ADICEAM
Laki Michel Faustin

Mémoire de Master 2 de mathématiques fondamentales

Etude de quelques problèmes d'indépendance algébrique de valeurs de fonctions modulaires

Sous la direction de
Michel WALDSCHMIDT

ΑΓΕΩΜΕΤΡΗΤΟΣ ΜΗΔΕΙΣ ΕΙΣΙΤΟ

2010-2011 Université Pierre et Marie Curie (Paris VI)

Remerciements

Il me semble qu'il est de coutume de réserver une page en début d'écrit pour remercier les quelques personnes qui ont contribué à son aboutissement. Si cette coutume n'avait pas existé, je l'aurais instaurée pour l'occasion ! Car comment ne pas remercier Michel Waldschmidt, qui m'a tout d'abord proposé des thèmes de travail qui m'ont passionné de bout en bout : la longueur de ce mémoire illustre tout à fait ce propos. J'ai en effet pu découvrir au cours des six derniers mois une diversité de problèmes, de raisonnements, de résultats dont je ne soupçonnais pas même l'existence pour certains. Et le tout en étant encadré dans mes recherches par une personne qui aura toujours pris la peine de répondre à mes questions – qui n'ont sans doute pas toujours été pertinentes –, que soit par voie électronique ou en s'efforçant de me rencontrer quand j'en éprouvais le besoin, et ce malgré un emploi du temps que j'imagine très chargé. Pour ce qui constitue peut-être ma dernière production scolaire, je crois que, grâce aux conseils avisés de Michel Waldschmidt et à la tournure qu'il a fait prendre à mon travail, c'est aussi la plus aboutie. Je le remercie également de sa peine pour les différentes propositions de thèses auxquelles il m'a permis de postuler.

Si ces derniers mois ont été l'occasion de découvrir le monde de la recherche, c'est autant par le travail en lui-même que par la rencontre avec la «communauté des chercheurs» : j'ai vraiment apprécié le cadre informel et très plaisant que j'ai pu découvrir en discutant avec différents chercheurs à Paris VI. A ce titre, je me dois de remercier Patrice Philippon : d'abord pour m'avoir grandement éclairé dans la résolution d'un problème qui me tracassait sérieusement, ensuite pour avoir accepté de constituer le jury aux côtés de Michel Waldschmidt.

Je ne saurais conclure ces remerciements sans une pensée pour mes parents qui m'auront soutenu tout au long de mes études, bien qu'il eût été plus facile pour eux que je travaillasse [1].

1. Au lecteur curieux qui se demande enfin ce que signifie l'inscription grecque en première de couverture, j'ai voulu signifier par cette phrase qui ornait l'entrée de l'Académie de Platon – «Que nul n'entre ici s'il n'est géomètre» – à quel point ce mémoire m'avait permis de prendre conscience de la portée de la géométrie dans les mathématiques.

Sommaire

Notations

En sus des notations introduites au fur et à mesure de l'exposé, nous emploierons les suivantes :
- $D(a,r)$: disque ouvert de centre le point a et de rayon $r>0$ dans $\mathbb{C}$.
- $A^* = A\backslash\{0\}$.
- $\mathcal{M}_{p,q}(A)$: ensemble des matrices de taille $p\times q$ à coefficients dans un anneau A.
- $GL_n(A)$: ensemble des matrices de $\mathcal{M}_n(A)$ inversibles.
- $GL_n^+(A)$: ensemble des éléments de $GL_n(A)$ de déterminant positif ($A\subset\mathbb{R}$).
- (n,m) : plus grand commun diviseur de deux entiers n et m.
- $\lfloor x\rfloor$: partie entière d'un réel x.
- $|X|$ ou $\mathrm{Card}(X)$: cardinal d'un ensemble X.
- $\mathcal{P}$: ensemble des nombres premiers.
- $SL_2(\mathbb{R})$ (resp. $SL_2(\mathbb{Z})$) : matrices de $\mathcal{M}_2(\mathbb{R})$ (resp. de $\mathcal{M}_2(\mathbb{Z})$) de déterminant 1.
- $PSL_2(\mathbb{R}) = SL_2(\mathbb{R})/_{\{\pm 1\}}$.

Introduction

En 1996, Y.V. Nesterenko déduisait l'indépendance algébrique des trois nombres π, e^π et $\Gamma(1/4)$ d'un théorème plus général qui faisait suite à un série de résultats de transcendance exploitant la féconde complémentarité entre les points de vue modulaire et elliptique.

Nous nous proposons d'explorer et d'approfondir cette démarche afin, non seulement de présenter le raisonnement de Y.V.Nesterenko permettant d'aboutir à son résultat, mais aussi d'en proposer un autre. Il s'agira également d'appliquer ce résultat à diverses situations pour en déduire des conséquences variées qui en illustreront la portée.

Dans cette perspective, nous établirons dans les deux premières parties – d'un niveau assez élémentaire – un dictionnaire permettant de relier les propriétés des fonctions elliptiques à celles de certaines formes modulaires, et réciproquement. Si nous supposons quelques légers prérequis concernant la théorie des courbes elliptiques dans le cadre complexe, l'essentiel des notions utiles à cette fin sera introduit au fur et à mesure de l'exposé. En application de cette correspondance, nous étudierons le théorème stéphanois – ainsi nommé car démontré par une équipe stéphanoise – ainsi que quelques corollaires. L'intérêt de ce théorème est tout particulier dans notre perspective puisqu'il s'agit du résultat dont la preuve a directement inspiré Y.V.Nesterenko en vue de la démonstration de son propre théorème. Nous tâcherons par la suite d'introduire dans les deux parties suivantes l'ensemble des outils nécessaires à une démonstration alternative d'un résultat général impliquant l'indépendance algébrique de π, e^π et $\Gamma(1/4)$, que nous proposerons à la suite de l'étude de quelques corollaires du théorème de Y.V.Nesterenko : cette preuve alternative passe par une mesure d'indépendance algébrique due à G.Philibert, mesure que nous essaierons de déduire d'un critère d'indépendance algébrique mis au point par P.Philippon et dont la preuve nécessite de fait l'étude des variétés algébriques et de quelques unes des grandeurs qui leur sont attachées (hauteur, degré,...). Enfin, dans une dernière partie, nous déduirons du résultat ainsi démontré divers corollaires, plus ou moins directs, et, dans la droite lignée de cette démarche, nous apporteront une démonstration conjecturale de l'indépendance algébrique d'au moins trois des quatre nombres π, $e^{\pi\sqrt{5}}$, $\Gamma(1/5)$ et $\Gamma(2/5)$, problème encore ouvert à ce jour.

1 Fonctions modulaires

Les résultats d'indépendance algébrique à venir feront essentiellement intervenir des valeurs de fonctions modulaires. Une étude préalable permettra de cerner quelques unes de leurs propriétés.

1.1 Définitions et premières propriétés

Notation. $\mathfrak{H} = \{x + iy / x, y \in \mathbb{R}, y > 0\}$ *désignera l'ensemble des nombres complexes de partie imaginaire strictement positive. C'est le* demi-plan de Poincaré.

Définition 1.1.1. *Le* groupe modulaire *est le groupe* $G{=}SL_2(\mathbb{Z})/\{\pm 1\}$, *image du groupe* $SL_2(\mathbb{Z})$ *dans* $PSL_2(\mathbb{R})$.

Si $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est un élément de $SL_2(\mathbb{Z})$, on notera encore g son image dans le groupe modulaire. Le groupe modulaire agit de façon naturelle sur $\mathfrak{H}$:

$$\text{pour } z \in \mathfrak{H}, \text{ on pose } g(z) = \tfrac{az+b}{cz+d}.$$

Le demi-plan $\mathfrak{H}$ est stable par l'action de G, puisque l'on vérifie aisément que, en adoptant les notations précédentes, on a :

$$\mathrm{Im}(gz) = \tfrac{\mathrm{Im}(z)}{|cz+d|^2}.$$

De plus, l'action est fidèle.

Définition 1.1.2. *Le* domaine fondamental D *pour l'action du groupe modulaire* G *sur* $\mathfrak{H}$ *est l'ensemble*

$$D = \left\{ z \in \mathfrak{H} \middle/ |z| \geq 1 \wedge |Re(z)| \leq \frac{1}{2} \right\}.$$

L'intérêt d'une telle dénomination est donné par le lemme suivant :

Lemme 1.1.3. *Pour tout* $z \in \mathfrak{H}$, *il existe* $g \in G$ *tel que* $gz \in D$. *De plus, si* z *et* z' *sont deux points distincts de* D *congrus modulo* G, *alors soit* $Re(z) = \pm\frac{1}{2}$ *et* $z = z' \pm 1$, *soit* $|z| = 1$ *et* $z' = -\frac{1}{z}$.

Démonstration. Soit G' le sous-groupe de G engendré par $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ (matrice d'inversion) et $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ (matrice de translation). A $n_0 \in \mathbb{N}$ fixé, le nombre de couples $(c, d) \in \mathbb{Z}^2$ tels que $|cz + d| \geq n_0$ (i.e. $\mathrm{Im}(gz) \leq \frac{\mathrm{Im}(z)}{n_0^2}$ en posant $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, avec a et b entiers quelconques) est fini. Il existe donc $g_0 \in G'$ tel que $\mathrm{Im}(g_0 z)$ soit maximal.

Soit alors $n \in \mathbb{N}$ tel que $\frac{1}{2} \leq \mathrm{Re}(T^n g_0 z) \leq \frac{1}{2}$. Posons $g' = T^n g_0$: $g' \in G$ et $z' = g'z$ est un élément de D par maximalité de $\mathrm{Im}(g_0 z)$ (si on avait $|z'| < 1$, on perdrait la maximalité de $\mathrm{Im}(g_0 z)$ en considérant $\frac{-1}{z'}$).

Pour le résultat d'unicité partielle, soit $z \in D$ et $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ tels que $gz \in D$. Quitte à remplacer (z, g) par (gz, g^{-1}), on peut supposer que $\mathrm{Im}(gz) \geq \mathrm{Im}(z)$, i.e. $|cz + d| \leq 1$. Ceci est évidemment impossible si $|c| \geq 2$. Reste les cas $c = 0, 1, -1$, qui se traitent «à la main» sans difficulté et qui conduisent au résultat. □

Remarque 1.1.4. *On peut en fait montrer que le groupe modulaire* G *est engendré par les matrices d'inversion* S *et de translation* T.

Du lemme précédent, on déduit immédiatement le corollaire qui suit :

Corollaire 1.1.5. *L'application canonique $D \mapsto G\backslash\mathfrak{H}$ est surjective ; sa restriction à l'intérieur de D est injective.*

Définition 1.1.6. *Soit k un entier. Une* fonction faiblement modulaire de poids 2k *est une fonction méromorphe f sur le demi-plan $\mathfrak{H}$ qui y vérifie la relation*

$$f(z) = (cz+d)^{-2k} f\left(\tfrac{az+b}{cz+d}\right)$$

pour tout $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ *et tout* $z \in \mathfrak{H}$.

En particulier, $f(z+1) = f(z)$ pour tout $z \in \mathfrak{H}$. On peut donc exprimer f à partir de son développement de Fourier comme une fonction de $q = e^{2i\pi z}$, fonction que l'on notera $\tilde{f}$. Par le caractère holomorphe de la surjection

$$\begin{aligned} \mathfrak{H} &\to D(0,1)^* \\ z &\mapsto e^{2i\pi z}, \end{aligned}$$

$\tilde{f}$ est méromorphe dans le disque unité ouvert privé de l'origine. Si $\tilde{f}$ se prolonge en une fonction méromorphe (resp. holomorphe) à l'origine, f est dite *méromorphe* (resp. *holomorphe*) *à l'infini*. Cela signifie que $\tilde{f}$ admet un développement de Laurent au voisinage de l'origine de la forme

$$\tilde{f}(q) = \sum_{n=-\infty}^{+\infty} a_n q^n,$$

où les a_n sont soit nuls pour $n < 0$ si $\tilde{f}$ est holomorphe en l'origine, soit nuls pour n assez petit si $\tilde{f}$ est méromorphe en l'origine.

Définition 1.1.7. *Une fonction faiblement modulaire est* modulaire *si elle est méromorphe à l'infini ; on pose alors $f(\infty) = \tilde{f}(0)$: c'est la* valeur de f à l'infini.

Définition 1.1.8. *Une* forme modulaire *est une fonction modulaire partout holomorphe (y compris à l'infini) ; si une telle fonction s'annule à l'infini, il s'agit d'une* forme parabolique [2].

Une forme parabolique est donc une forme modulaire telle que le terme constant dans son développement en série entière de $q = e^{2i\pi z}$ est nul.

Les principaux exemples de fonctions modulaires seront étudiés aux sections 1.3 et 1.4 : ce sont les séries d'Eisenstein, la fonction Δ et l'invariant modulaire j.

Remarque 1.1.9. *L'ensemble des formes modulaires de poids k forme un espace vectoriel ; le produit de deux formes modulaires de poids respectifs k et l est une forme modulaire de poids $k+l$.*

1.2 Réseaux

Définition 1.2.1. *Soit V un $\mathbb{R}$-espace vectoriel de dimension finie. Un réseau de V est un sous-groupe Ω de V tel qu'il existe une $\mathbb{R}$-base $(e_1, \ldots, e_n)$ de V qui soit une $\mathbb{Z}$-base de Ω (i.e. $\Omega = \bigoplus_{i=1}^n \mathbb{Z}e_i$).*

Soit $\mathcal{R}$ l'ensemble des réseaux de $\mathbb{C}$, vu comme $\mathbb{R}$-espace vectoriel. Soit M l'ensemble des couples (ω_1, ω_2) d'éléments de $\mathbb{C}^*$ tels que $\omega_1/\omega_2 \in \mathfrak{H}$. A un tel couple, on associe le réseau

$$\Omega(\omega_1, \omega_2) = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$$

de base (ω_1, ω_2). On obtient de la sorte une application surjective $M \to \mathcal{R}$.

2. *Spitzenform* en allemand, *cusp form* en anglais

Proposition 1.2.2. *Pour que deux éléments de M définissent le même réseau, il faut et il suffit qu'ils soient congrus modulo $SL_2(\mathbb{Z})$.*

Démonstration. Soit $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ et soit $(\omega_1, \omega_2), (\omega_1', \omega_2') \in M$ tels que

$$\begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}.$$

La famille (ω_1', ω_2') est clairement une base de $\Omega(\omega_1, \omega_2)$. En posant par ailleurs $z = \omega_1/\omega_2$ et $z' = \omega_1'/\omega_2'$, on a :

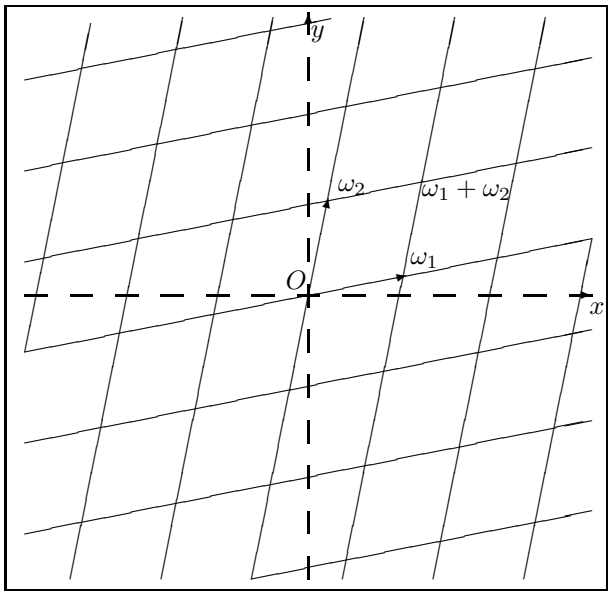
$$z' = \frac{az+b}{cz+d} = gz.$$

Par conséquent, $z' \in \mathfrak{H}$ et donc (ω_1', ω_2') appartient à M : la condition est suffisante.

Réciproquement, si (ω_1, ω_2) et (ω_1', ω_2') sont deux éléments M définissant le même réseau, il existe une matrice entière $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ de déterminant ± 1 qui transforme la première base en la seconde. Si $\det(g)$ était négatif, le signe de $\mathrm{Im}(\omega_1'/\omega_2')$ serait l'opposé de celui de $\mathrm{Im}(\omega_1/\omega_2)$, ce qui n'est pas. Par conséquent, $\det(g) = 1$ et la condition est aussi nécessaire □

On fixe dorénavant un réseau complexe $\Omega = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ pour lequel on supposera, sans perte de généralité, que $\tau = \omega_1/\omega_2$ est dans $\mathfrak{H}$.

Définition 1.2.3. *Un* parallélogramme fondamental *du réseau $\Omega = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ est un parallélogramme de sommets $(a, a+\omega_1, a+\omega_1+\omega_2, a+\omega_2)$ avec $a \in \mathbb{C}$, dans lequel on ôte $a+\omega_1$, $a+\omega_2$ et les côtés adjacents à $a+\omega_1+\omega_2$.*



1.3 Séries d'Eisenstein

Notation. *On notera $\Omega^* = \Omega \backslash \{0\}$.*

Voici tout d'abord un lemme qui nous sera très utile pour systématiquement justifier de l'existence des séries que nous considèrerons par la suite :

Lemme 1.3.1. *Si s est un nombre réel >2, alors la série*

$$\sum_{\omega \in \Omega^*} \frac{1}{|\omega|^s}$$

est convergente.

Démonstration. On identifie $\mathbb{C}$ à $\mathbb{R}\omega_1 \oplus \mathbb{R}\omega_2$. Comme, sur $\mathbb{C}$, la valeur absolue usuelle et la norme infinie sont équivalentes, il existe une constante C telle que l'on ait :

$$\begin{aligned}\sum_{\omega\in\Omega^*}\frac{1}{|\omega|^s} &\leq C\sum_{(m,n)\in(\mathbb{Z}^2)^*}\frac{1}{[\max(|m|,|n|)]^s}\\ &\leq C\left(\sum_{\substack{m\in\mathbb{Z}\\ m\neq 0}}\sum_{n\leq m}\frac{1}{|m|^s}+\sum_{m\in\mathbb{Z}}\sum_{\substack{n>m\\ n\neq 0}}\frac{1}{|n|^s}\right)\\ &\leq 2C\sum_{n\in\mathbb{Z}}\sum_{\substack{m\geq n\\ m\neq 0}}\frac{1}{|m|^s},\end{aligned}$$

qui converge dès que $s > 2$. □

Définition 1.3.2. *Si Ω est un réseau complexe, on définit, pour tout entier $k \geq 2$, la* série d'Eisenstein d'indice 2k du réseau Ω *en posant*[3] *:*

$$G_{2k}(\Omega) = \sum_{\omega\in\Omega^*}\frac{1}{\omega^{2k}}.$$

Cette série converge absolument en vertu du lemme 1.3.1. On peut également considérer G_{2k} comme une fonction définie sur $\mathfrak{H}$ en posant, pour $\Omega = \mathbb{Z}\oplus\mathbb{Z}\tau$ avec $\tau\in\mathfrak{H}$,

$$\boxed{G_{2k}(\tau) = \sum_{(m,n)\in(\mathbb{Z}^2)^*}\frac{1}{(m\tau+n)^{2k}}}$$

Lemme 1.3.3. *Soit $k \geq 2$ un entier. Alors $G_{2k}(\tau)$ et ω_2 déterminent $G_{2k}(\Omega)$.*

Démonstration. On a successivement :

$$\begin{aligned}G_{2k}(\Omega) &= G_{2k}(\mathbb{Z}\omega_1\oplus\mathbb{Z}\omega_2)\\ &= \omega_2^{-2k}G_{2k}\left(\mathbb{Z}\oplus\mathbb{Z}\frac{\omega_1}{\omega_2}\right)\\ &= \omega_2^{-2k}G_{2k}\left(\frac{\omega_1}{\omega_2}\right)\end{aligned}$$

car on a supposé que $\tau = \frac{\omega_1}{\omega_2}\in\mathfrak{H}$. □

Remarque 1.3.4. *Une fonction de réseaux F de poids $2k$ ($k\in\mathbb{Z}$) étant définie comme une fonction définie sur $\mathcal{R}$ (ensemble des réseaux complexes) et vérifiant :*

$$\forall\Gamma\in\mathcal{R},\quad\forall\lambda\in\mathbb{C}^*,\quad F(\lambda\Gamma) = \lambda^{-2k}F(\Gamma),$$

ce lemme illustre le fait que les fonctions modulaires de poids $2k$ s'identifient à certaines fonctions de réseaux de poids $2k$. Cette remarque fait sens d'après le résultat qui suit :

Proposition 1.3.5. *Soit $k \geq 2$ un entier. La série d'Eisenstein G_{2k} est une forme modulaire de poids $2k$.*

3. Certains auteurs l'appellent *série d'Eisenstein d'indice k.*

Démonstration. Soit $\tau \in \mathfrak{H}$ et $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$. On a $\mathrm{Im}\left(\frac{a\tau+b}{c\tau+d}\right) = \frac{\mathrm{Im}(\tau)}{|c\tau+d|^2} > 0$, donc, d'après la proposition 1.2.2,

$$\begin{aligned} G_{2k}\left(\frac{a\tau+b}{c\tau+d}\right) &= G_{2k}\left(\mathbb{Z} \oplus \frac{a\tau+b}{c\tau+d}\mathbb{Z}\right) \\ &= (c\tau+d)^{2k} G_{2k}\left((c\tau+d)\mathbb{Z} \oplus (a\tau+b)\mathbb{Z}\right) \\ &= (c\tau+d)^{2k} G_{2k}\left(\mathbb{Z} \oplus \tau\mathbb{Z}\right) \\ &= (c\tau+d)^{2k} G_{2k}(\tau). \end{aligned}$$

Montrons à présent que G_{2k} est holomorphe sur $\mathfrak{H}$. On rappelle que D désigne le domaine fondamental pour l'action du groupe modulaire sur $\mathfrak{H}$. Pour $z \in D$ et $(m,n) \in \mathbb{Z}^2$, on a :

$$|mz+n|^2 = m^2 z\bar{z} + 2mn\mathrm{Re}(z) + n^2 \geq m^2 - |mn| + n^2 = |m\rho \pm n|^2,$$

où $\rho = \exp\left(\frac{2i\pi}{3}\right)$. Le lemme 1.3.1 garantit alors la convergence de la série

$$\sum_{(m,n)\in(\mathbb{Z}^2)^*} \frac{1}{|m\rho \pm n|^{2k}}$$

pour $k \geq 2$. Par conséquent, G_{2k} converge normalement sur D, donc aussi (en appliquant le résultat à $G_{2k}\left(g^{-1}z\right)$, $g \in G$) dans chacun des transformés gD de D par G, qui recouvrent $\mathfrak{H}$ d'après le lemme 1.1.3.

Reste à démontrer que G_{2k} est holomorphe à l'infini, chose qui sera faite dans la proposition 1.3.8. □

Définition 1.3.6. *Pour $k \geq 1$ et $\tau \in \mathfrak{H}$, on pose*

$$E_{2k} = 1 + (-1)^k \frac{4k}{B_{2k}} \sum_{n=1}^{+\infty} n^{2k-1} \frac{q^n}{1-q^n},$$

en notant $B_k = \frac{\zeta(2k)2(2k)!}{(2\pi)^{2k}}$ ($k \geq 1$) le $k^{\text{ème}}$ nombre de Bernoulli[4]*, où ζ désigne la fonction zêta de Riemann.*

Remarque 1.3.7. *Pour $n \geq 1$ et $p \geq 0$, on pose $\sigma_p(n) = \sum_{d|n} d^p$. On a alors pour tout $k \geq 1$, par simple interversion des sommations,*

$$\sum_{n=1}^{+\infty} \sigma_k(n) q^n = \sum_{n=1}^{+\infty} \frac{n^k q^n}{1-q^n}.$$

Par conséquent, on peut aussi écrire

$$E_{2k} = 1 + (-1)^k \frac{4k}{B_{2k}} \sum_{n=1}^{+\infty} \sigma_{2k-1}(n) q^n.$$

Proposition 1.3.8. *Soit $k \geq 2$ et $\tau \in \mathfrak{H}$. On a :*

$$G_{2k}(\tau) = 2\zeta(2k) E_{2k}(\tau).$$

En particulier, $G_{2k}(\infty) = 2\zeta(2k)$.

4. Les nombres de Bernoulli $(B_k)_{k\geq 0}$ se définissent plus naturellement comme étant les coefficients du développement de Laurent en l'origine de la fonction $\frac{z}{e^z-1}$:

$$\frac{z}{e^z-1} = \sum_{k=0}^{+\infty} B_k \frac{z^{2k}}{(2k)!}$$

Démonstration. La seconde assertion résulte simplement de la définition de E_{2k}. Pour la première, établissons tout d'abord un résultat préliminaire. On part de la formule bien connue suivante, valable pour tout $z \in \mathbb{C}$ non entier :

$$\pi \cot(\pi z) = \frac{1}{z} + \sum_{m=1}^{+\infty} \left(\frac{1}{z+m} + \frac{1}{z-m} \right).$$

Par ailleurs, on a aussi :

$$\pi \cot(\pi z) = \pi \frac{\cos(\pi z)}{\sin(\pi z)} = i\pi \frac{q+1}{q-1} = i\pi - \frac{2i\pi}{1-q} = i\pi - 2i\pi \sum_{n=0}^{+\infty} q^n.$$

En égalisant les deux expressions, il vient :

$$\frac{1}{z} + \sum_{m=1}^{+\infty} \left(\frac{1}{z+m} + \frac{1}{z-m} \right) = i\pi - 2i\pi \sum_{n=0}^{+\infty} q^n.$$

En dérivant successivement cette formule, on obtient, pour tout $k \geq 2$,

$$\sum_{m \in \mathbb{Z}} \frac{1}{(z+m)^k} = \frac{-1}{(k-1)!} (2i\pi)^k \sum_{n=1}^{\infty} n^{k-1} q^n.$$

Il suffit à présent de développer G_{2k} et d'appliquer la formule que l'on vient de démontrer :

$$\begin{aligned}
G_{2k}(\tau) &= \sum_{(m,n) \in (\mathbb{Z}^2)^*} \frac{1}{(m\tau+n)^{2k}} \\
&= 2\zeta(2k) + 2 \sum_{n=1}^{+\infty} \sum_{m \in \mathbb{Z}} \frac{1}{(m\tau+n)^{2k}} \\
&= 2\zeta(2k) + \frac{-2(2i\pi)^{2k}}{(2k-1)!} \sum_{n=1}^{+\infty} \sum_{l=1}^{\infty} n^{2k-1} q^{ln} \\
&= 2\zeta(2k) + \frac{-2(2i\pi)^{2k}}{(2k-1)!} \sum_{n=1}^{+\infty} n^{2k-1} \frac{q^n}{1-q^n} \\
&= 2\zeta(2k) \left(1 + \frac{4k(-1)^k}{B_{2k}} \sum_{n=1}^{+\infty} n^{2k-1} \frac{q^n}{1-q^n} \right).
\end{aligned}$$

□

Remarque 1.3.9. *La convergence de E_2 permet de poser $G_2 = 2\zeta(2) E_2$, ce qui étend la définition de G_{2k} à tout $k \geq 1$.*

Notation. *On note $g_2 = 60G_4$ et $g_3 = 140G_3$. On emploiera de plus les notations de Ramanujan : les fonction P, Q et R désigneront respectivement les séries E_2, E_4 et E_6.*

A l'aide de la définition 1.3.6 et de la remarque 1.3.7, on obtient les formules suivantes :

$$P(z) = E_2(z) = 1 - 24 \sum_{n=1}^{+\infty} \frac{nz^n}{1-z^n} = 1 - 24 \sum_{n=1}^{+\infty} \sigma_1(n) z^n$$

$$Q(z) = E_4(z) = 1 + 240 \sum_{n=1}^{+\infty} \frac{n^3 z^n}{1-z^n} = 1 + 240 \sum_{n=1}^{+\infty} \sigma_3(n) z^n$$

$$R(z) = E_6(z) = 1 - 540 \sum_{n=1}^{+\infty} \frac{n^5 z^n}{1-z^n} = 1 - 540 \sum_{n=1}^{+\infty} \sigma_5(n) z^n$$

En remarquant par ailleurs que $g_2(\infty) = 120\zeta(4)$ et que $g_3(\infty) = 280\zeta(6)$, les valeurs connues $\zeta(4) = \frac{\pi^4}{90}$ et $\zeta(6) = \frac{\pi^6}{945}$ permettent d'écrire

$$g_2(\infty) = \frac{4}{3}\pi^4 \text{ et } g_3(\infty) = \frac{8}{27}\pi^6.$$

On définit alors la fonction Δ en posant

$$\boxed{\Delta = \frac{g_2^3 - 27g_3^2}{(2\pi)^{12}}}$$

Il résulte de cette définition que $\Delta(\infty) = 0$, l'ordre d'annulation étant de plus simple ; Δ est donc une forme parabolique de poids 12. On peut en fait montrer que

$$\Delta = q\prod_{n=1}^{+\infty}(1-q^n)^{24}.$$

Certaines propriétés de la fonction Δ demeurent encore inconnues. Mentionnons par exemple la conjecture suivante, due à Lehmer :

Conjecture 1.3.10 (Lehmer)**.** *Soit le développement de Δ en série entière de q :*

$$\Delta = \sum_{n=1}^{\infty}\tau(n)\,q^n,$$

τ ainsi défini étant la fonction de Ramanujan*. Alors*

$$\forall n \geq 1, \quad \tau(n) \neq 0.$$

Démontrons à présent un premier résultat qui contribuera à établir un dictionnaire entre la théorie des fonctions modulaires et celle des fonctions elliptiques.

Si Ω désigne encore un réseau complexe $\mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$,

$$\begin{aligned} g_2(\Omega) &= \frac{60}{\omega_1^4}G_4\left(\frac{\omega_2}{\omega_1}\right) \\ &= \frac{120}{\omega_1^4}\zeta(4)\,E_4\left(\frac{\omega_2}{\omega_1}\right), \end{aligned}$$

d'où, connaissant la valeur de $\zeta(4)$,

$$\frac{1}{(2i\pi)^4}g_2(\Omega)\,\omega_1^4 = \frac{1}{12}\left(1 + 240\sum_{n=1}^{+\infty}\frac{n^3z^n}{1-z^n}\right).$$

De la même manière, on obtient :

$$\frac{1}{(2i\pi)^6}g_3(\Omega)\,\omega_1^6 = \frac{1}{216}\left(-1 + 540\sum_{n=1}^{+\infty}\frac{n^5z^n}{1-z^n}\right).$$

On a donc démontré le résultat suivant :

Proposition 1.3.11.

$$\begin{aligned} Q(q) &= \frac{3}{4}\left(\frac{\omega_1}{\pi}\right)^4 g_2(\Omega) \\ R(q) &= \frac{27}{8}\left(\frac{\omega_1}{\pi}\right)^6 g_3(\Omega) \end{aligned}$$

Le fait que P ne définisse pas une forme modulaire de poids 2 rend l'établissement d'une formule analogue la concernant plus compliquée. Cependant, P est « presque» une forme modulaire de poids 2, comme le montre la formule suivante, dont on trouvera mention dans [9] :

$$\forall \tau \in \mathfrak{H},\ P\left(e^{-2i\pi/\tau}\right) = \tau^2 P\left(e^{2i\pi\tau}\right) + \frac{6\tau}{i\pi}\cdot$$

On peut de ce fait exprimer $P(q)$ en fonction de ω_1, mais aussi de la pseudo-période associée, comme nous le verrons plus loin.

Terminons ce paragraphe en énonçant sans démonstration deux résultats classiques qui seront fondamentaux dans la démonstration de l'indépendance algébrique de π, e^π et $\Gamma(1/4)$. Le premier a été établi par Ramanujan en 1916 à la suite de la définition des fonctions P, Q et R :

Théorème 1.3.12 (Ramanujan, 1916)**.** *En introduisant l'opérateur $\Theta = q\frac{d}{dq} = \frac{1}{2i\pi}\frac{d}{d\tau}$, les fonctions P, Q et R vérifient le système d'équations différentielles*

$$\begin{cases} \Theta P = \frac{1}{12}\left(P^2 - Q\right) \\ \Theta Q = \frac{1}{3}\left(PQ - R\right) \\ \Theta R = \frac{1}{2}\left(PR - Q\right) \end{cases}$$

Démonstration. On pourra soit se référer à l'article [23] de Ramanujan lui-même, soit trouver une démonstration utilisant des outils plus sophistiqués dans [12], p. 159-162. □

Théorème 1.3.13 (Mahler)**.** *Les trois fonctions P, Q et R sont algébriquement indépendantes sur le corps $\mathbb{C}(z)$.*

Démonstration. On pourra consulter l'article [15] de Mahler, où sont également exposés des résultats plus généraux d'indépendance algébrique de fonctions. □

1.4 L'invariant modulaire

Définition 1.4.1. *L'invariant modulaire j est défini par*

$$\boxed{j = \frac{1728}{(2\pi)^{12}} \cdot \frac{g_2^3}{\Delta} = 1728\frac{g_2^3}{g_2^3 - 27g_3^2}}$$

Proposition 1.4.2. *La fonction j est une fonction modulaire de poids nul. De plus, elle est holomorphe sur $\mathfrak{H}$ et a un pôle simple à l'infini.*

Démonstration. La première assertion provient du fait que la fonction g_2 est modulaire de poids 4 et Δ modulaire de poids 12. Etant donné que g_2 est non nulle à l'infini, pour établir la seconde assertion, il suffit de montrer que Δ ne s'annule pas sur $\mathfrak{H}$. On peut, pour démontrer ce fait, faire appel à la théorie des courbes elliptiques, bien qu'il existe une démonstration utilisant des outils plus élémentaires. Les propos présentés ci-après seront repris dans la section 2.2.
La cubique projective d'équation $y^2 = 4x^3 - g_2 x - g_3$, où $g_2 = g_2(\Omega) = 60G_2(\Omega)$ et $g_3 = g_3(\Omega) = 140G_3(\Omega)$ (pour Ω réseau de $\mathbb{C}$) est isomorphe à la courbe elliptique $\mathbb{C}/\Omega$; en particulier, elle est non sigulière, donc Δ, qui est à un facteur numérique près le discriminant du polynôme $4X^3 - g_2 X - g_3$, est non nul. □

Le coefficient $1728 = 12^3$ a été introduit pour que l'invariant modulaire ait un résidu nul en l'infini. Plus précisément, en posant $q = e^{2i\pi\tau}$ pour $\tau \in \mathfrak{H}$, on a le développement suivant :

$$j(\tau) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + \sum_{n=3}^{+\infty} c(n)\, q^n,$$

où les $c(n)$ sont des entiers jouissant de remarquables proprités de divisibilité (cf.[26], p.147).

L'importance de l'invariant modulaire réside notamment dans le fait que l'on peut montrer que toute fonction modulaire de poids nul s'écrit comme fonction rationnelle de j (cf.[26], p.146). On peut également citer le résultat suivant, qui énonce en substance qu'un réseau est complètement caractérisé par son image par j :

Théorème 1.4.3. *Soit Γ et Λ deux réseaux de $\mathbb{C}$. Alors $j(\Gamma) = j(\Lambda)$ si, et seulement si, Γ et Λ sont des réseaux homothétiques.*

Démonstration. Ceci est démontré dans [11], chapitre 3, paragraphe 3. Le résultat découle précisément du fait que j établit par passage au quotient une bijection de $_G\backslash\mathfrak{H}$ sur $\mathbb{C}$. □

Nous serons amené à établir au fur et à mesure de l'exposé d'autres propriétés relatives à l'invariant modulaire.

2 Fonctions elliptiques

L'étude des principales fonctions elliptiques que sont les fonctions $\wp$, ζ et σ de Weierstrass permettra de peaufiner la correspondance entre le point de vue modulaire et le point de vue elliptique, correspondance déjà entrevue à la section précédente. Nous commençons par quelques généralités sur les fonctions elliptiques.

On fixe un réseau $\Omega = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ de $\mathbb{C}$.

2.1 Généralités

Définition 2.1.1. *Une* fonction elliptique *f (relativement au réseau Ω) est une fonction méromorphe sur $\mathbb{C}$ qui est Ω-périodique, i.e.*

$$\forall z \in \mathbb{C}, \quad \forall \omega \in \Omega, \quad f(z+\omega) = f(z).$$

Du fait de sa périodicité, f peut être vue comme une fonction définie sur $\mathbb{C}/\Omega$.

Remarque 2.1.2. *Toute fonction elliptique et holomorphe est constante.*
En effet, une fonction elliptique et holomorphe est bornée sur l'adhérence d'un parallélogramme fondamental, donc sur $\mathbb{C}$ tout entier par Ω-périodicité. Un théorème de Liouville permet alors de conclure.

Théorème 2.1.3. *Soit f une fonction elliptique non nulle. Si l'on considère un parallélogramme fondamental $P = (a, a+\omega_1, a+\omega_1+\omega_2, a+\omega_2)$ dont les bords ne contiennent ni les pôles ni les zéros de f (ce qui est possible puisque ces derniers sont isolés), alors le nombre de zéros de f dans P est égal au nombre de pôles de f dans P comptés avec multiplicité.*

Notation. *Pour une fonction elliptique f, on notera $\mathcal{Z}_f$ l'ensemble de ses zéros et $\mathcal{P}_f$ l'ensemble de ses pôles. On posera également $E_f = \mathcal{Z}_f \cup \mathcal{P}_f$. Enfin, ∂P désignera le bord d'un parallélogramme fondamental préalablement fixé.*

Démonstration. D'après le théorème des résidus, on a :

$$\begin{aligned}
|\mathcal{Z}_f| - |\mathcal{P}_f| &= \frac{1}{2i\pi}\int_{\partial P} \frac{f'(z)}{f(z)}dz \\
&= \frac{1}{2i\pi}\int_a^{a+\omega_1} \frac{f'(z)}{f(z)}dz + \frac{1}{2i\pi}\int_{a+\omega_1}^{a+\omega_1+\omega_2} \frac{f'(z)}{f(z)}dz \\
&\quad + \frac{1}{2i\pi}\int_{a+\omega_1+\omega_2}^{a+\omega_2} \frac{f'(z)}{f(z)}dz + \frac{1}{2i\pi}\int_{a+\omega_2}^{a} \frac{f'(z)}{f(z)}dz \\
&= \frac{1}{2i\pi}\int_a^{a+\omega_1} \left(\frac{f'(z)}{f(z)} - \frac{f'(z+\omega_2)}{f(z+\omega_2)}\right)dz \\
&\quad + \frac{1}{2i\pi}\int_{a+\omega_2}^{a} \left(\frac{f'(z)}{f(z)} - \frac{f'(z+\omega_1)}{f(z+\omega_1)}\right)dz \\
&= 0,
\end{aligned}$$

en invoquant la périodicité de f. □

Notation. *$\mathcal{M}(\mathbb{C}/\Omega)$ désignera l'ensemble des fonctions méromorphes sur la surface de Riemann $\mathbb{C}/\Omega$.*

Définition 2.1.4. *Le* diviseur *d'un élément $f \in \mathcal{M}(\mathbb{C}/\Omega)^*$ est la somme formelle à support fini*

$$\operatorname{div}(f) = \sum_{x \in \mathbb{C}/\Omega} \nu_x(f)\, x,$$

où $\nu_x(f)$ désigne l'ordre de f en x. Le degré du diviseur de f *est alors l'entier naturel*

$$\deg(\mathrm{div}(f)) = \sum_{x\in\mathbb{C}/\Omega} \nu_x(f).$$

Le théorème 2.1.3 revient donc à affirmer que, pour tout élément f de $\mathcal{M}(\mathbb{C}/\Omega)^*$, on a $\deg(\mathrm{div}(f))=0$.

Définition 2.1.5. *Le nombre de pôles (ou de zéros) d'une fonction elliptique f de réseau Ω contenus dans un parallélogramme fondamental est le* degré de f.

Lemme 2.1.6. *Soit f une fonctions elliptique. Alors*

$$\sum_{a\in E_f} \nu_a(f)\, a \in \Omega.$$

Démonstration. Soit P un parallélogramme fondamental $(\alpha_0, \alpha_0+\omega_1, \alpha_0+\omega_1+\omega_2, \alpha_0+\omega_2)$ dont le bord ne rencontre ni zéro ni pôle de f. On fixe une détermination du logarithme sur le bord ∂P de P, de sorte que l'on a :

$$\begin{aligned}
\sum_{a\in E_f} \nu_a(f)\, a &= \frac{1}{2i\pi}\int_{\partial P} z\frac{f'(z)}{f(z)}dz \\
&= \frac{1}{2i\pi}\int_{\alpha_0}^{\alpha_0+\omega_1}\left(z\frac{f'(z)}{f(z)} - (z+\omega_2)\frac{f'(z+\omega_2)}{f(z+\omega_2)}\right)dz \\
&\quad + \frac{1}{2i\pi}\int_{\alpha_0}^{\alpha_0+\omega_2}\left(-z\frac{f'(z)}{f(z)} + (z+\omega_1)\frac{f'(z+\omega_1)}{f(z+\omega_1)}\right)dz \\
&= -\frac{\omega_2}{2i\pi}\int_{\alpha_0}^{\alpha_0+\omega_1}\frac{f'(z)}{f(z)}dz + \frac{\omega_1}{2i\pi}\int_{\alpha_0}^{\alpha_0+\omega_2}\frac{f'(z)}{f(z)}dz \\
&= \omega_2\underbrace{\left(\frac{-\log f(\alpha_0+\omega_1)+\log f(\alpha_0)}{2i\pi}\right)}_{\in\mathbb{Z}} + \omega_1\underbrace{\left(\frac{\log f(\alpha_0+\omega_2)-\log f(\alpha_0)}{2i\pi}\right)}_{\in\mathbb{Z}},
\end{aligned}$$

donc $\sum_{a\in E_f}\nu_a(f)\,a \in \Omega$. □

Voici enfin un résultat qui vient conclure ce paragraphe et qui nous sera utile dans le suivant :

Lemme 2.1.7. *Si f est elliptique de degré au plus* 1*, alors f est constante.*

Démonstration. Si f n'est pas constante, alors elle a un unique zéro a dans $\mathbb{C}/\Omega$, qui est simple, et donc un unique pôle b. D'après le lemme 2.1.6, $a-b\in\Omega$, donc a et b sont à la fois pôles et zéros de f, ce qui est absurde et achève la preuve. □

2.2 La fonction elliptique $\wp$ de Weierstrass

Théorème 2.2.1. *Il existe une unique fonction elliptique (relativement à Ω) de degré ≤ 2, ayant un pôle double en zéro et pas d'autres pôles, et de développement de Laurent en zéro égal à $\frac{1}{z^2}+O(z)$. On note cette fonction $\wp_\Omega$. Elle est de plus paire.*

Démonstration. On procède en trois temps :

Unicité : Si f et g sont deux fonction elliptiques de degré ≤ 2 vérifiant au voisinage de 0 $f \underset{0}{\sim} g \underset{0}{\sim} \frac{1}{z^2}$, alors $f-g$ est constante. En effet, cette dernière fonction est elliptique, sans pôle en dehors de zéro (car elle est de degré ≤ 2 et a un pôle d'ordre 2 en zéro), et vérifie $f-g=O(z)$ au voisinage de zéro. On en déduit qu'elle est de degré ≤ 1 et donc constante d'après le lemme 2.1.7. De plus, par hypothèse, le terme constant de son développement de Laurent en zéro est nul, ce qui entraîne la nullité de la constante.

