Formes modulaires et indépendance algébrique

Céline Chevalier — Thomas Vidick
sujet proposé par Stéphane Fischler

18 juin 2003

Table des matières

L'objectif de cet exposé est de présenter une démonstration de l'indépendance algébrique des trois nombres π, e^π et $\Gamma(1/4)$, qui découle d'un théorème plus général que Yu. V. Nesterenko a démontré en 1996. Cette preuve fait suite à une série de résultats de transcendance basés sur l'étude des courbes elliptiques, dont un des premiers fut le théorème suivant démontré par Schneider en 1937, où j désigne l'invariant modulaire : soit τ un nombre complexe de partie imaginaire > 0. Si τ et $j(\tau)$ sont simultanément algébriques, alors τ est quadratique.

Pour cela, nous allons commencer par rappeler quelques résultats de la théorie des fonctions modulaires et des courbes elliptiques dans les deux premières parties, puis nous donnerons comme application un premier résultat de transcendance (démontré par une équipe stéphanoise en 1995) dans la troisième partie : si $\alpha \in \mathbb{C}$ est un nombre algébrique vérifiant $0 < |\alpha| < 1$, alors $J(\alpha)$ est transcendant (où $J(e^{2i\pi\tau}) = j(\tau)$). Puis nous introduirons la théorie de l'élimination et son application à l'étude des variétés, ce qui nous fournira des outils fondamentaux pour la preuve. Finalement, dans la dernière partie, nous déduirons quelques corollaires du théorème de Nesterenko, dont l'indépendance algébrique de π, e^π et $\Gamma(1/4)$, et nous en donnerons également une preuve directe.

1 Fonctions modulaires

1.1 Définitions

Notation. *On note* $\mathfrak{H} = \{x + iy \mid y > 0\}$ *l'ensemble des nombres complexes de partie imaginaire strictement positive. C'est* le demi-plan de Poincaré.

Définition 1.1. *On appelle* groupe modulaire *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 $\mathfrak{H}$:

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

Le demi-plan $\mathfrak{H}$ est stable par l'action de G, et de plus cette action est fidèle.

Définition 1.2. *Soit* k *un entier. On appelle* fonction faiblement modulaire de poids 2k *toute fonction méromorphe* f *sur le demi-plan* $\mathfrak{H}$ *qui vérifie la relation*

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

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

On a en particulier pour tout $z \in \mathfrak{H}$, $f(z+1) = f(z)$. On peut donc exprimer f comme une fonction de $q = e^{2i\pi z}$, fonction que l'on notera $\tilde{f}$; elle est méromorphe dans le disque $\{z \in \mathbb{C} \mid |z| < 1\}$ privé de l'origine. Si $\tilde{f}$ se prolonge en une fonction méromorphe (resp. holomorphe) à l'origine, nous dirons que f est méromorphe (resp. holomorphe) à l'infini.

Définition 1.3. *Une fonction faiblement modulaire est dite* modulaire *si elle est méromorphe à l'infini ; on pose alors* $f(\infty) = \tilde{f}(0)$.

Définition 1.4. *On appelle* forme modulaire *toute fonction modulaire qui est holomorphe partout (y compris à l'infini) ; si une telle fonction s'annule à l'infini, on dit que c'est* une forme parabolique.

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

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

1.2 Réseaux

Définition 1.5. *Soit V un $\mathbb{R}$-espace vectoriel de dimension finie n.* 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. $\Omega = \mathbb{Z}e_1 \oplus \ldots \oplus \mathbb{Z}e_n$).*

Soit R l'ensemble des réseaux de $\mathbb{C}$, considéré comme $\mathbb{R}$-espace vectoriel. Soit M l'ensemble des couples (ω_1, ω_2) d'éléments de $\mathbb{C}^*$ tels que $\omega_1/\omega_2 \in \mathfrak{H}$; à 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 ainsi une application surjective $M \to R$.

