3}\left(\log^+ t(\alpha)\right)^{8/3},$$

où $x = (1, x_1, \ldots, x_n) \in \mathbb{P}_n(\mathbb{C})$ et $t(\alpha) = h(\alpha) + \log d(\alpha)$. Il est alors facile de voir que ce résultat est contradictoire avec le théorème 5.6, d'où l'on déduit que

$\mathrm{degtr}_{\mathbb{Q}}\,\mathbb{Q}(q, P(q), Q(q), R(q)) \geqslant 3$. Voir [**NP01**, chap. 4] et [**Phi97**, § 7 (a)] pour les détails.

Cette preuve du théorème de Nesterenko est donc d'une nature différente de celles décrites précédemment. En effet, on effectue d'abord ici une descente à la dimension 0 via le théorème 5.6, mais cette descente est *indépendante* de la construction de transcendance : cette dernière n'est utilisée qu'ensuite, lors d'un dernier pas, pour conclure. Il en va tout autrement avec la méthode des §§ 5.1, 5.2 ou 2.5, où on effectue une descente à la dimension -1 (éventuellement incluse dans la démonstration des critères d'indépendance algébrique utilisés), en utilisant *à chaque pas* la construction de transcendance. On consultera à ce sujet, et notamment pour une étude de la façon dont les propriétés d'approximation interviennent au sein des preuves des critères d'indépendance algébrique, les premières pages de [**NP01**, chap. 8].

Références

[Abl92] M. Ably – « Résultats quantitatifs d'indépendance algébrique pour les groupes algébriques », *J. Number Theory* **42** (1992), p. 194–231.

[Ber97] D. Bertrand – « Theta Functions and Transcendence », *The Ramanujan Journal* **1** (1997), p. 339–350.

[BM80] W.D. Brownawell & D. Masser – « Multiplicity estimates for analytic functions II », *Duke Math. J.* **47** (1980), p. 273–295.

[Bou85] N. Bourbaki – *Algèbre commutative, chapitres 5 à 7*, Masson, Paris, 1985.

[Chu84] G.V. Chudnovsky – *Contributions to the theory of transcendental numbers*, Math. Surveys and Monographs, vol. 19, American Mathematical Society, 1984.

[Eic66] M. Eichler – *Algebraic Numbers and Functions*, Academic Press, 1966.

[Eis95] D. Eisenbud – *Commutative Algebra with a view toward Algebraic Geometry*, Graduate Texts in Math., Springer, 1995.

[Gra] P. Graftieaux – « Théorème stéphanois et méthode des pentes », ce volume.

[Har77] R. Hartshorne – *Algebraic Geometry*, Graduate Texts in Math., Springer, 1977.

[Iwa93] K. Iwasawa – *Algebraic Functions*, Translations of Mathematical Monographs, vol. 118, American Mathematical Society, 1993.

[Jab92] E.M. Jabbouri – « Sur un critère pour l'indépendance algébrique de P. Philippon », in *Approximations Diophantiennes et Nombres Transcendants, Luminy 1990* (P. Philippon, éd.), Walter de Gruyter, 1992, p. 195–202.

[Jad96] C. Jadot – « Critères pour l'indépendance linéaire et algébrique », Thèse, Université Paris 6, 1996.

[Lan76] S. Lang – *Introduction to Modular Forms*, Springer-Verlag, 1976.

[Lan87] ———, *Elliptic Functions*, 2e éd., Springer-Verlag, 1987.

[Lau92] M. Laurent – « Hauteur de matrices d'interpolation », in *Approximations Diophantiennes et Nombres Transcendants, Luminy 1990* (P. Philippon, éd.), Walter de Gruyter, 1992, p. 215–238.

[Lel92] P. Lelong – « Mesure de Mahler des polynômes et majoration par convexité », *C. R. Acad. Sci. Paris Sér. I Math.* **315** (1992), p. 139–142.

[Lel94] ———, « Mesure de Mahler et calcul de constantes universelles pour les polynômes de N variables », *Math. Ann.* **299** (1994), p. 673–695.

[Mac94] F.S. Macaulay – *Algebraic Theory of Modular Systems*, Cambridge University Press, 1994.