Existence : On définit, pour $z \in \mathbb{C}$,

$$\boxed{\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Omega^*} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)}$$

Si z est dans un compact et ω suffisamment grand, on a :

$$\left| \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right| \leq \left| \frac{-2\omega z + z^2}{\omega^2 (\omega - z)^2} \right| = O\left(\frac{1}{\omega^3} \right).$$

Le lemme 1.3.1 donne alors la convergence uniforme sur tout compact. Montrons que $\wp$ est elliptique. Soit $z \in \mathbb{C}$ et $\omega_0 \in \Omega$:

$$\wp'(z) = \sum_{\omega \in \Omega} \frac{-2}{(z-\omega)^3},$$

d'où l'on déduit que $\wp'(z+\omega_0) = \wp'(z)$ puis $\wp(z+\omega_0) - \wp(z) = a_0$, avec a_0 dépendant *a priori* de ω_0. De même, $a_0 = \wp((-z-\omega_0)+\omega_0) - \wp(-z-\omega_0) = \wp(z) - \wp(z+\omega_0) = -a_0$ par parité de $\wp$, d'où $a_0 = 0$. De plus, on a $\left(\wp(z) - \frac{1}{z^2}\right)_{|z=0} = 0$, donc le développement de $\wp$ en zéro a bien la forme souhaitée. Finalement, $\wp$ est de degré 2 car ses pôles sont dans Ω et zéro est un pôle d'ordre 2.

Parité : $\wp$ comme précédemment construite est l'unique solution au problème et est paire. On peut aussi remarquer que, si f elliptique vérifie les conditions du théorème, alors la fonction $z \mapsto f(-z)$ aussi, donc, par unicité, f est paire.

□

Définition 2.2.2. *La fonction $\wp_\Omega$ (souvent notée $\wp$ s'il n'y a pas d'ambiguïté) est la* fonction de Weierstrass du réseau Ω.

Proposition 2.2.3. *Pour tout $z \in \mathbb{C}$, la relation suivante est vérifiée :*

$$\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{+\infty} (2n+1) G_{2n+2} z^{2n}.$$

Démonstration. On rappelle tout d'abord que, pour tout $k \geq 2$,

$$G_{2k} = \sum_{\omega \in \Omega} \frac{1}{\omega^{2k}}.$$

Soit $z \in \mathbb{C} \backslash \Omega$ et $\omega \in \Omega$:

$$\begin{aligned} \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} &= \frac{1}{\omega^2} \left(\frac{1}{\left(1 - \frac{z}{\omega}\right)^2} - 1 \right) \\ &= \sum_{k=1}^{+\infty} \frac{k+1}{\omega^{k+2}} z^k. \end{aligned}$$

Dès lors :

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Omega^*} \sum_{k=1}^{+\infty} \frac{k+1}{\omega^{k+2}} z^k.$$

L'absolue convergence de cette série double permet d'intervertir les sommations. La parité de $\wp$ permet alors de conclure :

$$\wp(z) = \frac{1}{z^2} + 3G_4 z^2 + 5G_6 z^4 + \cdots + (2n+1) G_{2n+2} z^{2n} + \ldots$$

□

La fonction $\wp$ vérifie une équation différentielle du premier ordre fondamentale en ce sens qu'elle détermine bon nombre de ses propriétés. Si g_2 et g_3 sont les invariants du réseau Ω définis à la section 1.3, on a en effet la proposition qui suit :

Proposition 2.2.4. *Pour tout $z \in \mathbb{C}$, l'égalité suivante est vérifiée :*

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3.$$

Démonstration. Rappelons que $g_2 = 60G_4$ et $g_3 = 140G_6$. On a :

$$\begin{aligned}
\wp(z) &= \frac{1}{z^2} + 3G_4 z^2 + 5G_6 z^4 + o\big(z^4\big), \\
\wp(z)^3 &= \frac{1}{z^6} + 9G_4\frac{1}{z^2} + 15G_6 + O\big(z^2\big), \\
\wp'(z) &= \frac{-2}{z^3} + 6G_4 z + 20G_6 z^3 + o\big(z^3\big), \\
\wp'(z)^2 &= \frac{4}{z^6} - 24G_4\frac{1}{z^2} - 80G_6 + O\big(z^2\big),
\end{aligned}$$

et donc

$$\begin{aligned}
\wp'(z)^2 - 4\wp(z)^3 &= -60G_4\frac{1}{z^2} - 140G_6 + O\big(z^2\big) \\
&= -60G_4\wp(z) - 140G_6 + O\big(z^2\big).
\end{aligned}$$

On en déduit que la fonction différence est elliptique et holomorphe (puisque $O\big(z^2\big)$ désigne une fonction dont le développement de Laurent commence avec un terme en z^2), donc constante puis nulle (car en $O\big(z^2\big)$ en l'origine). □

Proposition 2.2.5. *Modulo Ω, la fonction $\wp'$ a trois zéros simples en $\frac{\omega_1}{2}$, $\frac{\omega_2}{2}$ et $\frac{\omega_3}{2}$, où $\omega_3 = \frac{\omega_1+\omega_2}{2}$. En outre, les points $e_1 = \wp\left(\frac{\omega_1}{2}\right)$, $e_2 = \wp\left(\frac{\omega_2}{2}\right)$ et $e_3 = \wp\left(\frac{\omega_3}{2}\right)$ sont deux à deux distincts et la fonction $\wp$ vérifie l'équation différentielle*

$$\wp'(z)^2 = 4\left(\wp(z) - e_1\right)\left(\wp(z) - e_2\right)\left(\wp(z) - e_3\right). \tag{1}$$

Démonstration. En tenant compte du fait que la fonction $\wp'$ est impaire et qu'elle est doublement périodique, on obtient, pour $k = 1, 2$:

$$\begin{aligned}
\wp'\left(\frac{\omega_k}{2}\right) &= -\wp'\left(-\frac{\omega_k}{2}\right) \\
&= -\wp'\left(-\frac{\omega_k}{2} + \omega_k\right) \\
&= -\wp'\left(\frac{\omega_k}{2}\right),
\end{aligned}$$

d'où $\wp'\left(\frac{\omega_k}{2}\right) = 0$. De la même manière, on a :

$$\begin{aligned}
\wp'\left(\frac{\omega_1+\omega_2}{2}\right) &= -\wp'\left(-\frac{\omega_1+\omega_2}{2}\right) \\
&= -\wp'\left(-\frac{\omega_1+\omega_2}{2} + \omega_1 + \omega_2\right) \\
&= -\wp'\left(\frac{\omega_1+\omega_2}{2}\right),
\end{aligned}$$

d'où $\wp'\left(\frac{\omega_1+\omega_2}{2}\right) = 0$.

Pour montrer que e_1, e_2 et e_3 sont deux à deux distincts, on remarque tout d'abord que la fonction $\wp(z) - e_j$ $(j = 1, 2, 3)$ est de degré 2 comme $\wp$ (ses pôles sont ceux de $\wp$). Or, les relations $\wp\left(\frac{\omega_j}{2}\right) - e_j = 0$ et $\wp'\left(\frac{\omega_j}{2}\right) = 0$ impliquent que le $\frac{\omega_j}{2}$ est un pôle double pour $\wp(z) - e_j$. Si l'on

avait $e_j = e_k$ pour $j \neq k$ dans $\{1,2,3\}$, alors le degré de $\wp(z) - e_j$ serait strictement supérieur à 2.

La dernière assertion résulte quand à elle du fait que les deux membres de l'égalité 1 définissent des fonctions méromorphes qui ont, d'après ce qui précède, les mêmes diviseurs. Ils diffèrent donc d'une constante multiplicative qui peut être déterminée en faisant tendre les deux termes vers 0 : comme $\wp'(z)^2 \underset{0}{\sim} \left(\frac{-2}{z^2}\right)^2$ et que le second membre est équivalent en 0 à $4\left(\frac{1}{z^2}\right)^3$, la constante vaut 1. □

Remarque 2.2.6. *La démonstration montre en particulier que, d'une part,*

$$\operatorname{div}(\wp'(z)) = \left(\frac{\omega_1}{2}\right) + \left(\frac{\omega_2}{2}\right) + \left(\frac{\omega_3}{2}\right) - 3(0)$$

et que, d'autre part, pour $j = 1,2,3$,

$$\operatorname{div}\left(\wp(z) - \wp\left(\frac{\omega_j}{2}\right)\right) = 2\left(\frac{\omega_j}{2}\right) - 2(0).$$

On déduit alors des propositions 2.2.4 et 2.2.5 que e_1, e_2 et e_3 sont les racines distinctes du polynôme $4X^3 - g_2X - g_3$. Le discriminant de ce polynôme est donc non nul, ce qui est exactement traduit par le fait que, comme mentionné à la section 1,

$$g_2^3 - 27g_3^2 \neq 0.$$

Donnons une réciproque partielle à ce résultat, démontrée dans [11] (corollaire 2, p.39) :

Théorème 2.2.7. *Soit c_2 et c_3 des nombres complexes tels que $c_2^3 - 27c_3^2 \neq 0$. Alors il existe un réseau complexe Ω tel que $c_2 = g_2(\Omega)$ et $c_3 = g_3(\Omega)$.*

De plus, g_2 et g_3 caractérisent le réseau (à homothétie près). Ceci est une conséquence du théorème 1.4.3.

Le théorème 2.2.7 est le premier pas vers la paramétrisation de l'espace des modules des courbes elliptiques complexes à l'aide des fonctions $\wp$ de Weierstrass, paramétrisation établissant une correspondance univoque entre courbes elliptiques sur $\mathbb{C}$ et réseaux complexes. Cette correspondance, qui est en fait un isomorphisme de groupes abéliens, permet de très aisément démontrer, par transport de structure, les formules d'addition pour la fonction $\wp$ que nous mentionnons ici simplement en renvoyant à [11], p.12 pour une preuve détaillée.

Proposition 2.2.8 (Formule d'addition pour la fonction $\wp$)**.** *Soit $u_1, u_2 \in \mathbb{C}/\Omega$ tels que $u_1 \not\equiv \pm u_2$ modulo Ω. Alors*

$$\wp(u_1 + u_2) = \frac{1}{4}\left(\frac{\wp'(u_2) - \wp'(u_1)}{\wp(u_2) - \wp(u_1)}\right)^2 - \wp(u_1) - \wp(u_2).$$

Par passage à la limite lorsque u_1 tend vers u_2 et à l'aide de l'équation différentielle vérifiée par $\wp$, on obtient une formule de duplication :

Corollaire 2.2.9 (Formule de duplication pour la fonction $\wp$)**.** *Soit $u \in \mathbb{C}/\Omega$ tels que $2u \notin \mathbb{C}/\Omega$. Alors*

$$\wp(2u) = \frac{\left(3\wp(u)^2 - \frac{g_2}{4}\right)^2}{4\wp(u)^3 - g_2\wp(u) - g_3} - 2\wp(u).$$

La formule de duplication est un cas particulier d'un résultat plus général dont on trouvera la preuve dans [8], p.209 :

Proposition 2.2.10 (Formule de multiplication pour la fonction $\wp$)**.** *Pour tout $n \in \mathbb{N}^*$, $\wp(nz)$ est une fraction rationnelle de $\wp(z)$ à coefficients dans $\mathbb{Q}(g_2, g_3)$.*

Toutes ces formules seront d'un grand secours dans la section 7.2.

En sus du dictionnaire établi entre courbes elliptiques et réseaux complexes, l'importance de la fonction $\wp$ réside dans le fait qu'elle constitue en quelque sorte la fonction elliptique «de base», en un sens précisé par le théorème qui suit :

Théorème 2.2.11. *Le corps des fonctions elliptiques (par rapport au réseau Ω) est engendré par $\wp$ et $\wp'$.*

Démonstration. Si f est une fonction elliptique, on peut l'écrire comme somme d'une fonction elliptique paire et d'une fonction elliptique impaire en la décomposant sous la forme

$$f(z) = \frac{f(z) + f(-z)}{2} + \frac{f(z) - f(-z)}{2}.$$

Or si f est impaire, $\frac{f}{\wp'}$ est paire : il suffit donc de prouver que, si f est paire, alors f est une fonction rationnelle de $\wp$.

Lemme 2.2.12. *Soit f une fonction elliptique paire. Il existe alors $Q \in \mathbb{C}(X)$ tel que $f = Q(\wp)$.*

Démonstration. On considère les ensembles $\mathcal{Z}_f$ et $\mathcal{P}_f$ modulo Ω. Supposons dans un premier temps que f n'admette ni zéro ni pôle en l'origine. Comme f est paire, $\mathcal{Z}_f$ et $\mathcal{P}_f$ sont invariants par $z \mapsto -z$ modulo Ω. Il s'ensuit que $\operatorname{div}(f)$ est une somme formelle à support fini de la forme

$$\operatorname{div}(f) = \sum_{\substack{a \in \mathbb{C}/\Omega \\ a \neq 0}} m_a \left((a) + (-a) - 2(0) \right),$$

où les coefficients m_a sont entiers. Or on montre de la même manière que dans la preuve de la proposition 2.2.5 que l'on a, plus généralement,

$$\forall a \in (\mathbb{C}/\Omega)^*, \operatorname{div}(\wp(z) - \wp(a)) = (a) + (-a) - 2(0).$$

Par conséquent, f et le produit

$$\prod_{a \in (\mathbb{C}/\Omega)^*} (\wp(z) - \wp(a))^{m_a}$$

ont même diviseur, donc diffèrent d'une constante multiplicative.

Dans le cas où f admet un pôle ou un zéro en l'origine, il suffit d'appliquer le raisonnement précédent au produit $g = f\wp^n$ pour n entier choisi de telle sorte que g, qui est encore une fonction elliptique paire, n'ait ni pôle ni zéro en l'origine. □

Le théorème 2.2.11 est ainsi entièrement démontré. □

Nous terminons ce paragraphe par l'étude des variations de la fonction $\wp$ restreinte à un intervalle réel : ceci nous permettra de justifier par la suite plusieurs changement de variable.

Proposition 2.2.13. *Soit $\Omega = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ un réseau complexe tel que ω_1 soit réel. On dispose alors du tableau de variations suivant :*

t	0^+		$\frac{\omega_1}{2}$		ω_1
$\wp'(t)$		$-$	0	$+$	
$\wp(t)$	$+\infty$	↘	e_1	↗	$+\infty$

Démonstration. On a $\wp'(z) \underset{0}{\sim} \frac{-2}{z^3}$. La fonction $\wp'$ est donc strictement négative dans un voisinage réel de 0^+. Sur l'intervalle $]0;\omega_1[$, elle ne s'annule qu'en $\frac{\omega_1}{2}$ qui est de plus un zéro simple. D'où le signe de $\wp'$ dans cet intervalle. Les limites aux bornes de l'intervalle résultent du fait que ces bornes sont des pôles pour $\wp$. □

En remarquant que, pour tout $\lambda \in \mathbb{C}^*$, $\wp_\Omega = \lambda^2 \wp_{\lambda\Omega}$, on obtient une variante de la proposition précédente :

Corollaire 2.2.14. *Soit $\Omega = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ un réseau complexe tel que ω_2 soit imaginaire pur. Alors la fonction $s \mapsto \wp(is)$ est à valeurs réelles sur $]0; -i\omega_2[$ et l'on dispose du tableau de variations suivant :*

s	0^+		$-\frac{i\omega_2}{2}$		$-i\omega_2$
$\wp'(is)$		$+$	0	$-$	
$\wp(is)$	$-\infty$	↗	e_2	↘	$-\infty$

2.3 La fonction ζ de Weierstrass

Définition 2.3.1. *La* fonction ζ de Weierstrass *est définie par :*

$$\begin{cases} \zeta' = -\wp \\ \lim\limits_{z\to 0} \left(\zeta(z) - z^{-1}\right) = 0 \end{cases}$$

D'après l'expression de définition de la fonction $\wp$ (cf. démonstration du théorème 2.2.1), on a donc

$$\boxed{\zeta(z) = \frac{1}{z} + \sum_{\omega\in\Omega^*} \left(\frac{1}{z-\omega} + \frac{1}{\omega} + \frac{z}{\omega^2}\right)}$$

Par la proposition 2.2.3, on a également :

$$\zeta(z) = \frac{1}{z} - \sum_{n=1}^{+\infty} G_{2n+2} z^{2n+1}.$$

ζ apparaît ainsi comme une fonction impaire pour laquelle la périodicité de $\wp$ assure l'existence de *quasi-périodes* η_1 et η_2 telles que, pour tout $z \in \mathbb{C}\backslash\Omega$,

$$\begin{aligned} \zeta(z+\omega_1) &= \zeta(z) + \eta_1, \\ \zeta(z+\omega_2) &= \zeta(z) + \eta_2. \end{aligned}$$

L'évaluation de ces relations respectivement en $\frac{-\omega_1}{2}$ et en $\frac{-\omega_2}{2}$ ainsi que l'imparité de ζ donnent $\eta_1 = \frac{1}{2}\zeta\left(\frac{\omega_1}{2}\right)$ et $\eta_2 = \frac{1}{2}\zeta\left(\frac{\omega_2}{2}\right)$.

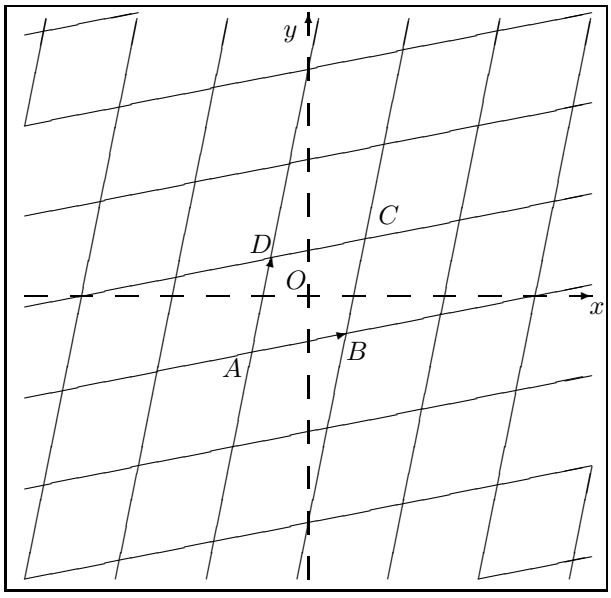
Remarque 2.3.2. *Les coefficients du développement de ζ, tout comme ceux du développement de $\wp$, sont dans $\mathbb{Q}(g_2, g_3)$.*
En effet, pour tout $k \geq 4$, G_{2k} s'écrit comme une fraction rationnelle en g_2 et g_3 à coefficients dans $\mathbb{Q}$. Ceci se voit facilement en remplaçant les développements de $\wp$ et $\wp'$ dans l'équation différentielle vérifiée par $\wp$ et en identifiant.

Le théorème de Legendre fournit une relation entre les périodes et quasi-périodes :

Théorème 2.3.3 (Legendre)**.** *Si (ω_1, ω_2) est une base du réseau associé à la fonction $\wp$ de Weierstrass, base choisie de telle sorte que $\tau = \frac{\omega_2}{\omega_1} \in \mathfrak{H}$, alors on a la relation :*

$$\eta_1\omega_2 - \eta_2\omega_1 = 2i\pi.$$

Démonstration. Soit un parallélogramme fondamental du réseau de sommets A, B, C et D tel que l'origine soit en son centre.



En remarquant que ζ a un pôle de résidu 1 en l'origine, le théorème des résidus permet d'écrire que

$$\int_{ABCD} \zeta(z)dz = 2i\pi.$$

D'autre part, les relations de quasi-périodicité donnent

$$\int_{CD} \zeta(z)dz = \int_{BA} \zeta(z+\omega_2)dz = \int_{BA} \zeta(z)dz + \int_{BA} \eta_2 dz = \int_{BA} \zeta(z)dz - \eta_2\omega_1,$$

d'où

$$\int_{AB} \zeta(z)dz + \int_{CD} \zeta(z)dz = -\eta_2\omega_1.$$

On montre de même que

$$\int_{BC} \zeta(z)dz + \int_{DA} \zeta(z)dz = \eta_1\omega_2,$$

ce qui fournit la relation recherchée. □

2.4 Le produit canonique σ de Weierstrass

Définition 2.4.1. *La* fonction σ de Weierstrass*, dite aussi* produit canonique de Weierstrass*, est définie par :*

$$\begin{cases} \frac{\sigma'}{\sigma} = \zeta \\ \lim\limits_{z\to 0} \frac{\sigma(z)}{z} = 1 \end{cases}$$

La première expression de ζ suivant la définition 2.3.1 permet alors de définir explicitement la fonction σ comme étant le produit

$$\boxed{\sigma(z) = z \prod_{\omega\in\Omega^*} \left(1 - \frac{z}{\omega}\right) e^{\frac{z}{\omega} + \frac{1}{2}\left(\frac{z}{\omega}\right)^2}}$$

La fonction σ apparaît ainsi comme étant une fonction impaire admettant un pôle simple en chaque point du réseau Ω.

La relation de quasi-périodicité vérifiée par la fonction ζ admet naturellement un équivalent pour la fonction σ.

Notation. *Nous désignons par ω l'une quelconque des périodes fondamentales du réseau Ω et $\eta(\omega)$ (parfois simplement notée η) sera la quasi-période associée.*

Proposition 2.4.2. *Avec les notations ci-dessus,*

$$\forall z \in \mathbb{C}, \quad \sigma(z+\omega) = -\sigma(z)e^{\eta\left(z+\frac{\omega}{2}\right)}.$$

Démonstration. Par définition de σ et par quasi-périodicité de ζ, pout tout $z \in \mathbb{C}\backslash\Omega$,

$$\frac{d}{dz}\ln\left(\frac{\sigma(z+\omega)}{\sigma(z)}\right) = \eta(\omega),$$

d'où l'existence d'une constante $c(\omega)$ telle que

$$\ln\left(\frac{\sigma(z+\omega)}{\sigma(z)}\right) = \eta(\omega)z + c(\omega).$$

En prenant l'exponentielle de chacun des termes de cette égalité et en posant $\Psi(\omega) = e^{c(\omega)-\eta(\omega)\frac{\omega}{2}}$, on obtient

$$\sigma(z+\omega) = \sigma(z)e^{\eta(\omega)z+c(\omega)} = \Psi(\omega)e^{\eta\left(z+\frac{\omega}{2}\right)}.$$

Comme ω est une période fondamentale du réseau Ω, $\frac{\omega}{2} \notin \Omega$ et la première égalité évaluée en $z = \frac{-\omega}{2}$ donne immédiatement $\Psi(\omega) = -1$ par imparité de σ. □

Comme pour la fonction $\wp$, nous établissons à présent des formules d'addition (en fait de conjugaison) et de duplication pour la fonction σ qui nous seront utiles dans la section 7.2. Elles font intervenir la fonction $\wp$:

Proposition 2.4.3 (Formule de conjugaison pour le produit canonique de Weierstrass)**.**

$$\forall z, a \in \mathbb{C}\backslash\Omega, \quad \frac{\sigma(z+a)\sigma(z-a)}{\sigma(z)^2\sigma(a)^2} = \wp(a) - \wp(z).$$

Démonstration. On travaille à $a \in \mathbb{C}\backslash\Omega$ fixé. Comme rappelé dans la démonstration du lemme 2.2.12,

$$\operatorname{div}\left(\wp(z) - \wp(a)\right) = (a) + (-a) - 2(0),$$

qui correspond exactement au diviseur de la fonction

$$\frac{\sigma(z+a)\sigma(z-a)}{\sigma(z)^2}$$

d'après les propos qui suivent la définition 2.4.1. Les deux fonctions diffèrent donc d'une constante multiplcative C_a qui se détermine en multipliant les deux membres de l'égalité

$$\wp(z) - \wp(a) = C_a\frac{\sigma(z+a)\sigma(z-a)}{\sigma(z)^2}$$

par z^2 et en faisant tendre $z \to 0$: comme $\frac{\sigma^2(z)}{z^2} \to 1$ et $z^2\wp(z) \to 1$, il vient $C_a = \frac{-1}{\sigma^2(a)}$, ce qui prouve le résultat. □

Corollaire 2.4.4 (Formule de duplication pour le produit canonique de Weierstrass)**.**

$$\forall z \in \mathbb{C}\backslash\Omega, \quad \sigma(2z) = -\wp'(z)\sigma(z)^4.$$

Démonstration. Pour $a, z \in \mathbb{C}\backslash\Omega$, la formule de conjugaison permet d'écrire :

$$\frac{\sigma(z+a)}{\sigma(z)^2\sigma(a)^2} = \frac{\wp(a)-\wp(z)}{z-a}\cdot\frac{z-a}{\sigma(z-a)}.$$

On obtient le résultat voulu lorsque a tend vers z, d'après la seconde propriété définissant σ (définition 2.4.1). □

2.5 Multiplication complexe

On s'intéresse à l'ensemble des $\alpha \in \mathbb{C}$ tels que $\alpha\Omega \subset \Omega$; ces nombres complexes induisent exactement les endormorphismes du tore $\mathbb{C}/\Omega$. Un tel endomorphisme est dit trivial s'il est induit par un entier.

Notation. *En identifiant les endomorphismes du tore $\mathbb{C}/\Omega$ et les nombres complexes laissant invariant le réseau Ω, on notera*

$$\mathrm{End}\,(\mathbb{C}/\Omega) = \{\alpha \in \mathbb{C}/\alpha\Omega \subset \Omega\}$$

Définition 2.5.1. *Le réseau Ω est à* multiplication complexe *s'il existe $\alpha \in \mathbb{C}\backslash\mathbb{Z}$ tel que $\alpha\Omega \subset \Omega$.*

D'après le dictionnaire existant entre courbes elliptiques sur $\mathbb{C}$ et réseaux complexes, une courbe elliptique sera dite à multiplication complexe si le réseau auquel elle est attachée est à multiplication complexe.

La situation est résumée dans la proposition suivante :

Proposition 2.5.2. *Soit (ω_1, ω_2) une base de Ω telle que $\tau = \frac{\omega_1}{\omega_2} \in \mathfrak{H}$. Alors :*

$$\mathrm{End}\,(\mathbb{C}/\Omega) = \mathrm{End}\left(\mathbb{C}/(\mathbb{Z} \oplus \mathbb{Z}\tau)\right) = \begin{cases} \mathbb{Z} & si\ [\mathbb{Q}(\tau) : \mathbb{Q}] > 2 \\ \mathcal{O} = \mathbb{Z}a\tau + \mathbb{Z} & si \begin{cases} a\tau^2 + b\tau + c = 0 \\ a, b, c \in \mathbb{Z}, a > 0 \\ (a, b, c) = 1 \end{cases} \end{cases}$$

En particulier, dans le second cas, $\mathcal{O}$ est un ordre dans $\mathbb{Q}(\tau) = \mathbb{Q}\left(\sqrt{b^2 - 4ac}\right)$.

Dans le cas où Ω est à multiplication complexe, on dit parfois que $\mathbb{Q}(\tau)$ est le *corps de multiplication complexe* de Ω.

Démonstration. La première égalité est évidente, de sorte que l'on peut se restreindre, sans perte de généralité, au cas où $\Omega = \mathbb{Z} \oplus \mathbb{Z}\tau$ avec $\tau \in \mathfrak{H}$. Il est de plus clair que $\mathbb{Z} \subset \mathrm{End}\,(\mathbb{C}/\Omega)$.

Supposons qu'il existe $\lambda \in (\mathrm{End}\,(\mathbb{C}/\Omega)\setminus\mathbb{Z})$: la condition $\lambda\Omega \subset \Omega$ assure l'existence de A, B, C et $D \in \mathbb{Z}$, $A \neq 0$, tels que

$$\begin{cases} \lambda.1 = A\tau + B \\ \lambda\tau = C\tau + D \end{cases}$$

On en déduit que $A\tau^2 + (B - C)\tau - D = 0 \qquad (1)$.
Quitte à diviser par $\pm d = \pm\mathrm{pgcd}(A, B - C, D)$, on obtient l'existence de a, b et $c \in \mathbb{Z}$ premiers entre eux tels que $a > 0$ et $a\tau^2 + b\tau + c = 0 \qquad (2)$.

Reste alors à montrer que, pour $\lambda \in \mathbb{C}\backslash\mathbb{Z}$, $\lambda\Omega \subset \Omega$ si, et seulement si, $a|A$, i.e. si, et seulement si, $\lambda \in \mathbb{Z}a\tau + \mathbb{Z}$ en adoptant les notations précédentes.

Pour l'implication directe, en écrivant $\lambda.1 = A\tau + B$ avec A, $B \in \mathbb{Z}$, $A \neq 0$, et en remarquant que l'on passe de l'égalité (1) à l'égalité (2) en multipliant par $\pm d$, on a, au signe près, $A = ad$, donc $\lambda = da\tau + B \in \mathbb{Z}a\tau + \mathbb{Z}$.

Pour la réciproque, $\lambda\Omega$ sera inclus dans Ω dès lors que $a\tau\Omega$ sera inclus dans $\Omega = \mathbb{Z} + \mathbb{Z}\tau$. Ceci découle du fait que

$$\begin{cases} a\tau.1 = a\tau \in \Omega \\ a\tau.\tau = a\tau^2 = -b\tau - c \in \Omega \end{cases}$$

□

3 Le théorème stéphanois

Nous présentons dans cette section un théorème établi en 1995 par une équipe stéphanoise : K.Barré-Siriex, G.Diaz, F.Gramain et G.Philibert dans [2]. Répondant à une conjecture formulée par Mahler et Manin, il est le résultat dont la démonstration a inspiré Y.V.Nesterenko en vue de la preuve de son propre théorème, étudié à la section 6.

Avant d'en formuler le contenu, nous introduisons quelques résultats préliminaires dont les énoncés et/ou les preuves font intervenir des idées récurrentes en théorie des nombres transcendants.

3.1 Résultats préliminaires

Définition 3.1.1. *La* fonction J *est définie par* $j(\tau) = J(e^{2i\pi\tau})$ *pour tout* $\tau \in \mathfrak{H}$.

Il découle de la définition 1.4.1 de l'invariant modulaire et de la proposition 1.3.11 que l'on a

$$\boxed{J = \frac{1}{1728}\left(Q^3 - R^2\right)}$$

On peut associer à la fonction J une famille de polynômes à deux variables jouissant de propriétés fondamentales en vue de la démonstration du théorème stéphanois :

Proposition 3.1.2. *Pour tout entier* $n \geq 2$*, il existe un polynôme irréductible* $\Phi_n \in \mathbb{Z}[X, Y]$ *tel que, pour tout* $z \in \mathbb{C}^*$ *de module* < 1*, on ait* $\Phi_n\left(J(z), J(z^n)\right) = 0$.

Ce polynôme, appelé polynôme modulaire d'ordre n*, est symétrique en* X *et en* Y*, son coefficient dominant en l'indéterminée* X *(ou* Y*) est 1 et son degré partiel par rapport à chacune des variables est*

$$\psi(n) = n \prod_{\substack{p|n \\ p\in\mathcal{P}}} \left(1 + \frac{1}{p}\right).$$

De plus, il existe une constante réelle $c > 0$ *telle que la somme des valeurs absolues des coefficients du polynôme* Φ_n *soit inférieure ou égale à* e^{cn^2}.

Démonstration. Le résultat est démontré dans [11] (chapitre 5, paragraphe 2, théorème 3). La dernière majoration se déduit d'un résultat de K. Mahler (qui donne pour borne $e^{cn^{3/2}}$) que l'on trouvera dans [16]. □

Nous poursuivons en énonçant un résultat d'indépendance algébrique dont l'élégante démonstration est un exemple de preuve de l'indépendance algébrique de fonctions. Si ladite démonstration est beaucoup plus simple que pour le théorème 1.3.13 que nous avons admis, elle n'en demeure pas moins profonde.

Proposition 3.1.3. *Les fonctions* z *et* $J(z)$ *sont algébriquement indépendantes.*

Démonstration. Soit $P \in \overline{\mathbb{Q}}[X, Y]$ telle que la série de Laurent $P\left(z, J(z)\right)$ soit nulle. On a alors $P\left(\tau, j(\tau)\right) = 0$ pour tout $\tau \in \mathfrak{H}$.

Pour $c \in \mathbb{Z}$, notons $\alpha_c = \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} \in PSL_2(\mathbb{Z})$. Si $t \geq 1$ est un nombre réel transcendant, tous les nombres $\exp(2i\pi\alpha_c(it))$ $(c \in \mathbb{Z})$ sont distincts. En effet, l'égalité $\alpha_c(it) - \alpha'_c(it) = k \in \mathbb{Z}$ s'écrit $(c - c' + kcc')t^2 - ik(c + c')t - k = 0$, et la transcendance de t implique $k = c - c' = 0$. La fonction modulaire j étant invariante sous l'action de $PSL_2(\mathbb{Z})$, il en résulte que le polynôme $P(X, j(i\tau))$ admet une infinité de zéros, donc est nul.

Si l'on écrit à présent $P(X, Y) = \sum_{k=0}^{m} P_k(Y)X^k$, on a $P_k(X, j(it)) = 0$ pour tout $k \in [\![0, m]\!]$ et tout $t \geq 1$ transcendant. Mais j est injective sur $\{it/t \geq 1\}$ [5] (qui est contenu dans le domaine fondamental de $PSL_2(\mathbb{Z})$), donc P_k a une infinité de zéros et P est nul. □

5. Ceci résulte du corollaire 1.1.5 et du résultat (admis) selon lequel j établit par passage au quotient une bijection de ${}_G\backslash\mathfrak{H}$ sur $\mathbb{C}$.

La méthode de transcendance, dont le théorème stéphanois et le théorème de Y.V.Nesterenko en sont des illustrations, nécessite de construire des polynômes satisfaisant des contraintes portant sur leurs coeffcients. A cette fin, le lemme suivant est très utile : il permet essentiellement de trouver des solutions entières «pas trop grandes» à un système d'équations linéaires à coefficients entiers où le nombre d'inconnues est strictement supérieur au nombre d'équations.

Lemme 3.1.4 (Lemme de Thue-Siegel)**.** *Soit* $B = (b_{ij})_{\substack{1\leq i\leq M\\ 1\leq j\leq N}}$ *une matrice entière de taille* $M\times N$ *telle que* $N > M$*. Alors il existe un vecteur non nul* $X = \begin{pmatrix} x_1 \\ \vdots \\ x_N \end{pmatrix} \in \mathbb{Z}^N$ *tel que* $BX = 0$ *et vérifiant la contrainte*

$$\max_{1\leq j\leq N} |x_j| \leq \left(\prod_{i=1}^{M} B_i\right)^{\frac{1}{N-M}},$$

où l'on a posé $B_i = \max\left\{1, \sum_{j=1}^{N} |b_{ij}|\right\}$.

Démonstration. Quite à rajouter des composantes nulles au vecteur solution, on se ramène au cas où, pour tout $i \in [\![1, M]\!]$, $B_i = \sum_{j=1}^{N} |b_{ij}|$ (i.e. aucune des lignes de la matrice B n'est nulle).

La preuve du lemme consiste en une application du principe des tiroirs : en posant $\widetilde{B} = \left\lfloor \left(\prod_{i=1}^{M} B_i\right)^{\frac{1}{N-M}} \right\rfloor$, il existe $\left(\widetilde{B}+1\right)^N$ vecteurs distincts $x = {}^t(x_1, \ldots, x_N)$ à coordonnées entières vérifiant

$$\forall j \in [\![1, N]\!], \quad 0 \leq x_j \leq \widetilde{B}.$$

A un tel vecteur x on associe un second vecteur $y = {}^t(y_1, \ldots, y_M) \in \mathbb{Z}^M$ défini pour tout $i \in [\![1, M]\!]$ par

$$y_i = \sum_{j=1}^{N} b_{ij} x_j.$$

Soit, pour $i \in [\![1, M]\!]$,

$$\begin{cases} n_i = \sum_{\substack{1\leq j\leq N\\ b_{ij}<0}} |b_{ij}| \in \mathbb{N} \\ p_i = \sum_{\substack{1\leq j\leq N\\ b_{ij}>0}} |b_{ij}| \in \mathbb{N} \end{cases}$$

Il est dès lors clair que, pour tout $i \in [\![1, M]\!]$, $-n_i\widetilde{B} \leq y_i \leq p_i\widetilde{B}$ et que $B_i = n_i + p_i$. Chaque coordonnée y_i de y peut donc prendre au plus $n_i\widetilde{B} + p_i\widetilde{B} + 1 = \widetilde{B}B_i + 1$ valeurs distinctes. Par conséquent, il existe au plus $(\widetilde{B}B_1 + 1)\ldots(\widetilde{B}B_M + 1)$ vecteurs y distincts.

Or par définition de $\widetilde{B}$,

$$(\widetilde{B}+1)^N = (\widetilde{B}+1)^M(\widetilde{B}+1)^{N-M} > (\widetilde{B}+1)^M B_1 \ldots B_M \geq (1+B_1\widetilde{B})\ldots(1+B_M\widetilde{B}),$$

la dernière inégalité résultant de la relation $(1+a)b \geq 1+ab$ valable pour tous $a, b \in \mathbb{N}^*$.

Il existe donc deux vecteurs x et x' *distincts* ayant même vecteur y associé, i.e. deux vecteurs x et x' vérifiant les relations

$$\begin{cases} x - x' \neq 0 \\ B(x - x') = 0 \end{cases}$$

et, pour tout $j \in [\![1, N]\!]$,

$$\begin{cases} 0 \leq x_j \leq \widetilde{B} \\ 0 \leq x'_j \leq \widetilde{B} \end{cases}$$

Le vecteur $\widetilde{x} = x - x'$, dont les coordonnées sont comprises entre $-\widetilde{B}$ et $\widetilde{B}$, répond alors au problème. □

3.2 Enoncé et schéma de preuve

Théorème 3.2.1 (Théorème stéphanois)**.** *Soit α une nombre algébrique vérifiant $0 < |\alpha| < 1$. Alors le nombre $J(\alpha)$ est transcendant.*

Nous exposons de ce théorème les grandes lignes de la preuve pour constater l'analogie avec le raisonnement de Y.V.Nesterenko dans la démonstration de son résultat.

Schéma de preuve. Dans la démonstration originale [2] des stéphanois, le point de départ était une estimation de la croissance des coefficients du développement de Laurent des puissances de J. Cette majoration peut cependant être avantageusement remplacée par une estimation, plus simple à obtenir, des coefficients du développement de Taylor à l'origine de $\Delta^{2N}J^k$ pour N et k entiers naturels (cf. [28], lemme1).

On procède en quatre étapes :

Première étape : Construction d'une fonction auxiliaire.
On construit un polynôme non nul $A(X,Y) \in \mathbb{Z}[X,Y]$ de degré $\leq N$ en chaque variable tel que la fonction analytique

$$F(z) = \Delta(z)^{12N} A(z, J(z))$$

ait un zéro d'ordre au moins $L = N^2/2$ à l'origine. On utilise pour ce faire le lemme de Thue-Siegel 3.1.4, qui permet de borner les coefficients de A en fonction de N, de telle sorte qu'en posant

$$A(X,Y) = \sum_{1 \leq i,j \leq N} a_{i,j} X^i Y^j,$$

on ait

$$\sum_{1 \leq i,j \leq N} |a_{i,j}| \leq N^{25N}$$

pour N suffisamment grand.

Deuxième étape : Majoration de $|F(z)|$.
Les fonctions z et $J(z)$ étant algébriquement indépendantes d'après la proposition 3.1.3, la fonction F n'est pas identiquement nulle. On désigne alors par $M = \mathrm{ord}_0 F$ sa multiplicité en l'origine. On majore les coefficients du développement en série entière de F sur le disque unité. En adoptant la démonstration d'un théorème de Hecke donnée dans [26] (théorème 5, paragraphe 4.3, chapitre VII), on obtient que, pour tous entiers N et k tels que $N \geq 0$ et $0 \leq k \leq N$, la fonction $\Delta^{2N}J^k$ a un développement de Taylor à l'origine

$$\Delta^{2N}(z)J(z)^k = \sum_{m=1}^{+\infty} c_{N,k}(m) z^m$$

dont les coefficients sont majorés en valeur absolue par $C^N m^{12N}$ où $C > 0$ est une constante absolue. En utilisant le fait que $L \geq M$ d'après la première étape, ceci permet d'obtenir la majoration

$$|F(z)| \leq |z|^M M^{31N}.$$

Trosième étape : Définition et majoration du paramètre S.
C'est à ce stade qu'entre en jeu α. En adoptant les notations de la proposition 3.1.2, pour tout z et tout entier $n \geq 2$, $\Phi_n(J(z), J(z^n)) = 0$. Si l'on suppose la conclusion du théorème fausse, on en déduit que, pour tout entier naturel k, $J(\alpha^k)$ est algébrique. Comme F est non identiquement nulle, il existe un plus petit entier naturel S tel que

$$F(\alpha^S) \neq 0.$$

En appliquant le principe du maximum à la fonction

$$H(z) = \frac{F(z)}{z^M} \prod_{s=1}^{S-1} \frac{r^2 - z\overline{q}^s}{r(z-q^s)},$$

on arrive à la majoration

$$S^2 \leq \frac{63}{\ln\left(\frac{1}{|\alpha|}\right)} N \log M.$$

Quatrième étape : Minoration de $|F(\alpha^S)|$
La majoration de la somme des modules des coefficients de Φ_n couplée à une série d'autres majorations assez fines utilisant le fait que α et $J(\alpha^S)$ sont algébriques permet d'arriver à la minoration suivante, où $\widetilde{C}$ est une constante pouvant dépendre de α :

$$|F(\alpha^S)| \geq e^{\widetilde{C} S^{3/2} N(S+\log M)}.$$

Conclusion
En utilisant la majoration de S donnée à la troisième étape, on vérifie que la minoration de $|F\left(\alpha^S\right)|$ de la quatrième étape n'est pas compatible avec la majoration établie à la deuxième étape (cette majoration étant évaluée en $z = \alpha^S$). L'hypothèse d'algébricité de $J(\alpha)$ se trouve ainsi contredite. □

Comme on le voit, la démonstration repose très fortement sur les propriétés des polynômes modulaires. Plus généralement, l'apport majeur de ce raisonnement réside dans le fait qu'il s'agit là de la première preuve de transcendance ne faisant intervenir que les propriétés des fonctions modulaires. Mais les conséquences du théorème sont aussi d'«ordre elliptique» :

Corollaire 3.2.2. *Soit $\wp$ la fonction elliptique de Weierstrass d'invariants g_2 et g_3 algébriques. Soit $\mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ le réseau des périodes de $\wp$, avec $\tau = \frac{\omega_1}{\omega_2} \in \mathfrak{H}$. Alors pour tout nombre algébrique non nul α et toute détermination $\log \alpha$ de son logarithme, le déterminant*

$$\begin{vmatrix} 2i\pi & \log\alpha \\ \omega_2 & \omega_1 \end{vmatrix}$$

ne s'annule pas.