Proposition 1.6. *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 $(\omega_1, \omega_2) \in$M. Posons :

$$\omega_1' = a\omega_1 + b\omega_2 \qquad \text{et} \qquad \omega_2' = c\omega_1 + d\omega_2.$$

La famille (ω_1', ω_2') est clairement une base de $\Omega(\omega_1, \omega_2)$. De plus, si on pose $z = \omega_1/\omega_2$ et $z' = \omega_1'/\omega_2'$ on a

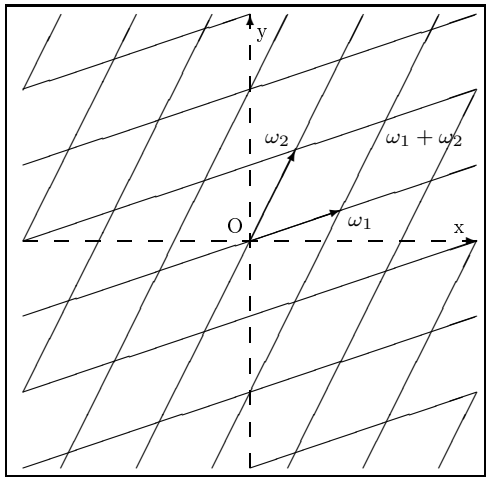
$$z' = \frac{az+b}{cz+d} = g(z)$$

On en conclut que $z' \in \mathfrak{H}$, donc que (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 de M qui définissent 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 le cas, donc $\det(g) = 1$, et la condition est nécessaire. □

Dans toute la suite, on considèrera un réseau $\Omega = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ de $\mathbb{C}$. On supposera de plus que $\tau = \omega_1/\omega_2$ est dans $\mathfrak{H}$.

Définition 1.7. *On appelle* parallélogramme fondamental *du réseau $\mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ un parallélogramme $(a, a+\omega_1, a+\omega_1+\omega_2, a+\omega_2)$, 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 note* $\sum_{\omega\in\Omega}{}' = \sum_{\omega\in\Omega\setminus\{0\}}$

Lemme 1.8. *Si $s > 2$ est un nombre réel, 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 et la norme infinie sont équivalentes, il existe une constante C telle que

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

qui converge dès que $s > 2$. □

Définition 1.9. *Si Ω est un réseau de $\mathbb{C}$, on définit, pour tout entier $k \geq 2$,*

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

G_{2k} est appelée la série d'Eisenstein d'indice $2k$ *du réseau* Ω.[1]

Cette série converge absolument par le lemme 1.8. On peut également considérer G_{2k} comme une fonction sur $\mathfrak{H}$ en posant, si $\Omega = \mathbb{Z} \oplus \mathbb{Z}\tau$ avec $\tau \in \mathfrak{H}$,

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

Lemme 1.10. *Cette fonction est holomorphe en τ sur $\mathfrak{H}$. De plus, $G_{2k}(\tau)$ et ω_2 déterminent $G_{2k}(\Omega)$.*

Démonstration. On a

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

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

Proposition 1.11. *Soit k un entier ≥ 2. La série d'Eisenstein G_{2k} est une forme modulaire de poids $2k$.*

[1] Certains auteurs l'appelent la 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 $\mathrm{Im}\,(\frac{a\tau+b}{c\tau+d}) = \frac{\mathrm{Im}\,(\tau)}{|c\tau+d|^2} > 0$, donc, d'après la Proposition 1.6,

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

Il reste à montrer que G_{2k} est holomorphe à l'infini. Ce sera fait dans la proposition 1.13. □

Définition 1.12. *On pose, pour $k \geq 1$ et $\tau \in \mathfrak{H}$, $E_{2k} = 1 + \frac{4k(-1)^k}{B_{2k}} \sum_{n=1}^{+\infty} n^{2k-1} \frac{q^n}{1-q^n}$, en notant B_i le ième nombre de Bernoulli.*

Proposition 1.13. *Soit $k \geq 2$ et $\tau \in \mathfrak{H}$. On a $G_{2k}(\tau) = 2\zeta(2k)E_{2k}(\tau)$, en notant ζ la fonction de Riemann.*

Démonstration. Etablissons un résultat préliminaire. On part de la formule

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

Par ailleurs, on a

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

En comparant, il vient

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

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

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

Maintenant, il suffit de développer G_{2k} et d'appliquer la formule que l'on vient de montrer.

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

En particulier, $G_{2k}(\infty) = 2\zeta(2k)$, ce qui termine la preuve de la proposition 1.11. □

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

Notation. *On note g_2 et g_3 respectivement $60\,G_4$ et $140\,G_6$. De plus, on utilise les notations de Ramanujan ; les fonctions P, Q et R sont les séries E_2, E_4 et E_6. D'après la définition 1.13, on a les formules*

$$P(z) = E_2(z) = 1 - 24\sum_{n=1}^{\infty} \frac{nz^n}{1-z^n}$$
$$Q(z) = E_4(z) = 1 + 240\sum_{n=1}^{\infty} \frac{n^3z^n}{1-z^n}$$
$$R(z) = E_6(z) = 1 - 504\sum_{n=1}^{\infty} \frac{n^5z^n}{1-z^n}$$

On a $g_2(\infty) = 120\zeta(4)$ et $g_3(\infty) = 280\zeta(6)$. En utilisant les valeurs connues de $\zeta(4)$ et $\zeta(6)$, on trouve :

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

Si on pose

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

on en déduit que $\Delta(\infty) = 0$; Δ est donc une forme parabolique de poids 12.