[Mah69] K. Mahler – « On algebraic differential equations satisfied by automorphic functions », *J. Austral. Math. Soc.* **10** (1969), p. 445–450.

[Mas75] D. Masser – *Elliptic Functions and Transcendence*, Lect. Notes in Math., vol. 437, Springer-Verlag, 1975.

[Mat96] H. Matsumura – *Commutative ring theory*, Cambridge University Press, 1996.

[Nes74] Yu.V. Nesterenko – « On the algebraic dependence of the components of solutions of a system of linear differential equation », *Math. USSR Izv.* **8** (1974), p. 501–518.

[Nes77] ______, « Estimates for the orders of zeros of functions of a certain class and applications in the theory of transcendental numbers », *Math. USSR Izv.* **11** (1977), p. 239–270.

[Nes85a] ______, « Estimates for the characteristic function of a prime ideal », *Math. USSR Sb.* **51** (1985), p. 9–32.

[Nes85b] ______, « On the algebraic independence of algebraic powers of numbers », *Math. USSR Sb.* **51** (1985), p. 429–454.

[Nes96] ______, « Modular functions and transcendence questions », *Sb. Math.* **187** (1996), p. 1319–1348.

[Nes97] ______, « On the Measure of Algebraic Independence of the Values of Ramanujan Functions », *Proc. Steklov Inst. Math.* **218** (1997), p. 294–331.

[NP01] Yu.V. Nesterenko & P. Philippon (éds.) – *Introduction to Algebraic Independence Theory*, Lect. Notes in Math., vol. 1752, Springer, 2001.

[Pel04] F. Pellarin – « Lemmes de multiplicité associés aux groupes triangulaires de Riemann-Schwarz », tapuscrit ; arXiv : `math.NT/0407380` (41 pages), 2004.

[Pel05] ______, « La structure différentielle de l'anneau des formes quasi-modulaires pour $\mathbf{SL}_2(\mathbf{Z})$ », tapuscrit, `https://hal.ccsd.cnrs.fr/ccsd-00005554/en/` (23 pages), 2005.

[Phi86] P. Philippon – « Critères pour l'indépendance algébrique », *Publ. Math. Inst. Hautes Études Sci.* **64** (1986), p. 5–52.

[Phi91] ______, « Sur des hauteurs alternatives I », *Math. Ann.* **289** (1991), p. 255–283.

[Phi94] ______, « Sur des hauteurs alternatives II », *Ann. Inst. Fourier (Grenoble)* **44** (1994), p. 1043–1065.

[Phi95] ______, « Sur des hauteurs alternatives III », *J. Math. Pures Appl.* **74** (1995), p. 345–365.

[Phi97] ______, « Une approche méthodique pour la transcendance et l'indépendance algébrique de valeurs de fonctions analytiques », *J. Number Theory* **64** (1997), p. 291–338.

[Phi98] ______, « Indépendance algébrique et K-fonctions », *J. reine angew. Math.* **497** (1998), p. 1–15.

[Phi00] ______, « Approximations algébriques des points dans les espaces projectifs I », *J. Number Theory* **81** (2000), p. 234–253.

[Sch74] B. Schoeneberg – *Elliptic Modular Functions*, Springer-Verlag, 1974.

[Sha77] I.R. Shafarevich – *Basic Algebraic Geometry 1*, 2^{e} éd., Springer-Verlag, 1977.

[Wal74] M. Waldschmidt – *Nombres transcendants*, Lect. Notes in Math., vol. 402, Springer-Verlag, 1974.

[Wal97] ———, « Sur la nature arithmétique des valeurs de fonctions modulaires », in *Séminaire Bourbaki 1996/1997*, Astérisque, vol. 245, Société Mathématique de France, 1997, Exp. n° 824, p. 105–140.

[Wal00] ———, *Diophantine approximation on linear algebraic groups*, Springer, 2000.

[ZS58] O. Zariski & P. Samuel – *Commutative Algebra, Vol. 1 & 2*, Van Nostrand, 1958.

V. Bosser, Mathematisches Institut, Universität Basel, Rheinsprung 21, CH-4051 Basel, Switzerland
E-mail : Vincent.Bosser@unibas.ch