Comme mentionné au chapitre 2 de [18], aucune démonstration de ce résultat reposant sur les fonctions elliptiques et exponentielle (et non sur les fonction modulaires) n'est connue à l'heure actuelle.

Démonstration. On raisonne par l'absurde en supposant que le déterminant considéré s'annule. Cela revient exactement à affirmer que $\alpha = e^{2i\pi\tau}$. Dès lors, $J(\alpha) = j(\tau)$. Mais, par le théorème stéphanois, $J(\alpha)$ est transcendant alors que, par définition de l'invariant modulaire (définition 1.4.1), g_2 et g_3 étant supposés algébriques, $j(\tau)$ est algébrique. L'égalité précédente ne peut donc être. □

Ce corollaire est un analogue du problème bien connu suivant, dont les conséquences en théorie des nombres sont colossales (cf. par exemple [27] ou [28]) :

Conjecture 3.2.3 (Conjecture des quatre exponentielles)**.** *Soit une matrice*

$$\begin{pmatrix} \log\alpha_1 & \log\alpha_2 \\ \log\alpha_3 & \log\alpha_4 \end{pmatrix}$$

dont les coefficients sont des logarithmes de nombres algébriques. Si les deux lignes sont linéairement indépendantes sur $\mathbb{Q}$ et si les deux colonnes le sont aussi, alors le déterminant de la matrice ne s'annule pas.

4 Théorie de l'élimination

Dans cette section, nous présentons quelques résultats d'élimination homogène et nous les appliquerons ensuite à la définition d'un degré, d'une hauteur et d'une distance sur les variétés dans la section suivante. Ces résultats serviront à la démonstration du critère d'indépendance algébrique de P.Philippon dans la partie 6.2.2.

On travaillera dans l'anneau $\mathbb{L}[X] = \mathbb{L}[X_0, \ldots, X_n]$, où $\mathbb{L}$ est un corps de nombres. A tout idéal homogène I (i.e. engendré par des polynômes homogènes) de $\mathbb{L}[X]$, on associe des idéaux éliminants $\mathfrak{E}_d(I)$ puis, lorsque ces idéaux sont principaux, des formes éliminantes, suivant une construction que nous détaillons ci-dessous.

4.1 Décomposition primaire

Nous commençons par quelques résultats d'algèbre commutative : le but de cette sous-partie est précisément d'établir l'existence, puis un résultat partiel d'unicité de la décomposition d'un idéal comme intersection d'idéaux dits primaires. Cette décomposition nous sera utile par la suite.

Notation. *Nous désignons par A un anneau commutatif, par M un A-module et par* $\mathrm{Spec}(A)$ *sera l'ensemble des idéaux premiers de A. Enfin, si $\mathfrak{p} \in \mathrm{Spec}(A)$, $M_\mathfrak{p}$ sera le localisé de M en le système multiplicatif $S = A\backslash\mathfrak{p}$, i.e. $M_\mathfrak{p} = S^{-1}M$.*

On travaillera de plus avec la topologie de Zariski sur $\mathrm{Spec}(A)$, pour laquelle les fermés sont de la forme

$$\mathcal{Z}(I) = \{\mathfrak{p} \in \mathrm{Spec}(A)/I \subset \mathfrak{p}\}$$

pour I idéal de A.

Définition 4.1.1. *Le* support *du A-module M est le sous ensemble de* $\mathrm{Spec}(A)$ *défini par*

$$\mathrm{Supp}(M) = \{\mathfrak{p} \in \mathrm{Spec}(A)/M_\mathfrak{p} \neq 0\}.$$

Définition 4.1.2. *L'*annulateur d'un élément $m \in M$ *est l'idéal* $\mathrm{Ann}(m)$ *de A tel que*

$$\mathrm{Ann}(m) = \{f \in A/fm = 0\}.$$

*L'*annulateur $\mathrm{Ann}(M)$ du module M *est alors l'intersection des annulateurs de chacun des éléments de M, i.e.*

$$\mathrm{Ann}(M) = \{f \in A/fM = 0\}.$$

De ces définitions découlent une première série de propriétés :

Proposition 4.1.3. *On adopte les notations précédentes :*

1. *Si M est engendré en tant que A-module par un élément $x \in M$, et si l'on pose $I = \mathrm{Ann}(x)$, alors* $\mathrm{Supp}(M) = \mathcal{Z}(I)$
2. *Si M peut s'écrire comme une somme $\sum_{i\in J} M_i$ de A-modules, alors* $\mathrm{Supp}(M) = \cup_{i\in J}\mathrm{Supp}(M_i)$.
3. *Si M est de type fini sur A, alors* $\mathrm{Supp}(M) = \mathcal{Z}(\mathrm{Ann}(M))$*, qui est un fermé de* $\mathrm{Spec}(A)$ *pour la topologie de Zariski.*

Démonstration.

1. Par définition d'un anneau localisé, on a, pour $\mathfrak{p} \in \mathrm{Spec}(A)$, les équivalences :

$$M_\mathfrak{p} = 0 \quad \Leftrightarrow \quad \frac{x}{1} = 0 \in M_\mathfrak{p} \quad \Leftrightarrow \quad \exists s \in A\backslash\mathfrak{p}, sx = 0 \quad \Leftrightarrow \quad (A\backslash\mathfrak{p}) \cap \mathrm{Ann}(x) \neq \emptyset$$

   Il suffit alors de remarquer que l'on peut obtenir la négation de ces équivalences comme suit :

$$M_\mathfrak{p} \neq 0 \quad \Leftrightarrow \quad \frac{x}{1} \neq 0 \in M_\mathfrak{p} \quad \Leftrightarrow \quad I = \mathrm{Ann}(x) \subset \mathfrak{p} \quad \Leftrightarrow \quad \mathfrak{p} \in \mathcal{Z}(I)$$

2. Pour tout $i \in J$, $M_i \subset M$, donc, pour $\mathfrak{p} \in \mathrm{Spec}(A)$, $(M_i)_\mathfrak{p} \subset M_\mathfrak{p}$, ce qui prouve une inclusion. Pour l'autre, il suffit de remarquer que, si, pour tout $i \in J$, $(M_i)_\mathfrak{p} = 0$, alors tout élément de M est annulé par un élément $s \notin \mathfrak{p}$, i.e. $M_\mathfrak{p} = 0$.
3. Si M est engendré par k éléments $m_1, \ldots, m_k$, alors, d'après les deux points précédents, on a les égalités :

$$M = \bigcap_{i=1}^{k} \mathrm{Supp}(Am_i) = \bigcap_{i=1}^{k} \mathcal{Z}(\mathrm{Ann}(m_i)) = \mathcal{Z}\left(\bigcup_{i=1}^{k} \mathrm{Ann}(m_i)\right) = \mathcal{Z}\left(\mathrm{Ann}(M)\right).$$

□

Définition 4.1.4. *Un* assassin de M [6] *est un idéal premier* $\mathfrak{p}$ *de* A *tel que* M *contienne un sous-module isomorphe au quotient* $A/\mathfrak{p}$ *ou, de manière équivalente, tel qu'il existe* $x \in M$ *vérifiant* $\mathfrak{p} = \mathrm{Ann}(x)$. *On désigne alors par* $\mathrm{Ass}(M)$ *l'ensemble des assassins de* M.

Si le sens réciproque est évident (il suffit de choisir le sous-module de M engendré par x), l'équivalence résulte, pour le sens direct, de ce que l'on peut prendre pour x un élément non nul quelconque de $A/\mathfrak{p}$.

Remarque 4.1.5. *Au vu de cette définition, il est clair que tout assassin contient* $\mathrm{Ann}(M)$.

Là encore, une série de propriétés peuvent être déduites de cette définition. La troisième est la plus importante pour l'usage que l'on en fera :

Proposition 4.1.6. *Soit* $\mathfrak{p} \in \mathrm{Spec}(A)$ *:*

1. *Si* $x \in M$ *est tel que* $\mathfrak{p} = \mathrm{Ann}(x)$, *alors, pour tout élément non nul* y *du* A*-module engendré par* x, $\mathfrak{p} = \mathrm{Ann}(y)$. *En particulier,* $\mathrm{Ass}\left(A/\mathfrak{p}.\right) = \{\mathfrak{p}\}$
2. *Tout élement maximal de l'ensemble d'idéaux* $\{\mathrm{Ann}(x)/0 \neq x \in M\}$ *est un idéal premier, donc est dans* $\mathrm{Ass}(M)$.
3. *Si* A *est un anneau nœthérien et* M *un* A*-module non nul, alors* $\mathrm{Ass}(M)$ *est non vide.*

Démonstration.

1. Le sous-module $Ax \subset M$ est isomorphe à $A/\mathfrak{p}$ qui, en tant qu'anneau, est intègre. La première assertion s'ensuit. La seconde en découle clairement puisque $\mathfrak{p} = \mathrm{Ann}(1)$, où $1 \in A/\mathfrak{p}$.
2. Soit $x \in M$ tel que $P = \mathrm{Ann}(x)$ soit maximal parmi les annulateurs d'éléments. Supposons que le produit fg d'élements de A soit dans P. Deux cas de figure se présentent : si $gx = 0$, alors $g \in P$. Si, en revenche, $gx \neq 0$, alors $\mathrm{Ann}(x) \subset \mathrm{Ann}(gx)$ et, par maximalité, $\mathrm{Ann}(x) = \mathrm{Ann}(gx)$. Dès lors, l'égalité $fgx = 0$ implique $f \in P$.
3. M est non nul donc l'ensemble d'idéaux (de A) $\{\mathrm{Ann}(x)/0 \neq x \in M\}$ est non vide. A étant nœthérien, cet ensemble admet un élément maximal qui, d'après le point précédent, est dans $\mathrm{Ass}(M)$.

□

Nous admettrons le théorème qui suit, dont la démonstration est très technique :

Théorème 4.1.7. *Si l'anneau* A *est nœthérien, alors tout élément minimal de* $P \in \mathrm{Supp}(M)$ *est dans* $\mathrm{Ass}(M)$.

Démonstration. L'idée consiste à montrer, dans un premier temps, que $\mathrm{Ass}_{A_P}(M_P) = \{PA_P\}$ puis de remonter de ce cas local au cas global. Ce dernier point constitue la partie difficile du théorème. On trouvera les détails de la démonstration dans [24] (chapitre 7, paragraphe 5). □

6. Une illustration du sens de l'humour bourbakiste.

L'ensemble des notions jusqu'ici abordées dans ce paragraphe sert à l'exploitation des objets introduits par la définition suivante :

Définition 4.1.8. *Un* idéal primaire Q *de* A *est un idéal strictement inclus dans* A *tel que pour tous éléments* f, g *de* A *tels que leur produit est dans* Q, *soit* f *est dans* Q, *soit une puissance non nulle de* g *est dans* Q.

Autrement dit, le quotient A/Q *est non nul et les diviseurs de zéros de* A/Q *sont nilpotents.*

Remarque 4.1.9. *Il découle trivialement de cette définition que, si* Q *est un idéal primaire de* A, *alors son radical est un idéal premier.*

Définition 4.1.10. *Un idéal* Q *de* A *est* P*-primaire si* Q *est primaire et si* P *est un idéal de* A *tel que* $P = \mathrm{rad}(Q) = \bigcap_{\substack{P' \in \mathrm{Spec}(A) \\ Q \subset P'}} P'$.

Voici à présent un théorème qui établit un lien entre idéal primaire et assassin :

Théorème 4.1.11. *Soit* A *un anneau nœthérien et* Q *et* P *des idéaux de* A. *Alors* Q *est* P*-primaire si, et seulement si,* $\mathrm{Ass}\left(A/Q\right) = \{P\}$.

Démonstration. Supposons Q P-primaire. Alors les diviseurs de zéro de A/Q sont contenus dans $P = \mathrm{rad}(Q)$, de telle sorte que, pour tout élément non nul x de A/Q, on a :

$$Q \subset \mathrm{Ann}_{A/Q}(x) \subset P = \mathrm{rad}(Q).$$

D'où $P = \mathrm{rad}\left(\mathrm{Ann}(x)\right)$. $\mathrm{Ann}(x)$ n'est alors premier qu'à la seule condition qu'il soit égal à P. On conclut en invoquant le troisième point de la proposition 4.1.6 pour justifier du fait que $\mathrm{Ass}\left(A/Q\right) \neq \emptyset$.

Réciproquement, supposons que $\mathrm{Ass}\left(A/Q\right) = \{P\}$. Etablissons tout d'abord un résultat préliminaire en montrant que, si $0 \neq M \subset A/Q$, alors $\mathrm{rad}(\mathrm{Ann}(M)) = P$. A cette fin, remarquons que l'on a tout d'abord :

$$\mathrm{rad}(\mathrm{Ann}(M)) = \bigcap_{\substack{P' \in Spec(A) \\ \mathrm{Ann}(M) \subset P'}} P' = \bigcap_{P' \in \mathcal{Z}(\mathrm{Ann}(M))} P' = \bigcap_{P' \in \mathrm{Supp}(M)} P' = \bigcap_{P' \in \mathrm{Ass}(M)} P',$$

la troisième égalité résultant du dernier point de la proposition 4.1.3 et la dernière du théorème 4.1.7. Comme $\mathrm{Ass}(M)$ est ici encore non vide (proposition 4.1.6), on déduit de l'hypothèse que $\mathrm{Ass}(M) = \{P\}$, ce qui prouve le résultat intermédiaire.

On applique à présent ce résultat au cas où $M = A/Q$: l'idéal $Q = \mathrm{Ann}\left(A/Q\right)$ est donc tel que $\mathrm{rad}(Q) = P$. Soit alors f, $g \in A$ tel que $fg \in Q$ avec $f \notin Q$. Posons $\overline{f}{=}f \bmod Q$. On obtient $g \in \mathrm{Ann}(\overline{f}) \subset \mathrm{rad}(\mathrm{Ann}(\overline{f})) = P$, i.e. $g^n \in Q$ pour un $n \geq 1$. □

Définition 4.1.12. *Une* décomposition primaire *d'un idéal* $I \subset A$ *est la donnée d'un entier naturel* n *et de* n *idéaux primaires* $Q_1, \ldots, Q_n$ *tels que*

$$I = \bigcap_{i=1}^{n} Q_i.$$

Une telle décomposition est minimale, *ou* normale, *si aucun des* Q_j *n'est redondant et si* Q_i *est* P_i*-primaire avec* $P_i \neq P_j$ *pour* $i \neq j$.

Remarque 4.1.13. *Etant donné une décomposition primaire d'un idéal, il est toujours possible d'en déduire une décomposition primaire normale en regroupant les termes redondants et en remarquant que l'intersection de deux idéaux* P*-primaires est encore un idéal* P*-primaire.*

Dans un anneau nœthérien, il y a toujours existence d'une telle décomposition :

Théorème 4.1.14. *Tout idéal I d'un anneau nœthérien A admet une décomposition primaire normale.*

Démonstration. En vertu de la remarque 4.1.13, il suffit de démontrer l'existence d'une décomposition primaire pour tout idéal I de A. On procède en deux temps.

Première étape :
Un idéal sera dit *indécomposable* s'il ne peut pas s'écrire comme intersection de deux idéaux qui lui sont tous les deux strictement plus grands. On a alors la proposition suivante :

Proposition 4.1.15. *Tout idéal I de A s'écrit comme intersection d'un nombre fini d'idéaux indécomposables.*

Démonstration. Soit Σ l'ensemble des idéaux qui ne s'expriment pas comme intersection finie d'idéaux indécomposables. Supposons par l'absurde que $\Sigma \neq \emptyset$. Par le caractère nœthérien de A, Σ admet un élément maximal J, qui est décomposable : on peut écrire $J = K \cap L$ avec K et L des idéaux strictement plus grands que J.

Par maximalité de J, K et L ne sont pas dans Σ, donc sont intersection d'un nombre fini d'idéaux indécomposables, et donc J aussi, ce qui est exclu. □

Deuxième étape :

Proposition 4.1.16. *Tout idéal indécomposable Q de A est primaire.*

Démonstration. Comme Q est indécomposable (resp. primaire) si, et seulement si, l'idéal nul de A/Q est indécomposable (resp. primaire), il suffit d'établir que, si l'idéal nul d'un anneau nœthérien B est indécomposable, alors il est primaire.

Soit donc x,$y \in B$ tels que $xy = 0$: alors $y \in \mathrm{Ann}(x)$. La chaîne croissante $\mathrm{Ann}(x) \subset \mathrm{Ann}(x^2) \subset \cdots \subset \mathrm{Ann}(x^n) \subset \ldots$ étant stationnaire, il existe un entier $n \geq 1$ tel que $\mathrm{Ann}(x^n) = \mathrm{Ann}(x^{n+1})$.

Dans ces conditions, $(x^n) \cap (y) = (0)$. En effet, si $a \in (x^n) \cap (y)$, alors, d'une part, $ax = 0$ (puisque a est aussi multiple de y). D'autre part, $a = bx^n$; mais alors $ax = bx^{n+1}$ et donc $b \in \mathrm{Ann}(x^{n+1}) = \mathrm{Ann}(x^n)$, d'où $a = bx^n = 0$.

Ainsi donc, si l'idéal nul est indécomposable et qu'un produit xy est nul, alors $x^n = 0$ ou $y = 0$: l'idéal nul est primaire. □

Les deux étapes démontrent le théorème 4.1.14. □

Nous terminons par un résultat partiel d'unicité qui sera essentiel à la démonstration du théorème de Bézout géométrique et dont la preuve est le but de ce paragraphe.

Théorème 4.1.17. *Soit A un anneau nœthérien et I un idéal de A admettant pour décomposition primaire minimale $I = \bigcap_{i=1}^{k} Q_i$, où Q_i est P_i-primaire. Alors* $\mathrm{Ass}\,(A/I) = \{P_1, \ldots, P_k\}$.

En particulier, l'ensemble des idéaux premiers $\{P_1, \ldots, P_k\}$ est déterminé de manière unique par I.

Démonstration. On dispose de l'inclusion canonique

$$A/I \hookrightarrow \bigoplus_{i=1}^{k} A/Q_i.$$

Ainsi $\mathrm{Ass}\,(A/I) \subset I = \bigcup_{i=1}^{k} \mathrm{Ass}\left(A/Q_i\right) = \{P_1, \ldots, P_k\}$ d'après le théorème 4.1.11.

Réciproquement, par la condition de non-redondance,

$$\forall j \in [\![1,k]\!], \quad 0 \neq N = \bigcap_{i \neq j} Q_i/I \subset A/I.$$

Or sous l'inclusion précédente, N s'envoie sur 0 en chaque composante A/Q_i pour $i \neq j$. Par conséquent, $0 \neq N \hookrightarrow A/Q_j$. Mais d'après le théorème 4.1.11, $\mathrm{Ass}\left(A/Q_j\right) = \{P_j\} : A/I$ contient ainsi un sous-module N vérifiant $\emptyset \neq \mathrm{Ass}(N) \subset \{P_j\}$, donc $P_j \in \mathrm{Ass}(A/I)$. □

4.2 Idéaux éliminants

Soit $n \in \mathbb{N}$ un entier naturel fixé et $X_0, \ldots, X_n$ des indéterminées, dont on notera X la collection. Soit B un anneau nœthérien. On introduit l'anneau $A = B[X_0, \ldots, X_n]$ des polynômes en $n+1$ variables à coefficients dans B. Pour $k \in \mathbb{N}$, on note $\mathfrak{M}_k$ l'ensemble des monômes unitaires de degré k :

$$\mathfrak{M}_k = \{X_0^{\alpha_0} \ldots X_n^{\alpha_n} / \alpha_0 + \cdots + \alpha_n = k\}.$$

Cet ensemble est de cardinal C_{n+k}^k.

On fixe un entier $r \geq 0$ et un r-uplet $d = (d_1, \ldots, d_r) \in \mathbb{N}^r$. Si $r = 0$, on notera $B[\boldsymbol{u}] = B$ et $A[\boldsymbol{u}] = A$. Si $r \geq 1$, $B[\boldsymbol{u}]$ (resp. $A[\boldsymbol{u}]$) sera l'anneau des polynômes à coefficients dans B (resp. A) en les indéterminées $u^{l,d_l} = \left\{ u_{\mathfrak{m}}^{l,d_l} \Big/ \mathfrak{m} \in \mathfrak{M}_{d_l} \right\}$, où $1 \leq l \leq r$. On pose, pour $1 \leq l \leq r$,

$$U_{l,d_l} = \sum_{\mathfrak{m} \in \mathfrak{M}_{d_l}} u_{\mathfrak{m}}^{l,d_l} \mathfrak{m} \in A[\boldsymbol{u}].$$

Lorsque I est un idéal de A, on désigne par $I[\boldsymbol{u}]$ l'idéal de $A[\boldsymbol{u}]$, soit égal à I si $r = 0$, soit égal à l'idéal engendré par I et les éléments $U_{1,d_1}, \ldots, U_{r,d_r}$ si $r \geq 1$.

Définition 4.2.1. *Soit I un idéal de A. On définit l'*idéal caractéristique d'indice d de I *par*

$$\mathfrak{U}_d(I) = \{f \in A[\boldsymbol{u}] / \exists k \in \mathbb{N}, f\mathfrak{M}_k \subset I[\boldsymbol{u}]\} = \bigcup_{k \geq 1} \{f \in A[\boldsymbol{u}] / f\mathfrak{M}_k \subset I[\boldsymbol{u}]\}$$

*et l'*idéal éliminant d'indice d de I par

$$\mathfrak{E}_d(I) = \mathfrak{U}_d(I) \cap B[\boldsymbol{u}].$$

Plus concrètement, l'idéal éliminant d'indice d de I est donc l'idéal de $B[\boldsymbol{u}]$ formé par les éléments $a \in B[\boldsymbol{u}]$ tels que, pour tout $i \in [\![0,n]\!]$, il existe $N_i \in \mathbb{N}$ tel que $aX_i^{N_i} \in I[\boldsymbol{u}]$.

Remarque 4.2.2. *Du fait du caractère nœthérien de $A[\boldsymbol{u}]$, les réunion infinie d'idéaux définissant $\mathfrak{U}_d(I)$ est en fait finie. Comme les idéaux sont de plus emboités, on obtient l'existence d'un entier $N \in \mathbb{N}$ tel que*

$$\mathfrak{U}_d(I) = \{f \in A[\boldsymbol{u}] / f\mathfrak{M}_N \subset I[\boldsymbol{u}]\}.$$

On s'intéresse au comportement des idéaux éliminants par rapport à la décomposition primaire ; la proposition qui suit nous sera en particulier utile pour la démonstration du théorème de Bézout géométrique.

Proposition 4.2.3. *Soit I un idéal homogène de A.*

1. *Si $\mathfrak{M}_1 \subset \sqrt{I}$, alors $\mathfrak{U}_d(I) = A[\boldsymbol{u}]$ et $\mathfrak{E}_d(I) = B[\boldsymbol{u}]$.*
2. *Si I est premier et $\mathfrak{M}_1 \not\subset \sqrt{I}$, alors $\mathfrak{U}_d(I)$ et $\mathfrak{E}_d(I)$ sont premiers.*
3. *Si I est primaire et $\mathfrak{M}_1 \not\subset \sqrt{I}$, alors $\mathfrak{U}_d(I)$ et $\mathfrak{E}_d(I)$ sont primaires et, de plus, $\sqrt{\mathfrak{U}_d(I)} = \mathfrak{U}_d(\sqrt{I})$ et donc $\sqrt{\mathfrak{E}_d(I)} = \mathfrak{E}_d(\sqrt{I})$.*

4. Si $I = \bigcap_{i=1}^{h} I_i$ *est une décomposition primaire normale de* I*, alors* $\mathfrak{U}_d(I) = \bigcap_{i=1}^{h} \mathfrak{U}_d(I_i)$ *et* $\mathfrak{E}_d(I) = \bigcap_{i=1}^{h} \mathfrak{E}_d(I_i)$.

Démonstration. La démonstration, technique et peu intéressante dans notre perspective, se trouve dans [21] (proposition I.3). □

Le théorème suivant donne une interprétation géométrique de l'idéal éliminant en termes d'équations polynômiales ; c'est le théorème fondamental de la théorie de l'élimination et l'on s'y réfèrera par (TE) dans la suite :

Théorème 4.2.4 (Théorème fondamental de la théorie de l'élimination)**.** *Soit* $\rho : B[\boldsymbol{u}] \to \mathbb{L}$ *un morphisme d'anneaux (fixant* B*) dans un corps* $\mathbb{L}$*. On note encore* ρ *son prolongement à* $A[\boldsymbol{u}]$*, obtenu en posant* $\rho(X_i) = X_i$ *pour tout* $i \in [\![0, n]\!]$*. Alors, pour tout idéal homogène* I *de* A*, les conditions suivantes sont équivalentes :*

- **i)** $\rho(\mathfrak{E}_d(I)) = 0$.
- **ii)** *Il existe une extension de corps* $\mathbb{K}/\mathbb{L}$ *et un zéro non trivial de* $\rho(I[\boldsymbol{u}])$ *dans* $\mathbb{K}^{n+1}$*, i.e. il existe* $z \in \mathbb{K}^{n+1} \backslash \{0\}$ *tel que pour tout* $P \in I[\boldsymbol{u}]$*, on ait* $\rho(P)(z) = 0$.
- **iii)** *Il existe une extension de corps finie* $\mathbb{K}/\mathbb{L}$ *et un zéro non trivial de* $\rho(I[\boldsymbol{u}])$ *dans* $\mathbb{K}^{n+1}$.

Démonstration. L'implication ***iii)*** $\Rightarrow$ ***ii)*** est évidente.

Démontrons que ***ii)*** $\Rightarrow$ ***i)*** : si $a \in \mathfrak{E}_d(I)$, alors il existe $N \in \mathbb{N}$ tel que $a.\mathfrak{M}_N \subset I[\boldsymbol{u}]$. Par conséquent, si $(x_0, \ldots, x_n)$ est un zéro non trivial de $\rho(I[\boldsymbol{u}])$ dans $\mathbb{K}^{n+1}$, on écrit pour un indice $i_0 \neq 0$ tel que $x_{i_0} \neq 0$ que $\rho(aX_{i_0}^N)(x_0, \ldots, x_n) = \rho(a)x_{i_0}^N = 0$ pour conclure que $\rho(a) = 0$.

L'implication ***i)*** $\Rightarrow$ ***iii)*** est la plus délicate : nous n'en donnerons que les idées directrices permettant de comprendre le raisonnement amenant la conclusion, en renvoyant à [21] (proposition I.4) pour les détails, qui allongeraient inutilement le propos étant donné les perspectives poursuivies. Si ρ est le morphisme nul, tout point non nul de $\mathbb{L}^{n+1}$ répond au problème. On peut donc supposer le morphisme non identiquement nul. Sous cette condition, il apparaît que, pour tout $N > 0$, $\mathfrak{M}_N \not\subset \rho(I[\boldsymbol{u}])$. Dès lors, il existe $i_0 \in [\![0, n]\!]$ tel que $X_{i_0}^N \notin \rho(I[\boldsymbol{u}])\,\mathbb{L}[X_0, \ldots, X_n]$ pour tout $N > 0$. Ceci permet de montrer que $1 - X_{i_0} \in \mathbb{L}[X_0, \ldots, X_n]$ n'est pas inversible modulo $\rho(I[\boldsymbol{u}])\,\mathbb{L}[X_0, \ldots, X_n]$, donc appartient à un idéal maximal $\mathcal{M}$ de $\mathbb{L}[X_0, \ldots, X_n]$ contenant $\rho(I[\boldsymbol{u}])$. Par conséquent, ρ induit un morphisme

$$\begin{aligned} \widetilde{\rho} \ : A[\boldsymbol{u}] &\to \mathbb{K} = \mathbb{L}[X_0, \ldots, X_n]/_{\mathcal{M}} \\ X_{i_0} &\mapsto 1 \neq 0 \end{aligned}$$

On vérifie aisément que l'extension $\mathbb{K}$ ainsi définie est finie sur $\mathbb{L}$. Comme $\widetilde{\rho}(p) = 0$ pour tout $p \in I[\boldsymbol{u}]$ et que $\widetilde{\rho}(p) = \rho(p)\,(\widetilde{\rho}(X_0), \ldots, \widetilde{\rho}(X_n))$, $(\widetilde{\rho}(X_0), \ldots, \widetilde{\rho}(X_n))$ apparaît comme un zéro non trivial de $\rho(I[\boldsymbol{u}])$ dans $\mathbb{K}^{n+1}$, ce qui conclut le raisonnement. □

4.3 Formes éliminantes

On rappelle la définition suivant :

Définition 4.3.1. *La* hauteur *ou* dimension de Krull *d'un anneau* B*, notée* $\mathrm{ht}(B)$*, est le supremum des longueurs des chaînes d'idéaux premiers dans* B*, où la longueur d'une chaîne* $P_r \subsetneq P_{r-1} \subsetneq \cdots \subsetneq P_0$ *est choisie comme valant* r*. Si* I *est un idéal premier de* B*, la hauteur* $\mathrm{ht}(I)$ *de* I *est le supremum des longueurs des chaînes d'idéaux premiers décroissantes commençant en* I *:* $P_r \subsetneq P_{r-1} \subsetneq \cdots \subsetneq P_0 = I$.

Théorème 4.3.2. *Soit* $\mathbb{L}$ *un corps infini,* r *un entier,* I *un idéal premier homogène de* $\mathbb{L}[X]$ *et* d *un élément de* $(\mathbb{N}^*)^r$*. On a alors :*

1. $\mathfrak{E}_d(I) = (0) \Leftrightarrow \mathrm{ht}(I) < n - r + 1$.

2. *Si* $\mathrm{ht}(I) = n - r + 1$, *alors* $\mathfrak{E}_d(I)$ *est principal.*

Démonstration. On se réfèrera à [18] (théorème 2.13, p.65) □

L'intérêt d'un tel résultat de principalité est de remplacer la manipulation d'un idéal par celle d'un élément de l'anneau, son générateur. Celui-ci n'étant défini qu'à une constante multiplicative près, il est commode de privilégier arbitrairement un générateur. Pour cela, on fixe un ensemble $\mathrm{Irr}(\mathbb{L}[X])$ de représentants des irréductibles de $\mathbb{L}[\boldsymbol{u}]$ modulo les inversibles (on peut par exemple ne retenir que les irréductibles dont le coefficient dominant est 1 dans un certain ordre lexicographique sur les variables).

Définition 4.3.3. *Soit* I *un idéal homogène de* $\mathbb{L}[X]$, $r \in \mathbb{N}$, $d \in \mathbb{N}^r$. *Une* forme éliminante d'indice d de I *est un p.g.c.d. quelconque des éléments de l'idéal* $\mathfrak{E}_d(I)$. *On note en particulier* $\mathrm{élim}_d(I)$ *l'unique p.g.c.d. qui s'écrit comme produit d'éléments de* $\mathrm{Irr}(\mathbb{L}[X])$.

L'intérêt d'une telle définition est essentiellement résumé dans cette conséquence immédiate du théorème 4.3.2 :

Corollaire 4.3.4. *Sous les hypothèses et notations du théorème 4.3.2, notons* $f = \mathrm{élim}_d(I)$. *Alors :*

1. $f = 0 \Leftrightarrow \mathrm{ht}(I) < n - r + 1$.
2. *Si* $\mathrm{ht}(I) = n - r + 1$, *alors* f *engendre* $\mathfrak{E}_d(I)$.

Remarque 4.3.5. *On peut montrer que, si* $\mathrm{ht}(I) > n - r + 1$, *alors* $f = 1$.

5 Géométrie Diophantienne

Dans cette section, $\mathbb{K}$ désignera, sauf mention du contraire, un corps algébriquement clos. On pose $A = \mathbb{K}[X_0, \ldots, X_n]$, qui est un anneau gradué de manière naturelle pour une décomposition que l'on écrira $\bigoplus_{d\geq 0} A_d$. On notera enfin $A_+ = \bigoplus_{d\geq 1} A_d$, qui est un idéal maximal homogène de A.

Si I est un idéal homogène (i.e. engendré par des polynômes homogènes) de A, on notera $\mathfrak{Z}(I)$ l'ensemble des zéros de I dans $\mathbb{P}_n(\mathbb{K})$. De manière duale, si X est un sous-ensemble de $\mathbb{P}_n(\mathbb{K})$, on note $I(X)$ l'idéal homogène formé des polynômes qui s'annulent en tout point de X.

On rappelle le théorème suivant :

Théorème 5.0.6 (Version homogène du *Nullstellensatz*)**.** *Pout tout idéal homogène J de A tel que $\mathfrak{Z}(J) \neq \emptyset$, $I(\mathfrak{Z}(J)) = \sqrt{J}$.*

Il est bien connu que la condition $\mathfrak{Z}(J) = \emptyset$ équivaut à ce que $\sqrt{J} = A$ ou $\sqrt{J} = A_+$, ce qui revient encore à affirmer de manière équivalente qu'il existe un entier $d > 0$ tel que $A_d \subset J$ [7].

Nous définirons comme suit une variété projective :

Définition 5.0.7. *Soit n un entier. Une* variété projective de $\mathbb{P}_n(\mathbb{K})$ *est un sous ensemble X de $\mathbb{P}_n(\mathbb{K})$ tel qu'il existe un idéal premier homogène I de $\mathbb{K}[X_0, \ldots, X_n]$, $I \neq A_+$, tel que $X = \mathfrak{Z}(I)$.*

En particulier, et il est important de garder ce point à l'esprit pour certains résultats qui suivront, la condition $I \neq A_+$ assure que $\mathfrak{M}_1 \not\subset I$.

Une *hypersurface* est une variété V qui s'écrit $V = \mathfrak{Z}(I)$ pour I idéal premier homogène principal. Si $I = (F)$, $F \in A$ homogène irréductible, on notera plus simplement $V = \mathfrak{Z}(F)$.

On définit la dimension d'une variété de manière analogue à la dimension de Krull d'un anneau :

Définition 5.0.8. *Soit V une variété. La* dimension de V *est la borne supérieure des entiers n tel qu'il existe une chaîne $Z_0 \subsetneq Z_1 \subsetneq \cdots \subsetneq Z_n$ de sous-ensembles fermés de V (pour la topologie de Zariski) irréductibles (i.e. ne s'écrivant pas comme réunion de deux sous-ensembles fermés propres)* [8].

Le lien entre cette définition et la hauteur d'un idéal I est donné par la proposition suivante :

Proposition 5.0.9. *Pour tout idéal premier homogène I de A,*

$$\mathrm{ht}(I) + \dim \mathfrak{Z}(I) = \dim(A) = n.$$

Démonstration. On se reportera au besoin à [17], chapitre 5, paragraphe 14. □

Dans toute la suite, on se fixe un entier r, un r-uplet $d \in (\mathbb{N}^*)^r$ d'entiers strictement positifs et une variété projective V de dimension $r-1$. L'idéal $I = I(V)$ est donc de hauteur $n-r+1$ et, en vertu du théorème 4.3.2, $\mathfrak{E}_d(I)$ est principal.

Notation. *On garde celles des parties précédentes, en posant de plus $\boldsymbol{u} = (u^{1,d_1}, \ldots, u^{r,d_r})$. On notera $f_{V,d}$ la forme éliminante d'indice d associée à la variété V, i.e. $f_{V,d} = \mathrm{élim}_d(I(V))$. Si $d = \mathbf{1} = (1, \ldots, 1)$, $f_{V,d}$ est une* forme de Chow de V.

Pour $i \in [\![1, r]\!]$, on note $N_i = C^{d_i}_{n+d_i}$ le cardinal de $\mathfrak{M}_i$.

Définition 5.0.10. *La* variété caractéristique $C(V)$ *de V est définie par :*

$$C(V) = \{(x, u) \in \mathbb{P}_n(\mathbb{K}) \times \mathbb{P}_{n_1}(\mathbb{K}) \times \cdots \times \mathbb{P}_{N_r}(\mathbb{K}) / (x \in V) \wedge (U_{1,d_1}(x) = \cdots = U_{r,d_r}(x) = 0)\}.$$

A l'aide du *Nullstellensatz*, on vérifie alors que $I(C(V)) = I(V)A[\boldsymbol{u}] + U_{1,d_1}A[\boldsymbol{u}] + \cdots + U_{h,d_h}A[\boldsymbol{u}]$.

7. On pourra touver une démonstration de tous ces résultats dans [10].
8. On odopte la convention $\sup\emptyset = -1$

Donnons deux exemples d'utilisation du théorème d'élimination (TE) avec $d = (1, \dots, 1)$:

Exemple 1

Supposons que la variété V soit réduite à un point : $V = \{x\}$. Alors $r = 1$ et $U = U_{1,1} = u_0X_0 + \cdots + u_nX_n$. Le polynôme $f_{V,1}$ est alors dans $\mathbb{K}[\boldsymbol{u}] = \mathbb{K}[u_0, \dots, u_n]$ et $I(C(V)) = I(V)\mathbb{K}[X][\boldsymbol{u}] + U\mathbb{K}[X][\boldsymbol{u}]$, avec $I(V) = (X - x)$. Comme $\mathbb{K}$ est algébriquement clos, $f_{V,1}$ a toutes ses racines dans $\mathbb{K}^{n+1}$.

Appliquons maintenant (TE) : pour tout morphisme de $\mathbb{K}$-algèbres $\rho : \mathbb{K}[\boldsymbol{u}] \to \mathbb{K}$, on a l'équivalence

$$\rho(f_{V,1}) = 0 \iff \exists y \in \mathbb{K}^{n+1}\backslash\{0\}, \quad \forall F \in I(C(V)), \quad \rho(F)(y) = 0.$$

Comme $\rho(\mathbb{K}[X][\boldsymbol{u}]) = I(V)\rho(\mathbb{K}[\boldsymbol{u}])[X] + \rho(U)\rho(\mathbb{K}[\boldsymbol{u}])[X]$, pour que l'image par ρ de tout élément $F \in I(C(V))$ soit nulle, il faut et il suffit que $\rho(U(y)) = 0$ et que $\rho(F)(y) = F(y) = 0$ pour tout $F \in I(C(V))$. Puisque $I(V) = (X - x)$, on a nécessairement $y = \rho(x) = x$.

On a ainsi montré que, pour tout morphisme $\rho : \mathbb{K}[\boldsymbol{u}] \to \mathbb{K}$, on avait $\rho(f_{V,1}) = 0$ si, et seulement si, $(\rho(U))(\rho(x)) = \rho(U(x)) = 0$. En choisissant successivement pour ρ le morphisme qui envoie $\boldsymbol{u}$ sur une racine de $f_{V,1}$ dans un sens et sur une racine de $U(x)$ dans l'autre, il apparaît que $f_{V,1}$ et $U(x)$ ont exactement les mêmes racines, et sont donc proportionnels (le coefficient de proportionnalité étant un scalaire).

Toute forme de Chow de V est donc proportionnelle à $U(x)$.

Exemple 2

Supposons que $V = \mathfrak{Z}(F)$ soit une hypersurface. Comme $\dim(V) = n - 1$, on a ici $r = n$. Par ailleurs, $I(C(V)) = F.\mathbb{K}[X][\boldsymbol{u}] + \sum_{j=1}^{n} U_{j,1}\mathbb{K}[X][\boldsymbol{u}]$.

En adaptant sans difficulté le raisonnement tenu dans l'exemple 1, le théorème de l'élimination fournit une élément $y \in \mathbb{K}^{n+1}\backslash\{0\}$ tel que, pour tout morphisme de $\mathbb{K}$-algèbres $\rho : \mathbb{K}[\boldsymbol{u}] \to \mathbb{K}$, $\rho(f_{V,1}) = 0$ si, et seulement si, $F(y) = 0$ et pour tout $j \in [\![1, n]\!]$, $\rho(U_{j,1})(y) = 0$. Autrement dit, $\rho(f_{V,1}) = 0$ si, et seulement si, il existe $y \in V$ tel que, pour tout $j \in [\![1, n]\!]$, $\rho(U_{j,1})(y) = \sum_{k=0}^{n} \rho(u_k^{j,1})y_k = 0$. Or en fixant provisoirement ρ, ce dernier système d'équations linéaires s'écrit matriciellement sous la forme :

$$\underbrace{\begin{pmatrix} \rho\left(u_0^{1,1}\right) & \cdots & \rho\left(u_n^{1,1}\right) \\ \rho\left(u_0^{2,1}\right) & \cdots & \rho\left(u_n^{2,1}\right) \\ \vdots & \ddots & \vdots \\ \rho\left(u_0^{n,1}\right) & \cdots & \rho\left(u_n^{n,1}\right) \end{pmatrix}}_{=A_\rho(\boldsymbol{u}) \in M_{n,n+1}(\mathbb{K})} \begin{pmatrix} y_0 \\ y_1 \\ \vdots \\ \vdots \\ y_n \end{pmatrix} = 0.$$

En posant, pour $i \in [\![0, n]\!]$, $\Delta_i = (-1)^i.\rho\left[\det\left(u_\alpha^{j,1}\right)_{\substack{1 \le j \le n \\ 0 \le \alpha \le n, \alpha \neq i}}\right]$, Δ est solution du système linéaire puisqu'il traduit la nullité du déterminant de la matrice $A_\rho(\boldsymbol{u})$ à laquelle on a rajouté une dernière ligne nulle. La solution proposée est de plus non nulle si, et seulement si, $A_\rho(\boldsymbol{u})$ est de rang plein – cas auquel on se ramène facilement – et, dans ce cas, il s'agit là de l'unique solution au système à la multiplication par un scalaire près (par le théorème du rang).

On a donc montré que $\rho(f_{V,1}) = 0$ si, et seulement si, $\widetilde{F}[\rho(\boldsymbol{u})] = F[\rho(\Delta_0), \dots, \rho(\Delta_n)] = 0$. Par le même raisonnement que celui tenu dans l'exemple 1, on en déduit que toute forme de Chow de V est proportionnelle à la forme multi-homogène $F[\Delta_0, \dots, \Delta_n]$ (le facteur de proportionnalité étant un scalaire).

On va à présent définir différentes quantités attachées à une variété projective à travers sa forme éliminante d'indice d, que l'on a définie au paragraphe précédent.

5.1 Degré d'une variété

Si $f_{V,d}$ est un générateur de l'idéal $\mathfrak{E}_d(I)$, le polynôme $f^{\sigma}_{V,d}$ obtenu en permutant les arguments de $f_{V,d}$ selon une permutation σ de $[\![1,r]\!]$ apparaît comme un générateur de $\mathfrak{E}_{d^\sigma}(I)$ (avec des notations évidentes). En particulier, si d est invariant par permutation de ses coordonnées, $f_{V,d}$ est symétrique. Ceci justifie la définition suivante :

Définition 5.1.1. *On définit le* degré de la variété V *à partir de sa forme de Chow en posant*

$$\mathrm{d}(V) = \deg_{u^{i,d_i}} f_{V,(1,\dots,1)}.$$

Remarque 5.1.2. *Cette définition coïncide avec la définition habituelle du degré d'une variété, qui est le nombre d'éléments contenus dans l'intersection de V avec $r-1$ hypersurfaces dont les positions sont* suffisamment générales*. Pour plus de détails, on se reportera au chapitre 6 de [18].*

On cherche à présent à caractériser le degré de V en fonction du degré d'une forme éliminante d'indice d quelconque de V.