Pour terminer, nous déduisons des formules précédentes des développements de g_2 et g_3 qui nous seront utiles dans la section 6. Si Ω est le réseau $\omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$,

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

D'où, comme $\zeta(4) = \dfrac{\pi^4}{90}$

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

On obtient de la même manière que

$$\frac{1}{(2i\pi)^6} g_3(\Omega)\omega_1^6 = \frac{1}{6^3}\left(-1 + 504\sum_{n=1}^{\infty}\frac{n^5q^n}{1-q^n}\right)$$

1.4 L'invariant modulaire j

Définition 1.14. *On pose*

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

Proposition 1.15. *La fonction j est une fonction modulaire de poids 0. De plus, elle est holomorphe dans $\mathfrak{H}$ et elle 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 de poids 12. Pour la seconde, on sait que Δ ne s'annule pas sur $\mathfrak{H}$, et qu'elle a un zéro simple à l'infini, tandis que g_2 est non nulle à l'infini. □

Un réseau est complètement caractérisé par son image par j.

Théorème 1.16. *Soit Γ et Λ deux réseaux de $\mathbb{C}$. Alors $j(\Gamma) = j(\Lambda)$ si, et seulement si, Γ et Λ sont identiques.*

Démonstration. Ceci est démontré dans [3], Chapitre 3, paragraphe 3. □

2 Fonctions elliptiques

2.1 Généralités

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

Définition 2.1. *Une* fonction elliptique *f (relativement à Ω) est une fonction méromorphe sur $\mathbb{C}$ qui est Ω-périodique, i.e.*

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

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

Remarque. *Toute fonction elliptique et holomorphe est constante.*

Démonstration. Une fonction elliptique et holomorphe est bornée sur l'adhérence d'un parallélogramme fondamental, et donc sur $\mathbb{C}$ par Ω-périodicité. □

Théorème 2.2. *Soit f une fonction elliptique. 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 pôles ni zéros de f (ce qui est possible car ces derniers sont isolés), le nombre de zéros de f dans P est égal au nombre de pôles de f dans P (comptés avec multiplicité).*

Démonstration. On a

$$\begin{aligned}
\mathrm{Card}\{\rho \mid f(\rho) = 0\} - \mathrm{Card}\{\rho \mid f(\rho) = \infty\} &= \int_{\partial P} \frac{f'}{f}(z)\, \frac{\mathrm{d}z}{2\mathrm{i}\pi} \\
&= \int_a^{a+\omega_1} \frac{f'}{f}(z)\, \frac{\mathrm{d}z}{2\mathrm{i}\pi} + \int_{a+\omega_1}^{a+\omega_1+\omega_2} \frac{f'}{f}(z)\, \frac{\mathrm{d}z}{2\mathrm{i}\pi} \\
&\quad + \int_{a+\omega_1+\omega_2}^{a+\omega_2} \frac{f'}{f}(z)\, \frac{\mathrm{d}z}{2\mathrm{i}\pi} + \int_{a+\omega_2}^{a} \frac{f'}{f}(z)\, \frac{\mathrm{d}z}{2\mathrm{i}\pi} \\
&= \int_a^{a+\omega_1} \left(\frac{f'}{f}(z) - \frac{f'}{f}(z+\omega_2) \right) \frac{\mathrm{d}z}{2\mathrm{i}\pi} \\
&\quad + \int_{a+\omega_2}^{a} \left(\frac{f'}{f}(z) - \frac{f'}{f}(z+\omega_1) \right) \frac{\mathrm{d}z}{2\mathrm{i}\pi} \\
&= 0.
\end{aligned}$$

□

Définition 2.3. *Le nombre de pôles (ou de zéros) d'une fonction elliptique f de réseau Ω qui sont contenus dans un parallélogramme fondamental est appelé le degré de f.*

Lemme 2.4. *Soit f une fonction elliptique. On note E_f l'ensemble des pôles et des zéros de f. Alors $\sum_{a \in E_f} v_a(f)\, a \in \Omega$.*