Posons $\mathbb{L} = \mathbb{K}(u^{1,d_1}, \dots, u^{r-1,d_{r-1}})$ et, pour $i = 1, \dots, h-1$, $H_i = \mathfrak{Z}(U_{i,d_i})$ (dans $\mathbb{L}$). Si I est tel que $V = \mathfrak{Z}(I)$, on a

$$\mathfrak{E}_d(I) = \mathfrak{E}_{d_r}(I[d_1, \dots, d_{r-1}]) = \mathfrak{E}_{d_h}(\mathfrak{U}_{(d_1,\dots,d_{r-1})})(I).$$

D'après la proposition 4.2.3, $\mathfrak{U}_{(d_1,\dots,d_{r-1})})(I)$ est un idéal premier de $A[(d_1, \dots, d_{r-1})]$ que l'on associe à une variété W. Par (TE) appliqué à l'extension $\mathbb{L}$ de $\mathbb{K}$ et en raisonnant de la même manière que dans les exemples 1 et 2 ci-dessus, $f_{V,d} = f_{W,d_h}$ s'annule sur le même ensemble que $\prod_{x \in V \cap H_1 \cap \dots \cap H_{h-1}} U_{h,d_h}(x)$; comme $f_{V,d}$ est irréductible ($\mathfrak{E}_d(I(V))$ est premier), elle est proportionnelle à cette dernière forme, le facteur de proportionnalité étant dans $\mathbb{L}^*$.

Posons $\boldsymbol{u'} = (u^{1,d_1}, \dots, u^{r-1,d_{r-1}}, u^{r,1})$ et $d' = (d_1, \dots, d_{r-1}, 1)$ et considérons le morphisme d'anneaux

$$\begin{aligned} \rho' \ &: \mathbb{K}[\boldsymbol{u}] \to \mathbb{K}[\boldsymbol{u'}] \\ &U_{h,d_h} \mapsto (U_{r,1})^{d_r} \end{aligned}$$

Ce qui précède montre que $f_{V,d}$ (resp. $f_{V,d'}$) est proportionnel à $\prod_{x \in V \cap H_1 \cap \dots \cap H_{r-1}} U_{r,d_h}(x)$ (resp. $\prod_{x \in V \cap H_1 \cap \dots \cap H_{r-1}} U_{r,1}(x)$). Comme le premier produit est envoyé par ρ' sur le second élevé à la puissance d_h, $\rho'(f_{V,d})$ est proportionnel à $(f_{V,d'})^{d_r}$ via une constante multiplicative dans $\mathbb{L}^*$. Le lemme suivant, qui découle de (TE) et qui se place dans un cadre plus général que celui qui nous intéresse, prouve que le facteur de proportionnalité est en fait dans $\mathbb{K}^*$:

Lemme 5.1.3. $\mathbb{K}$ *n'est plus supposé algébriquement clos. Soit P est un élément de $\mathbb{K}[u^{1,d_1}, \dots, u^{r-1,d_{r-1}}]$ qui divise $f_{V,d}$. Alors $P \in \mathbb{K}^*$.*

Démonstration. On considère le morphisme $\widetilde{\rho} : \mathbb{F}[\boldsymbol{u}] \to \mathbb{F}$, où $\mathbb{F}$ est une extension de $\mathbb{K}$ dans laquelle P a une racine, qui envoie les u^{i,d_i}, $1 \le i \le r-1$, sur une racine de P et U_{h,d_h} sur 1. Alors $\widetilde{\rho}(P) = 0$, donc $\widetilde{\rho}(f_{V,d}) = 0$; par (TE), il existe une extension $\mathbb{F}'$ de $\mathbb{F}$ et $x \in (\mathbb{F}')^{n+1}$ tel que x soit un zéro de $\widetilde{\rho}\,[I(C(V))]$. Ceci implique en particulier que $\widetilde{\rho}\,(U_{r,d_r})\,(x) = 0$, ce qui est absurde puisque $\widetilde{\rho}\,(U_{r,d_r}) = 1$. Donc P n'a pas de racines, i.e. $P \in \mathbb{K}^*$. □

Le lemme montre de même qu'aucun élément non constant de $\mathbb{K}[u^{1,d_1}, \dots, u^{r-1,d_{r-1}}]$ ne peut diviser $f_{V,d'}$, donc $(f_{V,d'})^{d_r}$.

En itérant le même raisonnement, il apparaît que, si l'on considère le morphisme ρ qui envoie chacun des U_{i,d_i} sur $(U_{i,1})^{d_i}$ pour $1 \le i \le r$, alors $\rho(f_{V,d})$ est proportionnel à $(f_{V,1})^{d_1 \dots d_r}$.

Ainsi,

$$\begin{aligned} \mathrm{d}(V) = \deg_{u^{i,d_i}} f_{V,(1,\dots,1)} &= \frac{1}{d_1 \dots d_r} \deg_{u^{i,d_i}} (f_{V,1})^{d_1 \dots d_h} \\ &= \frac{1}{d_1 \dots d_r} \deg_{u^{i,d_i}} \rho(f_{V,d}). \end{aligned}$$

Comme ρ préserve l'homogénéité et est de degré d_i en u^{i,d_i}, et comme $f_{V,1}$ est symétrique en chaque ensemble de variables, on a finalement montré que

$$\deg_{u^{i,d_i}} \rho(f_{V,d}) = \mathrm{d}(V)\frac{d_1 \dots d_r}{d_i}.$$

5.2 Hauteur d'une variété

Dans cette section, $\mathbb{L}$ désigne un corps de nombres

On veut définir la hauteur $\mathrm{h}(V)$ d'une variété définie sur un corps de nombres $\mathbb{L}$. Dans la même logique que ce qui précède, on posera $\mathrm{h}(V) = \mathrm{h}(f_{V,1})$ pour h une hauteur convenable sur $\mathbb{L}[\boldsymbol{u}]$.

Afin d'introduire au mieux la définition de la hauteur d'une variété, nous commençons par quelques rappels sur les valeurs absolues de corps de nombres.

5.2.1 Eléments de théorie de la valuation

Définition 5.2.1. *Une* norme sur $\mathbb{L}$ *est une application* $|.| : \mathbb{L} \to \mathbb{R}_+$ *vérifiant, pour tous* $x, y \in \mathbb{L}$ *:*

V1. $|x| = 0 \quad \Leftrightarrow \quad x = 0$ *;*

V2. $|xy| = |x||y|$ *;*

V3. $|x + y| \leq |x| + |y|$.

Si l'on fixe un nombre premier p et que l'on pose $\left|p^n \frac{a}{b}\right|_p = p^{-n}$ pour a, $b \in \mathbb{Z}$ non nuls premiers à p et $|0|_p = 0$, alors $|.|_p$ définit une norme sur $\mathbb{Q}$: la *norme p-adique*.

Définition 5.2.2. *Une* valeur absolue sur $\mathbb{L}$ *est une application* $|.| : \mathbb{L} \to \mathbb{R}_+$ *vérifiant (V1) et (V2) et telle qu'il existe une constante* $C \geq 0$ *satisfaisant* $|x + 1| \leq 1$ *pour tout* $x \in \mathbb{L}$ *tel que* $|x| \leq 1$.

Un corps muni d'une valeur absolue est un corps valué.

La constante d'Artin *de la valeur absolue* $|.|$ *est alors l'infimum des* $C > 0$ *satisfaisant la condition précédente.*

Un corps admet toujours au moins une valeur absolue qui, en l'occurrence, est aussi une norme : l'application qui vaut 0 en 0 et 1 en toute autre valeur. On la qualifie de *norme triviale*.

Voici un lemme presque évident mais très utile :

Lemme 5.2.3. *On munit* $\mathbb{L}$ *d'une valeur absolue* $|.|$*. Soit* $C \in [1; +\infty[$*. Les deux assertions suivantes sont alors équivalentes :*

i) $\forall x \in \mathbb{L}, \quad |x| \leq 1 \Rightarrow |x + 1| \leq C$.

ii) $\forall x, y \in \mathbb{L}, \quad |x + y| \leq C. \max(|x|, |y|)$.

Démonstration. L'implication $ii) \Rightarrow i)$ résulte du choix $y = 1$.

Pour la réciproque, on peut supposer sans perte de généralité $0 < |x| \leq |y|$. Comme $\left|\frac{x}{y}\right| \leq 1$, $\left|\frac{x}{y} + 1\right| \leq C$ et le résultat s'ensuit en multipliant cette dernière inégalité par y. □

Lemme 5.2.4. *On munit* $\mathbb{L}$ *d'une valeur absolue* $|.|$ *de constante d'Artin* C*. Alors* $|.|$ *est une norme si, et seulement si,* $C \leq 2$.

Nous figurons ci-dessous la démonstration dans son intégralité pour donner un archétype de preuve d'un résultat liant valeur absolue et norme.

Démonstration. Le sens direct ne présente aucune difficulté et découle de la simple inégalité triangulaire vérifiée par la norme. Intéressons-nous à la réciproque : soit x, $y \in \mathbb{L}$ que l'on supposera tels que $0 < |x| \leq |y|$. Alors

$$\left|\frac{x}{y}\right| \leq 1 \quad \Longrightarrow \quad \left|1 + \frac{x}{y}\right| \leq C \leq 2 \quad \Longrightarrow \quad |x + y| \leq 2|y| = 2\max(|x|, |y|).$$

Par récurrence, on en déduit que, pour tous $x_1, \ldots, x_{2^n} \in \mathbb{L}$ tels que $0 < |x_1| \leq \cdots \leq |x_{2^n}|$, $|x_1 + \cdots + x_{2^n}| \leq 2^n \max\limits_{1 \leq i \leq 2^n} |x_i|$. Pour $r \in \mathbb{N}$ tel que $n \leq 2^r < 2n$, il vient alors :

$$|x_1 + \cdots + x_n| = |x_1 + \cdots + x_n + \underbrace{0 + \cdots + 0}_{(2^r - n) fois}| \leq 2^r \max_{1 \leq i \leq 2^r} |x_i| \leq 2n \max_{1 \leq i \leq n} |x_i| .$$

En évaluant d'une part cette inégalité en $x_1 = \cdots = x_n = 1$, on a $|n| \leq 2n$. D'autre part, on a aussi $|x_1 + \cdots + x_n| \leq 2n \max\limits_{1 \leq i \leq n} |x_i| \leq 2n \sum_{i=1} |x_i|$. Ces deux dernières relations permettent finalement d'écrire que, pour tous x, $y \in \mathbb{L}$ tels que $0 < |x| \leq |y|$ et pour tout entier naturel n,

$$\begin{aligned} |x+y|^n = \left| \sum_{k=0}^{n} C_n^i x^i y^{n-i} \right| &\leq 2(n+1) \sum_{k=0}^{n} \left| C_n^i \right| \left| x^i \right| \left| y^{n-i} \right| \\ &\leq 4(n+1) \sum_{k=0}^{n} C_n^i \left| x^i \right| \left| y^{n-i} \right| = 4(n+1) \left(|x| + |y| \right)^n . \end{aligned}$$

En prenant la racine $n^{ème}$ des deux inégalités extrêmes et faisant tendre n vers l'infini, on obtient bien $|x + y| \leq |x| + |y|$. □

Le principal intérêt des valeurs absolues par rapport aux normes est exposé dans le lemme suivant dont la démonstration est triviale dès lors que l'on fait appel au précédent énoncé :

Lemme 5.2.5. *Soit* $|.| : \mathbb{L} \to \mathbb{R}_+$ *une valeur absolue sur* $\mathbb{L}$ *de constante d'Artin* $C > 0$. *Soit* $\alpha > 0$ *et*

$$\begin{aligned} |.|^\alpha \ : \mathbb{L} &\to \mathbb{R}_+ \\ x &\mapsto |x|^\alpha \end{aligned}$$

Alors :

1. $|.|^\alpha$ *est une valeur absolue de constante d'Artin* C^α.
2. *Même si* $|.|$ *est une norme,* $|.|^\alpha$ *n'est pas toujours une norme.*

Définition 5.2.6. *Une valeur absolue* $|.|$ *sur* $\mathbb{L}$ *est* non archimédienne *ou* ultramétrique *si sa constante d'Artin est égale à 1. Elle vérifie alors l'*inégalité ultramétrique *:*

$$\forall x, y \in \mathbb{L}, \quad |x + y| \leq \max\left(|x|, |y| \right) .$$

Une valeur absolue dont la constante d'Artin est strictement supérieure à 1 est archimédienne.

Remarque 5.2.7. *D'après le lemme 5.2.5, une valeur absolue sur* $\mathbb{L}$ *est archimédienne (resp. non archimédienne) si, et seulement si, toute valeur absolue qui lui est équivalente est archimédienne (resp. non archimédienne), où l'équivalence entre valeurs absolues est définie comme suit :*

Définition 5.2.8. *Deux valeurs absolues* $|.|_1$ *et* $|.|_2$ *sont équivalentes s'il existe* $\alpha > 0$ *tel que* $|.|_2 = |.|_1^\alpha$.

On notera alors $|.|_1 \sim |.|_2$, $\sim$ ainsi définie étant clairement une relation d'équivalence.

Remarque 5.2.9. *D'après le lemme 5.2.4, toute valeur absolue sur* $\mathbb{L}$ *est équivalente à une norme.*

Définition 5.2.10. *Une* place *sur* $\mathbb{L}$ *est une classe d'équivalence de valeurs absolues.*

Le résultat qui suit prouve que deux valeurs absolues équivalentes et non triviales sur $\mathbb{L}$ y déterminent un même espace topologique : on peut donc choisir des représentants quelconques des classes d'équivalence des places pour parler du complété de $\mathbb{L}$, le corps obtenu étant indépendant du choix effectué.

Théorème 5.2.11. *Soit $|.|_1$ et $|.|_2$ deux valeurs absolues non triviales sur $\mathbb{L}$. Les propositions suivantes sont équivalentes :*

i) $|.|_1 \sim |.|_2$

ii) *Pour tout $x \in \mathbb{L}$,*

$$\begin{cases} |x|_1 < 1 & \Leftrightarrow & |x|_2 < 1 \\ |x|_1 > 1 & \Leftrightarrow & |x|_2 > 1 \\ |x|_1 = 1 & \Leftrightarrow & |x|_2 = 1 \end{cases}$$

Démonstration. L'implication $i) \Rightarrow ii)$ est immédiate. Supposons donc $ii)$. Soit $a \in \mathbb{L}$ tel que $|a|_1$ soit non nul et différent de 1 (ce qui est possible puisque la valeur absolue est non triviale). Quitte à remplacer a par a^{-1}, on peut supposer $|a|_1 < 1$. Par hypothèse, on a alors $|a|_2 < 1$. Posons $\alpha = \frac{\log |a|_2}{\log |a|_1} > 0$. On va montrer que $|.|_1^\alpha = |.|_2$.

Soit $x \in \mathbb{L}$ et, pour $i \in \{1, 2\}$, $\gamma_i = \frac{\log |x|_i}{\log |a|_i}$. Il suffit de montrer que $\gamma_1 = \gamma_2$. On prend $\frac{p}{q} \in \mathbb{Q}$, avec $q > 0$:

$$\frac{p}{q} \geq \gamma_1 \Leftrightarrow p \log |a|_1 \leq q \log |x|_1 \Leftrightarrow |a^p|_1 \leq |x^q|_1 \Leftrightarrow \left|\frac{x^q}{a^p}\right|_1 \geq 1 \underset{ii)}{\Leftrightarrow} \left|\frac{x^q}{a^p}\right|_2 \geq 1 \Leftrightarrow p \log |a|_2 \leq q \log |x|_2$$
$$\Leftrightarrow \frac{p}{q} \geq \gamma_2,$$

ce qui achève la preuve. □

Nous terminons ces rappels par l'évocation d'un résultat fondamental dont la preuve, même si elle n'est pas très difficile, requiert l'introduction d'outils qui ne nous seront pas utiles par la suite. Nous l'admettrons donc, en renvoyant à [6] (chapitre 1) pour en trouver la substance.

La valeur absolue usuelle sur $\mathbb{C}$ sera notée $|.|_\infty$.

Théorème 5.2.12 (Théorème d'Ostrowski pour les corps de nombres)**.** *Soit $\mathbb{L}$ un corps de nombres. Ecrivons $\mathbb{L} = \mathbb{Q}[X]/(P(X))$. Alors :*

1. *Toute valeur absolue ultramétrique $|.|$ de $\mathbb{L}$, lorsqu'on la restreint à $\mathbb{Q}$, est équivalente à une valuation p-adique pour un certain $p \in \mathcal{P}$. On dit alors que p est le* nombre premier sous $|.|$.
2. *A équivalence près, toute valeur absolue archimédienne de $\mathbb{L}$ est de la forme $x \mapsto |\iota(x)|_\infty$ où $\iota : \mathbb{L} \hookrightarrow \mathbb{C}$ est un plongement de corps.*
3. *Si r_1 est le nombre de racines réelles de P et r_2 la moitié du nombre de racines complexes de P, alors le nombre de plongements de $\mathbb{L}$ dans $\mathbb{C}$, donc le nombre de places archimédiennes de $\mathbb{L}$ vaut $r = r_1 + r_2$.*

5.2.2 Définitions et premières propriétés

A la lumière des propos tenus dans le paragraphe précédent, si ν est une place de $\mathbb{L}$, on notera $\mathbb{L}_\nu$ le complété de $\mathbb{L}$ pour une valeur absolue $|.|_\nu$ associée à ν.

Pour chaque place, on fixe une valeur absolue représentant ν : dans le cas archimédien, cela revient à fixer un plongement $\sigma_\nu : \mathbb{L} \to \mathbb{C}$ tel que le valeur absolue normalisée soit simplement $|\sigma_\nu(.)|$; dans le cas ultramétrique, on impose $|p|_\nu = p^{-1}$ pour le nombre premier p sous ν. On désignera alors par $\mathcal{M}_\mathbb{L}$ (resp. $\mathcal{M}_\mathbb{L}^\infty$) l'ensemble des représentants normalisés des places de $\mathbb{L}$ (resp. des places archimédiennes de $\mathbb{L}$). On rappelle la formule du produit : en notant $n_\nu = [\mathbb{L}_\nu : \mathbb{Q}_\nu]$ pour $\nu \in \mathcal{M}_\mathbb{L}$, on a [9], pour tout $x \in \mathbb{L}\backslash\{0\}$,

$$\prod_{\nu \in \mathcal{M}_\mathbb{L}} |x|_\nu^{n_\nu} = 1.$$

9. On trouvera une démonstration de cette propriété dans [29], chap.3, paragraphe 1.

Pour $x \in \mathbb{L}^s$, on pose $|x|_\nu = \sqrt{|x_1|_\nu^2 + \cdots + |x_s|_\nu^2}$ si ν est archimédienne et $|x|_\nu = \max(|x_1|_\nu, \ldots, |x_s|_\nu)$ si ν est ultramétrique.

On peut à présent définir la *hauteur invariante* d'un élément $f \in \mathbb{L}[\boldsymbol{u}]$:

Définition 5.2.13. *Avec les notations précédentes, on pose*

$$\mathrm{h}(f) = \sum_{\nu \in \mathcal{M}_{\mathbb{L}}} \frac{[\mathbb{L}_\nu : \mathbb{Q}_\nu]}{[\mathbb{L} : \mathbb{Q}]} \log M_\nu(f),$$

où $M_\nu(f)$ est le maximum des valeurs absolues ν-adiques des coefficients de f si ν est ultramétrique et, si $\sigma_\nu : \mathbb{L} \to \mathbb{C}$ est le plongement associé à ν dans le cas archimédien,

$$\log M_\nu(f) = \int_{S_{N_1+1} \times \cdots \times S_{N_r+1}} \log |\sigma_\nu(f)| \eta_{N_1+1} \wedge \cdots \wedge \eta_{N_1+1} + \sum_{i=1}^{r} \deg_{u^{i,d_i}}(f) \sum_{j=1}^{N_i} \frac{1}{2j},$$

où $\sigma_\nu(f)$ se déduit naturellement de f, S_{N+1} est la sphère unité de $\mathbb{C}^{N+1}$ et η_{N+1} la mesure de Haar sur la sphère S_{N+1} de masse totale unité[10].

On rappelle que, dans cette définition, N_i $(1 \leq i \leq r)$ est le cardinal de $\mathfrak{M}_i$.

Remarque 5.2.14. *A $x \in \mathbb{L}$ fixé, le cardinal des valeurs absolues ν telles que $|x|_\nu \neq 1$ est fini. Ceci justifie l'existence de* $\mathrm{h}(f)$ *telle que définie ci-dessus. Par ailleurs, on vérifie à l'aide de la formule du produit que* $\mathrm{h}(f)$ *est indépendant du choix du corps contenant les coefficients de f (pour approfondir ces deux remarques, cf. [29], p.74-75).*

Dans le cas archimédien, le terme additif correctif est étudié pour que la hauteur ainsi définie soit toujours positive. On remarquera également que, par application directe de la formule du produit, $\mathrm{h}(\lambda f) = \mathrm{h}(f)$ pour tout $\lambda \in \mathbb{L}^*$.

Il est évident que, dans le cas ultramétrique, $\log M_\nu(U_{i,d_i}(x)) = d_i \log \|x\|_\nu$. Ceci est encore vrai dans le cas archimédien puisqu'un petit calcul montre que

$$M_\nu\left(U_{i,d_i}(x)\right) = M_\nu\left(\sum_{\mathfrak{m} \in \mathfrak{M}_{d_i}} u_{\mathfrak{m}}^{(i,d_i)} \mathfrak{m}(x)\right) = \sqrt{\sum_{\mathfrak{m} \in \mathfrak{M}_{d_i}} |\mathfrak{m}(x)|_\nu^2} = \|x\|_\nu^{d_i}.$$

En réitérant le résonnement tenu dans le paragraphe 5.1, la prise en compte de l'égalité précédente permet finalement d'aboutir à la relation :

$$\mathrm{h}(f_{V,d}) = d_1 \ldots d_h . \mathrm{h}(V)$$

Remarque 5.2.15. *Si $V = \mathfrak{Z}(F)$ est une hypersurface, la formule donnée dans la définition 5.2.13 se simplifie sous la forme*

$$h(V) = h(F) + \deg F \sum_{i=1}^{n-1} \sum_{j=1}^{i} \frac{1}{2j}.$$

10. Dans [21], P. Philippon utilise dans le cas archimédien une mesure légèrement différente :

$$\log M_\nu(f) = \int_0^1 \mathrm{d}u_m \ldots \int_0^1 \mathrm{d}u_1 \log \left|\sigma(f)(e^{2i\pi u_1}, \ldots, e^{2i\pi u_m})\right|.$$

Les deux points de vue sont essentiellement équivalents.

5.3 Théorèmes de Bézout arithmétique et géométrique

Dans ce paragraphe, $\mathbb{L}$ désigne encore un corps de nombres et $\mathbb{K}$ une extension algébriquement close.

Il est fréquent en approximation diophantienne, lorsque l'on souhaite démontrer une propriété pour une variété V, de se ramener à un problème de dimension $\dim V - 1$ en considérant l'intersection avec une hypersurface H convenablement choisie. Il est alors important de pouvoir majorer le degré et la hauteur de $V \cap H$ en fonction des quantités correspondantes pour V et H. Un tel résultat porte le nom de *théorème de Bézout*. On peut dans les faits établir de tels théorèmes pour une intersection de variétés V et W quelconques, mais la situation est alors très compliquée. Nous nous restreindrons donc, et cela nous sera suffisant pour les objectifs poursuivis, au cas où W est une hypersuface $\mathfrak{Z}(F)$.

Définition 5.3.1. *Un* cycle *est une combinaison linéaire formelle Z de variétés à coefficients dans $\mathbb{N}$: $Z = \sum_{j=1}^{s} m_j V_j$. Un cycle est* équidimensionnel *de dimension $l \in \mathbb{N}$ si toutes les variétés concernées sont de dimension l.*

On étend naturellement par linéarité les notions de degré et de hauteur à un cycle.

En général, si ρ est un morphisme de $\mathbb{L}[u^{r,d_r}]$ dans $\mathbb{L}$, bien que l'on vérifie aisément que $\rho(f_{V,d}) \in \mathfrak{E}_{d_1,\dots,d_{r-1}}(\rho(I[d_r]))$, il n'est pas vrai que $\rho(f_{V,d})$ soit une forme éliminante d'indice $(d_1,\dots,d_{r-1})$ de $\rho(I[d_r])$. Cependant, le lemme suivant permet de caractériser $\rho(f_{V,d})$ comme une forme d'-éliminante associée à un cycle, où $d' = (d_1,\dots,d_{h-1})$:

Lemme 5.3.2. *Soit un morphisme $\rho : \mathbb{L}[u^{r,d_r}] \to \mathbb{K}$ tel que $\rho(f_{V,d}) \neq 0$ (i.e. $\rho(U_{r,d_r}) \notin I(V)$ par (TE)). Soit $f_1,\dots,f_t$ les formes éliminantes d'indice $(d_1,\dots,d_{r-1})$ des idéaux premiers minimaux contenant l'idéal $J = (I(V), \rho(U_{r,d_r}))$ de $\mathbb{K}[X]$.*

Alors il existe des entier naturels non nuls $l_1,\dots,l_t$ et un élément $\lambda \in \mathbb{K}$ tels que

$$\rho(f_{V,d}) = \lambda \prod_{h=1}^{t} f_h^{l_h}.$$

Remarque 5.3.3. *Le résultat est encore vrai si $\rho(f_{V,d}) = 0$ puisqu'il suffit de choisir $\lambda = 0$. Il revient plus généralement à affirmer que l'on connaît la forme des spécialisations des formes éliminantes, i.e. la valeur des formes éliminantes par un morphisme d'anneau non nul à valeurs dans un corps.*

Démonstration. Notons $\mathfrak{q}_1,\dots,\mathfrak{q}_t$ les idéaux premiers minimaux contenant J ordonnés en choisissant $t' \in [\![0,t]\!]$ tel que $\mathfrak{M}_1 \subset \mathfrak{q}_i \Leftrightarrow i > t'$. En particulier, $\sqrt{J} = \bigcap_{i=1}^{t} \mathfrak{q}_i$.

Soit un morphisme de $\mathbb{K}$-algèbres $\rho' : \mathbb{K}[d'] \to \mathbb{K}$. On note $\widetilde{\rho}$ le morphisme $\mathbb{L}[\boldsymbol{u}] \to \mathbb{K}$ obtenu à partir de ρ et de ρ'. On a donc $\widetilde{\rho}(f_{V,d}) = \rho'(\rho(f_{V,d}))$. Or par (TE), en posant $I = I(V)$, $\widetilde{\rho}(f_{V,d})$ est nul si, et seulement si, $\widetilde{\rho}(\mathfrak{E}_d(I))$ est nul, chose équivalente à l'existence d'un zéro non trivial de $\widetilde{\rho}(I[d])$ dans $\mathbb{K}^{n+1}$.

Mais par définition de $I[d]$ et de $\widetilde{\rho}$, $\widetilde{\rho}(I[d]) = (J, \rho'(U_{1,d_1}),\dots,\rho'(U_{r-1},d_{r-1})) = \rho'(J[d'])$. En outre, on a clairement

$$\begin{aligned}\left(J, \rho'(U_{1,d_1}),\dots,\rho'(U_{r-1,d_{r-1}})\right) &\subset \left(\sqrt{J}, \rho'(U_{1,d_1}),\dots,\rho'(U_{r-1,d_{r-1}})\right) \\ &\subset \sqrt{\left(J, \rho'(U_{1,d_1}),\dots,\rho'(U_{r-1,d_{r-1}})\right)},\end{aligned}$$

ce qui prouve que $\rho'(J[d'])$ et $\rho'(\sqrt{J}[d'])$ ont même ensemble de zéros.

En appliquant le théorème de l'élimination à ρ', il vient, d'après ce qui précède :

$$\rho'\left(\rho(f_{V,d})\right) = 0 \Leftrightarrow \rho'\left(J[d']\right) = 0 \Leftrightarrow \rho'\left(\sqrt{J}[d']\right) = 0 \Leftrightarrow \rho'\left(\mathfrak{E}_{d'}\left(\sqrt{J}\right)\right) = 0.$$

Ceci étant valable pour tout morphisme ρ', $\mathfrak{Z}\left(\rho(f_{V,d})\right) = \mathfrak{Z}\left(\mathfrak{E}_{d'}\left(\sqrt{J}\right)\right)$, puis, $\mathbb{K}$ étant algébriquement clos, par le *Nullstellensatz* (théorème 5.0.6), $\sqrt{\rho(f_{V,d})} = \sqrt{\mathfrak{E}_{d'}\left(\sqrt{J}\right)}$.

En invoquant à présent la proposition 4.2.3, il vient :

$$\mathfrak{E}_{d'}\left(\sqrt{J}\right) = \mathfrak{E}_{d'}\left(\bigcap_{i=1}^{t}\mathfrak{q}_i\right) = \bigcap_{i=1}^{t}\mathfrak{E}_{d'}\left(\mathfrak{q}_i\right) = \bigcap_{i=1}^{t'}\mathfrak{E}_{d'}\left(\mathfrak{q}_i\right),$$

la dernière égalité étant justifiée par le fait que, si $i > t'$, alors $\mathfrak{M}_1 \subset \mathfrak{q}_i$, d'où $\mathfrak{E}_{d'}\left(\mathfrak{q}_i\right) = \mathbb{K}[d']$.

Toujours d'après la proposition 4.2.3, chaque $\mathfrak{E}_{d'}\left(\mathfrak{q}_i\right)$ est premier pour $1 \leq i \leq t'$, donc

$$\sqrt{\rho(f_{V,d})} = \bigcap_{i=1}^{t'}\mathfrak{E}_{d'}\left(\mathfrak{q}_i\right).$$

Or pour $1 \leq i \leq t'$, $\mathrm{ht}(\mathfrak{q}_i) = \mathrm{ht}(J)$ par minimalité de $\mathfrak{q}_i$ et [11] $\mathrm{ht}(\mathfrak{q}_i) = n - r + 2$. Par conséquent, $\mathfrak{E}_{d'}(\mathfrak{q}_i)$ $(1 \leq i \leq t')$ est engendré par $f_i = \mathrm{élim}_{d'}(\mathfrak{q}_i)$ (d'après le théorème 4.3.2). Par factorialité, on a alors $\left(\sqrt{\rho(f)}\right) = \sqrt{(f_1, \ldots, f_{t'})}$ puis $\rho(f) = \lambda \prod_{i=1}^{t'} f_i^{l_i}$ avec $\lambda \in \mathbb{K}$ et $l_i \geq 1$ entier.

Enfin pour $i > t'$, on a $\mathcal{M}_i \subset \mathfrak{q}_i$, de sorte que $\mathfrak{E}_{d'}(\mathfrak{q}_i) = \mathbb{K}[d']$ et $f_i = \mathrm{élim}_{d'}(\mathfrak{q}_i) = 1$. En posant par exemple $l_i = 1$ pour $i > t'$, on a donc

$$\rho(f) = \lambda \prod_{i=1}^{t} f_i^{l_i}.$$

□

Sous les hypothèses du lemme, on dira que $\rho(f_{V,d})$ est une forme éliminante d'indice $(d_1, \ldots, d_{r-1})$ associé au cycle équidimensionel $Z = \sum_{j=1}^{t'} l_j V_j$ où V_j est une variété (de dimension $r-2$) associée à $f_j \neq 1$.

On considère l'intersection $V \cap W$ comme un ensemble algébrique : en général, ce n'est pas une variété. Il est néanmoins possible de lui associer une forme éliminante comme suit : si $P_1, \ldots, P_t$ sont les idéaux premiers minimaux associés à une décomposition primaire normale de l'idéal $I(V \cap W)$, on pose $d' = (d_1, \ldots, d_{r-1})$ et

$$f_{V\cap W, d'} = \prod_{i=1}^{t} f_i \quad \text{avec} \quad f_i = \mathrm{élim}_{d'}(P_i).$$

Il est ainsi possible de définir le degré de $V \cap W$ de manière analogue à celui de V, comme il a été vu précédemment.

Théorème 5.3.4 (Théorème de Bézout géométrique)**.** *Si $V \cap W \neq \emptyset$, alors*

$$\mathrm{d}(V \cap W) \leq \mathrm{d}(V)\mathrm{d}(W) = \mathrm{d}(V)\deg(F).$$

Démonstration. En utilisant la caractérisation du degré donnée au paragraphe 5.1 et le second exemple introductif à la section, on constate tout d'abord que l'on a bien $\mathrm{d}(W) = \deg F$.

On considère ensuite l'homorphisme de $\mathbb{K}$-algèbres $\rho_F : \mathbb{K}[\boldsymbol{u}] \to \mathbb{K}[\boldsymbol{u'}]$ (où l'on rappelle que $\boldsymbol{u'} = (u^{1,d_1}, \ldots, u^{r-1,d_{r-1}})$) défini comme le prolongement naturel du morphisme $\rho_F : \mathbb{K}[u^{r,d_r}] \to \mathbb{K}$ vérifiant $\rho_F(U_{r,d_r}) = F$. Par le lemme 5.3.2, il est possible d'associer un cycle $Z = \sum_{j=1}^{t} m_j V_j$ à $\rho_F(f_{V,d})$ de telle sorte que $\rho_F(f_{V,d}) = \lambda \prod_{j=1}^{t} f_{V_j,d'}^{m_j}$. Dans toute la suite, on notera $V.W$ ce cycle.

11. On utilise ici le caractère caténaire de l'anneau $\mathbb{K}[X]$

Comme $m_j \geq 1$ pour tout $j \in [\![1,t]\!]$, par définition de $f_{V\cap W,d'}$, il est clair que $f_{V\cap W,d'}$ divise $\rho_F(f_{V,d})$. Posons dès lors $d = (1,\dots,1,\deg F)$: en utilisant une fois encore la caractérisation du degré donnée plus haut, il vient :

$$\begin{aligned}\mathrm{d}(V)\mathrm{d}(W) = \mathrm{d}(V)\deg F = \deg_{u^{1,1}}(f_{V,d}) = \deg_{u^{1,1}}(\rho_F(f_{V,d})) = \mathrm{d}(V.W) \geq \deg_{u^{1,1}}(f_{V\cap W,d'}) \\ = \mathrm{d}(V\cap W).\end{aligned}$$

□

Remarque 5.3.5. *On a en particulier montré que* $\mathrm{d}(V.W) = \mathrm{d}(V)\mathrm{d}(W)$.

On s'intéresse maintenant au comportement de la hauteur définie à la section précédente par rapport à l'intersection.

Si $\alpha = (\alpha_0,\dots,\alpha_n) \in \mathbb{N}^{n+1}$ est un multi-indice et k un entier, on note $C_k^\alpha = C_{k!}^{\alpha_0!\dots\alpha_n!}$ et $|\alpha| = \sum_{i=0}^n \alpha_i$.

On définit une hauteur légèrement modifiée h_1 sur les polynômes homogènes $P \in \mathbb{L}[X_0,\dots,X_n]$ en posant

$$\mathrm{h}_1(P) = \sum_{\nu\in\mathcal{M}_{\mathbb{L}}} \frac{[\mathbb{L}_\nu : \mathbb{Q}_\nu]}{[\mathbb{L} : \mathbb{Q}]} \log \|P\|_\nu,$$

où $\|P\|_\nu$ est le maximum des valeurs absolues des coefficients P_α de P si ν est ultramétrique et $\left(\sum_{|\alpha|=d^\circ P} \left(C_{d^\circ P}^\alpha\right)^{-1} |\sigma_\nu(P_\alpha)|^2\right)^{1/2}$ si ν est archimédienne associée au plongement $\sigma_\nu : \mathbb{L} \to \mathbb{C}$.

Remarque 5.3.6. *Dans ces conditions, pour* $x \in \mathbb{P}_n(\mathbb{C}_\nu)$, $|F(x)|_\nu \leq \|F\|_\nu \|x\|_\nu$, *le résultat étant évident dans le cas ultramétrique et provenant de l'inégalité de Cauchy-Schwarz dans le cas archimédien. On en déduit que* $M_\nu(F) = \|F\|_\nu$ *si* ν *est ultramétrique et* $M_\nu(F) \leq \|F\|_\nu \exp\left(\deg F.\sum_{j=1}^n \frac{1}{2j}\right)$ *sinon.*

A l'inverse[12]*, on a* $\|F\|_\nu \leq M_\nu(F).(n+1)^{(\deg F)/2}$ *dans le cas archimédien.*

Les outils introduits servent à l'énoncé du théorème suivant dont la preuve, qui dépasse le cadre des propos ici tenus, figure dans [18] (chapitre 6) :

Théorème 5.3.7 (Théorème de Bézout arithmétique)**.** *En adoptant les mêmes notations que ci-dessus, si* $V \cap W \neq \emptyset$, *alors*

$$\mathrm{h}(V\cap W) \leq \mathrm{h}(V)\deg F + \mathrm{h}_1(F)\mathrm{d}(V).$$

5.4 Distance d'un point à une variété

On se restreint dans ce paragraphe au cas d'une variété projective V définie sur $\mathbb{K} = \mathbb{C}$.

Soit $x \in \mathbb{P}_n(\mathbb{C})$. On veut d'abord définir des formes générales qui s'annulent en $x \in \mathbb{P}_n(\mathbb{C})$. On posera à cet effet $f_{V,d} = f$ pour simplifier les notations.

Soit le morphisme de $\mathbb{K}$-algèbres :

$$\begin{aligned}\partial_x : \mathbb{C}[\boldsymbol{u}] &\to \mathbb{C}[\boldsymbol{s}] \\ u_{\mathfrak{m}}^{i,d_i} &\mapsto \sum_{\mathfrak{m}'\in\mathfrak{M}_{d_i}} s_{\mathfrak{m},\mathfrak{m}'}^{i,d_i}\mathfrak{m}'(x),\end{aligned}$$

où $(s_{\mathfrak{m},\mathfrak{m}'}^{i,d_i})$ est une collection de nouvelles variables liées par les seules relations $s_{\mathfrak{m},\mathfrak{m}'}^{i,d_i} + s_{\mathfrak{m}',\mathfrak{m}}^{i,d_i} = 0$. On remarquera que le morphisme ∂_x ainsi défini dépend du choix des coordonnées homogènes de x.

12. Toutes ces inégalités, et notamment la dernière, restent valables dans le cas où l'on définit dans le cas archimédien $M_\nu(F)$ comme dans la note de bas de page n°10. On trouvera la (difficile) preuve de la dernière inégalité pour les deux choix de $M_\nu(F)$ dans le lemme 3 du chapitre 7 de [18].

Du fait des relations d'antisymétrie, les formes $\partial_x(U_{i,d_i})$ $(1 \leq i \leq r)$ s'annulent en x :

$$\partial_x(U_{i,d_i}) = \partial_x\left(\sum_{\mathfrak{m}\in\mathfrak{M}_{d_j}} u^{i,d_i}_{\mathfrak{m}}\mathfrak{m}(x)\right) = \sum_{\mathfrak{m}\in\mathfrak{M}_{d_j}} \mathfrak{m}(x) \sum_{\mathfrak{m}'\in\mathfrak{M}_{d_j}} s^{j,d_j}_{\mathfrak{m},\mathfrak{m}'}\mathfrak{m}'(x)$$
$$= \frac{1}{2}\sum_{\mathfrak{m},\mathfrak{m}'\in\mathfrak{M}_{d_j}} \mathfrak{m}(x)\mathfrak{m}'(x)\underbrace{\left(s^{j,d_j}_{\mathfrak{m},\mathfrak{m}'} + s^{j,d_j}_{\mathfrak{m}',\mathfrak{m}}\right)}_{=0} = 0.$$

On déduit alors de (TE) que x est dans V si, et seulement si, $\partial_x f = 0$.

La «taille» de $\partial_x f$ va mesurer la distance de x à V. Plus précisément, on pose :

$$\mathrm{Dist}_d(x,V) = \frac{M(\partial_x f)}{M(f)\prod_{i=1}^r \|x\|^{d_i \deg_{u^{i,d_i}} f}},$$

où pour $P(X) = \sum a_{i_1,\ldots,i_n} X^{i_1}\ldots X^{i_n}$, on a noté $M(P) = \max_{i_1,\ldots,i_n}\{|a_{i_1,\ldots,i_n}|\}$ et où $\|.\|$ est la norme euclidienne canonique.

Il convient de noter que cette définition est indépendante du choix du représentant homogène de x.

Si $Z = \sum_{i=1}^p m_i V_i$ est un cycle équidimensionnel de dimension $r-1$, on définit de même la distance de x à Z pour l'indice d par :

$$\mathrm{Dist}_d(x,Z) = \prod_{i=1}^p \mathrm{Dist}_d(x,V_i)^{m_i}.$$

Remarque 5.4.1. *Si $W = \mathfrak{Z}(F)$ est une hypersurface, alors $\mathrm{Dist}(x,W) = \frac{|F(x)|}{M(F)\|x\|^{\deg F}}$. Ceci se déduit d'un calcul à partir de l'expression de $f_{V,d}$ en fonction de F donnée dans l'exemple 2 en préambule à la section.*

Si $d = (1,\ldots,1)$, on note plus simplement $\mathrm{Dist}(x,V)$ pour $\mathrm{Dist}_d(x,V)$. De même, si $V = \{y\}$, on pose $\mathrm{Dist}(x,\{y\}) = \mathrm{Dist}(x,y)$. On a alors le résultat suivant, qui nous servira par la suite et dont on trouvera la preuve au chapitre 6 de [18] :

Théorème 5.4.2 (Propriété du point le plus proche)**.** *Avec les notations précédentes, il existe $y \in V$ tel que*

$$\mathrm{Dist}(x,y) \leq \mathrm{Dist}^{1/\mathrm{d}(V)} \exp\left(\sum_{i=1}^n \frac{h}{i}\right).$$

5.5 Théorèmes métriques de Bézout

Les deux théorèmes qui suivent joueront un rôle fondamental dans la démonstration du critère d'indépendance algébrique de P.Philippon. Une démonstration en est donnée dans [18], chapitre 6.

Théorème 5.5.1 (Premier théorème métrique de Bézout)**.** *Soit V une sous-variété projective de $\mathbb{P}_n(\mathbb{C})$ définie sur un corps de nombres $\mathbb{L}$, $F \in \mathbb{L}[X_0,\ldots,X_n]$ un polynôme homogène de degré d, $x \in \mathbb{P}_n(\mathbb{C})$ et $T \in \mathbb{N}^*$. On fixe un plongement $\mathbb{L} \hookrightarrow \mathbb{C}$ et l'on pose $\Delta = [\mathbb{L}:\mathbb{Q}]$ si $\mathbb{L}$ est réel et $\Delta = [\mathbb{L}:\mathbb{Q}]/2$ si $\mathbb{L}$ est imaginaire. Soit $W = V.\mathfrak{Z}(F)$. On a alors :*

$$\frac{1}{\Delta}\log \mathrm{Dist}(x,W) + \mathrm{h}(W) \leq \frac{1}{\Delta}\log\left[\mathrm{Dist}(x,W)^T + \sum_{t=0}^{T-1}\frac{\|F^{(t)}(x)\|}{\|F\|}\mathrm{Dist}(x,V)^t\right]$$
$$+ d.\mathrm{h}(V) + \mathrm{d}(V)\left[\mathrm{h}_1(F) + \frac{(T+2d)r}{\Delta}\log(n+1)\right],$$

où

$$\|F^{(t)}\|(x) = \sqrt{\sum_{\substack{\tau\in\mathbb{N}^{n+1}\\|\tau|=t}} \frac{|F^{(\tau)}(x)|^2}{C_t^\tau \|x\|^{2(\deg F-\tau)}}},$$

$\|.\|$ *étant ici la norme euclidienne cononique (pour* x*) et* $F^\tau(x)$ *le coefficient de* $Y^{\tau_0}\dots Y^{\tau_n}$ *(*$\tau = (\tau_1,\dots,\tau_n)$*) dans le développement de* $F(x+Y)$*.*

Théorème 5.5.2 (Second théorème de Bézout métrique)**.** *Soit* $\sigma \geq 1$ *un réel,* V *une sous-variété projective de* $\mathbb{P}_n(\mathbb{C})$ *définie sur un corps de nombres* $\mathbb{L}$*,* $F \in \mathbb{L}[X_0,\dots,X_n]$ *un polynôme homogène de degré* d*,* $x \in \mathbb{P}_n(\mathbb{C})$ *et* $T \in \mathbb{N}^*$*. On fixe un plongement* $\mathbb{L} \hookrightarrow \mathbb{C}$ *et l'on pose* $\Delta = [\mathbb{L}:\mathbb{Q}]$ *si* $\mathbb{L}$ *est réel et* $\Delta = [\mathbb{L}:\mathbb{Q}]/2$ *si* $\mathbb{L}$ *est imaginaire. Soit* $W = V.\mathfrak{Z}(F)$*.*

Alors, si

$$\forall t \in [\![0, T-1]\!], \frac{\|F^{(t)}(x)\|}{\|F\|} \leq \min_{y\in V(\mathbb{C})} \left(\mathrm{Dist}(x,y)^{(T-t)/\sigma}\right),$$

on a :

$$\begin{aligned}\frac{1}{\Delta}\log \mathrm{Dist}(x,W) + \mathrm{h}(W) \leq & \frac{T}{\sigma\Delta}\log \mathrm{Dist}(x,V) + d.\mathrm{h}(V)\\ & + \mathrm{d}(V)\left(\mathrm{h}_1(F) + \left(\frac{Tr}{\sigma} + 3d\right)\log(n+1)\right).\end{aligned}$$

6 Théorème de Y.V. Nesterenko et indépendance algébrique de π, e^π et $\Gamma(1/4)$

Nous présentons dans cette section le théorème de Nesterenko pour en déduire quelques corollaires, dont l'un qui nous donnera l'indépendance algébrique de π, e^π et $\Gamma(1/4)$. La mesure d'indépendance algébrique de G.Philibert, que nous chercherons à déduire du critère d'indépendance algébrique de P.Philippon, nous permettra dans un second temps de proposer une démonstration alternative de ce résultat.

6.1 Quelques corollaires du théorème de Y.V. Nesterenko

Y.V.Nesterenko a démontré en 1996 dans [19] le résultat suivant, dont nous donnons trois corollaires :

Théorème 6.1.1 (Nesterenko, 1996). *Soit $q \in \mathbb{C}$ satisfaisant $0 < |q| < 1$. Alors le degré de transcendance sur $\mathbb{Q}$ du corps*

$$\mathbb{Q}\left(q, P(q), Q(q), R(q)\right)$$

est supérieur ou égal à trois.

La démonstration passe par la preuve d'un lemme des zéros (majoration de l'ordre en zéro d'une fonction auxiliaire) difficile.

Notation. *Dans toute la suite, on fixe un réseau $\Omega = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$. On note η_1 et η_2 les quasi-périodes de la fonction ζ correspondant à ω_1 et à ω_2, et on pose $\tau = \frac{\omega_2}{\omega_1} \in \mathfrak{H}$. On notera parfois $\omega = \omega_1$ et $\eta = \eta_1$.*

Corollaire 6.1.2. *Soit q un nombre complexe vérifiant $0 < |q| < 1$ et tel que $J(q)$ soit algébrique. Alors les trois nombres q, $P(q)$ et $\Delta(q)$ sont algébriquement indépendants.*

Démonstration. (à partir du Théorème 6.1.1) D'après la proposition 1.3.11,

$$Q(q) = \frac{3}{4}\left(\frac{\omega_1}{\pi}\right)^4 g_2 \quad \text{et} \quad R(q) = \frac{27}{8}\left(\frac{\omega_1}{\pi}\right)^6 g_3,$$

d'où l'on déduit que

$$\Delta = \left(\frac{\omega_1}{2\pi}\right)^{12}\left(g_2^3 - 27g_3^2\right) = \frac{1}{1728}\left(Q^3 - R^2\right).$$

D'après les propos suivants la définition 3.1.1, la fonction J est également liée aux fonctions Q et R par la relation

$$J = \frac{Q^3}{\Delta}.$$

Si on suppose $J(q)$ algébrique, alors $Q(q)$ et $R(q)$ sont algébriquement dépendants, et donc les trois nombres algébriquement indépendants donnés par le théorème 6.1.1 sont soit q, $P(q)$ et $Q(q)$, soit q, $P(q)$ et $R(q)$. Dans les deux cas, on obtient l'indépendance algébrique de q, $P(q)$ et $\Delta(q)$. □

Les deux corollaires suivants se déduisent du corollaire 6.1.2 :

Corollaire 6.1.3. *Soit $\wp$ la fonction elliptique de Weierstrass attachée au réseau Ω, d'invariants g_2 et g_3 algébriques. Alors les trois nombres*

$$e^{2i\pi\tau}, \frac{\omega}{\pi} \text{ et } \frac{\eta}{\pi}$$

sont algébriquement indépendants.

Nous donnerons une preuve directe de ce corollaire dans le paragraphe 6.3.2, qui elle n'utilise pas de lemme de zéros mais passe par une mesure d'indépendance algébrique de $\frac{\omega}{\pi}$ et $\frac{\eta}{\pi}$ due à G.Philibert et qui sera exposée au paragraphe 6.3.1.

Démonstration. On note $q = e^{2i\pi\tau}$. Afin de parfaire le dictionnaire entre fonctions elliptiques et formes modulaires initié par la proposition 1.3.11, il est nécessaire d'établir une formule exprimant P à l'aide des invariants attachés au réseau Ω. Démontrée dans [11](chapitre 18), ladite formule fait intervenir la pseudo-période η_1 :

$$P(q) = 3\frac{\omega_1\eta_1}{\pi^2}.$$

D'après l'expression de Δ en fonction de Q et R donnée dans la démontration du corollaire 6.1.2, et en invoquant le fait que les nombres algébriques forment un corps, cette formule et le théorème 6.1.1 entraînent de suite que q, $\frac{\omega}{\pi}$ et $\frac{\eta}{\pi}$ sont algébriquement indépendants. □

Corollaire 6.1.4. *Sous les hypothèses du corollaire précédent, et en supposant de plus que le réseau Ω est à multiplication complexe par le corps*[13] *$\mathbb{M}$, les éléments*

$$\pi, \omega \text{ et } e^{2i\pi\tau}$$

sont algébriquement indépendants sur $\mathbb{Q}$.

Démonstration. Nous aurons tout d'abord besoin du lemme qui suit :

Lemme 6.1.5 (Relation de Masser)**.** *Si la fonction $\wp$ de Weierstrass (attachée au réseau Ω) est à multiplication complexe, alors il existe $k \in \mathbb{M}(g_2, g_3)$ (où $\mathbb{M} = \mathbb{Q}(\tau)$) et des entiers A et C tels que*

$$A\eta_1 - C\tau\eta_2 = k\omega_2.$$

Démonstration. D'après la proposition 2.5.2, dans le cas de la multiplication complexe, τ est un nombre quadratique : il existe A, B et $C \in \mathbb{Z}$ tel que le polynôme minimal de τ soit $A+BX+CX^2$ (avec $C \neq 0$).

Soit $f \in \mathcal{M}(\mathbb{C})$ définie par

$$\forall z \in \mathbb{C}, \quad f(z) = -A\zeta(Cz) + C\tau\zeta(C\tau z) + C\tau kz,$$

où $k = \frac{A\eta_1 - C\tau\eta_2}{\omega_2}$. Il s'agit de montrer que $k \in \mathbb{M}(g_2, g_3)$.

Par pseudo-périodicité de la fonction ζ et par définition de k, on a, pour tout $z \in \mathbb{C}$:

$$f(z+\omega_1) - f(z) = -AC\eta_1 + C^2\tau\eta_2 + C\tau k\omega_1 = 0.$$

De même, de la relation $C\tau\omega_2 = -A\omega_1 - B\omega_2$, on tire :

$$\forall z \in \mathbb{C}, \quad f(z+\omega_2) - f(z) = -AC\eta_2 + C\tau(-A\eta_1 - B\eta_2) + C\tau k\omega_2 = 0.$$

f a donc mêmes périodes que la fonction $\wp$ de Weierstrass : d'après le thérorème 2.2.11, elle est rationnelle en $\wp$ et $\wp'$.

Soit σ un automorphisme de $\mathbb{M}(g_2, g_3, k)$ qui fixe $\mathbb{M}(g_2, g_3)$ et soit f^σ la fonction obtenue en appliquant σ au développement de Laurent de f à l'origine. Alors σ fixe $\wp$ et $\wp'$ car leurs développements à l'origine ont leurs coefficients dans $\mathbb{Q}(g_2, g_3)$ d'après la remarque 2.3.2. La fonction f^σ est donc rationnelle en $\wp$ et en $\wp'$. De même, ζ étant fixé par σ, on a :

$$\forall z \in \mathbb{C}, \quad f(z) - f^\sigma(z) = C\tau(k - k^\sigma)z.$$

Or $f - f^\sigma$ est une fonction elliptique, d'où $f - f^\sigma = 0$ puis $k - k^\sigma = 0$. Ceci étant vrai pour tout automorphisme d'extension σ, le nombre k est dans $\mathbb{M}(g_2, g_3)$. □

Ce lemme prouve que, si l'on suppose les invariants g_2 et g_3 algébriques, ω_2 et η_2 sont, dans le cas de la multiplication complexe, algébriques sur $\mathbb{Q}(\omega, \eta)$. En utilisant à présent la relation de Legendre (cf. théorème 2.3.3)

$$\eta_1\omega_2 - \eta_2\omega_1 = 2i\pi,$$

π apparaît comme étant algébrique sur $\mathbb{Q}(\omega, \eta)$. Le résultat découle alors du corollaire 6.1.3. □

13. $\mathbb{M} = \mathbb{Q}(\tau)$ d'après la proposition 2.5.2.

Remarque 6.1.6. *Sous les hypothèses du corollaire 6.1.4, la relation de Legendre montre aussi que η est algébrique sur $\mathbb{Q}(\omega, \pi)$ (en invoquant également le fait que ω_2 et η_2 sont algébriques sur $\mathbb{Q}(\omega, \eta)$ par la relation de Masser). On obtient donc également, dans ces conditions, l'indépendance algébrique des éléments de l'ensemble $\{\omega, \eta, e^{2i\pi\tau}\}$.*

Corollaire 6.1.7. *Les trois nombres*

$$\pi, e^{\pi}, \Gamma\left(\frac{1}{4}\right) \qquad \left(\textit{resp. } \pi, e^{\pi\sqrt{3}}, \Gamma\left(\frac{1}{3}\right)\right)$$

sont algébriquement indépendants. En particulier, π ***et*** *e^{π}* ***sont algébriquement indépendants.***

L'indépendance algébrique de π et de $\Gamma\left(\frac{1}{4}\right)$ a été démontrée en 1976 par G.V. Chudnosky. En revanche, celle de π et de e^{π} n'était pas connue. On rapprochera ce résultat de la curieuse approximation suivante :

$$e^{\pi} - \pi \approx 19,999099979189.$$

Démonstration. On considère la courbe elliptique donnée par l'équation $y^2 = 4x^3 - 4x$ que l'on paramètre à l'aide de la fonction $\wp$ de Weierstrass attachée au réseau complexe correspondant. On a alors $g_2 = 4$ et $g_3 = 0$, qui sont bien algébrqiues. Les racines de l'équation $4\wp(z)^3 - 4\wp(z) = 0$ étant, d'après la proposition 2.2.5, $\wp(\frac{\omega_1}{2})$, $\wp(\frac{\omega_2}{2})$ et $\wp(\frac{\omega_1+\omega_2}{2})$, en appliquant éventuellement une transformation unimodulaire, on se ramène au cas où $\wp(\frac{\omega}{2}) = 1$. D'après les variations de $\wp$ restreinte à l'intervalle réel $]0; \omega/2]$ (proposition 2.2.13), on peut effectuer le changement de variable $u = \wp^{-1}(t)$, de sorte que

$$\frac{\mathrm{d}t}{\mathrm{d}u} = -2\sqrt{t(t+1)(t-1)}.$$

En intégrant cette équation pour t allant de 1 à l'infini, il vient

$$\omega = 2\int_1^{+\infty} \frac{\mathrm{d}t}{\sqrt{4t^3 - 4t}}.$$

Pour calculer cette intégrale, on effectue le changement de variables $t = x^{-1/2}$. On obtient alors :

$$\omega = \frac{1}{2}\int_0^1 x^{-3/4}(1-x)^{-1/2}\mathrm{d}x = \frac{1}{2}B\left(\frac{1}{4}, \frac{1}{2}\right),$$

où

$$\forall a, b > 0, \quad B(a,b) = \int_0^1 s^{a-1}(1-s)^{b-1}\mathrm{d}s = \frac{\Gamma(a)\Gamma(b)}{\Gamma(a+b)}.$$

Le formule des compléments

$$\Gamma(x)\Gamma(1-x) = \frac{\pi}{\sin(\pi x)}$$

évaluée en $x = \frac{1}{4}$ permet alors de déduire

$$\omega = \frac{\Gamma(1/4)^2}{\sqrt{8\pi}}.$$

Reste à montrer que le réseau Ω attaché à la courbe elliptique considérée est à multiplication complexe. Comme g_2 (resp. g_3) est homogène de degré -4 (resp. -6), $g_2(\Omega) = g_2(i\Omega)$ et $g_3(i\Omega) = -g_3(\Omega) = 0$: les réseaux Ω et $i\Omega$, ayant mêmes invariants, sont, d'après la remarque succédant au théorème 2.2.7, homothétiques. On en déduit que Ω est à multiplication complexe par l'ordre $\mathbb{Z}[i]$. On peut dès lors appliquer le corollaire 6.1.4 pour obtenir l'indépendance algébrique des éléments de l'ensemble $\left\{e^{-2\pi}, \frac{\Gamma(1/4)^2}{\sqrt{8\pi}}, \pi\right\}$.

Pour l'indépendance algébrique de π, $e^{\pi\sqrt{3}}$ et $\Gamma(1/3)$, on procède de même avec la courbe elliptique $y^2 = 4x^3 - 4$, qui est à multiplication complexe par l'ordre $\mathbb{Z}[\rho]$, où $\rho = e^{2i\pi/3}$. □

6.2 Le critère d'indépendance algébrique de P. Philippon

Nous établissons dans ce paragraphe le critère d'indépendance algébrique de P.Philippon, duquel nous essaierons de déduire par la suite le corollaire 6.1.3 à l'aide de la mesure d'indépendance algébrique de G.Philibert.

Nous désignons par $\mathbb{L}$ un corps de nombres.

Rappelons que, pour tout polynôme $Q \in \mathbb{L}[X_0, \ldots, X_n]$, on note $\|Q\| = \sqrt{\sum_\alpha \frac{|Q_\alpha|^2}{C^\alpha_{degQ}}}$, $\mathrm{h}_1(Q) = \log \|Q\|$ et $\|Q(x)\| = \frac{|Q(x)|}{\|x\|^{\mathrm{deg}Q}}$. Ces définitions ont été données dans le paragraphe 5.3.

On suppose une série d'hypothèses notées $\boldsymbol{(H)}$:

– Pour $x \in \mathbb{P}_n(\mathbb{C})$, il existe $k \in [\![0, n]\!]$ et des réels δ, τ, σ, U tels que

$$\delta \geq 1, \quad \sigma \geq 1, \quad \sigma^{k+1} < \tau < U.$$

– Pour tout S réel satisfaisant $\frac{\tau}{\sigma^{k+1}} < S \leq \frac{U}{\sigma^{k+1}}$, il existe une famille de polynômes homogènes $Q_1, \ldots, Q_m \in \mathbb{L}[X_0, \ldots, X_n]$ vérifiant, pour tout $i = 1, \ldots, m$:

H1. $\deg Q_i \leq \delta, \quad \mathrm{h}_1(Q_i) \leq \tau$;

H2. $\frac{\|Q_i(x)\|}{\|Q_i\|} \leq \exp\left(-S\sigma^{k+1}\right)$;

H3. Les polynômes Q_i n'ont pas de zéro commun dans la boule

$$B\left(x, \exp(-S\sigma^{k+2})\right) = \left\{y \in \mathbb{P}_n(\mathbb{C}) / \mathrm{Dist}(x, y) \leq \exp(-S\sigma^{k+2})\right\}.$$

On suppose encore une hypothèse $\boldsymbol{(\widetilde{H})}$: il existe une sous-variété projective de $\mathbb{P}_n(\mathbb{C})$ de dimension d définie sur $\mathbb{L}$ telle que, en adoptant les notations de l'hypothèse (H),

$$\left[\delta \mathrm{h}(V) + ((k+1)\tau + 3\delta \log(n+1)\mathrm{d}(V))\right] \delta^k < \frac{U}{(k+1)\sigma^{k+1}}.$$

On peut alors énoncer le lemme suivant, qui constitue de fait l'étape clé dans la démonstration du critère d'indépendance algébrique :

Lemme 6.2.1. *Sous les hypothèses (H) et $(\widetilde{H})$, on suppose que $\log \mathrm{Dist}(x, V) < -U$. Alors pour $h = d+1, \ldots, \max(0, d_k)$, il existe une variété projective Z_h de dimension $h-1$ définie sur $\mathbb{L}$ vérifiant :*

1. $\mathrm{d}(Z_h) \leq \delta^{d-h+1}\mathrm{d}(V)$;
2. $\mathrm{h}(Z_h) \leq \left[\delta \mathrm{h}(V) + (d-h+1)\tau \mathrm{d}(V)\right] \delta^{d-h}$;
3. $\log \mathrm{Dist}(x, Z_h) < -h'\sigma^{h'} \left[\delta \mathrm{h}(Z_h) + (h'\tau + 3\delta \log(n+1))\mathrm{d}(Z_h)\right] \delta^{h'-1}$, *où* $h' = h + k - d$.

La preuve fait intervenir l'ensemble des outils mis au point dans la section 5 pour obtenir l'existence de Z_h et les majorations annoncées. Etant donné le nombre de paramètres entrant en jeu, le détail de ces majorations, même si elles ne sont pas compliquées, n'est pas très éclairant de prime abord. Aussi proposons-nous dans un premier temps de dégager les idées sous-jacentes à la démonstration ainsi que le rôle des théorèmes établis à la section 5 dans cette dernière. Nous exposerons dans un second temps ladite démonstration en détail.

La preuve se fait par récurrence descendante sur h, le cas $h = d+1$ étant résolu en posant $Z_{d+1} = V$.

Si Z_h est construit et que l'on veut construire Z_{h-1}, la propriété du point le plus proche (théorème 5.4.2) montre que l'intersection de $Z_h(\mathbb{C})$ avec la boule de centre x et de rayon $\exp(-S'\sigma^{k+2})$ est non vide pour un S' dans l'intervalle $\left]\frac{\tau}{\sigma^{k+1}}; \frac{U}{\sigma^{k+1}}\right]$. On considère astucieusement la borne supérieure S des réels S' vérifiant cette propriété, de sorte que l'hypothèse (H) assure l'existence d'un polynôme homogène Q_i non nul sur $Z_h(\mathbb{C})$.

L'idée essentielle consiste alors à considérer le cycle $W = Z_h \mathfrak{Z}(Q_i)$, équidimensionnel de dimension $h-2$: les théorèmes de Bézout arithmétique (théorème 5.3.7) et géométrique (théorème 5.3.4) permettent aisément d'obtenir les conclusions du lemmes relatives à la hauteur et au degré pour le cycle W. On obtient plus difficilement la majoration de $\log \mathrm{Dist}(x, W)$ en distinguant le cas $S = \frac{U}{\sigma^{k+1}}$ du cas $S < \frac{U}{\sigma^{k+1}}$: dans la première situation, la conclusion est apportée par le premier théorème de Bézout métrique (théorème 5.5.1) tandis que, dans la seconde, elle résulte du second théorème de Bézout métrique (théorème 5.5.2).

Il suffit finalement de considérer une composante idoine du cycle W pour achever la récurrence.

Dans le détail, la preuve prend la forme suivante :

Démonstration. (du lemme 6.2.1) Sans perte de généralité, on peut tout d'abord supposer que $U = (k+1)\sigma^{k+1}\left[\delta \mathrm{h}(V) + ((k+1)\tau + 4\delta \log(n+1)\mathrm{d}(V))\right]\delta^k$, qui permet encore de vérifier (H) et $(\widetilde{H})$.

On procède par récurrence descendante sur h : pour $h = d+1$, on pose $Z_{d+1} = V$, qui vérifie clairement les conclusions du lemme relatives au degré et à la hauteur. $Z_{d+1} = V$ vérifie également la troisième condition puisque, d'une part, $\log \mathrm{Dist}(x, V) < -U$ par hypothèse et que, d'autre part, $U > (k+1)\sigma^{k+1}\left[\delta \mathrm{h}(V) + ((k+1)\tau + 3\delta \log(n+1)\mathrm{d}(V))\right]$ par $(\widetilde{H})$.

Supposons l'existence de Z_h et cherchons à établir celle de Z_{h-1}, avec $h \geq \max(1, d-k+1)$. Par la propriété du point le plus proche (théorème 5.4.2), il existe $y \in Z_h(\mathbb{C})$ tel que

$$\log \mathrm{Dist}(x, y) \leq \frac{1}{\mathrm{d}(Z_h)} \log \mathrm{Dist}(x, Z_h) + \sum_{i=1}^{n} \frac{h}{i}.$$

L'hypothèse de récurrence appliquée au second terme de l'inégalité donne

$$\begin{aligned} \log \mathrm{Dist}(x, y) &< -h\sigma^{k-d+h}(h\tau + 3\delta \log(n+1))\delta^{k-d+h-1} + \sum_{i=1}^{n} \frac{h}{i} \\ &< -\sigma\tau, \end{aligned}$$

la dernière majoration résultant de l'inégalité $\sum_{i=1}^{n} \frac{1}{i} < \log(n+1)$.

Il existe par conséquent $S' > \frac{\tau}{\sigma^{k+1}}$ tel que $y \in B_{S'} = B\left(x, \exp(-S'\sigma^{k+2})\right)$. On peut sans perte de généralité supposer $S' < \frac{U}{\sigma^{k+1}}$. Soit alors S la borne supérieure des réels $S' \in \left]\frac{\tau}{\sigma^{k+1}}; \frac{U}{\sigma^{k+1}}\right]$ tels que $Z_h \cap B_{S'} \neq \emptyset$. L'hypothèse $(H3)$ fournit l'existence d'un polynôme homogène $Q_{i_0} \in \mathbb{L}[X_0, \ldots, X_n]$ tel que $Q_{i_0}(y) \neq 0$. On pose W égal au cyle $Z_h.\mathfrak{Z}(Q_{i_0})$ équidimensionnel de dimension $h-2$ et défini sur $\mathbb{L}$.

Les théorèmes de Bézout arithmétique (théorème 5.3.7) et géométrique (théorème 5.3.4) permettent de suite d'obtenir les majorations

$$\begin{aligned} &\mathrm{d}(W) \leq \delta \mathrm{d}(Z_h) \leq \delta^{d-h+2}\mathrm{d}(V), \\ &\mathrm{h}(W) \leq \delta \mathrm{h}(Z_h) + \tau \mathrm{d}(Z_h) \leq \left[\delta \mathrm{h}(V) + (d-h+2)\tau \mathrm{d}(V)\right]\delta^{d_h+1}. \end{aligned}$$

Reste à majorer $\mathrm{Dist}(x, W)$. On distingue à cet effet deux cas :

– *Premier cas* : $S = \frac{U}{\sigma^{k+1}}$.
D'après $(H2)$, (H) et le premier théorème métrique de Bézout (théorème 5.5.1 avec $T = 1$), on obtient :

$$\begin{aligned} \log \mathrm{Dist}(x, W) &\leq \max[-(h'-1)\sigma^{h'}\left(\delta \mathrm{h}(Z_h) + (h'\tau + 2\delta \log(n+1))\,\mathrm{d}(Z_h)\right)\delta^{h'-1}; \\ &\qquad - k\sigma^{k+1}\left(\delta \mathrm{h}(V) + ((k+1)\tau + 3\delta \log(n+1))\,\mathrm{d}(V)\right)\delta^k] \\ &\leq -(h'-1)\sigma^{h'-1}\left(\delta \mathrm{h}(W) + ((h'-1)\tau + 3\delta \log(n+1))\,\mathrm{d}(W)\right). \end{aligned}$$

– *Second cas* : $S < \frac{U}{\sigma^{k+1}}$.
Par maximalité de S, pour tout $\widetilde{S} > S$, $Z_h \cap B_{\widetilde{S}} \neq \emptyset$, et donc

$$\frac{1}{\sigma} \log \underset{y \in Z_h(\mathbb{C})}{\mathrm{Dist}}(x, y) > -S\sigma^{k+1} \geq \log\left(\frac{\|Q_{i_0}(x)\|}{\|Q_{i_0}\|}\right).$$

On peut alors appliquer le second théorème de Bézout métrique (théorème 5.5.2 avec $T = 1$) :

$$\begin{aligned}\log \mathrm{Dist}(x, W) &\leq \frac{1}{\sigma} \log \mathrm{Dist}(x, Z_h) + \delta \mathrm{h}(Z_h) + (\tau + 3\delta \log(n+1))\, \mathrm{d}(Z_h) \\ &< -(h'-1)\sigma^{h'-1} \left(\delta \mathrm{h}(Z_h) + (h'\tau + 3\delta \log(n+1))\, \mathrm{d}(Z_h)\right) \delta^{h'-1} \\ &< -(h'-1)\sigma^{h'-1} \left(\delta \mathrm{h}(W) + (h'\tau + 3\delta \log(n+1))\, \mathrm{d}(W)\right) \delta^{h'-2},\end{aligned}$$

où $h' = h + k - d$.

Dans les deux cas, on a vérifié que W satisfaisait les conclusions du lemme. Comme les fonctions degré, hauteur et $\log \mathrm{Dist}(x, .)$ sont additives sur les cycles, il en résulte qu'au moins une des composantes irréductibles de W satisfait les mêmes conclusions : on pose Z_{h-1} égal à une telle composante. □

De ce lemme découle directement le critère d'indépendance algébrique :

Théorème 6.2.2 (Critère d'indépendance algébrique, P.Philippon)**.** *On suppose* (H) *et* $(\widetilde{H})$ *satisfaites. Dans ces conditions, si* $d \leq k$*, alors* $\log \mathrm{Dist}(x, V) \geq -U$*.*

Démonstration. Lorsque $d \leq k$, la conclusion du lemme 6.2.1 est fausse. En effet, Z_0 serait dans le cas contraire un cycle de dimension -1, i.e. le cycle vide admettant pour forme de Chow $f = 1$: Z_0 serait alors de hauteur et de degré nul. Le fait que $\mathrm{Dist}(x, Z_0) = 1$ est alors contradictoire avec la troisième inégalité du lemme, qui affirme que $\log \mathrm{Dist}(x, Z_0) < 0$.

Ceci prouve que les hypothèses faites dans le lemme 6.2.1 sont contradictoires lorsque $d \leq k$ et que, sous (H), on a nécessairement $\log \mathrm{Dist}(x, y) \geq -U$ pour toute variété V de dimension $d \leq k$ définie sur $\mathbb{L}$ et vérifiant $(\widetilde{H})$. □

L'appellation de *critère d'indépendance algébrique* est justifiée par le fait que, si l'hypothèse (H) est satisfaite pour une famille de paramètres $(\delta, \tau, \sigma, U)$ tels que $(\widetilde{H})$ peut être vérifié pour toute variété projective de dimension $\leq k$ définie que $\mathbb{Q}$, alors $\mathrm{Dist}(x, V) \neq 0$ pour toutes ces variétés. Ceci implique que le degré de transcendance du corps de définition de x est $> k$ (pour plus de détail, on pourra consulter [18], p.136).

6.3 Une démonstration alternative de l'indépendance algébrique de π, e^π et $\Gamma(1/4)$

Nous introduisons dans ce paragraphe une mesure d'indépendance algébrique des deux nombres $\frac{\omega}{\pi}$ et $\frac{\eta}{\pi}$ établie par G.Philibert puis nous en déduisons une démonstration alternative du corollaire 6.1.3, donc en particulier de l'indépendance algébrique de π, e^π et $\Gamma(1/4)$.

6.3.1 Mesure d'indépendance algébrique de G.Philibert

En toute généralité, mesurer l'indépendance algébrique de m nombres complexes $\omega_1, \ldots, \omega_m$ consiste à définir une fonction ϕ de deux variables telle que, pour tout polynôme non nul $P(X_1, \ldots, X_m)$ à coefficients dans un corps de nombres fixé, de degré $\leq d$ et dont les coefficients sont de module majoré par H, on ait

$$|P(\omega_1, \ldots, \omega_m)| > \phi(d, H).$$

La quantité $d + H$ majore alors la *taille* de P, définie comme la somme de son degré et de sa hauteur usuelle $H(P)$, à savoir le maximum des modules de ses coefficients. L'existence d'une mesure d'indépendance algébrique implique évidemment l'indépendance algébrique (sur $\mathbb{Q}$) des nombres considérés.

Le résultat de G.Philibert s'énonce avec une définition de la hauteur d'un polynôme différente de celles mentionnées jusqu'à présent :

Définition 6.3.1. *Soit $\mathbb{L}$ un corps de nombres et $P \in \mathbb{L}[X_1, \ldots, X_n]$. La* hauteur logarithmique absolue *du polynôme P est la quantité*

$$\overline{\mathrm{h}}(P) = \frac{1}{[\mathbb{L} : \mathbb{Q}]} \sum_{\nu \in \mathcal{M}_{\mathbb{L}}} [\mathbb{L}_\nu : \mathbb{Q}_\nu] \max\left[0, \log M_\nu(P)\right],$$

où $M_\nu(P)$ est le maximum des valeurs absolues des coefficients de P si $\nu \notin \mathcal{M}_{\mathbb{L}}^{\infty}$ et

$$M_\nu(P) = \exp\left(\int_0^1 du_n \ldots \int_0^1 du_1 \log\left|\sigma_\nu(P)(e^{2i\pi u_1}, \ldots, e^{2i\pi u_n})\right|\right)$$

si $\nu \in \mathcal{M}_{\mathbb{L}}^{\infty}$ correspond au plongement $\sigma_\nu : \mathbb{L} \hookrightarrow \mathbb{C}$.

Eu égard à cette définition, il est évident que $\mathrm{h}(P) \leq \overline{\mathrm{h}}(P)$, où $\mathrm{h}(P)$ est la hauteur invariante introduite au paragraphe 5.2.13.

On définit également une nouvelle notion de taille :

Définition 6.3.2. *Si $\mathbb{L}$ est un corps de nombres et $P \in \mathbb{L}[X_1, \ldots, X_n]$, on définit sa* taille modifiée *par la quantité*

$$\mathrm{t}(P) = \mathrm{deg}P + \overline{\mathrm{h}}(P),$$

où deg$P$ *désigne le degré total de P.*

Nous sommes à présent en mesure d'énoncer le résultat de G.Philibert :

Théorème 6.3.3 (Mesure d'indépendance algébrique, Philibert, 1988)**.** *On fixe comme précédemment un réseau complexe $\Omega = \mathbb{Z}\omega \oplus \mathbb{Z}\omega'$ à invariants g_2 et g_3 algébriques et de fonction de Weierstrass associée $\wp$, avec $\tau = \frac{\omega'}{\omega} \in \mathfrak{H}$. Soit $\mathbb{K} = \mathbb{Q}\left(g_2, \wp\left(\frac{\omega}{2}\right)\right)$.*

Pour tout $\varepsilon > 0$, il existe alors deux constantes c et c' dépendant de Ω, ω et de ε telles que pour tout polynôme $P \in \mathbb{K}[X, Y]$ non constant et de taille supérieure à c' on ait

$$\left|P\left(\frac{\omega}{\pi}, \frac{\eta}{\omega}\right)\right| \geq \exp\left[-\left(c.\mathrm{t}(P)\right)^{3+\varepsilon}\right],$$

où l'on note ici encore $\eta = \eta(\omega)$ la pseudo-période associée à ω.

Démonstration. Toute la démarche de G.Philibert figurée dans [20] consiste à construire une suite $(Q_{N,i})_{N,i}$ de polynômes de $\mathbb{K}[X, Y]$ permettant d'appliquer le théorème suivant de P.Philippon :

Théorème 6.3.4 (Philippon, 1986)**.** *Soit $\mathbb{L}$ un corps de nombres et $\underline{\theta} = (\theta_1, \theta_2) \in \mathbb{C}^2$. Soit $t_1 : \mathbb{R}_+ \to \mathbb{R}_+$ une fonction croissante et $v : \mathbb{R}_+ \to \mathbb{R}_+$ une bijection croissante. Soit $\varepsilon \in [0; 1[$.*

On suppose qu'il existe une suite d'idéaux $(I_N)_{N \geq 0}$ telle que, pour tout $N \geq 0$, l'ensemble des zéros de I_N dans la boule $B\left(\underline{\theta}, \exp(-t_1^2(N)v(N)^{1+\varepsilon/2})\right)$ soit vide et telle que l'idéal I_N soit engendré par des polynômes $Q_{N,1}, \ldots, Q_{N,m(N)}$ de taille majorée par $t_1(N)$ et vérifiant

$$\max_{1 \leq j \leq m(N)} \frac{|Q_{N,j}(\underline{\theta})|}{\|Q_{N,j}\|} \leq \exp\left[-t_1^2(N+1)v(N+1)\right].$$

Il existe alors des nombres réels c et c', c ne dépendant que de $\mathbb{L}$, tels que pour tout polynôme non constant $P \in \mathbb{L}[X, Y]$ de taille supérieure à c', on ait, en notant w la fonction réciproque de $c^{-1}v^{1-\varepsilon}$,

$$|P(\underline{\theta})| \geq \exp\left[-\left(c.\mathrm{t}(P)\right)^{\frac{1}{1-\varepsilon}} t_1^2\left(w\left(\mathrm{t}(P)\right)\right)\right].$$

Ce cas particulier correspond à $n = 2$, $k = 1$ et J idéal principal dans l'énoncé du théorème général de P.Philippon que l'on trouvera avec la démonstration qui s'y rapporte dans [22].

G.Philibert utilise ce théorème dans le cas $\mathbb{L} = \mathbb{K}$ et montre que, pour la suite $(Q_{N,i})_{N,i}$ construite, les fonctions $t_1(N) = N^{1+\varepsilon}$ et $v(N) = N^{1-\alpha}$ avec $\varepsilon \in \left]0; \frac{1}{2}\right[$ et $\alpha \in \left]2\varepsilon; \frac{5\varepsilon}{2+\varepsilon}\right[$ conviennent. Par suite, pour $P \in \mathbb{K}[X,Y]$ non constant de taille supérieure à c', on a, en choisissant $\underline{\theta} = \left(\frac{\pi}{\omega}; \frac{\eta}{\omega}\right)$ et en adoptant les notations du théorème de P.Philippon,

$$|P(\underline{\theta})| \geq \exp\left[-\left(c.\mathrm{t}(P)\right)^{\frac{1}{1-\varepsilon}} \left(w\left(\mathrm{t}(P)\right)\right)^{2+2\varepsilon}\right].$$

Comme $w(N) = (cN)^{\frac{1}{(1-\alpha)(1-\varepsilon)}}$, il vient $|P(\underline{\theta})| \geq \exp\left[-\left(c.\mathrm{t}(P)\right)^{3+\varepsilon_1}\right]$ avec $\varepsilon_1 = \frac{2\alpha+5\varepsilon-3\alpha\varepsilon}{(1-\alpha)(1-\varepsilon)}$. Puisque $\alpha \in \left]2\varepsilon; \frac{5\varepsilon}{2+\varepsilon}\right[$, $\varepsilon_1 \underset{\varepsilon\to 0}{\to} 0$, ce qui permet de conclure. □

Nous proposons de déduire le théorème 6.3.4 de P.Philippon présenté dans la démonstration précédente à partir du critère d'indépendance algébrique établi par le théorème 6.2.2. A cette fin, nous adoptons les notations du théorème 6.2.2.

Démonstration. (du théorème 6.3.4)
On travaille naturellement dans $\mathbb{P}_2(\mathbb{C})$ et l'on note identiquement un polynôme de $\mathbb{K}[X,Y]$ et son homogénéisé dans $\mathbb{K}[X,Y,Z]$. Cette convention est étayée par le fait que $\underline{x}$ désignera indistinctement l'élément (θ_1, θ_2) de $\mathbb{C}^2$ ou le point $(\theta_1 : \theta_2 : 1)$ de $\mathbb{P}_2(\mathbb{C})$ dont on fixe le représentant $(\theta_1, \theta_2, 1)$ de $\mathbb{C}^3$. En particulier, dans ces conditions, $\|x\| \geq 1$.

Au vu du résultat à montrer, on pose (pour $P \in \mathbb{K}[X,Y]$ fixé)

$$V = \mathfrak{Z}(P)$$

et

$$U = (c.\mathrm{t}(V))^{\frac{1}{1-\varepsilon}} t_1 \left[w(t(V))\right]^2,$$

où c est une constante ajustable ne dépendant que de $\mathbb{K}$ et t_1 et w des fonctions qui restent à définir. Plutôt que de travailler avec $\mathrm{t}(P)$, on considèrera sans perte de généralité $\mathrm{t}(V) = \mathrm{deg}V + \mathrm{h}(V)$ qui, d'après la remarque 5.2.15, s'exprime en fonction de $\mathrm{h}(P)$ et de $\mathrm{deg}P$.

Montrons d'abord que la conclusion du critère d'indépendance algébrique 6.2.2 permet d'aboutir à celle du théorème 6.3.4. On suppose donc que

$$\log \mathrm{Dist}(x, V) \geq -U.$$

On établit dans cette perspective un lemme :

Lemme 6.3.5. *Avec les notations précédentes, pour tout $\nu \in \mathcal{M}_{\mathbb{K}}$,*

$$M_\nu(P) \geq \exp\left(-\frac{[\mathbb{L}:\mathbb{Q}]}{[\mathbb{L}_\nu:\mathbb{Q}_\nu]}\overline{\mathrm{h}}(P)\right).$$

Démonstration. Si $M_\nu(P) \geq 1$, le résultat est évident. On suppose donc $M_\nu(P) < 1$. Comme $\mathrm{h}(P) \geq 0$, on a :

$$\begin{aligned}
[\mathbb{K}_\nu : \mathbb{Q}_\nu] \log M_\nu(P) &\geq -\sum_{\mu \neq \nu} [\mathbb{K}_\mu : \mathbb{Q}_\mu] \log M_\mu(P) \\
&\geq -\sum_{\mu \neq \nu} [\mathbb{K}_\mu : \mathbb{Q}_\mu] \max\left(0, \log M_\mu(P)\right) \\
&\geq -\sum_{\mu \in \mathcal{M}_{\mathbb{K}}} [\mathbb{K}_\mu : \mathbb{Q}_\mu] \max\left(0, \log M_\mu(P)\right) = -[\mathbb{K}:\mathbb{Q}]\overline{\mathrm{h}}(P),
\end{aligned}$$

la dernière inégalité résultant du fait que $\max\left(0, \log M_\nu(P)\right) = 0$. □

A l'aide de ce lemme et du fait que $\mathrm{Dist}(x,V) = \frac{|P(\underline{x})|}{\|\underline{x}\|^{\deg P} M(P)}$ (cf. remarque 5.4.1), on déduit l'existence d'une constante γ ne dépendant que de $\mathbb{K}$ telle que

$$\exp\left[\gamma \overline{\mathrm{h}}(P)\right] .|P(\underline{x})| \geq \frac{|P(\underline{x})|}{M(P)} \geq \frac{|P(\underline{x})|}{\|\underline{x}\|^{\deg P} M(P)} \geq \exp\left[-\left(c.\mathrm{t}(V)\right)^{\frac{1}{1-\varepsilon}} t_1^2\left[w(\mathrm{t}(V))\right]\right]. \qquad (1)$$

Or d'après l'expression de $\mathrm{h}(V)$ (remarque 5.2.15), il existe une constante κ absolue dès lors que n est fixé (ici $n=2$) telle que $\mathrm{t}(V) = \deg(V) + \mathrm{h}(V) \leq \kappa(\deg P + \overline{\mathrm{h}}(P)) = \kappa.\mathrm{t}(P)$. Quitte à choisir c suffisamment grand en fonction de γ et de κ, la minoration du théorème 6.3.4 de P.Philippon découle de l'inégalité entre les termes extrêmes de la série d'inégalités (1).

Voyons à présent comment vérifier les hypothèses du critère d'indépendance algébrique en les listant une à une : nous le ferons en supposant de plus que $t_1(N) > v(N)^{\varepsilon}$. On peut en fait montrer que si cette condition n'est pas vérifiée, les hypothèses du théorème 6.3.4 sont trop fortes et irréalisables.