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 a

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

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

Lemme 2.5. *Si f est elliptique de degré ≤ 1, alors f est constante.*

Démonstration. Si f n'est pas constante, elle a un unique zéro a dans $\mathbb{C}/\Omega$, qui est simple, et donc un unique pôle b. D'après le lemme 2.4, $a-b\in\Omega$, donc a et b sont à la fois pôles et zéros de f, ce qui est impossible. □

2.2 Fonction elliptique de Weierstrass

Théorème 2.6. *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 $\dfrac{1}{z^2} + O(z)$. On note cette fontion $\wp_\Omega$. Elle est paire.*

Démonstration. Unicité Si f et g sont deux fonctions elliptiques de degré ≤ 2 vérifiant au voisinage de zéro $f\sim g\sim \dfrac{1}{z^2}$, la fonction $f-g$ est constante. En effet, elle est elliptique, sans pôles 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 2.5. De plus, par hypothèse, le terme constant de son développement de Laurent en zéro est nul, ce qui entraîne la nullité de la constante.
Si f elliptique vérifie les conditions du théorème, la fonction $z\mapsto f(-z)$ aussi, donc, par unicité, f est paire.
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 1.8 donne alors la convergence uniforme sur tout compact.
Montrons que $\wp$ est elliptique. Soit $z\in\mathbb{C}$ et $\omega_0\in\Omega$. On a

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

On en déduit $\wp'(z+\omega_0) = \wp'(z)$ puis $\wp(z+\omega_0) - \wp(z) = a_0$ avec a_0 constante 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, d'où $a_0 = 0$. De plus, on a $(\wp(z) - \frac{1}{z^2})_{z=0} = 0$, donc le développement de $\wp$ en zéro a bien la forme souhaitée. Finalement, $\wp$ est de degré 2 car les pôles de $\wp$ sont dans Ω et zéro est un pôle d'ordre 2. □

Définition 2.7. *La fonction $\wp_\Omega$ (souvent notée $\wp$ s'il n'y a pas d'ambiguité) est appelée* la fonction de Weierstrass *du réseau Ω.*

Théorème 2.8. *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 :

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

Si f est impaire, alors $\dfrac{f}{\wp'}$ est paire, donc il suffit de prouver que, si f est paire, alors f est une fonction rationnelle de $\wp$. □

Lemme 2.9. *Soit f une fonction elliptique paire. Il existe $Q \in \mathbb{C}(X)$ tel que $f = Q(\wp)$.*

Démonstration. On considère les zéros et les pôles de f modulo Ω. Comme f est paire, ces ensembles sont invariants par $z \mapsto -z$ modulo Ω. On note $\omega_3 = \omega_1 + \omega_2$. On remarque que si f a un zéro ou un pôle en 0 ou en ω_i, il est d'ordre pair. En effet, f' est elliptique impaire, donc $f'(\frac{\omega_i}{2}) = 0$. En notant $a_1, \ldots, a_n, a_{-1}, \ldots, a_{-n}$ les zéros de f, et $b_1, \ldots, b_n, b_{-1}, \ldots, b_{-n}$ ses pôles, on pose

$$\boxed{Q(\wp) = \prod_{i=1}^{n} \frac{\wp - \wp(a_i)}{\wp - \wp(b_i)}}$$

C'est une fonction elliptique dont les pôles sont en les z tels que $\wp(z) = \wp(b_i)$, c'est-à-dire en les $\pm b_i$. Ainsi, $\dfrac{f}{Q(\wp)}$ est une fonction elliptique sans pôles, donc constante. □

Proposition 2.10. *On a $\wp(z) = \dfrac{1}{z^2} + \sum\limits_{n=1}^{+\infty} (2n+1) G_{2n+2}\, z^{2n}$, pour tout $z \in \mathbb{C}$.*

Démonstration. Rappelons que, pour tout $k \geq 2$, $G_{2k} = \sum\limits_{\omega \in \Omega}{}' \dfrac{1}{\omega^{2k}}$. Soit $z \in \mathbb{C}$ et $\omega \in \Omega$. On a

$$\begin{aligned} \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} &= \frac{1}{\omega^2}\left(\frac{1}{(1-z/\omega)^2} - 1\right) \\ &= \frac{1}{\omega^2}\left(\frac{2z}{\omega} + \frac{3z^2}{\omega^2} \ldots\right) \end{aligned}$$

Comme $\wp$ est paire, on a donc $\wp(z) = \dfrac{1}{z^2} + 3G_4 z^2 + 5G_6 z^4 + \ldots + (2n+1)G_{2n+2} z^{2n} + \ldots$ □

La fonction $\wp$ vérifie une équation différentielle du premier ordre. Si g_2 et g_3 sont les invariants du réseau Ω définis à la section 1.3, on a la proposition suivante.