La marge de manœuvre réside essentiellement dans le choix de N :

– Etant donné les hypothèses, la relation

$$\left[\delta \mathrm{h}(V) + ((k+1)\tau + 3\delta\log(n+1)\mathrm{d}(V))\right]\delta^k < \frac{U}{(k+1)\sigma^{k+1}}$$

sera satisfaite dès lors que l'on aura

$$\mathrm{t}(V)(k+1)\delta^k\sigma^{k+1}\left[(1+3\log 3)\delta + (k+1)\tau\right] < \left(c.\mathrm{t}(V)\right)^{\frac{1}{1-\varepsilon}} t_1\left[w(\mathrm{t}(V))\right]^2. \qquad (2)$$

Un choix naturel consiste à prendre

$$k = 1$$

et $\tau = \delta$. De plus, on posera

$$\sigma = v(N)^{\varepsilon/2}$$

ainsi que $\tau = \delta = t_1(N)$. Nous modifierons légèrement ce dernier choix par la suite. La relation (2) se réécrit alors

$$\kappa \mathrm{t}(V) t_1(N)^2 v(N)^{\varepsilon} < \left(c.\mathrm{t}(V)\right)^{\frac{1}{1-\varepsilon}} t_1\left[w(\mathrm{t}(V))\right]^2, \qquad (3)$$

où κ est une constante absolue. Une valeur judicieuse de N consiste à prendre

$$N = \lfloor w(\mathrm{t}(V))\rfloor .$$

En effet, de ce choix découlent les encadrements

$$v(N) \leq \left[c.\mathrm{t}(V)\right]^{\frac{1}{1-\varepsilon}} < v(N+1), \qquad (4)$$
$$t_1(N) \leq t_1\left[w(\mathrm{t}(V))\right] < t_1(N+1), \qquad (5)$$

de sorte que (3) est vérifié si l'on choisit c suffisamment grand en fonction de κ. Il convient de remarquer – et cela sera important dans la suite – que l'on peut également remplacer κ par toute autre constante dépendant uniquement du corps $\mathbb{K}$ quitte à modifier c en conséquence.

– D'après l'hypothèse $t_1(N) > v(N)^{\varepsilon}$ et le choix de N, la condition $\sigma^2 < \tau < U$ est clairement vérifiée.

– Quitte à choisir $\mathrm{t}(V)$, et donc N suffisamment grand, on peut supposer $\delta = t_1(N) \geq 1$ et $\sigma = v(N)^{\varepsilon/2} \geq 1$.

Soit à présent $S \in \left]\frac{\tau}{\sigma^2}; \frac{U}{\sigma^2}\right]$: d'après les inégalités (4) et (5), $S\sigma^2 \leq U \leq t_1^2(N+1)v(N+1)$. Il existe donc un entier $M \leq N$ tel que $t_1(M)^2 v(M) \leq S\sigma^2 < t_1(M+1)^2 v(M+1)$: on considère la famille de polynômes $Q_{M,1}, \ldots, Q_{M,m(M)}$ fournis par le théorème 6.3.4. Il s'agit dès lors de satisfaire les hypothèses suivantes :

- Pour tout $i \in [\![1, m(M)]\!]$, $\frac{\|Q_{M,i}(\underline{x})\|}{\|Q_{M,i}\|} \leq \exp\left(-S\sigma^2\right)$. Il suffit pour cela que $S\sigma^2 \leq t_1(M+1)^2 v(M+1)$, relation vérifiée par définition de M.
- Les $Q_{M,i}$ (pour $1 \leq i \leq m(M)$) ne doivent pas avoir de zéro commun dans la boule $B(\underline{x}, \exp(-S\sigma^3))$. Cette condition sera vérifiée dès que l'on aura $t_1(M)^2 v(M)^{1+\varepsilon/2} \leq \tau\sigma = t_1(N)v(N)^{\varepsilon/2}$. Comme $t_1(N)v(N)^{\varepsilon/2} \underset{N\to+\infty}{\longrightarrow} +\infty$, quitte à imposer $\mathrm{t}(V)$ suffisamment grand, on peut trouver un entier M satisfaisant cette contrainte additionnelle.
- Pour tout $i \in [\![1, m(M)]\!]$, les hypothèses et le choix des paramètres permettent d'obtenir les majorations $\deg Q_{M,i} \leq t_1(M) \leq \delta = t_1(N)$.
- Il nous faut également nous assurer que $\mathrm{h}_1(Q_{M,i}) \leq \tau$ pour tout $i \in [\![1, m(M)]\!]$. En faisant appel à la minoration de $M_\nu(Q_{M,i})$ fournie par la remarque 5.3.6 ainsi qu'au fait que le nombre de places archimédiennes d'un corps de nombres est fini (théorème 5.2.12), on obtient aisément l'existence d'une constante β ne dépendant que de $\mathbb{K}$ telle que l'on ait successivement

$$\mathrm{h}_1(Q_{M,i}) \leq \mathrm{h}(Q_{M,i}) + \beta.\deg Q_{M,i} \leq \overline{\mathrm{h}}(Q_{M,i}) + \beta.\deg Q_{M,i} \leq \beta.\mathrm{t}(Q_{M,i}) \leq \beta.t_1(M),$$

  la dernière inégalité étant vraie par hypothèse. On modifie en conséquence légèrement le choix de τ en posant

$$\tau = \beta.t_1(N),$$

  de sorte que l'on a à présent $\mathrm{h}_1(Q_{M,i}) \leq \tau$ pour tout $i \in [\![1, m(M)]\!]$. On vérifie par ailleurs aisément que ce choix ne modifie pas les inégalités précédemment établies.

Toutes les hypothèses du critère d'indépendance algébrique sont ainsi vérifiées : le théorème 6.3.4 est démontré. □

6.3.2 Démonstration de l'indépendance algébrique de π, e^π et $\Gamma(1/4)$

Avant d'exposer une démonstration alternative du corollaire 6.1.3, donc de l'indépendance algébrique de π, e^π et $\Gamma(1/4)$, nous proposons une reformulation plus faible de la mesure d'indépendance algébrique de G.Philibert, reformulation qui sera celle que nous utiliserons et qui nécessite le lemme suivant :

Lemme 6.3.6. *Soit $\mathbb{L}$ un corps de nombres admettant $\sigma_1, \ldots, \sigma_{r_1}$ pour plongements réels et $\sigma_{r_1+1}, \ldots, \sigma_{r_1+r_2}, \overline{\sigma}_{r_1+1}, \ldots, \overline{\sigma}_{r_1+r_2}$ pour plongements complexes, de sorte que $r_1 + 2r_2 = [\mathbb{L} : \mathbb{Q}]$. Soit $P(X,Y) = \sum_{i,j} a_{ij} X^i Y^j \in \mathbb{L}[X,Y]$. Pour $\nu \in \mathcal{M}_\mathbb{L}$, on note $H_\nu(P) = \max_{i,j} |a_{ij}|_\nu$ et $H(P)$ la hauteur usuelle de P.*

Il existe alors une constante $\mu > 0$ ne dépendant que de $\mathbb{L}$ telle que

$$\overline{\mathrm{h}}(P) \leq \mu \left(\deg P + \sum_{\nu \notin \mathcal{M}_\mathbb{L}^\infty} \frac{[\mathbb{L}_\nu : \mathbb{Q}_\nu]}{[\mathbb{L} : \mathbb{Q}]} \max\{0, \log H_\nu(P)\} + \sum_{i=1}^{r_1+r_2} \max\{0, \log H(\sigma_i(P))\} \right),$$

où les polynômes $\sigma_i(P)$ se déduisent de manière évidente de P.

En particulier, si $P \in \mathbb{Z}[X,Y]$ est non nul, alors

$$\overline{\mathrm{h}}(P) \leq \mu \left(\deg P + \log H(P) \right).$$

Démonstration. La seconde assertion est évidente dès lors que l'on garde à l'esprit que toute valeur absolue ultramétrique normalisée sur $\mathbb{Q}$ est à valeurs dans $[0;1]$ lorsqu'elle est restreinte à $\mathbb{Z}$ (théorème 5.2.12) et que le seul plongement de $\mathbb{Q}$ dans $\mathbb{C}$ est réduit à l'identité.

Dans le cas général, nous allons montrer que pour tout $\nu \in \mathcal{M}_{\mathbb{L}}^{\infty}$, on a $M_\nu(P) \leq H_\nu(P)(1+\deg P)$, où $M_\nu(P)$ est défini comme dans l'énoncé de la mesure d'indépendance algébrique de G.Philibert (théorème 6.3.3). Soit donc $\nu \in \mathcal{M}_{\mathbb{L}}^{\infty}$ associé à un plongement $\sigma : \mathbb{L} \hookrightarrow \mathbb{C}$. Remarquons tout d'abord que, dans ce cas, $H_\nu(P) = H(\sigma(P))$. Par ailleurs, d'après l'inégalité arithmético-géométrique,

$$\exp\left(\int_0^1\int_0^1 \log\left|P\left(e^{2i\pi u}, e^{2i\pi v}\right)\right| \mathrm{d}u\mathrm{d}v\right) \leq \int_0^1\int_0^1 \left|P\left(e^{2i\pi u}, e^{2i\pi v}\right)\right| \mathrm{d}u\mathrm{d}v.$$

En utilisant cette majoration pour $\sigma(P)^2$, il vient :

$$\begin{aligned} M_\nu(P) &\leq \left(\int_0^1\int_0^1 \left|\sigma(P)\left(e^{2i\pi u}, e^{2i\pi v}\right)\right|^2 \mathrm{d}u\mathrm{d}v\right)^{1/2} \\ &= \left(\int_0^1\int_0^1 \sigma(P)\left(e^{2i\pi u}, e^{2i\pi v}\right)\sigma(\overline{P})\left(e^{-2i\pi u}, e^{-2i\pi v}\right) \mathrm{d}u\mathrm{d}v\right)^{1/2}. \end{aligned}$$

Or un calcul aisé utilisant le fait que, pour $n \in \mathbb{N}$, l'intégrale $\int_0^1 e^{2i\pi nt}dt$ est nulle si, et seulement si, $n = 0$ montre que

$$\int_0^1\int_0^1 \sigma(P)\left(e^{2i\pi u}, e^{2i\pi v}\right).\sigma(\overline{P})\left(e^{-2i\pi u}, e^{-2i\pi v}\right) \mathrm{d}u\mathrm{d}v = \sum_{i,j}\left|\sigma(a_{i,j})\right|^2,$$

d'où

$$M_\nu(P) \leq \sqrt{\sum_{i,j}\left|\sigma(a_{i,j})\right|^2} \leq H\left(\sigma(P)\right)(1+\deg P) = H_\nu\left(P\right)(1+\deg P).$$

Dès lors :

$$\begin{aligned} \overline{\mathrm{h}}(P) &= \sum_{\nu\in\mathcal{M}_{\mathbb{L}}} \frac{[\mathbb{L}_\nu:\mathbb{Q}_\nu]}{[\mathbb{L}:\mathbb{Q}]} \max\left\{0, \log M_\nu(P)\right\} \\ &\leq \sum_{\nu\notin\mathcal{M}_{\mathbb{L}}^{\infty}} \frac{[\mathbb{L}_\nu:\mathbb{Q}_\nu]}{[\mathbb{L}:\mathbb{Q}]} \max\left\{0, \log H_\nu(P)\right\} + \sum_{\nu\in\mathcal{M}_{\mathbb{L}}^{\infty}} \frac{[\mathbb{L}_\nu:\mathbb{Q}_\nu]}{[\mathbb{L}:\mathbb{Q}]} \max\left\{0, \log(1+\deg P) + \log H_\nu(P)\right\} \\ &\leq \sum_{\nu\notin\mathcal{M}_{\mathbb{L}}^{\infty}} \frac{[\mathbb{L}_\nu:\mathbb{Q}_\nu]}{[\mathbb{L}:\mathbb{Q}]} \max\left\{0, \log H_\nu(P)\right\} + \log(1+\deg P)\left(\sum_{\nu\in\mathcal{M}_{\mathbb{L}}^{\infty}} \frac{[\mathbb{L}_\nu:\mathbb{Q}_\nu]}{[\mathbb{L}:\mathbb{Q}]}\right) \\ &\quad + \sum_{\nu\in\mathcal{M}_{\mathbb{L}}^{\infty}} \frac{[\mathbb{L}_\nu:\mathbb{Q}_\nu]}{[\mathbb{L}:\mathbb{Q}]} \max\left\{0, \log H_\nu(P)\right\} \\ &\leq \sum_{\nu\notin\mathcal{M}_{\mathbb{L}}^{\infty}} \frac{[\mathbb{L}_\nu:\mathbb{Q}_\nu]}{[\mathbb{L}:\mathbb{Q}]} \max\left\{0, \log H_\nu(P)\right\} \\ &\quad + \left(\sum_{\nu\in\mathcal{M}_{\mathbb{L}}^{\infty}} \frac{[\mathbb{L}_\nu:\mathbb{Q}_\nu]}{[\mathbb{L}:\mathbb{Q}]}\right)\left(\deg P + \sum_{i=1}^{r_1+r_2} \max\left\{0, \log H(\sigma_i(P))\right\}\right). \end{aligned}$$

Le résultat s'ensuit en posant $\mu = \max\left\{1, \sum_{\nu\in\mathcal{M}_{\mathbb{L}}^{\infty}} \frac{[\mathbb{L}_\nu:\mathbb{Q}_\nu]}{[\mathbb{L}:\mathbb{Q}]}\right\}$. □

La mesure d'indépendance algébrique de G.Philibert couplée à ce lemme permet alors d'affirmer que, pour tout polynôme $P \in \mathbb{Z}[X,Y]$ non constant de taille suffisamment grande étant donné $\varepsilon > 0$, il existe une constante $c > 0$ telle que

$$\left|P\left(\frac{\omega}{\pi}, \frac{\eta}{\pi}\right)\right| \geq \exp\left[-\left(c.\left(\deg P + \log H(P)\right)\right)^{3+\varepsilon}\right].$$

En définissant la *longueur* $L(P)$ du polynôme P comme la somme des modules des coefficients de P, on a encore :

$$\left|P\left(\frac{\omega}{\pi},\frac{\eta}{\pi}\right)\right| \geq \exp\left[-\left(c.\left(\deg P+\log L(P)\right)\right)^{3+\varepsilon}\right].$$

C'est sous cette forme que nous utiliserons le résultat de G.Philibert dans la démonstration alternative du corollaire 6.1.3 que nous proposons présentement.

La preuve passe tout d'abord par la proposition suivante :

Proposition 6.3.7. *Soit $q \in \mathbb{C}$ tel que $0 < |q| < 1$. Il existe alors deux constantes positives c et κ (dépendant de $|q|$) ayant la propriété suivante : pour tout entier N suffisamment grand, il existe un entier $M \geq N^4$ et un polynôme non nul $A_N \in \mathbb{Z}[z, X_1, X_2, X_3]$ tels que*

1. $\deg A_N \leq cN \log M$,
2. $\log L(A_N) \leq cN(\log M)^2$,
3. $0 < |A_N(q, P(q), Q(q), R(q))| \leq e^{-\kappa M}$.

Démonstration. La preuve suit les grandes lignes du paragraphe 2 de [19] que nous détaillons et adaptons à nos objectifs. En fait, la démonstration qui suit permet essentiellement à Y.V. Nesterenko de réduire le théorème 6.1.1 à un lemme de zéros qui constitue la partie difficile de sa preuve, et que nous esquivons. C'est P.Philippon qui a repris ces arguments pour envisager une démonstration directe du corollaire 6.1.3 (cf. [28]).

Commençons par démontrer deux lemmes :

Lemme 6.3.8. *Soit $N \in \mathbb{N}$. Il existe un polynôme non nul $A \in \mathbb{Z}[z, X_1, X_2, X_3]$ de degré $\leq N$ par rapport à chacune de ses variables tel que la fonction*

$$F(z) = A(z, P(z), Q(z), R(z))$$

ait, à l'origine, un zéro de multiplicité au moins $L = \lfloor \frac{(N+1)^4}{2} \rfloor$ et dont la hauteur $H(A)$ soit majorée par N^{85N}.

Démonstration. Pour $k \geq 1$, on a :

$$\sigma_k(n) = \sum_{d|n} d^k \leq n^k \sum_{d|n} 1 \leq n^{k+1}.$$

De plus,

$$1 + \sum_{n=1}^{+\infty} n^k z^n \ll \sum_{n=0}^{+\infty} (n+1)\dots(n+k) z^n = \frac{k!}{(1-z)^{k+1}}, \tag{1}$$

où $\sum a_n z^n \ll \sum b_n z^n$ signifie que $|a_n| \leq |b_n|$ pour tout n. D'après les développements des fonctions P, Q et R en séries entières dont les coefficients s'expriment en fonction des $\sigma_k(n)$ (cf. formules qui suivent la remarque 1.3.9), on a :

$$P(z) \ll \frac{24.2!}{(1-z)^3}, \quad Q(z) \ll \frac{240.4!}{(1-z)^5}, \quad R(z) \ll \frac{540.6!}{(1-z)^7}, \quad z \ll \frac{1}{1-z}.$$

Il s'ensuit que, pour tout vecteur $k = (k_0, k_1, k_2, k_3) \in [\![1, N]\!]^4$,

$$z^{k_0} P(z)^{k_1} Q(z)^{k_2} R(z)^{k_3} = \sum_{n=0}^{+\infty} d(k,n) z^n \ll \frac{c_1^{3N}}{(1-z)^{16N}}, \tag{2}$$

où $c_1 = 504.6!$ et $d(k,n) \in \mathbb{Z}$. De (1) et de (2), on déduit que

$$|d(k,n)| \leq c_1^{3N}(n+16N)^{16N} \leq (nN)^{17N} \qquad (n \geq 1) \tag{3}$$

pour N suffisamment grand, et que $|d(k,0)| \leq 1$.

Posons $A = \sum_{k \in [\![1,N]\!]^4} a(k) z^{k_0} x_1^{k_1} x_2^{k_2} x_3^{k_3}$, où les $a(k)$ sont choisis comme étant une solution non triviale du système d'équations linéaires

$$\sum_{k \in [\![1,N]\!]^4} d(k,n) a(k) = 0, \qquad n \in \left[\!\left[0; \left\lfloor \frac{(N+1)^4}{2} \right\rfloor - 1 \right]\!\right].$$

Ici le nombre de variables est $u = (N+1)^4$ et le nombre d'équations est $v = \left\lfloor \frac{(N+1)^4}{2} \right\rfloor$. D'après (3) et le lemme de Thue-Siegel (lemme 3.1.4), le système admet une solution entière non triviale vérifiant l'inégalité

$$\max_{k \in [\![1,N]\!]^4} |a(k)| \leq (N+1)^4 \left(\frac{(N+1)^4}{2} N \right)^{17N} \leq N^{85N} \tag{4}$$

pour N suffisamment grand. □

Soit N un entier naturel suffisamment grand. On considère le polynôme A donné par le lemme précédent et l'on note $M = \mathrm{ord}_0 F$ l'ordre de F en 0. La construction de A donne $M \geq L \geq N^4/2$.

Posons $r = \mathrm{Min}\left\{ \frac{1+|q|}{2}, 2|q| \right\}$ de sorte que $|q| < r < 1$. Prouvons un deuxième lemme :

Lemme 6.3.9. *Si N est suffisamment grand par rapport à $|q|$, alors pour tout $z \in \mathbb{C}$ tel que $|z| \leq r$, on a*

$$|F(z)| \leq |z|^M M^{48N}.$$

Démonstration. Le développement de Taylor de F à l'origine s'écrit sous la forme

$$F(z) = \sum_{n=M}^{+\infty} b_n z^n,$$

où $b_n = \sum_{k \in [\![1,N]\!]^4} d(k,n) a(k) \in \mathbb{Z}$. D'après (3) et (5), il vient :

$$|b_n| \leq \sum_{k \in [\![1,N]\!]^4} (nN)^{17N} N^{85N} \leq n^{17N} N^{103N} \qquad (n \geq M).$$

Ainsi donc, si $|z| \leq r$, on a :

$$\begin{aligned}
|F(z)| &\leq \sum_{n=M}^{+\infty} |b_n||z|^n = \sum_{n=0}^{+\infty} |b_{n+M}||z|^{n+M} \\
&\leq |z|^M N^{103N} \sum_{n=0}^{+\infty} (n+M)^{17N} |z|^n \\
&\leq |z|^M N^{103N} (M+1)^{17N} \left(1 + \sum_{n=1}^{+\infty} n^{17N} |z|^n \right) \\
&\leq |z|^M N^{103N} (M+1)^{17N} \frac{(17N)!}{(1-r)^{17N+1}} \\
&\leq |z|^M N^{103N} (M+1)^{17N} N^{17N} \\
&\leq |z|^M M^{48N}
\end{aligned}$$

pour N suffisamment grand. □

L'étape suivante consiste à montrer que $T = \mathrm{ord}_q F \leq \alpha N \log M$, où $\alpha = 48\left(\log \frac{r}{|q|}\right)^{-1}$. On considère pour cela la fonction

$$H(z) = \frac{F(z)}{z^M}\left(\frac{r^2 - \overline{q}z}{r(z-q)}\right)^T.$$

Le principe du maximum permet d'affirmer que $|H(0)| \leq |H|_r = \sup_{|z|\leq r} |H(z)|$. Or le nombre $b_M = \frac{F^{(M)}(0)}{M!}$ est un entier non nul : en minorant sa valeur absolue par 1, on trouve

$$|H(0)| \geq \left(\frac{r}{|q|}\right)^T.$$

Finalement,

$$\left(\frac{r}{|q|}\right)^T \leq |H|_r \leq r^{-M}|F|_r \leq M^{48N},$$

d'où la majoration annoncée pour T.

On exploite à présent le système d'équations différentielles vérifiées par les fonctions P, Q et R et mentionné au théorème 1.3.12 en introduisant l'opérateur de dérivation

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

L'opérateur D est spécialement étudié pour que, pour tout polynôme $B \in \mathbb{C}[z, X_1, X_2, X_3]$, on ait l'égalité

$$z\frac{d}{dz}B(z, P(z), Q(z), R(z)) = (DB)(z, P(z), Q(z), R(z)). \tag{5}$$

Pour N suffisamment grand, on définit ensuite le polynôme A_N en posant

$$A_N(z, X_1, X_2, X_3) = (12z)^T(z^{-1}D)^T A(z, X_1, X_2, X_3),$$

où A est le polynôme construit au lemme 6.3.8 et T l'entier ci-dessus défini. Une récurrence immédiate sur T montre par ailleurs que

$$(z^{-1}D)^T = z^{-T}\prod_{k=0}^{T-1}(D-k), \tag{6}$$

ce qui prouve que $A_N \in \mathbb{Z}[z, X_1, X_2, X_3]$. Par (5), il vient de plus

$$A_N(z, X_1, X_2, X_3) = (12z)^T F^{(T)}(z).$$

Pour obtenir la majoration annoncée, on utilise la formule de Cauchy :

$$F^{(T)}(q) = \frac{T!}{2i\pi}\int_{C_2}\frac{F(z)}{(z-q)^{T+1}}\mathrm{d}z,$$

où C_2 est le cercle $\{z \in \mathbb{C}/|z-q| = r - |q|\}$. En utilisant les inégalités $|z| \leq |z-q| + |q| = r$ ainsi que le lemme 6.3.9 et la majoration de T établie plus haut, on obtient

$$|A_N(q, P(q), Q(q), R(q))| \leq 12^T T!(r-|q|)^{-T} r^M M^{48N} \leq e^{-\kappa M},$$

où $\kappa = \frac{1}{4}\log\frac{1}{r}$.

Pour montrer les majorations sur le degré et la hauteur, on utilise l'égalité (6). Si $B \in \mathbb{C}[z, X_1, X_2, X_3]$ est tel que $B \ll a.(1 + z + X_1 + X_2 + X_3)^S$ (où $a \in \mathbb{R}, S \in \mathbb{N}$), alors, pour tout entier k, on a :

$$\begin{aligned}(D+k)B &\ll |k|.a.(1+z+X_1+X_2+X_3)^S + a.S.(1+z+X_1+X_2+X_3)^{S-1} \\ &\quad \times (z + (X_1^2 + X_2) + (X_1X_2 + X_3) + (X_1X_3 + X_2^2)) \\ &\ll |k|.a.(1+z+X_1+X_2+X_3)^S + a.S.(1+z+X_1+X_2+X_3)^{S+1} \\ &\ll a.(S+|k|)(1+z+X_1+X_2+X_3)^{S+1},\end{aligned}$$

d'où, par une récurrence immédiate,

$$12^T \prod_{k=0}^{T-1} (D-k)B(z, X_1, X_2, X_3) \ll 12^T.a.(S+2T)^T(1+z+X_1+X_2+X_3)^{S+T}.$$

Par le lemme 6.3.8, on a

$$A \ll N^{85N}(1+z+X_1+X_2+X_3)^{4N},$$

d'où

$$A_N(1, z, X_1, X_2, X_3) \ll N^{85N}\left[12(4N+2T)\right]^T (1+z+X_1+X_2+X_3)^{4N+T},$$

ce qui implique que

$$\begin{aligned}&\deg A_N \leq 4N + T \leq (\alpha+1)N\log M, \\ &L(A_N) \leq N^{85N}5^{4N+T}(48N+24T)^T \leq \exp(2\alpha N(\log M)^2)\end{aligned}$$

et achève ainsi la démonstration. □

Nous pouvons désormais nous lancer dans la démonstration du corollaire 6.1.3 à proprement parler.

Démonstration. (du corollaire 6.1.3)

On notera $CD(B)$ le coefficient dominant d'un polynôme B. On raisonne par l'absurde en supposant $q = e^{2i\pi\tau}$, $\frac{\omega}{\eta}$ et $\frac{\eta}{\pi}$ algébriquement liés, avec g_2 et g_3 algébriques par hypothèse.

D'après les formules permettant d'exprimer $P(q)$, $Q(q)$ et $R(q)$ en fonction de ω et de η (cf. la première démonstration du corollaire 6.1.3 et la proposition 1.3.11), chacun des quatres nombres q, $P(q)$, $Q(q)$ et $R(q)$ est racine d'un polynôme non nul $A_i\left(X_i, \frac{\omega}{\eta}, \frac{\eta}{\pi}\right)$, $0 \leq i \leq 3$, avec $A_i \in \mathbb{Z}[X_i, Y_1, Y_2]$. L'idée de la démonstration consiste à éliminer dans l'anneau des polynômes à six variables $\mathbb{Z}[X_0, X_1, X_2, X_3, Y_1, Y_2]$ les quatre variables X_0, X_1, X_2 et X_3 entre les cinq polynômes A, A_0, A_1, A_2 et A_3, où A sera l'un des polynômes A_N fournis par la proposition 6.3.7 pour un entier $N \geq 0$ à déterminer.

On calcule ainsi en premier lieu le résultant en X_0 de A et de A_1, résultant qui est un polynôme en $X_1, X_2, X_3, \frac{\omega}{\eta}$ et $\frac{\eta}{\pi}$:

$$\mathrm{Res}_{X_0}(A_0, A)\left(X_1, X_2, X_3, \frac{\omega}{\eta}, \frac{\eta}{\pi}\right) = CD(A_0)^{\deg A} \times \prod_{\alpha \in \mathbb{C}/A_0\left(\alpha, \frac{\omega}{\eta}, \frac{\eta}{\pi}\right)=0} A(\alpha, X_1, X_2, X_3).$$

On itère en prenant le résultant du polynôme obtenu avec A_1, puis A_2 et A_3. On obtient ainsi l'existence d'un polynôme $B \in \mathbb{Z}[Y_1, Y_2]$ tel que, en notant

$$\mathcal{Z} = \left\{(\alpha_0, \alpha_1, \alpha_2, \alpha_3) \in \mathbb{C}^4 / \forall i \in [\![0, 3]\!], A_i\left(\alpha, \frac{\omega}{\eta}, \frac{\eta}{\pi}\right) = 0\right\},$$

on ait

$$B\left(\frac{\omega}{\eta},\frac{\eta}{\pi}\right) = b^{\deg A} \times \prod_{(\alpha_0,\alpha_1,\alpha_2,\alpha_3)\in\mathcal{Z}} A(\alpha_0,\alpha_1,\alpha_2,\alpha_3)$$
$$= b^{\deg A} A\left(q,P(q),Q(q),R(q)\right) \times \prod_{(\alpha_0,\alpha_1,\alpha_2,\alpha_3)\in\mathcal{Z}\setminus\{q,P(q),Q(q),R(q)\}} A(\alpha_0,\alpha_1,\alpha_2,\alpha_3),$$

où b est un entier naturel.

Soit $C \geq 1$ une constante qui majore tous les modules des racines complexes des $A_i\left(X_i,\frac{\omega}{\eta},\frac{\eta}{\pi}\right)$, $0 \leq i \leq 3$. A l'aide de la proposition 6.3.7, il vient alors :

$$\begin{aligned}\left|B\left(\frac{\omega}{\eta},\frac{\eta}{\pi}\right)\right| &\leq e^{-\kappa M}\left(C^{\deg A}H(A)\right)^{\prod_{i=0}^{3}\deg A_i} \times b^{\deg A}\\ &\leq e^{-\kappa M}\left(C^{cN\log M}e^{cN(\log M)^2}\right)^{\prod_{i=0}^{3}\deg A_i} \times b^{cN\log M}\\ &\leq e^{-\kappa M + C'N(\log M)^2}\\ &\leq e^{-\kappa M + C'M^{1/4}(\log M)^2} \ (\text{car } N^4 \leq M).\end{aligned}$$

Quitte à multiplier B par un entier idoine et à modifier C en conséquence, on peut le supposer de taille suffisamment grande pour qu'il soit redevable de la mesure d'indépendance algébrique de G.Philibert : pour tout $\varepsilon > 0$, il existe une constante $c' = c'(\varepsilon) > 0$ telle que

$$\left|B\left(\frac{\omega}{\eta},\frac{\eta}{\pi}\right)\right| \geq \exp\left(-c'.\left(\deg B + \log L(B)\right)^{3+\varepsilon}\right).$$

Or en écrivant le résultant comme un déterminant, on constate l'existence de trois constantes δ, δ' et δ'' telles que :

$$\begin{aligned}&\deg B \leq \delta.\deg A\\ &L(B) \leq (\delta')^{\deg A}L(A)^{\delta''},\end{aligned}$$

d'où il résulte que

$$\begin{aligned}\left|B\left(\frac{\omega}{\eta},\frac{\eta}{\pi}\right)\right| &\geq \exp\left(-c''\left(N\log M + N(\log M)^2\right)^{3+\varepsilon}\right)\\ &\geq \exp\left(-\widetilde{c}\left(M^{1/4}(\log M)^2\right)^{3+\varepsilon}\right).\end{aligned}$$

La minoration ainsi obtenue est incompatible avec la majoration précédente lorsque N, donc M est suffisamment grand. L'hypothèse faite, à savoir l'existence d'une relation algébrique non triviale entre $e^{2i\pi\tau}$, $\frac{\omega}{\eta}$ et $\frac{\eta}{\pi}$, est ainsi contredite, ce qui termine la preuve. □

En conclusion de cette démonstration, on peut remarquer que la preuve de la proposition 6.3.7 que nous avons donnée ressemble beaucoup à la preuve du théorème stéphanois esquissée à la section 3. Dans les deux cas, on considère en effet une fonction F dont on minore la multiplicité en l'origine, puis on essaie de majorer, soit la valeur de F en un point α^S, soit l'ordre de la dérivée $T^{ème}$ de F en un point q. Ce type de démonstration est essentiellement le seul dont on dispose actuellement pour des preuves d'indépendance algébrique. Hermite a introduit en premier ce genre d'argument lors de la démonstration de la transcendance de e en 1873.

7 Preuve de quelques résultats à l'aide du théorème de Y.V.Nesterenko

Nous exposons à présent différents résultats qui se déduisent plus ou moins directement du corollaire 6.1.4. Nous proposerons également dans la dernière sous-partie, comme prolongement naturel de cette perspective, une démonstration conjecturale portant sur l'indépendance algébrique d'au moins trois des quatre nombres π, $e^{\pi\sqrt{5}}$, $\Gamma(1/5)$ et $\Gamma(2/5)$.

7.1 Transcendance de quelques valeurs de séries

L'indépendance algébrique de π et de e^{π} permet de déduire la transcendance de quelques valeurs de séries. Nous illustrons ce propos par la proposition qui suit :

Proposition 7.1.1. *Les nombres*

$$\sum_{n=2}^{+\infty}\frac{1}{n^4-1}=\frac{7}{8}-\frac{\pi}{4}\coth(\pi)\quad\text{et}\quad\sum_{n=2}^{+\infty}\frac{(-1)^n}{n^2+1}=\frac{\pi}{2\mathrm{sh}(\pi)}$$

sont transcendants.

La démonstration consiste évidemment en un petit exercice de calcul de somme de série.

Démonstration. L'ingrédient de base de la preuve est le développement eulérien de la cotangeante, rappelé dans la démonstration de la proposition 1.3.8. De la relation $\coth(x)=i\mathrm{cotan}(ix)$, on déduit le développement eulérien de la cotangeante hyperbolique :

$$\forall x\in\mathbb{R}^*,\quad \pi\coth(\pi x)=\frac{1}{x}+\sum_{m=1}^{+\infty}\frac{2x}{m^2+x^2}\cdot$$

On a alors :

$$\begin{aligned}\sum_{n=2}^{+\infty}\frac{1}{n^4-1}&=\sum_{n=2}^{+\infty}\frac{1}{(n^2+1)(n-1)(n+1)}\\&=-\frac{1}{2}\sum_{n=2}^{+\infty}\frac{1}{n^2+1}+\frac{1}{4}\underbrace{\sum_{n=2}^{+\infty}\left(\frac{1}{n-1}-\frac{1}{n+1}\right)}_{=1+\frac{1}{2}}.\end{aligned}$$

On conclut en évaluant le développement eulérien de la cotangeante hyperbolique en $x=1$, ce qui nous donne

$$\sum_{n=2}^{+\infty}\frac{1}{n^2+1}=\frac{\pi}{2}\coth(\pi)-1.$$

Pour le calcul de la seconde somme, on considère la somme partielle d'indice $2n$:

$$\sum_{k=0}^{2n}\frac{(-1)^k}{k^2+1}=\sum_{k=0}^{2n}\frac{1}{k^2+1}-2\sum_{k=0}^{n-1}\frac{1}{(2k+1)^2+1},$$

d'où, par passage à la limite,

$$\begin{aligned}\sum_{n=0}^{+\infty}\frac{(-1)^n}{n^2+1}&=\sum_{n=0}^{+\infty}\frac{1}{n^2+1}-2\sum_{n=0}^{+\infty}\frac{1}{(2n+1)^2+1}\\&=-\sum_{n=0}^{+\infty}\frac{1}{n^2+1}+2\sum_{n=0}^{+\infty}\frac{1}{(2n)^2+1}\cdot\end{aligned}$$

En évaluant le développement eulérien de la cotangeante hyperbolique en $x = 1/4$, on obtient

$$\sum_{n=0}^{+\infty} \frac{1}{(2n)^2+1} = \frac{1}{4}\sum_{n=0}^{+\infty} \frac{1}{n^2+\frac{1}{4}} = \frac{1}{4}\left(\pi \coth\left(\frac{\pi}{2}\right) - 1\right),$$

d'où l'on déduit

$$\sum_{n=0}^{+\infty} \frac{(-1)^n}{n^2+1} = \left(-\frac{\pi}{2}\coth(\pi)+1\right) + 2\left(\frac{\pi}{4}\coth\left(\frac{\pi}{2}\right) - \frac{1}{4}\right) = \frac{\pi}{2}\underbrace{\left(\coth\left(\frac{\pi}{2}\right) - \coth(\pi)\right)}_{=\frac{1}{\mathrm{sh}(\pi)}} + \frac{1}{2}\cdot$$

□

Remarque 7.1.2. *Comme on le justifiera avec le théorème 7.3.5 du paragraphe 7.3.1, le développement eulérien de la cotangeante hyperbolique permet plus généralement d'affirmer la transcendance des nombres*

$$\sum_{m=1}^{+\infty} \frac{1}{m^2+D} = \frac{1}{2\sqrt{D}}\left(\pi \coth(\pi\sqrt{D}) - \frac{1}{\sqrt{D}}\right),$$

pour tout entier $D \geq 1$.

Le résultat de la proposition 7.1.1 est moins anecdotique qu'il n'y paraît : elle a trait à la *fonction de Golomb* γ, définie pour tout entier $n \geq 2$ par $\gamma(n) = \mathrm{Card}\{(a,b) \in \mathbb{N}^2 / a^b = n\}$. Sa série génératrice de Dirichlet est

$$\sum_{n=2}^{+\infty} \frac{\gamma(n)}{n^s} = \sum_{n=2}^{+\infty} \frac{1}{n^s - 1},$$

qui converge pour tout complexe s de partie réelle > 1. P.Bundschuh, ayant remarqué dans [4] que la série était télescopique de valeur $\frac{3}{4}$ en $s = 2$, émet la conjecture selon laquelle elle prend des valeurs transcendantes en tout $s \geq 4$ entier pair. Dans le cas $s = 4$, le théorème de Nesterenko permet donc d'apporter une réponse affirmative [14].

Dans le cas s entier naturel impair, P.Bundschuh remarque que la situation est sans doute bien plus compliquée au égard au fait que l'on est naturellement amené à travailler avec les valeurs de la fonction zeta de Riemann en ces points, chose que l' «on sait être difficile», précise-t-il.

7.2 Transcendance de quelques valeurs du produit canonique de Weierstrass attaché au réseau gaussien

L'indépendance algébrique de π, e^π et $\Gamma(1/4)$ énoncé par le corollaire 6.1.7 permet de prouver la transcendance de quelques constantes numériques. A cet égard, le résultat suivant est particulièrement significatif :

Proposition 7.2.1. *On note $\sigma_{\mathbb{Z}[i]}$ le produit canonique de Weierstrass attaché au réseau gaussien. Alors la* constante de Weierstrass

$$\sigma_{\mathbb{Z}[i]}\left(\frac{1}{2}\right) = \frac{2^{5/4}\sqrt{\pi}e^{\pi/8}}{\Gamma(\frac{1}{4})^2} \approx 0,4749493799$$

est un nombre transcendant.

Démonstration. Le calcul de la constante de Weierstrass se fera en trois étapes. On notera σ le produit canonique de Weierstrass relatif à un réseau générique $\Omega = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ et $\sigma_{\mathbb{Z}[i]}$ celui relatif au réseau gaussien. On utilisera les formules d'addition et de duplication pour les fonctions σ (proposition 2.4.3 et corollaire 2.4.4) et $\wp$ (proposition 2.2.8 et corollaire 2.2.9) ainsi que la formule de quasi-périodicité vérifiée par la première fonction (proposition 2.4.2) et l'équation différentielle satisfaite par le seconde (proposition 2.2.4).

14. Dans le cas général, le résultat est vrai si l'on admet la conjecture de Schanuel. On se réfèrera à l'article initial pour plus de détails.

Première étape : Formule de triplication pour la fonction σ.
Soit $z \notin \frac{\Omega}{3} \cup \frac{\Omega}{2}$. Les formules de conjugaison et de duplication pour la fonction σ permettent d'écrire

$$\sigma(3z) = \sigma(2z)^2\sigma(z)\left(\wp(z) - \wp(2z)\right) = \wp'(z)^2\sigma(z)^9\left(\wp(z) - \wp(2z)\right).$$

La formule de duplication et l'équation fonctionnelle vérifiées par la fonction $\wp$ impliquent alors l'égalité (entre fonctions méromorphes définies sur $\mathbb{C}$) :

$$\sigma(3z) = \sigma(z)^9\left(3\wp(z)^4 - \frac{3}{2}g_2\wp(z)^2 - 3g_3\wp(z) - \frac{g_2^2}{16}\right).$$

Deuxième étape : Application au cas du réseau gaussien $\mathbb{Z} \oplus \mathbb{Z}i$.
Nous allons à présent calculer les invariants propres à ce réseau en vue d'exploiter la formule de triplication précédente. Dans le cas considéré, $\omega_1 = 1$ et $\omega_2 = i$. Des formules exprimant η_1 et η_2 en fonction de ω_1 et de ω_2 (cf. propos qui suivent la définition 2.3.1 de la fonction ζ), on déduit immédiatement que $\eta_1 = i\eta_2$, d'où, par la relation de Legendre (théorème 2.3.3), $\eta_1 = \pi$. Par ailleurs, comme le réseau considéré est invariant par multiplication par i, $g_3(\mathbb{Z}[i]) = g_3(i\mathbb{Z}[i]) = (-i)^6 g_3(\mathbb{Z}[i]) = -g_3(\mathbb{Z}[i])$, i.e. $g_3(\mathbb{Z}[i]) = 0$.

Le calcul de $g_2(\mathbb{Z}[i])$ est plus astucieux : on considére la courbe elliptique $\mathcal{E} : y^2 = 4x^3 - 4x$ pour laquelle on a vu lors de la démonstration du corollaire 6.1.7 que l'une des périodes fondamentales était

$$\widetilde{\omega_1} = \int_1^{+\infty} \frac{dx}{\sqrt{x^3 - x}} = \frac{\Gamma\left(\frac{1}{4}\right)^2}{2^{\frac{3}{2}}\sqrt{\pi}}.$$

A l'aide du tableau de variations de $\wp(i.)$ sur $]0; -i\widetilde{\omega_2}[$ (cf. corollaire 2.2.14), $\widetilde{\omega_2}$ étant l'autre période fondamentale de $\mathcal{E}$, on montre de la même manière que pour le calcul de $\widetilde{\omega_1}$ que

$$\widetilde{\omega_2} = \int_{-\infty}^{-1} \frac{dx}{\sqrt{x^3 - x}},$$

i.e. $\widetilde{\omega_2} = i\widetilde{\omega_1}$. Par conséquent,

$$g_2(\mathcal{E}) = 60 \sum_{(m,n)\in(\mathbb{Z}^2)^*} \frac{1}{(m\widetilde{\omega_1} + n\widetilde{\omega_2})^4} = \frac{60}{\widetilde{\omega_1}^4} \sum_{(m,n)\in(\mathbb{Z}^2)^*} \frac{1}{(m+ni)^4} = \frac{g_2(\mathbb{Z}[i])}{\widetilde{\omega_1}^4}.$$

Comme $g_2(\mathcal{E}) = 4$, il vient finalement [15]

$$g_2(\mathbb{Z}[i]) = \frac{\Gamma\left(\frac{1}{4}\right)^8}{2^4\pi^2}.$$

Troisième étape : Déduction du résultat.
Dans le cas d'un réseau $\Omega = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ quelconque, la combinaison des formules de pseudo-périodicité et de triplication pour la fonction σ permettent d'écrire

$$\begin{aligned}\sigma\left(\frac{3\omega_1}{2}\right) &= \sigma\left(\omega_1 + \frac{\omega_1}{2}\right) = -\sigma\left(\frac{\omega_1}{2}\right)e^{\eta_1\omega_1} \\ &= \sigma\left(3\frac{\omega_1}{2}\right) = \sigma\left(\frac{\omega_1}{2}\right)^9\left(3\wp\left(\frac{\omega_1}{2}\right)^4 - \frac{3}{2}g_2\wp\left(\frac{\omega_1}{2}\right)^2 - 3g_3\wp\left(\frac{\omega_1}{2}\right) - \frac{g_2^2}{16}\right),\end{aligned}$$

15. On a montré au passage que

$$\sum_{(m,n)\in(\mathbb{Z}^2)^*} \frac{1}{(m+ni)^4} = \frac{\Gamma\left(\frac{1}{4}\right)^8}{2^6.3.5.\pi^2}.$$

Un calcul similaire avec la courbe elliptique $y^2 = 4x^3 - 4$ montre que, en posant $\rho = e^{2i\pi/3}$,

$$\sum_{(m,n)\in(\mathbb{Z}^2)^*} \frac{1}{(m+n\rho)^4} = \frac{\Gamma\left(\frac{1}{3}\right)^{18}}{2^8.5.7.\pi^6}.$$

d'où il résulte

$$\sigma\left(\frac{\omega_1}{2}\right)^8 = \frac{-e^{\eta_1\omega_1}}{3\wp\left(\frac{\omega_1}{2}\right)^4 - \frac{3}{2}g_2\wp\left(\frac{\omega_1}{2}\right)^2 - 3g_3\wp\left(\frac{\omega_1}{2}\right) - \frac{g_2^2}{16}}. \tag{1}$$

Or dans le cas du réseau gaussien, l'équation fonctionnelle satisfaite par la fonction $\wp$ s'écrit $\wp'_{\mathbb{Z}[i]}(z)^2 = 4\wp_{\mathbb{Z}[i]}(z)^3 - g_2(\mathbb{Z}[i]).\wp_{\mathbb{Z}[i]}(z)$. Remarquant que $\frac{1}{2}$ est racine de $\wp'_{\mathbb{Z}[i]}$ sans annuler $\wp_{\mathbb{Z}[i]}$, il vient $\wp_{\mathbb{Z}[i]}\left(\frac{1}{2}\right)^2 = \frac{g_2(\mathbb{Z}[i])}{4}$.

Après simplification, (1) se réécrit

$$\sigma_{\mathbb{Z}[i]}\left(\frac{1}{2}\right)^8 = \frac{4e^{\pi}}{g_2(\mathbb{Z}[i])^2},$$

i.e., avec la valeur de $g_2(\mathbb{Z}[i])$ précédemment calculée,

$$\sigma_{\mathbb{Z}[i]}\left(\frac{1}{2}\right) = \alpha_8 2^{5/4}\pi^{1/2}e^{\pi/8}\Gamma(1/4)^{-2},$$

où α_8 est une racine huitième de l'unité.

Comme la conjugaison complexe réalise une bijection de $\mathbb{Z}[i]$ sur lui-même, $\sigma_{\mathbb{Z}[i]}$ est à valeurs réelles dès que son argument est réel. Ainsi, $\alpha_8 \in \{\pm 1\}$. Comme $\sigma_{\mathbb{Z}[i]}$ ne s'annule qu'en 0 et en 1 sur l'intervalle $[0;1]$, elle y est de signe constant. Enfin, le fait que $\sigma_{\mathbb{Z}[i]}(x) \underset{x\to 0^+}{\sim} x \geq 0$ montre que $\alpha_8 = 1$, d'où le résultat recherché. □

Remarque 7.2.2. *Un raisonnement en tout point identique au précédent avec le choix de $\omega_2 = i$ pour période du réseau gaussien (associée à la pseudo-période $\eta_2 = i\pi$) plutôt que $\omega_1 = 1$ conduit à établir la transcendance de*

$$\sigma_{\mathbb{Z}[i]}\left(\frac{i}{2}\right) = i2^{5/4}\pi^{1/2}e^{-\pi/8}\Gamma(1/4)^{-2}.$$

Le fait que π, e^{π} et $\Gamma(1/4)$ apparaissent de manière si peu triviale dans l'expression de $\sigma_{\mathbb{Z}[i]}\left(\frac{1}{2}\right)$ laisse à penser qu'il est possible d'envisager une démonstration de l'indépendance algébrique de ces trois nombres par l'étude des propriétés du produit canonique de Weierstrass.

En creusant cette idée, on est amené à émettre la conjecture suivante, qui ne peut cependant suffire à elle seule à proposer une preuve alternative à l'indépendance algébrique de π, e^{π} et $\Gamma(1/4)$:

Conjecture 7.2.3. *Soit Ω un réseau complexe admettant ω comme période non nulle. Soit η la pseudo-période associée et $u \in \mathbb{C}\backslash\Omega$ linéairement indépendant de ω sur $\mathbb{Q}$. Alors*

$$\operatorname{Tr\,deg}_{\mathbb{Q}}\mathbb{Q}(g_2, g_3, \wp(u), \zeta(u), \sigma(u), \eta, e^{\eta u}, e^{\eta\omega}) \geq 2.$$

La proposition 7.2.1 constitue de fait un cas particulier d'un énoncé plus général :

Proposition 7.2.4. *$\sigma_{\mathbb{Z}[i]}$ prend des valeurs transcendantes aux points de $\mathbb{Q} \oplus i\mathbb{Q}$ qui ne sont pas dans $\mathbb{Z} \oplus i\mathbb{Z}$.*

Remarque 7.2.5. *Il est intéressant de noter que ce résultat ne subsiste pas en dimension 1 : le produit de Weierstrass pour le réseau $\mathbb{Z}$ de $\mathbb{R}$ correspond au développement eulérien de la fonction $\sin(\pi z)$. On pourrait donc s'attendre à ce que les valeurs aux éléments de $\mathbb{Q}(i)$ de la fonction $\sigma_{\mathbb{Z}[i]}$ de Weierstrass aient une analogie avec les valeurs aux points rationnels de la fonction $\sin(\pi z)$. Or il n'en est rien : pour la fonction sinus interviennent des nombres algébriques (liées aux racines de l'unité) alors que pour la fonction $\sigma_{\mathbb{Z}[i]}$ ce sont des nombres transcendants.*

Démonstration. Les notations précédentes sont conservées.

La démonstration de la proposition 7.2.4 se fera en deux étapes : dans un premier temps, nous établirons un résultat général sur la nature arithmétique de la fonction σ d'un réseau complexe lorsqu'elle est évaluée en un multiple rationnel d'une période non nulle. Dans un second temps, l'application de ce résultat au cas du réseau $\mathbb{Z}[i]$ fournira la conclusion recherchée.

Première étape

On se fixe un réseau complexe $\Omega = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$. Sans autre précision, ω désignera indifféremment ω_1 ou ω_2 et η sera la pseudo-période associée.

Voici tout d'abord un lemme dont la démonstration par récurrence est sans difficulté dès lors que l'on dispose de la proposition 2.2.10 et des formules usuelles relatives à la fonction σ (proposition 2.4.3 et corollaire 2.4.4) :

Lemme 7.2.6. *Soit $m \in \mathbb{N}^*$. Il existe une fraction rationnelle $\Xi_m \in \mathbb{Q}(g_2, g_3)(X, Y)$ telle que, pour tout $z \in \mathbb{C}$, on ait*

$$\sigma(mz) = (-1)^{m-1}\sigma(z)^{m^2}\Xi_m\left(\wp(z), \wp'(z)\right).$$

La formule de duplication pour σ donne par exemple $\Xi_2(Y) = Y$, alors que la formule de triplication nous conduit à poser $\Xi_3(X) = 3X^4 - \frac{3}{2}g_2X^2 - 3g_2X - \frac{g_2^2}{16}$.

L'objectif de cette première étape est d'établir le lemme suivant, par ailleurs intéressant en lui-même :

Lemme 7.2.7. *Soit $p, q \in \mathbb{N}^*$, p et q premiers entre eux. Alors $\sigma\left(\frac{p}{q}\omega\right).\exp\left(\frac{-p^2}{2q^2}\eta\omega\right)$ est algébrique sur $\mathbb{Q}(g_2, g_3)$.*

Démonstration. Supposons tout d'abord $p = 1$. En écrivant $\sigma\left(\frac{\omega}{q} + \omega\right) = \sigma\left((q+1)\frac{\omega}{q}\right)$, les formules de pseudo-périodicité et le lemme 7.2.6 impliquent

$$-\sigma\left(\frac{\omega}{q}\right).\exp\left(\eta\omega\left(\frac{1}{q}+\frac{1}{2}\right)\right) = (-1)^q\sigma\left(\frac{\omega}{q}\right)^{(q+1)^2} \times \Xi_{q+1}\left(\wp\left(\frac{\omega}{q}\right), \wp'\left(\frac{\omega}{q}\right)\right),$$

d'où

$$\sigma\left(\frac{\omega}{q}\right)^{q(q+2)} = (-1)^{q-1}\frac{\exp\left(\eta\omega\frac{2+q}{2q}\right)}{\Xi_{q+1}\left(\wp\left(\frac{\omega}{q}\right), \wp'\left(\frac{\omega}{q}\right)\right)}.$$

Si p est quelconque, on se ramène au cas précédent en remarquant que, d'après le lemme 7.2.6,

$$\sigma\left(p\frac{\omega}{q}\right) = (-1)^{p-1}\sigma\left(\frac{\omega}{q}\right)^{p^2}\Xi_p\left(\wp\left(\frac{\omega}{q}\right), \wp'\left(\frac{\omega}{q}\right)\right).$$

Le problème revient donc à montrer que pour tout $q \in \mathbb{N}^*$, $\wp\left(\frac{\omega}{q}\right)$ et $\wp'\left(\frac{\omega}{q}\right)$ sont algébriques sur $\mathbb{Q}(g_2, g_3)$. D'après l'équation différentielle vérifiée par $\wp$, il suffit encore de le vérifier pour $\wp\left(\frac{\omega}{q}\right)$. On procède en trois temps :

1. Le nombre $\wp\left(\frac{\omega}{2}\right)$ est tout d'abord algébrique sur $\mathbb{Q}(g_2, g_3)$ d'après l'équation différentielle vérifiée par $\wp$ et le fait que $\frac{\omega}{2}$ est racine de $\wp'$.
2. Supposons ensuite que $2|q$: en écrivant $\wp\left(\frac{\omega}{2}\right) = \wp\left(\frac{q}{2}\frac{\omega}{q}\right)$, la proposition 2.2.10 permet de voir $\wp\left(\frac{\omega}{2}\right)$ comme une fraction rationnelle en $\wp\left(\frac{\omega}{q}\right)$ à coefficients dans $\mathbb{Q}(g_2, g_3)$. Le nombre $\wp\left(\frac{\omega}{q}\right)$ est donc en particulier lui-même algébrique sur $\mathbb{Q}(g_2, g_3)$.
3. Si, en revanche, $2 \not| q$, on se ramène au cas précédent à l'aide de la formule de duplication :

$$\wp\left(\frac{\omega}{q}\right) = \wp\left(2\frac{\omega}{2q}\right) = -2\wp\left(\frac{\omega}{2q}\right) + \frac{1}{4}\frac{\left(6\wp\left(\frac{\omega}{2q}\right)^2 - \frac{g_2}{2}\right)^2}{4\wp\left(\frac{\omega}{2q}\right)^3 - g_2\wp\left(\frac{\omega}{2q}\right) - g_3},$$

où l'on sait à présent que $\wp\left(\frac{\omega}{2q}\right)$ est algébrique sur $\mathbb{Q}(g_2, g_3)$.

Le lemme 7.2.7 est ainsi démontrée. □

Deuxième étape :
On applique dans un second temps le lemme 7.2.7 au cas du réseau $\mathbb{Z}[i]$ pour lequel les différents invariants ont été calculés lors la démonstration de la proposition 7.2.1.

Soit $r \in \mathbb{Q}\backslash\mathbb{Z}$. Le lemme 7.2.7 de la première étape prouve, en choisissant $\omega = 1$ et donc $\eta = \pi$, que $\sigma_{\mathbb{Z}[i]}(r).\exp\left(-\frac{r^2}{2}\pi\right)$ est algébrique non nul sur $\mathbb{Q}\left(g_2\left(\mathbb{Z}[i]\right)\right) = \mathbb{Q}\left(\frac{\Gamma(1/4)^8}{\pi^2}\right)$.

En choisissant à présent $\omega_2 = i$ pour période, qui est associée à la pseudo-période $\eta_2 = i\pi$, $\sigma_{\mathbb{Z}[i]}(is).\exp\left(\frac{s^2}{2}\pi\right)$ apparaît de même comme un nombre algébrique non nul sur $\mathbb{Q}\left(\frac{\Gamma(1/4)^8}{\pi^2}\right)$ pour $s \in \mathbb{Q}\backslash\mathbb{Z}$.

Or par la formule de conjugaison,

$$\sigma_{\mathbb{Z}[i]}(r+si).\sigma_{\mathbb{Z}[i]}(r-si) = \sigma_{\mathbb{Z}[i]}(r)^2 \times \sigma_{\mathbb{Z}[i]}(is)^2 \times \left(\wp_{\mathbb{Z}[i]}(is) - \wp_{\mathbb{Z}[i]}(r)\right). \tag{1}$$

Comme $\wp_{\mathbb{Z}[i]}\left(\frac{1}{q}\right)$ et $\wp_{\mathbb{Z}[i]}\left(\frac{i}{q}\right)$ sont algébriques sur $\mathbb{Q}\left(g_2\left(\mathbb{Z}[i]\right)\right)$ pour tout $q \in \mathbb{Z}^*$ d'après l'étape 1 et que $\wp_{\mathbb{Z}[i]}(nz)$ est une fraction rationnelle en $\wp_{\mathbb{Z}[i]}(z)$ à coefficients dans $\mathbb{Q}\left(g_2\left(\mathbb{Z}[i]\right)\right)$ pour tout $n \in \mathbb{N}^*$, $\wp_{\mathbb{Z}[i]}(is)$ et $\wp_{\mathbb{Z}[i]}(r)$ sont algébriques sur $\mathbb{Q}\left(g_2\left(\mathbb{Z}[i]\right)\right)$.

Dès lors, en multipliant (1) par $\exp\left((s^2-r^2)\pi\right)$, on constate que

$$\sigma_{\mathbb{Z}[i]}(r+is).\sigma_{\mathbb{Z}[i]}(r-is).\exp\left((s^2-r^2)\pi\right)$$

est algébrique non nul sur $\mathbb{Q}\left(g_2\left(\mathbb{Z}[i]\right)\right) = \mathbb{Q}\left(\frac{\Gamma(1/4)^8}{\pi^2}\right)$. Par indépendance algébrique de π, e^π et $\Gamma(1/4)$, on déduit la transcendance du produit $\sigma_{\mathbb{Z}[i]}(r+is).\sigma_{\mathbb{Z}[i]}(r-is)$. Comme par ailleurs $\overline{\sigma_{\mathbb{Z}[i]}(r+is)} = \sigma_{\mathbb{Z}[i]}(r-is)$, l'un des termes du produit est transcendant si, et seulement si, l'autre l'est. Ceci prouve la proposition 7.2.4, puisque les nombres algébriques forment un corps. □

7.3 Un essai de démonstration de l'indépendance algébrique d'au moins trois des quatre nombres π, $e^{\pi\sqrt{5}}$, $\Gamma(1/5)$ et $\Gamma(2/5)$

Nous cherchons maintenant à déduire du corollaire 6.1.4 la conjecture ci-dessous :

Conjecture 7.3.1. *Trois des quatre nombres*

$$\pi, \quad e^{\pi\sqrt{5}}, \quad \Gamma\left(\frac{1}{5}\right), \quad \Gamma\left(\frac{2}{5}\right)$$

sont algébriquement indépendants.

Nous serons amenés à introduire un nouvel outil, la notion de distribution universelle, pour proposer une démonstration conjecturale du résultat.

7.3.1 Théorème de Chowla-Selberg et périodes de courbes elliptiques

Nous déduisons dans un premier temps du corollaire 6.1.4 quelques autres résultats d'indépendance algébrique impliquant π et $e^{\pi\sqrt{D}}$ pour $D \geq 1$ entier. Nous aurons pour cela besoin du lemme suivant :

Lemme 7.3.2. *Soit $\tau \in \mathfrak{H}$ un nombre quadratique. Alors $j(\tau)$ est un entier algébrique.*

Remarque 7.3.3. *En 1937, T.Schneider a prouvé dans [25] que la réciproque était également vraie sous l'hypothèse que τ est un nombre algébrique.*

Démonstration. Notons $\mathbb{K} = \mathbb{Q}(\tau)$ et $\mathcal{O}_\mathbb{K}$ l'anneau des entier de $\mathbb{K}$. $\mathcal{O}_\mathbb{K}$ étant un anneau de Dedekind, il existe $z \in \mathcal{O}_\mathbb{K}$ tel que z et 1 engendrent $\mathcal{O}_\mathbb{K}$ [16].

16. On trouvera la démonstration de ce fait, caractéristique des anneaux de Dedekind, en *annexe 2*.

On peut toujours trouver $\lambda \in \mathcal{O}_{\mathbb{K}}$ tel que la norme de λ soit sans facteur carré : si $\mathbb{K} = \mathbb{Q}(i)$, il suffit de prendre $\lambda = 1 + i$ (qui est de norme 2) et, si $\mathbb{K} = \mathbb{Q}(\sqrt{m})$ avec $|m| > 1$ sans facteur carré, il suffit de prendre $\lambda = \sqrt{m}$ (de norme $-m$).

Ecrivons

$$\begin{cases} \lambda z = az + b \\ \lambda = cz + d \end{cases}$$

avec $a, b, c, d \in \mathbb{Z}$, de telle sorte que $ad - bc = n$. Alors $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est une matrice primitive telle que $z = \frac{az+b}{cz+d} = \alpha.z$.

Montrons que $j(z)$ est un entier algébrique : soit $\tau \in \mathfrak{H}$, $L = \mathbb{Z} \oplus \mathbb{Z}\tau$ un réseau complexe. On considère le sous-réseau $M = (a\tau+b)\mathbb{Z} \oplus (c\tau+d)\mathbb{Z}$ de L. Par le théorème des diviseurs élémentaires, il existe une base (ω_1, ω_2) de L et une base (ω_1', ω_2') de M telles que

$$\begin{cases} \omega_1' = e_1\omega_1 \\ \omega_2' = e_2\omega_2 \end{cases}$$

avec $e_1, e_2 \in \mathbb{N}$ et $e_1 | e_2$. La condition $\operatorname{pgcd}(a, b, c, d) = 1$ impose $e_1 = 1$. Comme par ailleurs deux bases d'un même réseau sont congrus modulo $SL_2(\mathbb{Z})$ (proposition 1.2.2), il existe une matrice $\gamma \in SL_2(\mathbb{Z})$ telle que $\gamma\alpha = \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} = \left[\frac{1}{n}\right]$. Les propriétés du polynôme modulaire (proposition 3.1.2) et la modularité de j permettent alors d'écrire :

$$\Phi_n(j(z), j(z)) = \Phi_n(j(\alpha.z), j(z)) = \Phi_n(j(\gamma\alpha.z), j(z)) = \Phi_n\left(j\left(\left[\frac{1}{n}\right]z\right), j(z)\right) = 0,$$

ce qui prouve bien que $j(z)$ est un entier algébrique.

Comme $\mathbb{Q}(\tau) = \mathbb{Q}(z)$, il existe $\beta \in GL_2^+(\mathbb{Z})$ de déterminant $p \in \mathbb{N}$ tel que $\tau = \beta z$. Alors $j(\beta)$ est racine du polynôme unitaire $\phi(X, j) \in \mathbb{Z}[j][X]$, donc est un entier algébrique sur $\mathbb{Z}[j]$. Il s'ensuit que $j(\beta z) = j(\tau)$ est un entier algébrique sur $\mathbb{Z}[j(z)]$, donc que $j(\tau)$ est aussi un entier algébrique. □

On déduit de ce lemme la proposition qui suit :

Proposition 7.3.4. *Pour tout $d \in \mathbb{N}^*$, il existe une courbe elliptique complexe à invariants algébriques admettant $\mathbb{Q}\left(\sqrt{-d}\right)$ comme corps de multiplication complexe.*

Démonstration. Soit $d \in \mathbb{N}^*$ et

$$\tau = \begin{cases} \sqrt{-d} & \text{si } d \equiv -1 \pmod 4 \\ \frac{1+\sqrt{-d}}{2} & \text{si } d \not\equiv -1 \pmod 4 \end{cases}$$

On pose $\Omega_\tau = \mathbb{Z}[\tau]$, qui est un réseau complexe de corps de multiplication complexe $\mathbb{Q}\left(\sqrt{-d}\right)$ et d'invariants notés $g_2(\Omega_\tau)$ et $g_3(\Omega_\tau)$.

D'après le lemme 7.3.2, $j(\tau)$ est un entier algébrique. Par ailleurs, pour tout $\lambda \in \mathbb{C}^*$, le réseau $\lambda\Omega_\tau$ est encore à multiplication complexe par le corps $\mathbb{Q}\left(\sqrt{-d}\right)$.

Si $g_2(\Omega_\tau) = 0$, on choisit $\lambda \in \mathbb{C}^*$ tel que $g_3(\lambda\Omega_\tau) = \lambda^{-6} g_3(\Omega_\tau)$ soit algébrique. Sinon, on choisit $\lambda \in \mathbb{C}^*$ tel que $g_2(\lambda\Omega_\tau) = \lambda^{-4} g_2(\Omega_\tau)$ soit un nombre algébrique (rappelons que $g_2(\Omega_\tau)$ et $g_3(\Omega_\tau)$ ne peuvent pas être simultanément nuls comme justifié à la suite de la remarque 2.2.6). Par homogénéité de j, on a alors :

$$j(\tau) = 1728\frac{g_2^3(\Omega_\tau)}{g_2^3(\Omega_\tau) - 27g_3^2(\Omega_\tau)} = 1728\frac{g_2^3(\lambda\Omega_\tau)}{g_2^3(\lambda\Omega_\tau) - 27g_3^2(\lambda\Omega_\tau)},$$

de sorte que $g_3(\lambda\Omega_\tau)$ est un nombre algébrique dans ce cas aussi.

La courbe elliptique attachée au réseau $\lambda\Omega_\tau$ répond donc dans tous les cas au problème. □

Cette proposition est particulièrement intéressante lorsqu'elle est associée au corollaire 6.1.4 du théorème de Y.V.Nesterenko puisqu'elle fournit d'emblée le théorème suivant :

Théorème 7.3.5. *Pour tout entier $d \geq 1$, π et $e^{\pi\sqrt{d}}$ sont algébriquement indépendants.*

Un énoncé plus fort consisterait à affirmer l'indépendance algébrique de π, $e^{\pi\sqrt{d}}$ et de ω pour tout $d \in \mathbb{N}^*$, où ω est une période intervenant dans les hypothèses du corollaire 6.1.4.

Dans cette perspective, le théorème de Chowla-Selberg permet de déterminer une expression de ω dans le cas de la multiplication complexe. La formulation n'est pas celle de l'article initial mais permet une application directe au problème de la détermination des périodes d'une courbe elliptique :

Théorème 7.3.6 (Chowla-Selberg)**.** *Soit E une courbe elliptique à multiplication complexe par le corps $\mathbb{K}$ de discriminant $-d$, $d > 0$. Soit w le nombre d'unités et h le nombre de classes de $\mathbb{K}$.*

Alors toute période de E est de la forme

$$\omega = \alpha\sqrt{\pi} \prod_{0<a<d} \Gamma\left(\frac{a}{d}\right)^{\frac{w\left(\frac{-d}{a}\right)}{4h}},$$

où α est un nombre algébrique et où $\left(\frac{-d}{a}\right)$ est le symbole de Jacobi.

Démonstration. On trouvera la preuve du théorème dans l'article original [5] des auteurs. Expliquons simplement la raison pour laquelle il est indispensable de considérer le discriminant $-d$ du corps $\mathbb{K}$ plutôt que l'entier $m > 0$ sans facteur carré tel que $\mathbb{K} = \mathbb{Q}(\sqrt{-m})$. La démonstration passe par l'étude de la *fonction zêta d'Epstein*, définie pour tout complexe σ de partie réelle > 1 et pour tous $a, b, c \in \mathbb{Z}$ par la série

$$E_{a,b,c}(\sigma) = \sum_{(m,n)\in(\mathbb{Z}^2)^*} \frac{1}{(am^2 + bmn + cn^2)^\sigma}.$$

Les auteurs montrent que les valeurs de cette fonction dépendent essentiellement du discriminant $-d = 4ac - b$ à σ fixé. Ils exploitent pour cela pleinement l'isomorphisme de groupes entre les classes d'idéaux du corps $\mathbb{Q}(\sqrt{-m})$ $(m > 0)$ et les classes de formes quadratiques binaires de discriminant égal à celui de $\mathbb{Q}(\sqrt{-m})$. □

Si $\mathbb{K}$ est le corps de multiplication complexe d'une courbe elliptique E, en écrivant $\mathbb{K}$ sous la forme $\mathbb{K} = \mathbb{Q}\left(\sqrt{-m}\right)$, où m est un entier naturel non nul sans facteur carré, son discriminant $-d$ vaut $-4m$ si $m \not\equiv -1 \pmod 4$ et $-m$ si $m \equiv -1 \pmod 4$.

A l'aide de la proposition 7.3.4, on en déduit l'indépendance algébrique de π avec certains «produits-quotients» de valeurs de la fonction Γ aux points rationnels :

Corollaire 7.3.7. *Soit $d \in \mathbb{N}^*$ tel que $d \equiv 0 \pmod 4$ ou $d \equiv -1 \pmod 4$. Si $d \equiv 0 \pmod 4$ (resp. $d \equiv -1 \pmod 4$), on suppose de plus que $\frac{d}{4}$ (resp. d) est sans facteur carré.*

Alors les trois nombres

$$\pi, e^{\pi\sqrt{d}} \text{ et } \prod_{\substack{0<a<d \\ (a,d)=1}} \Gamma\left(\frac{a}{d}\right)^{\left(\frac{-d}{a}\right)}$$

sont algébriquement indépendants.

Pour $d = 3$ et $d = 4$, on retrouve respectivement l'indépendance algébrique des éléments des ensembles $\left\{\pi, e^{\pi\sqrt{3}}, \Gamma\left(\frac{1}{3}\right)\right\}$ et $\left\{\pi, e^{\pi}, \Gamma\left(\frac{1}{4}\right)\right\}$.

Comme 5 n'est ni congru à 0, ni congru à -1 modulo 4, il n'est pas possible de déduire de ce corollaire une preuve de la conjecture 7.3.1. Puisque l'on impose à d ou à $\frac{d}{4}$ d'être sans facteur carré, le seul moyen de faire apparaître la racine de cinq en puissance de l'exponentielle est de traiter le cas $d = 20$. Calculs faits, on obtient après simplification (en utilisant la formule des compléments pour la fonction Γ rappelée en *annexe 1*) l'indépendance algébrique des trois éléments de l'ensemble $\left\{\pi, e^{\pi\sqrt{5}}, \Gamma\left(\frac{1}{20}\right) \times \Gamma\left(\frac{3}{20}\right) \times \Gamma\left(\frac{7}{20}\right) \times \Gamma\left(\frac{9}{20}\right)\right\}$. La formule de multiplication pour la fonction Γ permet alors de simplifier le troisième terme pour aboutir à l'indépendance algébrique des trois éléments de chacun des deux ensembles

$$\left\{\pi, e^{\pi\sqrt{5}}, \Gamma\left(\frac{1}{5}\right) \times \Gamma\left(\frac{7}{20}\right) \times \Gamma\left(\frac{9}{20}\right)\right\} \quad \text{et} \quad \left\{\pi, e^{\pi\sqrt{5}}, \frac{\Gamma\left(\frac{1}{20}\right) \times \Gamma\left(\frac{3}{20}\right)}{\Gamma\left(\frac{1}{5}\right)}\right\}$$

sans qu'il semble être possible de supprimer les facteurs additionnels des troisièmes termes pour disposer là d'une preuve de la conjecture 7.3.1.

On se propose dès lors de fournir une démonstration conjecturale à la question posée, en admettant les conjectures de Rohrlich et de Lang exposées ci-après. Celles-ci reposent sur les relations dites standard vérifiées par la fonction Γ, à savoir les formules de translation, de complément et de multiplication rappelées en *annexe 1.*

Conjecture 7.3.8 (Rohrlich)**.** *Toute relation multiplicative de la forme*

$$\prod_{a\in\mathbb{Q}} \Gamma(a)^{m_a} \in \overline{\mathbb{Q}}, \quad \textit{avec } m_a \in \mathbb{Z},$$

le produit étant à support fini, peut être déduite des relations standard vérifiées par la fonction Γ*.*

S.Lang propose dans [14] un renforcement de cette conjecture :

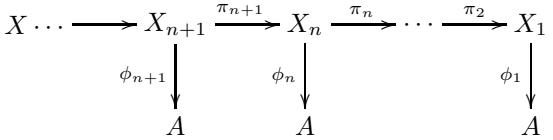
Conjecture 7.3.9 (Rohrlich-Lang)**.** *Toute relation de dépendance algébrique parmi les valeurs* $\Gamma(a)$*,* $a \in \mathbb{Q}\backslash(-\mathbb{N}^*)$*, est dans le radical de l'idéal engendré par les relations standard sur* $\overline{\mathbb{Q}}$*.*

L'intérêt de considérer le radical de l'idéal sera justifié plus loin à l'aide d'un exemple.

L'exploitation de ces conjectures dans le cadre qui nous intéresse nécessite une reformulation de ces dernières afin de les préciser et des les rendre plus «maniables» : c'est l'objet du paragraphe qui suit.

7.3.2 Distribution sur un système projectif et conjecture de Rohrlich-Lang

La notion de distribution sur un système projectif est présentée par S.Lang, dans son exposé [13], comme une «structure algébrique élémentaire» semblable «à la prose de M. Jourdain : nous en avons tous vu, sans lui avoir donné de nom». Commençons donc par la définir rigoureusement : on se donne une suite d'ensembles $(X_n)_{n\geq 1}$ et une suite $(\pi_{n+1} : X_{n+1} \to X_n)_{n\geq 1}$ d'applications surjectives, de sorte que l'on peut considérer la limite projective $X = \varprojlim_n X_n$. Soit également A un groupe abélien dont la loi est notée additivement et, pour tout $n \in \mathbb{N}^*$, une fonction $\phi_n : X_n \to A$.



Définition 7.3.10. $(\phi_n)_{n\geq 1}$ *(parfois notée* $\mathrm{d}\phi$ *ou encore* ϕ*) est une distribution sur* X *si elle satisfait de plus la relation de compatibilité :*

$$\forall n \in \mathbb{N}^*, \quad \forall x \in X_n, \quad \phi_n(x) = \sum_{\pi_{n+1} y = x} \phi_{n+1}(y),$$

où la somme porte sur l'ensemble des éléments $y \in \pi_{n+1}^{-1}(\{x\})$*.*

Remarque 7.3.11. *Si* f *est une fonction définie sur un* X_m *(à* $m \in \mathbb{N}^*$ *fixé) à valeurs dans* A*, alors* f *peut être considérée comme étant définie sur* X_n *pour tout* $n \geq m$ *en la composant avec la projection naturelle de* X_n *vers* X_m*. Une récurrence facile découlant de la relation de compatiblité satisfaite par* ϕ *prouve alors que*

$$\forall n \geq m, \quad \sum_{x \in X_m} f(x)\phi_m(x) = \sum_{x \in X_n} f(x)\phi_n(x).$$

Une telle fonction est dite localement constante sur X*. On peut définir son intégrale par rapport à la distribution* ϕ *en posant*

$$\int f \mathrm{d}\phi = \sum_{x \in X_n} f(x)\phi_n(x),$$

quantité qui est donc indépendante du choix de $n \geq m$*.*

Un système projectif peut être indéxé par d'autres indices que les entiers positifs ordonnés naturellement. A cet égard, l'exemple de l'ordre partiel issu de la divisibilité est fondamental : il permet en effet d'ordonner le système projectif $\left(\mathbb{Z}/N\mathbb{Z}\right)_{N\geq 1}$, qui est alors isomorphe au système $\left(\left(\frac{1}{N}\mathbb{Z}\right)/\mathbb{Z}\right)_{N\geq 1}$ pour le même ordre, et ce selon le diagramme commutatif suivant :

$$\begin{array}{ccc} \left(\frac{1}{N}\mathbb{Z}\right)/\mathbb{Z} & \xrightarrow[\sim]{\times N} & \mathbb{Z}/N\mathbb{Z} \\ \Big\downarrow{\scriptstyle \times \frac{N}{M}} & & \Big\downarrow{\scriptstyle r_M \text{ (réduction modulo } M)} \\ \left(\frac{1}{M}\mathbb{Z}\right)/\mathbb{Z} & \xrightarrow[\sim]{\times M} & \mathbb{Z}/M\mathbb{Z} \end{array}$$

Définition 7.3.12. *Une* distribution ordinaire ϕ *est une fonction définie sur* $\mathbb{Q}/\mathbb{Z}$ *telle que sa restriction à chaque* $\left(\frac{1}{N}\mathbb{Z}\right)/\mathbb{Z}$ *(*$N \geq 1$*) satisfait la relation de compatibilité :*

$$\forall N \in \mathbb{N}^*, \quad \forall x \in \mathbb{Q}/\mathbb{Z}, \quad \phi(x) = \sum_{i=0}^{N-1} \phi\left(\frac{x+i}{N}\right).$$

Nous utiliserons la relation de compatibilité vérifiée par une distribution ordinaire ϕ plutôt sous la forme suivante, qui se déduit de la précédente par simple changement de variable :

$$\forall N \in \mathbb{N}^*, \quad \forall x \in \mathbb{Q}/\mathbb{Z}, \quad \phi(Nx) = \sum_{i=0}^{N-1} \phi\left(x + \frac{i}{N}\right).$$

Définition 7.3.13. *Une* distribution ordinaire ϕ de poids $d \in \mathbb{N}$ *est une fonction sur* $\mathbb{Q}/\mathbb{Z}$ *satisfaisant la relation*

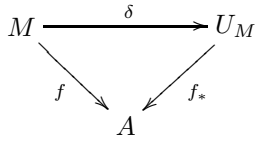
$$\forall N \in \mathbb{N}^*, \quad \forall x \in \mathbb{Q}/\mathbb{Z}, \quad \phi(Nx) = N^d \sum_{i=0}^{N-1} \phi\left(x + \frac{i}{N}\right).$$

La distribution est de plus trouée *si ces relations de compatibilité ne sont pas satisfaites lorsque* $Nx = 0$ *pour* $x \in \mathbb{Q}/\mathbb{Z}$ *et* $N \in \mathbb{N}^*$*.*

Remarque 7.3.14. *Si une distribution prend ses valeurs dans un groupe abélien où la multiplication par 2 est inversible, on peut former sa partie paire et sa partie impaire.*

L'ensemble des distributions ordinaires de poids $d \in \mathbb{N}$ forme une catégorie, un morphisme entre deux distributions $g : \mathbb{Q}/\mathbb{Z} \to A$ et $h : \mathbb{Q}/\mathbb{Z} \to B$ étant la donnée d'un morphisme de groupes $\alpha : A \to B$ tel que $h = \alpha \circ g$.

Il n'est pas difficile de voir que cette catégorie admet un objet initial, que nous appellerons *distribution universelle ordinaire de poids* $d \in \mathbb{N}$ *sur* $M = \mathbb{Q}/\mathbb{Z}$, et qui est la donnée d'un groupe abélien U_M et d'une distribution ordinaire $\delta : M \to U_M$ telle que pour toute autre distribution $f : M \to A$ de poids d à valeurs dans un groupe abélien A, il existe un unique homomorphisme de groupes $f_* : U_M \to A$ tel que le diagramme suivant commute :



La construction de U_M se fait comme celle du produit tensoriel de deux modules : il suffit de définir U_M comme quotient du groupe abélien libre de base M (qui est unique à isomorphisme près) par le sous-groupe engendré par toutes les relations de compatibilité, i.e. l'ensemble des sommes formelles

$$\left(\frac{N}{M}\right)^d \sum_{(\frac{N}{M})y=x} (y) - (x),$$

où N et M sont des entiers naturels non nuls tels que $M|N$, et où $x \in \left(\frac{1}{M}\mathbb{Z}\right)/\mathbb{Z}$.

On définit de manière analogue la *distribution universelle ordinaire paire* (resp. *impaire*) sur M à valeurs dans les groupes abéliens où la multiplication par 2 est inversible.

Cas de la distribution $\widetilde{\Gamma}$

Nous nous intéressons plus particulièrement au cas de la distribution induite par la fonction Γ. Introduisons dans cette perspective la fonction

$$\begin{aligned} \widetilde{\Gamma} : (\mathbb{Q}/\mathbb{Z})^* &\to \mathbb{C}^*/\overline{\mathbb{Q}}^* \\ z &\mapsto \frac{1}{\sqrt{2\pi}}\Gamma(z) \end{aligned}$$

Cette fonction est bien définie en vertu de la formule de translation vérifiée par la fonction Γ, que nous rappelons :

$$\forall x \in \mathbb{C}\backslash(-\mathbb{N}), \quad \Gamma(x+1) = x\Gamma(x).$$

Au besoin, nous étendrons la définition de $\widetilde{\Gamma}$ à $\mathbb{Q}/\mathbb{Z}$ tout entier en posant $\widetilde{\Gamma}(0) = 1$.

Voici à présent l'outil de base qui va nous permettre de faire le lien entre la théorie des distributions sur un système projectif et les conjectures de Rohrlich et de Rohrlich-Lang :

Proposition 7.3.15. $\widetilde{\Gamma}$ *définit une distribution (multiplicative) impaire de poids nul.*

Démonstration. La relation de distribution satisfaite par $\widetilde{\Gamma}$, à savoir

$$\forall z \in (\mathbb{Q}/\mathbb{Z})^*, \quad \forall N \in \mathbb{N}^*, \quad \prod_{i=0}^{N-1} \widetilde{\Gamma}\left(z + \frac{j}{N}\right) = \widetilde{\Gamma}(Nz),$$

découle directement de la formule de multiplication vérifiée par la fonction Γ :

$$\forall x \in \mathbb{C}\backslash(-\mathbb{N}^*), \quad \forall N \in \mathbb{N}^*, \quad \prod_{i=0}^{N-1} \frac{1}{\sqrt{2\pi}}\Gamma\left(x + \frac{j}{N}\right) = \frac{1}{\sqrt{2\pi}}\Gamma(Nx)N^{\frac{1}{2}-Nx}.$$

L'imparité de $\widetilde{\Gamma}$ (i.e. $\widetilde{\Gamma}(x)\widetilde{\Gamma}(-x) \in \overline{\mathbb{Q}}^*$) découle de la formule des compléments, qui, couplée à la formule de translation, peut s'écrire sous la forme :

$$\forall x \in \mathbb{C}\backslash\mathbb{Z}, \quad \Gamma(x)\Gamma(-x) = -\frac{\pi}{x\sin(\pi x)},$$

en remarquant que $\sin(\pi x)$ est algébrique si x est rationnel. □

Nous concluons ce paragraphe par l'énoncé et la démonstration d'un théorème qui nous sera très utile en vu de la démonstration conjecturale du résultat qui nous intéresse.

Notation. *On notera dans toute la suite* $Z_N = \left(\frac{1}{N}\mathbb{Z}\right)/\mathbb{Z}$ *pour* $N \geq 1$. *Par ailleurs,* $\varphi(N) = \left|(\mathbb{Z}/N\mathbb{Z})^*\right|$ *désignera l'indicatrice d'Euler.*

Pour une distribution ordinaire ϕ à valeurs dans un groupe abélien A dont on considère sa restriction à Z_N, son rang sera défini comme le rang du groupe abélien engendré par $\phi(Z_N)$. Si A_N désigne ce groupe, le rang est aussi la dimension du $\mathbb{Q}$-espace vectoriel $A_N \otimes \mathbb{Q}$.

Théorème 7.3.16 (Critère de Kubert)**.** *Soit* $\phi : \mathbb{Q}/\mathbb{Z} \to A$ *une distribution ordinaire (de poids nul) et* $r_N(\phi)$ *le rang du sous-groupe* A_N *pour tout* $N \geq 1$. *Alors :*

1. $r_N(\phi) \leq \varphi(N)$ *pour tout* $N \geq 2$ *(resp.* $r_N(\phi) \leq \frac{\varphi(N)}{2}$ *si* ϕ *est une distribution impaire et* $N > 2$*).*
2. ϕ *est une distribution universelle (resp.une distribution universelle impaire) si, et seulement si,* $r_N(\phi) = \varphi(N)$ *pour tout* $N > 1$ *(resp.* $r_N(\phi) = \frac{\varphi(N)}{2}$ *pour tout* $N > 2$*).*

Démonstration.

1. Traitons d'abord le cas où ϕ est une distribution quelconque. Soit $N > 1$ décomposé en facteurs premiers : $N = \prod_{i\geq 1} p_i^{n_i}$. Alors $Z_N \simeq \bigoplus_{i\geq 1} Z_{p_i^{n_i}}$ et tout élément $\frac{a}{N} \in Z_N$ se décompose sous la forme

$$\frac{a}{N} = \sum_{i\geq 1} \frac{a_i}{p_i^{n_i}} \bmod \mathbb{Z},$$

où a_i est bien défini modulo $p_i^{n_i}$ tandis que a est bien défini modulo N. Soit

$$V_N = \left\{ \frac{a}{N} \in Z_N / \quad \forall i \geq 1, \quad [((a_i, p_i) = 1) \wedge (a_i \neq 1)] \vee [a_i = 0] \right\},$$

qui est clairement un ensemble de cardinal $\varphi(n)$. On va montrer que l'image de V_N par ϕ engendre A_N, ce qui fournira la conclusion recherchée.

Montrons tout d'abord par récurrence sur le nombre de facteurs premiers de N que $\phi(\widetilde{V}_N)$ engendre A_N, où

$$\widetilde{V}_N = \left\{ \frac{a}{N} \in Z_N / \quad \forall i \geq 1, \quad [(a_i, p_i) = 1] \vee [a_i = 0] \right\}.$$

Si N est une puissance d'un nombre premier, le résultat découle simplement de la relation de distribution.

Supposons N composé et soit $\sum_{i\geq 1} \frac{b_i}{p_i^{n_i}} \in Z_N$. On écrit $b_1 = p_1^r a_1$, où $a_1 = 0$ ou a_1 est premier à p_1. Si $a_1 = 0$, l'hypothèse de récurrence appliquée à $\frac{N}{p_1^{n_1}}$ permet de conclure en remarquant que $V_{\frac{N}{p_1^{n_1}}} \subset V_N$. On suppose donc a_1 premier avec p_1, avec $1 \leq r < n_1$. On a alors :

$$\phi\left(\sum_{i\geq 1} \frac{b_i}{p_i^{n_i}}\right) = \phi\left(\frac{p_1^r a_1}{p_1^{n_1}} + \sum_{i\geq 2} \frac{b_i}{p_i^{n_i}}\right) = \phi\left[p_1^r\left(\frac{a_1}{p_1^{n_1}} + \sum_{i\geq 2} \frac{c_i}{p_i^{n_i}}\right)\right] \text{ avec } c_i \equiv p_1^{-r} b_i \bmod p_i^{n_i}$$

$$= \sum_{j \bmod p_1^r} \phi\left(\frac{a_1}{p_1^{n_1}} + \frac{j}{p_1^r} + \sum_{i\geq 2} \frac{c_i}{p_i^{n_i}}\right),$$

la dernière égalité résultant de la relation de distribution. Comme $r < n_1$, on peut écrire

$$\frac{a_1}{p_1^{n_1}} + \frac{j}{p_1^r} = \frac{a_1'}{p_1^{n_1}} \text{ avec } (a_1', p_1) = 1, a_1' \neq 1.$$

Par récurrence, on procède de même avec p_2, p_3, ...