Proposition 2.11. *On a $\wp'(z)^2 = 4\wp^3 - g_2\wp - g_3$, pour tout $z \in \mathbb{C}$.*

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

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

et donc

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

On en déduit que la fonction différence est elliptique et holomorphe (car $O\left(z^2\right)$ désigne une fonction dont le développement de Laurent commence avec des termes en z^2 ou plus), donc constante puis nulle (car $O\left(z^2\right)$ en 0). □

Proposition 2.12. *On note $\omega_3 = \omega_1 + \omega_2$, et $e_i = \wp(\frac{\omega_i}{2})$ pour $i = 1, 2, 3$. Alors*

$$\wp'^2(z) = 4(\wp(z) - e_1)(\wp(z) - e_2)(\wp(z) - e_3)$$

Démonstration. On pourra consulter [3] (p. 11). □

On en déduit alors que e_1, e_2, e_3 sont sont les racines de $4x^3 - g_2 x - g_3$. De plus, chacun des e_i est de multiplicité 2 pour $z \mapsto \wp(z) - \wp(\frac{\omega_i}{2})$, et $\wp$ n'a qu'un pôle d'ordre 2 modulo Ω, donc cette fonction n'a qu'un zéro d'ordre 2 et les e_i sont distincts. Par suite,

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

Donnons une réciproque partielle à ce résultat, démontrée dans [3] (corollaire 2 p. 39).

Théorème 2.13. *Soit c_2 et c_3 des nombres complexes tels que $c_2^3 - 27c_3^2 \neq 0$. Alors il existe un réseau Ω tel que $c_2 = g_2(\Omega)$ et $c_3 = g_3(\Omega)$.*

De plus, g_2 et g_3 caractérisent le réseau. Ceci est une conséquence du théorème 1.16 (voir [3], p. 39).

2.3 Fonction ζ de Weierstrass

Définition 2.14. *On définit* la fonction ζ de Weierstrass *par*

$$\frac{d\,\zeta(z)}{d\,z} = -\wp(z)$$

avec $\lim_{z \to 0} (\zeta(z) - z^{-1}) = 0$.

La périodicité de $\wp$ donne alors l'existence de η_1 et η_2 (*les quasi-périodes* de ζ) tels que

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

On a $\eta_1 = \frac{1}{2}\zeta(\frac{\omega_1}{2})$, et $\eta_2 = \frac{1}{2}\zeta(\frac{\omega_2}{2})$.

De la Proposition 2.10 on déduit le développement de ζ au voisinage de l'origine :

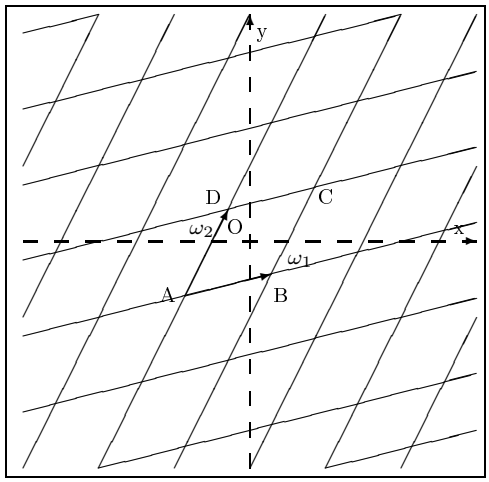
$$\zeta(z) = \frac{1}{z} - \sum_{n=1}^{\infty} G_{2n+2} z^{2n+1}.$$

Remarque. *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 de $\wp'$ dans l'équation différentielle vérifiée par $\wp$, et en identifiant.*

Théorème 2.15. *(Legendre). Si (ω_1,ω_2) est une base du réseau associé à la fonction de Weierstrass $\wp$, choisie telle que $\tau = \omega_2/\omega_1 \in \mathfrak{H}$, alors on a la relation de Legendre :*

$$\eta_1\omega_2 - \eta_2\omega_1 = \mathrm{i}\pi$$

Démonstration. On choisit un parallélogramme fondamental du réseau avec pour sommets A, B, C, D tel que l'origine soit située en son centre.