Il suffit alors de remarquer ce qui suit : lors de la première étape de ce raisonnement, lors de la factorisation par p_1^r et de l'échange de b_i en c_i, si b_i est premier à a_i, alors c_i aussi. En itérant le même procédé sur les autres nombres premiers, on conserve ainsi la propriété recherchée pour les nombres déjà traités. Ceci conclut la récurrence.

Dans un second temps, on montre – encore par récurrence sur le nombre de facteurs premiers de N – que l'on peut «récupérer» les éléments $\phi\left(\frac{a}{N}\right)$ pour lesquels certains a_i sont éventuellement égaux à 1 à partir des éléments de $\phi(V_N)$.

Si N est la puissance d'un nombre premier, cela découle encore de la relation de distribution. Dans le cas contraire, décomposons une nouvelle fois N est facteurs premiers – $N = \prod_{i\geq 1} p_i^{n_i}$ – et considérons $\frac{a}{N} = \sum_{i\geq 1} \frac{a_i}{p_i^{n_i}}$. Notons $i_1, \ldots, i_m$ les indices tels que $a_{i_j} = 1$. Soit $N_1 = \frac{N}{p_{i_1}^{n_{i_1}}}$ et $y_1 = \sum_{i\neq i_1} \frac{a_i}{p_i^{n_i}} \in Z_{N_1}$. D'après la relation de distribution,

$$\sum_{j \bmod p_{i_1}^{n_{i_1}}} \phi\left(\frac{j}{p_{i_1}^{n_{i_1}}} + y_1\right) = \phi(p_{i_1}^{n_{i_1}} y_1),$$

$$\sum_{k \bmod p_{i_1}^{n_{i_1}-1}} \phi\left(\frac{k}{p_{i_1}^{n_{i_1}-1}} + y_1\right) = \phi(p_{i_1}^{n_{i_1}-1} y_1),$$

d'où, par soustraction,

$$\sum_{\substack{j \bmod p_{i_1}^{n_{i_1}} \\ (j, p_{i_1})=1}} \phi\left(\frac{j}{p_{i_1}^{n_{i_1}}} + y_1\right) \equiv 0 \bmod A_{N_1},$$

où A_{N_1} est le groupe engendré par $\phi(Z_{N_1})$. Par conséquent,

$$-\phi\left(\frac{1}{p_{i_1}^{n_{i_1}}} + y_1\right) \equiv \sum_{\substack{a_1 \neq 1 \\ (a_1, p_{i_1})=1}} \phi\left(\frac{a_1}{p_{i_1}^{n_{i_1}}} + y_1\right) \bmod A_{N_1}.$$

Autrement dit, $\phi\left(\frac{1}{p_{i_1}^{n_{i_1}}} + y_1\right)$ est la somme d'un élément de A_N redevable de l'hypothèse de récurrence et d'une somme d'éléments de A_N où aucun des facteurs associés à $p_{i_1}^{n_{i_1}}$ dans la décomposition fractionnaire de l'argument de ϕ n'est égal à 1.

On procède de même pour l'indice i_2 : $\phi\left(\frac{a}{N}\right)$ s'écrit alors comme somme d'un élément de A_{N_1} et d'un nombre fini d'éléments de A_{N_2}, tous redevables de l'hypothèse de récurrence, et d'une somme d'éléments de A_N où aucun des facteurs associés à $p_{i_1}^{n_{i_1}}$ et à $p_{i_2}^{n_{i_2}}$ dans la décomposition fractionnaire de l'argument de ϕ n'est égal à 1.

En itérant le procédé jusqu'à l'indice i_m, on obtient le résultat voulu.

Dans le cas d'une distribution impaire, on procède de même avec le groupe $V_N/\{\pm 1\}$ (de cardinal $\frac{\varphi(N)}{2}$ dès que $N > 2$) en lieu et place de V_N.

2. Là encore, on se contentera de traiter le cas où ϕ est une distribution quelconque. Si l'on réussit à exhiber une distribution de poids nul dont le rang est $\varphi(N)$ pour tout $N > 1$, alors l'homomorphisme canonique défini par la distribution universelle est un isomorphisme en considération du fait que l'image de V_N engendre l'image de toute distribution d'après le premier point. Si cette démarche est possible en faisant intervenir la distribution dite de Stickelberger (cf. p.53 de [14]), nous adopterons un point de vue différent qui passe par un lemme, intéressant en soi, d'où découle directement le résultat recherché :

Lemme 7.3.17. *Soit $g : Z_N \to A$ une distribution de poids nul. On suppose que la distribution obtenue en composant g à gauche par le morphisme naturel $A \to \mathbb{Q}$ est de rang $\varphi(N)$ (i.e. l'espace vectoriel engendré par l'image de Z_N est de dimension $\varphi(N)$).*

Alors g est une distribution universelle.

Démonstration. Le rang de l'image est au plus $\varphi(N)$ d'après le premier point. Si l'espace vectoriel engendré par l'image a un tel rang, alors le système générateur $g(V_N)$ précédemment exhibé, libre car de cardinal égal au rang, reste libre par tensorisation, donc est linéairement indépendant sur $\mathbb{Z}$ dans le groupe engendré par $g(Z_N)$.

L'homomorphisme canonique entre la distribution universelle et g est donc un isomorphisme, d'où la conclusion. □

Le théorème 7.3.16 est ainsi démontré. □

Dans le cas d'une distribution universelle impaire, la borne $\frac{\varphi(N)}{2}$ apparaissant dans le théorème précédent ne doit pas laisser penser que les générateurs du groupe image engendré par $g(Z_N)$ ($N > 2$) sont donnés par les $\frac{\varphi(N)}{2}$ quantités $\phi\left(\frac{s}{N}\right)$, $s \in [\![1, \lfloor \frac{N}{2} \rfloor]\!]$. Un contre-exemple peut par exemple être trouvé avec $N = 24$. Pour voir cela, notons $\underset{\substack{N=n\\x=y}}{=}$ une égalité qui résulte directement de la relation de distribution appliquée en $N = n$ et $x = y$ (avec les notations de la définition 7.3.12).

Des égalités

$$\phi\left(\frac{-7}{24}\right) + \phi\left(\frac{1}{24}\right) \underset{\substack{N=3\\x=-7/24}}{=} -\phi\left(\frac{7}{8}\right) - \phi\left(\frac{3}{8}\right),$$
$$\phi\left(\frac{-5}{24}\right) + \phi\left(\frac{11}{24}\right) \underset{\substack{N=3\\x=-5/24}}{=} -\phi\left(\frac{5}{8}\right) - \phi\left(\frac{1}{8}\right),$$

on déduit successivement

$$\begin{aligned}\phi\left(\frac{-7}{24}\right) + \phi\left(\frac{1}{24}\right) + \phi\left(\frac{11}{24}\right) + \phi\left(\frac{-5}{24}\right) &= -\phi\left(\frac{-1}{8}\right) - \phi\left(\frac{3}{8}\right) - \phi\left(\frac{5}{8}\right) - \phi\left(\frac{7}{8}\right)\\ &\underset{\substack{N=8\\x=0}}{=} \phi\left(\frac{1}{4}\right) + \phi\left(\frac{1}{2}\right) + \phi\left(\frac{3}{4}\right)\\ &\underset{\substack{N=2\\x=0}}{=} 0,\end{aligned}$$

la dernière et l'avant-dernière égalités utilisant le fait que, ϕ étant une distribution impaire à valeurs dans un groupe où la multiplication par 2 est inversible, $\phi(0) = 0$.

Dans le cas de la distribution impaire $\widetilde{\Gamma}$, cette relation reflète l'identité plus précise suivante, qui s'établit par ailleurs de la même manière :

$$\frac{\Gamma\left(\frac{1}{24}\right) \times \Gamma\left(\frac{11}{24}\right)}{\Gamma\left(\frac{5}{24}\right) \times \Gamma\left(\frac{7}{24}\right)} = \sqrt{3}\sqrt{2+\sqrt{3}}.$$

7.3.3 Une démonstration conjecturale du résultat

La théorie jusque là mise en place va à présent nous servir à proposer une preuve conjecturale du résultat 7.3.1.

Dans cette perspective, notons tout d'abord que $\mathbb{C}^*/\overline{\mathbb{Q}}^*$ et $\mathbb{C}^*/\pi^{\mathbb{Q}}.\overline{\mathbb{Q}}^*$ sont des groupes uniquement divisibles et peuvent, en conséquence, être vus comme des $\mathbb{Q}$-espace vectoriels, point de vue que nous adoptons dorénavant. Il convient néanmoins de garder à l'esprit que la loi de groupe sur l'espace vectoriel est alors multiplicative.

Une reformulation de la conjecture de Rohrlich proposée par S.Lang dans [14] est la suivante :

($R\Gamma_1$) *$\widetilde{\Gamma}$ induit une distribution universelle impaire à valeurs dans $\mathbb{C}^*/\overline{\mathbb{Q}}^*$.*

La correspondance entre les deux formulations, si elle pose problème, apparaîtra plus clairement lors de la démonstration du lemme 7.3.18 à venir.

Nous allons de fait adopter une version de l'assertion précédente *a priori* légèrement renforcée :

($R\Gamma_2$) *$\widetilde{\Gamma}$ induit une distribution universelle impaire à valeurs dans $\mathbb{C}^*/\pi^{\mathbb{Q}}.\overline{\mathbb{Q}}^*$.*

pour laquelle nous démontrerons l'équivalence avec plusieurs variantes :

($R\Gamma_3$) *Pour tout $N > 2$, le $\mathbb{Q}$-sous-espace vectoriel de l'espace vectoriel $\mathbb{C}^*/\pi^{\mathbb{Q}}.\overline{\mathbb{Q}}^*$ engendré par les valeurs $\Gamma\left(\frac{r}{N}\right)$, $r \in [\![1, N-1]\!]$, est de dimension $\frac{\varphi(N)}{2}$.*

($R\Gamma_4$) *Les seules relations monomiales modulo $\pi^{\mathbb{Q}}.\overline{\mathbb{Q}}^*$ entre les valeurs $\Gamma(a)$, $a \in \mathbb{Q}\backslash(-\mathbb{N}^*)$, proviennent des équations fonctionnelles de Γ.*

($R\Gamma_5$) *Les seules relations monomiales modulo $\overline{\mathbb{Q}}^*$ entre les valeurs $\Gamma(a)$, $a \in \mathbb{Q}\backslash(-\mathbb{N}^*)$, proviennent des équations fonctionnelles de Γ.*

L'assertion ($R\Gamma_5$) correspond à l'énoncé de la conjecture 7.3.3 de Rohrlich que nous avions adopté.

Dans la même veine, nous proposons une reformulation – en fait une paraphrase – de la conjecture 7.3.9 de Lang :

($L\Gamma$) *Les seules relations polynomiales modulo $\overline{\mathbb{Q}}^*$ entre les valeurs $\Gamma(a)$, $a \in \mathbb{Q}\backslash(-\mathbb{N}^*)$, proviennent des équations fonctionnelles de Γ.*

Par «provenir de», nous entendons que les relations monomiales (resp. polynomiales) considérées s'écrivent en des puissances *rationnelles* des relations standard. Ce point de vue est justifié par le fait qu'une relation algébrique entre valeurs de la fonction Γ, même monomiale, ne s'écrit pas toujours comme un polynôme en les relations standard comme le prouve l'exemple suivant, dont la vérification est par ailleurs immédiate :

$$\begin{aligned}\frac{\Gamma\left(\frac{4}{15}\right)\Gamma\left(\frac{1}{5}\right)}{\Gamma\left(\frac{1}{3}\right)\Gamma\left(\frac{2}{15}\right)} &= \sqrt{\frac{\Gamma\left(\frac{1}{5}\right)}{\Gamma\left(\frac{1}{15}\right)\Gamma\left(\frac{2}{5}\right)\Gamma\left(\frac{11}{15}\right)} \times \frac{\Gamma\left(\frac{2}{5}\right)}{\Gamma\left(\frac{2}{15}\right)\Gamma\left(\frac{4}{5}\right)\Gamma\left(\frac{7}{15}\right)} \times \frac{\Gamma\left(\frac{1}{15}\right)\Gamma\left(\frac{4}{15}\right)\Gamma\left(\frac{7}{15}\right)\Gamma\left(\frac{2}{3}\right)\Gamma\left(\frac{13}{15}\right)}{\Gamma\left(\frac{1}{3}\right)}} \\ &\qquad \times \sqrt{\frac{\Gamma\left(\frac{4}{15}\right)\Gamma\left(\frac{11}{15}\right)}{\Gamma\left(\frac{1}{3}\right)\Gamma\left(\frac{2}{3}\right)} \times \frac{\Gamma\left(\frac{1}{5}\right)\Gamma\left(\frac{4}{5}\right)}{\Gamma\left(\frac{2}{15}\right)\Gamma\left(\frac{13}{15}\right)}} \\ &= 3^{-\frac{1}{5}} 5^{\frac{1}{12}} \sqrt{\frac{\sin\left(\frac{\pi}{3}\right)\sin\left(\frac{2\pi}{15}\right)}{\sin\left(\frac{4\pi}{15}\right)\sin\left(\frac{\pi}{5}\right)}}.\end{aligned}$$

Les relations entre les différents énoncés sont données par le lemme suivant :

Lemme 7.3.18.

$$(L\Gamma) \Longrightarrow (R\Gamma_5) \Longleftrightarrow (R\Gamma_4) \Longleftrightarrow (R\Gamma_3) \Longleftrightarrow (R\Gamma_2) \Longleftrightarrow (R\Gamma_1)$$

Démonstration. Les implications $(L\Gamma) \Longrightarrow (R\Gamma_5)$, $(R\Gamma_4) \Longrightarrow (R\Gamma_5)$ et $(R\Gamma_2) \Longrightarrow (R\Gamma_1)$ sont claires. L'implication $(R\Gamma_5) \Longrightarrow (R\Gamma_4)$ est tout aussi évidente dès lors que l'on remarque, en utilisant la formule des compléments, que $\Gamma\left(\frac{1}{2}\right)^2 = \pi$. Enfin, l'équivalence $(R\Gamma_2) \Longleftrightarrow (R\Gamma_3)$ est un cas particulier du critère de Kubert (théorème 7.3.16).

Pour établir l'équivalence $(R\Gamma_2) \Longleftrightarrow (R\Gamma_4)$, nous explicitons tout d'abord un dictionnaire entre les propriétés de la fonction Γ et celles de la distribution $\widetilde{\Gamma}$ qui lui est associée.

Propriétés de Γ	Propriétés de $\widetilde{\Gamma}$
Relation de réflexivité	Imparité
Relation de translation	Définition sur un ensemble quotienté par $\mathbb{Z}$
Relation de multiplication	Relation de distribution

TABLE 1 – Dictionnaire entre les propriété de la fonction Γ et celles de la distribution $\widetilde{\Gamma}$

Supposons $(R\Gamma_2)$ et prouvons $(R\Gamma_4)$: une relation monomiale telle que dans $(R\Gamma_4)$ se factorise pour définir une relation monomiale pour $\widetilde{\Gamma}$ égale à la classe de l'unité dans le quotient $\mathbb{C}^*/\pi^{\mathbb{Q}}.\overline{\mathbb{Q}}^*$. Or, $\widetilde{\Gamma}$ étant supposé être une distribution universelle impaire, le groupe engendré par l'image de $\widetilde{\Gamma}$ dans $\mathbb{C}^*/\pi^{\mathbb{Q}}.\overline{\mathbb{Q}}^*$ s'identifie au quotient du groupe abélien libre de base $(\mathbb{Q}/\mathbb{Z})^*$ par les relations de compatibilité et la relation d'imparité. La relation monomiale trouvée pour $\widetilde{\Gamma}$ appartient donc au sous-groupe engendré par les relations de compatibilité et la relation d'imparité ce qui, à l'aide du dictionnaire ci-dessus, permet de conclure.

Supposons à présent $(R\Gamma_4)$ et démontrons $(R\Gamma_2)$: il suffit de prouver le caractère universel de la distribution, que l'on sait par ailleurs être impaire. Soit donc A un groupe abélien dont la loi est notée multiplicativement et $f : (\mathbb{Q}/\mathbb{Z})^* \to A$ une distribution impaire. On va montrer que f s'écrit de manière unique sous la forme $g \circ \widetilde{\Gamma}$, où g est un morphisme de groupes de source le groupe engendré par l'image de $\widetilde{\Gamma}$ dans $\mathbb{C}^*/\pi^{\mathbb{Q}}.\overline{\mathbb{Q}}^*$ et de but A. Remarquons d'emblée qu'un tel homomorphisme est univoquement défini par la donnée de ses valeurs sur l'image de $\widetilde{\Gamma}$.

On définit de fait g sur l'image de $\widetilde{\Gamma}$ en posant

$$\forall x \in (\mathbb{Q}/\mathbb{Z})^*, \quad g\left(\widetilde{\Gamma}(x)\right) = f(x)$$

et on l'étend au groupe engendré par $\mathrm{Im}(\widetilde{\Gamma})$ en posant, pour tous $x_1, \ldots, x_n \in (\mathbb{Q}/\mathbb{Z})^*$ et tout monôme M en n variables (à puissances entières),

$$g\left[M\left(\widetilde{\Gamma}(x_1), \ldots, \widetilde{\Gamma}(x_n)\right)\right] = M\left[f(x_1), \ldots, f(x_n)\right].$$

Il s'agit alors de vérifier que cette définition a un sens pour pouvoir conclure : soit donc $x_1, \ldots, x_n \in (\mathbb{Q}/\mathbb{Z})^*$, $y_1, \ldots, y_n \in (\mathbb{Q}/\mathbb{Z})^*$ et M et N deux monômes en respectivement m et n variables tels que

$$M\left[\widetilde{\Gamma}(x_1), \ldots, \widetilde{\Gamma}(x_n)\right] = N\left[\widetilde{\Gamma}(y_1), \ldots, \widetilde{\Gamma}(y_n)\right] \text{ modulo } \pi^{\mathbb{Q}}.\overline{\mathbb{Q}}^*. \tag{1}$$

D'après le dictionnaire rappelé dans la *figure 1*, l'hypothèse $(R\Gamma_4)$ se traduit par le fait que les seules relations monomiales entre les valeurs prises par $\widetilde{\Gamma}$ égales à la classe de l'unité dans le groupe engendré par $\mathrm{Im}(\widetilde{\Gamma})$ proviennent de la relation d'imparité et des relations de distribution.

L'égalité (1) impose donc entre les arguments $x_1, \ldots, x_n, y_1, \ldots, y_m$ des contraintes de signe liées à l'imparité de $\widetilde{\Gamma}$ et des contraintes de «projection» liées aux relations de compatibilité.

Comme f est supposée être une distribution impaire, elle vérifie également les relations d'imparité et de compatibilité, de sorte que l'on a

$$M\left[f(x_1),\ldots,f(x_n)\right]=N\left[f(y_1),\ldots,f(y_m)\right].$$

Ceci finit la preuve de l'implication.

Enfin, l'implication $(R\Gamma_1)\Longrightarrow(R\Gamma_5)$ résulte d'un raisonnement analogue à celui tenu dans la preuve de l'implication $(R\Gamma_2)\Longrightarrow(R\Gamma_4)$. □

On déduit de ce lemme le théorème suivant :

Théorème 7.3.19. *Soit $N>2$. En supposant vraie $(L\Gamma)$,*

$$\mathrm{Tr}\,\deg_{\mathbb{Q}}\left[\mathbb{Q}\left(\pi,\Gamma\left(\frac{r}{N}\right),1\leq r\leq N-1\right)\right]=1+\frac{\varphi(N)}{2}\cdot$$

Démonstration. Comme $(L\Gamma)$ implique $(R\Gamma_3)$, il existe toujours une relation monomiale non triviale donnant un nombre algébrique entre π et $1+\frac{\varphi(N)}{2}$ éléments dans l'ensemble $\{\pi\}\cup\left\{\Gamma\left(\frac{r}{N}\right)\right\}_{1\leq r\leq N-1}$. Par conséquent, le degré de transcendance de l'extension considérée est au plus $1+\frac{\varphi(N)}{2}$.

Considérons une base $\left\{\Gamma\left(\frac{e_1}{N}\right),\ldots,\Gamma\left(\frac{e_{\varphi(N)/2}}{N}\right)\right\}$ du $\mathbb{Q}$-sous-espace vectoriel de l'espace vectoriel $\mathbb{C}^*/\pi^{\mathbb{Q}}.\overline{\mathbb{Q}}^*$ engendré par les valeurs $\Gamma\left(\frac{r}{N}\right)$, $r\in[\![1,N-1]\!]$ et montrons que $\left\{\pi,a_1=\Gamma\left(\frac{e_1}{N}\right),\ldots,a_{\frac{\varphi(N)}{2}}=\Gamma\left(\frac{e_{\varphi(N)/2}}{N}\right)\right\}$ est un ensemble de nombres algébriquement indépendants.

On raisonne par l'absurde et on suppose l'existence de $P\in\overline{\mathbb{Q}}\left[Z,X_1,\ldots,X_{\frac{\varphi(N)}{2}}\right]$ non nul annulateur de $\left(\pi=\Gamma\left(\frac{1}{2}\right)^2,a_1,\ldots,a_{\frac{\varphi(N)}{2}}\right)$. D'après $(L\Gamma)$, chaque monôme de P évalué en $\left(\pi,a_1,\ldots,a_{\frac{\varphi(N)}{2}}\right)$ peut s'écrire comme un monôme à puissances rationnelles en les équations fonctionnelles de la fonction Γ liant des points $\Gamma(a)$, $a\in\mathbb{Q}\backslash(-\mathbb{N}^*)$. Or chacune des équations fonctionnelles de la fonction Γ évaluée en des points rationnels fournit une relation à valeur dans $\pi^{\mathbb{Q}}.\overline{\mathbb{Q}}^*$. Chacun des monômes de P évalué en $\left(\pi,a_1,\ldots,a_{\frac{\varphi(N)}{2}}\right)$ se projette donc en l'origine du $\mathbb{Q}$-espace vectoriel $\left(\pi,a_1,\ldots,a_{\frac{\varphi(N)}{2}}\right)$. Comme $\left(a_1,\ldots,a_{\frac{\varphi(N)}{2}}\right)$ forme une base de cet espace vectoriel, les exposants des composantes de ce vecteur dans chacun des monômes de P évalué en $\left(\pi,a_1,\ldots,a_{\frac{\varphi(N)}{2}}\right)$ sont nuls. Autrement dit,

$$P\left(\pi,a_1,\ldots,a_{\frac{\varphi(N)}{2}}\right)=P(\pi,1,\ldots,1)=\widetilde{P}(\pi).$$

P fournit ainsi un polynôme non nul à coefficients algébriques en une variable annulateur de π, ce qui contredit la transcendance de ce nombre et achève la preuve. □

La principale difficulté lorsque l'on cherche à établir, à l'aide de la conjecture de Rohrlich-Lang, l'indépendance algébrique de π avec certaines valeurs de la fonction Γ évaluée en des points rationnels consiste donc à exhiber une base du $\mathbb{Q}$-sous-espace vectoriel de l'espace vectoriel $\mathbb{C}^*/\pi^{\mathbb{Q}}.\overline{\mathbb{Q}}^*$ engendré par les valeurs $\Gamma\left(\frac{r}{N}\right)$, $r\in[\![1,N-1]\!]$ $(N>2)$. A cet égard, l'algorithme LLL (pour Lenstra-Lenstra-Lovász), qui peut être utilisé pour déterminer des relations de dépendance linéaire à coefficients entiers entre des constantes numériques [17], peut être des plus utiles. On en trouvera une description théorique détaillée au chapitre 2 de [3] : l'idée à retenir est que l'algorithme LLL, étant donné des constantes numériques, permet de minimiser les valeurs des combinaisons linéaires à coefficients entiers entre ces constantes.

17. Cette dernière utilisation de l'algorithme LLL est précisément implémentée dans la commande *PSLQ* du *package IntegerRelations* de Maple.

Illustrons notre propos en expliquant la raison pour laquelle le théorème de Chowla-Selberg ne permet pas d'obtenir l'indépendance algébrique des éléments de l'ensemble $\left\{\pi, e^{\pi\sqrt{5}}, \Gamma\left(\frac{1}{5}\right)\right\}$ alors qu'il fournit celle des éléments des ensembles $\left\{\pi, e^{\pi\sqrt{5}}, \Gamma\left(\frac{1}{20}\right)\times\Gamma\left(\frac{3}{20}\right)\times\Gamma\left(\frac{7}{20}\right)\times\Gamma\left(\frac{9}{20}\right)\right\}$, $\left\{\pi, e^{\pi\sqrt{5}}, \Gamma\left(\frac{1}{5}\right)\times\Gamma\left(\frac{7}{20}\right)\times\Gamma\left(\frac{9}{20}\right)\right\}$ et $\left\{\pi, e^{\pi\sqrt{5}}, \frac{\Gamma\left(\frac{1}{20}\right)\times\Gamma\left(\frac{3}{20}\right)}{\Gamma\left(\frac{1}{5}\right)}\right\}$.

On cherche pour cela des relations de dépendance multiplicatives entre $\Gamma\left(\frac{1}{20}\right)$, $\Gamma\left(\frac{3}{20}\right)$, $\Gamma\left(\frac{7}{20}\right)$ et $\Gamma\left(\frac{9}{20}\right)$ modulo $\pi^{\mathbb{Q}}.\overline{\mathbb{Q}}^*$: comme l'algorithme LLL ne traite que des relations de dépendance linéaire, on recense l'ensemble des logarithmes des constantes numériques susceptibles de fournir une telle relation. A l'aide de la formule des compléments et de la formule de multiplication pour la fonction Γ, on voit que l'on est amené à rechercher une relation de dépendance $\mathbb{Q}$-linéaire entre les nombres

$$\log\Gamma\left(\frac{1}{20}\right), \log\Gamma\left(\frac{3}{20}\right), \log\Gamma\left(\frac{7}{20}\right), \log\Gamma\left(\frac{9}{20}\right),$$
$$\log\sin\left(\frac{\pi}{20}\right), \log\sin\left(\frac{3\pi}{20}\right), \log\sin\left(\frac{9\pi}{20}\right),$$
$$\log\pi, \log 2, \log 3.$$

L'algorithme LLL fournit une valeur minimale d'une combinaison $\mathbb{Z}$-linéaire de ces constantes pour la relation suivante :

$$-17\log\Gamma\left(\frac{1}{20}\right) + 17\log\Gamma\left(\frac{3}{20}\right) + 16\log\Gamma\left(\frac{9}{20}\right) - 2\log\sin\left(\frac{\pi}{20}\right) + \log\sin\left(\frac{3\pi}{20}\right)$$
$$- 17\log\sin\left(\frac{9\pi}{20}\right) + 16\log\pi - 17\log 2 - \log 3 \approx -2,2.10^{-7}$$

On vérifie qu'il ne s'agit pas là d'une approximation numérique de 0 en calculant le produit déduit de cette relation à 50 décimales près :

$$\frac{\Gamma\left(\frac{3}{20}\right)^{17}\Gamma\left(\frac{9}{20}\right)^{16}\sin\left(\frac{3\pi}{20}\right)\pi^{16}}{3.2^{17}\Gamma\left(\frac{1}{20}\right)^{17}\sin\left(\frac{9\pi}{20}\right)^{17}\sin\left(\frac{\pi}{20}\right)^{2}} \approx 0,99999978241873670618660753498401834895355347879470$$

L'algorithme LLL tend donc à exhiber le quadruplet (en fait la classe du quadruplet) $\left(\Gamma\left(\frac{1}{20}\right), \Gamma\left(\frac{3}{20}\right), \Gamma\left(\frac{7}{20}\right), \Gamma\left(\frac{9}{20}\right)\right)$ comme une base du $\mathbb{Q}$-espace vectoriel engendré par $\left\{\Gamma\left(\frac{r}{20}\right)\right\}_{1\leq r\leq 19}$ dans $\mathbb{C}^*/\pi^{\mathbb{Q}}.\overline{\mathbb{Q}}^*$. Supposons ce résultat effectivement vrai.

Un (petit) calcul mené à l'aide des formules de multiplication et de complément montre que l'on a

$$\Gamma\left(\frac{1}{5}\right) = \sqrt{\frac{\pi}{2^{19/5}}\cdot\frac{1}{\sin\left(\frac{3\pi}{5}\right)\sin\left(\frac{9\pi}{20}\right)\sin\left(\frac{7\pi}{20}\right)\sin\left(\frac{\pi}{10}\right)}\cdot\frac{\Gamma\left(\frac{1}{20}\right)\times\Gamma\left(\frac{3}{20}\right)}{\Gamma\left(\frac{9}{20}\right)\times\Gamma\left(\frac{7}{20}\right)}}$$
$$= \sqrt{\frac{\pi}{2^{9/5}}\cdot\frac{(5+\sqrt{5})\left(2\sqrt{5}-\sqrt{2(5+\sqrt{5})}\right)}{5}\cdot\frac{\Gamma\left(\frac{1}{20}\right)\times\Gamma\left(\frac{3}{20}\right)}{\Gamma\left(\frac{9}{20}\right)\times\Gamma\left(\frac{7}{20}\right)}}.$$

Autrement dit, $\Gamma\left(\frac{1}{5}\right) = \left(\frac{\Gamma\left(\frac{1}{20}\right)\times\Gamma\left(\frac{3}{20}\right)}{\Gamma\left(\frac{9}{20}\right)\times\Gamma\left(\frac{7}{20}\right)}\right)^{\frac{1}{2}}$ modulo $\pi^{\mathbb{Q}}.\overline{\mathbb{Q}}^*$. Or sous l'hypothèse que la famille $\left(\Gamma\left(\frac{1}{20}\right), \Gamma\left(\frac{3}{20}\right), \Gamma\left(\frac{7}{20}\right), \Gamma\left(\frac{9}{20}\right)\right)$ est libre modulo $\pi^{\mathbb{Q}}.\overline{\mathbb{Q}}^*$, il n'est pas possible d'exprimer le quotient $\frac{\Gamma\left(\frac{1}{20}\right)\times\Gamma\left(\frac{3}{20}\right)}{\Gamma\left(\frac{9}{20}\right)\times\Gamma\left(\frac{7}{20}\right)}$ comme une puissance rationnelle du produit $\Gamma\left(\frac{1}{20}\right)\times\Gamma\left(\frac{3}{20}\right)\times\Gamma\left(\frac{7}{20}\right)\times\Gamma\left(\frac{9}{20}\right)$ dans $\mathbb{C}^*/\pi^{\mathbb{Q}}.\overline{\mathbb{Q}}^*$. Ceci explique la nécessaire présence du facteur $\Gamma\left(\frac{7}{20}\right)\times\Gamma\left(\frac{9}{20}\right)$ (resp. $\Gamma\left(\frac{1}{20}\right)\times\Gamma\left(\frac{3}{20}\right)$) attaché à $\Gamma\left(\frac{1}{5}\right)$ (resp. $\Gamma\left(\frac{1}{5}\right)^{-1}$) lorsque l'on introduit $\Gamma\left(\frac{1}{5}\right)$ dans le produit $\Gamma\left(\frac{1}{20}\right)\times\Gamma\left(\frac{3}{20}\right)\times\Gamma\left(\frac{7}{20}\right)\times\Gamma\left(\frac{9}{20}\right)$.

Ainsi dispose-t-on d'une justification conjecturale de l'impossibilité de déduire du théorème de Chowla-Selberg l'indépendance algébrique des éléments de l'ensemble $\left\{\pi, e^{\pi\sqrt{5}}, \Gamma\left(\frac{1}{5}\right)\right\}$.

Revenons à présent à la conjecture 7.3.1 que l'on cherche à prouver : si l'on admet $(L\Gamma)$, alors

$$\text{Tr deg}_{\mathbb{Q}}\mathbb{Q}\left[\pi, \Gamma\left(\frac{1}{5}\right), \Gamma\left(\frac{2}{5}\right), \Gamma\left(\frac{3}{5}\right), \Gamma\left(\frac{4}{5}\right)\right] = 1 + \frac{\varphi(5)}{2} = 3.$$

On vérifie aisément, en utilisant la formule des compléments, qu'une base de transcendance de l'extension considérée est donnée par la famille $\left(\pi, \Gamma\left(\frac{1}{5}\right), \Gamma\left(\frac{2}{5}\right)\right)$. On obtient dès lors le théorème suivant, qui fournit le résultat recherché :

Théorème 7.3.20. *Si la conjecture de Rohrlich-Lang est vraie, alors les trois nombres*

$$\pi, \quad \Gamma\left(\frac{1}{5}\right) \quad \textit{et} \quad \Gamma\left(\frac{2}{5}\right)$$

sont algébriquement indépendants.

Bibliographie

[1] E. Artin. *The Gamma Function.* New York : Holt, Rinehart and Winston, 1964.

[2] K. Barré-Siriex, G. Diaz, F. Gramain, and G. Philibert. Une preuve de la conjecture de Mahler - Manin. *Inevnt. Math.*, pages 1–9, 1996.

[3] P. Borwein. *Computational Excursions in Analysis and Number Theory.* Springer Verlag, 2002.

[4] P. Bundschuh. Zwei Bemerkungen über transzendente Zahlen. *Mh. Math.*, 88 :293–304, 1979.

[5] S. Chowla and A. Selberg. On Epstein's zeta function. *J. reine angew. Math.*, 227 :86–110, 1967.

[6] P. Clark. *Lecture Notes on Valuation Theory*, chapter 1. University of Georgia, http ://www.math.uga.edu/ pete/MATH8410.html, 2010.

[7] Alain Connes (ed.), Frédéric Fauvet (ed.), and Jean-Pierre Ramis (ed.). *Renormalization and Galois theories. Selected papers of the CIRM workshop, Luminy, France, March 2006.*, chapter Galois theory, motives and transcendendal numbers (Y. André). IRMA Lectures in Mathematics and Theoretical Physics 15. Zürich : European Mathematical Society. viii, 270 p., 2009.

[8] D. Cox. *Primes of the Form $x^2 + ny^2$.* John Wiley & Sons, 1989.

[9] F. Gramain. Transcendance et fonctions modulaires. *Journal de théorie des nombres de Bordeaux*, tome 11(n°1) :73–90, 1000.

[10] R. Hartshorne. *Algebraic Geometry.* Springer-Verlag, 1977.

[11] S. Lang. *Elliptic functions.* Springer-Verlag, 1973.

[12] S. Lang. *Introduction to modular forms.* Springer-Verlag, 1976.

[13] S. Lang. Relations de distribution et exemples classiques. In *Séminaire DELANGE-PISOT-POITOU*, number 40, page 6p., 1977/1978.

[14] S. Lang. *Cyclotomic Fields I.* Springer Verlag, August 1978.

[15] K. Mahler. On algebraic differential equations satisfied by automorphic functions. *J. Austral. Math. Soc.*, 10 :445–450, 1969.

[16] K. Mahler. On the coefficients of transformation polynomials for the modular function. *Bull. Austral. Math. Soc.*, 10 :197–218, 1971.

[17] H. Matsumura. *Commutative Algebra.* W.A. Benjamin Co., New York, 1970.

[18] Y. V. Nesterenko and P. Philippon. *Introduction to Algebraic Independence Theory.* Springer-Verlag, lecture notes in mathematics edition, 2001.

[19] Y.V. Nesterenko. Modular fuctions and transcendence problems. *Math. Sb.*, 1996.

[20] G. Philibert. Une mesure d'indépendance algébrique. *Annales de l'institut Fourier*, 38(3) :85–103, 1988.

[21] P. Philippon. Critères pour l'indépendance algébrique. *Publications mathématiques de l'I.H.E.S.*, 64 :5–52, 1986.

[22] P. Philippon. Sur les mesures d'indépendance algébrique. In Birkäuser, editor, *Séminaire de théorie des nombres*, volume 59, pages 219–233. Paris, Progress in Math., 1986.

[23] S. Ramanujan. On certain arithmetical functions. *Trans. Camb. Phil. Soc.*, 22 :159–184, 1916.

[24] M. Reid. *Undergraduate Commutative Algebra*. London Math. Soc., 1995.

[25] T. Schneider. Arithmetischen Untersuchungen elliptischer Integrale. *Math. Ann.*, 113 :1–13, 1937.

[26] J.P. Serre. *Cours d'arithmétique*. PUF, 1970.

[27] M. Waldschmidt. Fonctions modulaires et transcendance. Conférence à l'université Bordeaux I, Novembre 1996.

[28] M. Waldschmidt. Sur la nature arithmétique de valeurs de fonctions modulaires. In *Séminaire BOURBAKI*, number 824, 1996-1997.

[29] M. Waldschmidt. *Diophantine approximation on linear algebraic groups. Transcendence Properties of the Exponential Function in Several Variables.* Springer, 2000.

Annexe 1 : Quelques propriétés de la fonction Gamma

Nous exposons ici quelques résutats classiques ayant trait à la fonction Γ en renvoyant par exemple à [1] pour les démonstrations.

Pour tout nombre complexe z tel que Re(z)>0, on définit la fonction Γ par

$$\Gamma \ : z \mapsto \int_0^{+\infty} t^{z-1}\, e^{-t}\, \mathrm{d}t.$$

Cette intégrale converge absolument sur le demi-plan complexe où la partie réelle est strictement positive. La fonction Γ ainsi définie peut être prolongée analytiquement en une fonction méromorphe sur l'ensemble des nombres complexes, excepté en $z = 0, -1, -2, -3, \ldots$ qui sont des pôles, et on désigne encore par Γ ce prolongement. Le résidu en $-n$ pour $n \in \mathbb{N}$ vaut $\frac{(-1)^n}{n}$.

Il existe des définitions alternatives pour la fonction Γ faisant intervenir des produits infinis. Citons à cet égard les expressions suivantes, respectivement dues à Euler et Weierstrass, qui ont un sens pour les nombres complexes z qui ne sont pas des entiers négatifs ou nuls :

$$\Gamma(z) = \lim_{n \to +\infty} \frac{n! n^z}{z(z+1)\ldots(z+n)}$$
$$\Gamma(z) = \frac{e^{-\gamma z}}{z} \prod_{n=1}^{+\infty} \left(1 + \frac{z}{n}\right)^{-1} e^{z/n},$$

où γ désigne la constante d'Euler-Mascheroni.

La fonction Γ vérifie trois relations dites standard :

1. **Relation de translation**

$$\forall z \in \mathbb{C}\backslash(-\mathbb{N}), \quad \Gamma(z+1) = z\Gamma(z).$$

2. **Formule des compléments**

$$\forall z \in \mathbb{C}\backslash(\mathbb{Z}), \quad \Gamma(z)\Gamma(1-z) = \frac{\pi}{\sin(\pi z)}.$$

3. **Formule de multiplication**

$$\forall z \in \mathbb{C}\backslash(-\mathbb{N}^*), \quad \forall m \in \mathbb{N}^*, \quad \prod_{k=0}^{m-1} \Gamma\left(z + \frac{k}{m}\right) = (2\pi)^{(m-1)/2} m^{1/2 - mz} \Gamma(mz).$$

La fonction Γ est enfin liée à la fonction bêta par la relation

$$B(x,y) = \frac{\Gamma(x)\Gamma(y)}{\Gamma(x+y)}$$

valable pour tous nombres complexes x et y de parties réelles strictement positives, où

$$B(x,y) = \int_0^1 t^{x-1}(1-t)^{y-1}\, \mathrm{d}t.$$

Annexe 2 : Un résultat sur les anneaux de Dedekind

Nous démontrons ici un résultat qui joue un rôle crucial dans la preuve du lemme 7.3.2.

Proposition 1. *Soit $\mathcal{R}$ un anneau de Dedekind et $\mathcal{I}$ un idéal de $\mathcal{R}$. Soit encore $\alpha \in \mathcal{I}$ non nul. Alors il existe $\beta \in \mathcal{I}$ tel que $\mathcal{I} = (\alpha, \beta)$, i.e. tel que $\mathcal{I}$ soit engendré par α et par β.*

En particulier, dans un anneau de Dedekind, il existe toujours deux élements qui engendrent un idéal donné. On peut de plus en fixer un arbitrairement à condition qu'il soit non nul. Dans le lemme 7.3.2, ce résultat est appliqué au cas où $\mathcal{R}$ est l'anneau des entiers d'un corps de nombres, qui est effectivement un anneau de Dedekind.

Démonstration. Il suffit en fait de montrer que, sous les hypothèses de la proposition, il existe β dans $\mathcal{R}$ tel que $\mathcal{I} = \text{pgcd}(\alpha, \beta)$: on aura alors en particulier $\beta \in \mathcal{I}$.

Décomposons $\mathcal{I}$ en produit d'idéaux maximaux : $\mathcal{I} = \prod_{i=1}^{n} P_i^{n_i}$. Comme $\mathcal{I}|(\alpha)$, (α) admet une décomposition en produit d'idéaux maximaux sous la forme

$$(\alpha) = \prod_{i=1}^{r} P_i^{l_i} \prod_{j=1}^{s} Q_j,$$

où $l_i \geq n_i$ pour tout $i \in [\![1, r]\!]$ et où $\text{pgcd}\left(P_i^{l_i}, Q_j\right) = (1) = \mathcal{R}$ pour tout $i \in [\![1, r]\!]$ et tout $j \in [\![1, s]\!]$.

Il s'agit donc de trouver β tel que, pour tout $j \in [\![1, s]\!]$, $Q_j \nmid (\beta)$ et, pour tout $i \in [\![1, r]\!]$, $\nu_{P_i}((\beta)) = n_i$ ($\nu_{P_i}(.)$ désignant la valuation P_i-adique d'un idéal). Autrement dit, il s'agit de trouver β tel que

$$\beta \in \left[\bigcap_{i=1}^{r} \left(P_i^{n_i} \backslash P_i^{n_i+1}\right)\right] \bigcap \left[\bigcap_{j=1}^{s} \left(\mathcal{R} \backslash Q_j\right)\right].$$

Or par unicité de la factorisation en idéaux maximaux, il existe pour tout $i \in [\![1, r]\!]$ un élément $\beta_i \in P_i^{n_i} \backslash P_i^{n_i+1}$. Comme, par ailleurs, $\text{pgcd}\left(P_i^{n_i+1}, Q_j\right) = (1)$ pour tout $i \in [\![1, r]\!]$ et tout $j \in [\![1, s]\!]$, le théorème chinois assure l'existence de $\beta \in \mathcal{R}$ tel que

$$\begin{aligned} &\forall i \in [\![1, r]\!], \quad \beta \equiv \beta_i \bmod P_i^{n_i+1} \\ &\forall j \in [\![1, s]\!], \quad \beta \equiv 1 \bmod Q_j \end{aligned}$$

□