D'après le théorème des résidus de Cauchy, on a $\displaystyle\int_{ABCD} \zeta(z)dz = 2\mathrm{i}\pi$. D'autre part, par la remarque précédente,

$$\int_{CD} \zeta(z)dz = \int_{BA} \zeta(z+\omega_2)dz = \int_{BA} \zeta(z)dz + \int_{BA} 2\eta_2 dz = \int_{BA} \zeta(z)dz - 2\eta_2\omega_1$$

d'où

$$\int_{AB} \zeta(z)dz + \int_{CD} \zeta(z)dz = -2\eta_2\omega_1$$

et de même

$$\int_{BC} \zeta(z)dz + \int_{DA} \zeta(z)dz = 2\eta_1\omega_2$$

ce qui prouve la formule de Legendre. □

2.4 Multiplication complexe

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

Définition 2.16. *On dit que le réseau* Ω a multiplication complexe *s'il existe $\alpha \in \mathbb{C} \setminus \mathbb{Z}$ tel que $\alpha\Omega \subset \Omega$.*

On dira alors qu'une courbe elliptique *a multiplication complexe* si le réseau auquel elle est attachée a multiplication complexe.

Si Ω a multiplication complexe, il existe des entiers a, b, c, d tels que

$$\alpha\omega_1 = a\omega_1 + b\omega_2$$

$$\alpha\omega_2 = c\omega_1 + d\omega_2$$

Le complexe α est donc une racine de l'équation polynômiale $(x-a)(x-d)-bc=0$ et est ainsi quadratique sur $\mathbb{Q}$. En divisant la deuxième équation par ω_2, on obtient

$$\alpha = c\tau + d$$

Comme $\tau \in \mathfrak{H}$, τ n'est pas réel ; si on suppose que α n'est pas entier alors $c \neq 0$ et donc

$$\mathbb{Q}(\tau) = \mathbb{Q}(\alpha)$$

est une extension imaginaire quadratique de $\mathbb{Q}$.

3 Le théorème Stéphanois

Le théorème suivant répond à une question posée par Mahler. Il a été établi en 1995 par une équipe stéphanoise : Barré-Sirieix, Diaz, Gramain et Philibert dans [1].

Théorème 3.1. *Soit $\alpha \in \mathbb{C}$ un nombre algébrique vérifiant $0 < |\alpha| < 1$. Alors le nombre $J(\alpha)$ est transcendant.*

Démonstration. (Schéma de la preuve)

Dans la démonstration originale des Stéphanois, le point de départ est une estimation de la croissance des coefficients de Laurent des puissances de J. Cette estimation peut cependant être remplacée avantageusement par une estimation, plus simple à obtenir (voir [17], chapitre 1, paragraphe 4), des coefficients du développement de Taylor à l'origine de $\Delta^{2N}J^k$. On procède en 4 étapes :

Première étape Construction d'une fonction auxiliaire.

On construit un polynôme non nul $A \in \mathbb{Z}[X,Y]$ de degré $\leq N$ par rapport à chaque variable, tel que la fonction analytique

$$F(z) = \Delta(z)^{2N} A(z, J(z))$$

ait un zéro d'ordre au moins $L = N^2/2$ à l'origine, en utilisant un lemme de Thue et Siegel (lemme 6.10 dans la section 6.3) qui permet de borner les coefficients de A en fonction de N.

$$\text{On pose } A(z) = \sum_{i,j=0}^{\infty} a_{i,j} X^i Y^j, \text{ avec } \sum_{i,j=0}^{\infty} |a_{i,j}| \leq N^{25N}$$

Deuxième étape Majoration de $|F(z)|$.

On majore les coefficients du développement en série entière de F sur le disque unité. En adaptant la démonstration d'un théorème de Hecke donnée dans [16], 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

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

dont les coefficients sont majorés par : $|c_{N,k}(m)| \leq C^N m^{12N}$. En notant M l'ordre en 0 de F, ceci permet d'obtenir la majoration suivante :

$$|F(z)| \leq |z|^M \, M^{31N} \tag{1}$$

Troisième étape Construction d'un nombre algébrique non nul.

On sait d'après [3] (chapitre 5, paragraphe 2, théorème 3) que pour tout entier n ≥ 2, il existe un polynôme irréductible $\Phi_n \in \mathbb{Z}[X,Y]$ tel que pour tout z, $\Phi_n(J(z), J(z^n)) = 0$. Si on suppose la conclusion du théorème fausse, on en déduit alors que pour tout entier k, $J(\alpha^k)$ est algébrique. Comme F est non nulle, il existe un plus petit entier S tel que

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

En appliquant le principe du maximum à la fonction

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

on arrive à la majoration, où $\omega = 63(log(1/|q|))^{-1}$:

$$S^2 \;\leq\; \omega N log M \tag{2}$$

Quatrième étape Minoration de $\left|F(\alpha^S)\right|$.

On utilise un résultat de Mahler (voir [4]) sur la longueur de Φ_n : la somme des modules des coefficients de Φ_n est majorée par $n^{3/2}$. Une série de majorations assez fines utilisant le fait que α et $J(\alpha^S)$ sont algébriques permettent d'arriver à la minoration, où C est une constante qui peut dépendre de α :

$$\left|F(\alpha^S)\right| \;\geq\; e^{CS^{3/2}N(S+logM)} \tag{3}$$

Conclusion

En utilisant la majoration (2) de S donnée à la troisième étape, on vérifie que la minoration (3) n'est pas compatible avec la majoration (1) établie à la deuxième étape. L'hypothèse $J(\alpha)$ algébrique est donc contredite. □

4 Théorie de l'élimination

Dans cette section, nous allons présenter quelques résultats d'élimination homogène, en général sans les démontrer. 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 Philippon dans la partie 6.2.

Nous allons travailler dans l'anneau $K[X] = K[X_0, \ldots, X_n]$, où K est un corps de nombres. A tout idéal homogène I (c'est-à-dire engendré par des polynômes homogènes) de $K[X]$ on associe des idéaux éliminants $\mathfrak{E}_d(I)$ puis, lorsque ces idéaux sont principaux, des formes éliminantes, suivant une construction que l'on va détailler ci-dessous.

4.1 Décomposition primaire

On commence par donner quelques résultats d'algèbre commutative concernant la décomposition d'un idéal comme intersection d'idéaux primaires, qui seront utiles par la suite.

Définition 4.1. *Soit B un anneau commutatif et unitaire. Un idéal I de A est dit primaire si $I \neq A$ et si pour tous $a, b \in B$,*

$$ab \in I \;\;\Longrightarrow\;\; a \in I \text{ ou } \exists n \in \mathbb{N},\; b^n \in I$$

Définition 4.2. *Un idéal I est dit P-primaire si I est primaire et $P = \operatorname{rad} I = \bigcap_{\substack{Q \text{premier} \\ \text{contenant} I}} Q$.*

Remarque. *Si I est P-primaire, alors P est premier.*

On peut alors définir une *décomposition primaire* d'un idéal $I \subset B$ comme la donnée d'un entier n et de n idéaux primaires $Q_1, \ldots, Q_n$ tels que

$$I \;=\; Q_1 \cap \ldots \cap Q_n$$

Une telle décomposition est dite *minimale*, ou *normale*, si aucun Q_j n'est redondant, et si Q_i est P_i-primaire avec $P_i \neq P_j$ pour $i \neq j$. Dans un anneau noethérien, il y a toujours existence.

Théorème 4.3. *Si B est un anneau noethérien, tout idéal $I \subset B$ a une décomposition primaire normale.*

Démonstration. La preuve est élémentaire ; on pourra se reporter à [14] (chapitre 7, paragraphe 11). □

On termine par un résultat partiel d'unicité, qui sera essentiel à la démonstration du théorème de Bézout géométrique.

Théorème 4.4. *Soit B un anneau noethérien, $I \subset B$ un idéal, et $I = \bigcap_{i=1}^{k} Q_i$ une décomposition primaire normale de I, où Q_i est P_i-primaire. Alors l'ensemble $\{P_1, \ldots, P_k\}$ est déterminé de manière unique par I.*

Démonstration. On pourra par exemple consulter [14] (chapitre 7, paragraphe 11). □

4.2 Idéaux éliminants

Soit $n \in \mathbb{N}$ un entier fixé et $X_0, \ldots, X_n$ des indéterminées, dont on notera X la collection. Soit B un anneau noethérien. 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 :

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

Fixons un entier $h \geq 0$ et un h-uplet $d = (d_1, \ldots, d_h) \in \mathbb{N}^h$. On note $B[\mathbf{u}]$ (resp $A[\mathbf{u}]$) l'anneau des polynômes à coefficients dans B (resp A) en les indéterminées $u^{l,d_l} = \{u_{\mathfrak{m}}^{l,d_l} \mid \mathfrak{m} \in \mathfrak{M}_{d_l}\}$ où $1 \leq l \leq h$. On définit, pour $1 \leq l \leq h$,

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

Lorsque I est un idéal de A, on désigne par $I[\mathbf{u}]$ l'idéal de $A[\mathbf{u}]$ engendré par I et les éléments $U_{1,d_1}, \ldots, U_{h,d_h}$.

Définition 4.5. *Soit I un idéal de A. On définit l'idéal caractéristique d'indice d de I par*

$$\mathfrak{U}_d(I) = \{f \in A[\mathbf{u}] \mid \exists k \in \mathbb{N},\ f\mathfrak{M}_k \subset I[\mathbf{u}]\}$$

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

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

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 4.6. *Soit I un idéal homogène de A.*

1. *Si* $\mathfrak{M}_1 \subset \sqrt{I}$ *alors* $\mathfrak{U}_d(I) = A[\mathbf{u}]$ *et* $\mathfrak{E}_d(I) = B[\mathbf{u}]$,
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.*
   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 donc* $\mathfrak{E}_d(I) = \bigcap_{i=1}^{h} \mathfrak{E}_d(I_i)$.

Démonstration. On se reportera à [12] (proposition I.3.). □

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

Théorème 4.7. *Soit* $\rho : B[\mathbf{u}] \to K$ *un morphisme d'anneaux (fixant* B*) dans un corps* K. *On note encore* ρ *son prolongement à* $A[\mathbf{u}]$, *obtenu en posant* $\rho(X_i) = X_i$ *pour* $i = 0, \ldots, n$. *Alors, pour tout idéal homogène* I *de* A, *les conditions suivantes sont équivalentes :*

1. $\rho(\mathfrak{E}_d(I)) = 0$
2. *Il existe une extension de corps* L/K *et un zéro non trivial de* $\rho(I[\mathbf{u}])$ *dans* L^{n+1}, *c'est-à-dire qu'il existe* $z \in L^{n+1} \setminus \{0\}$ *tel que pour tout* $P \in I[\mathbf{u}]$, *on ait* $\rho(P)(z) = 0$
3. *Il existe une extension finie de corps* L/K *et un zéro non trivial de* $\rho(I[\mathbf{u}])$ *dans* L^n

Démonstration. On pourra se référer à [12] (proposition I.4.). □

4.3 Formes éliminantes

Définition 4.8. *On définit la hauteur (ou dimension de Krull) d'un anneau* B, *notée* $\mathrm{ht}(B)$, *par le supremum des longueurs des chaînes d'idéaux premiers dans* B, *où la longueur d'une chaîne* $P_r \subsetneq P_{r-1} \subsetneq \ldots \subsetneq P_0$ *est choisie comme valant* r. *Si* I *est un idéal premier de* B, *on définit la hauteur* $\mathrm{ht}(I)$ *comme étant le supremum des longueurs des chaînes d'idéaux premiers* $P_r \subsetneq P_{r-1} \subsetneq \ldots \subsetneq P_0 = I$.

Théorème 4.9. *Soit* K *un corps infini,* h *un entier,* I *un idéal premier homogène de* $K[X]$ *et* d *un élément de* $(\mathbb{N} \setminus \{0\})^h$. *On a alors*

1. $\mathfrak{E}_d(I) = (0) \iff \mathrm{ht}(I) < n - h + 1$
2. *Si* $\mathrm{ht}(I) = n - h + 1$ *alors* $\mathfrak{E}_d(I)$ *est principal.*

Démonstration. On se réfèrera à [7] (théorème 2.13, p.65). □

L'intérêt du 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 près, il est commode de privilégier arbitrairement un générateur. Pour cela on fixe un ensemble $\mathrm{Irr}(K[\mathbf{u}])$ de représentants des irréductibles de $K[\mathbf{u}]$ modulo les inversibles.

Définition 4.10. *Soit* I *un idéal homogène de* $K[X]$, $h \in \mathbb{N}$ *et* $d \in \mathbb{N}^h$. *On appelle* forme éliminante *d'indice* d *de* I *tout p.g.c.d. des éléments de l'idéal* $\mathfrak{E}_d(I)$. *On note en particulier* $\mathrm{élim}_d(I)$ *l'unique tel p.g.c.d. qui s'écrit comme produit d'éléments de* $\mathrm{Irr}(K[\mathbf{u}])$.

L'intérêt de cette définition est essentiellement résumé dans la conséquence suivante du théorème.

Corollaire 4.11. *Sous les hypothèses et notations du théorème, nous noterons* $f = \mathrm{élim}_d(I)$. *Alors*

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

5 Géométrie diophantienne

Soit K un corps algébriquement clos. On pose $A = K[X_0, \ldots, X_n]$.
Si I est un idéal homogène (i.e. engendré par des polynômes homogènes) de $K[X_0, \ldots, X_n]$, on note $\mathfrak{Z}(I)$ l'ensemble des zéros de I dans $\mathbb{P}_n(K)$. De manière duale, si X est un sous-ensemble de $\mathbb{P}_n(K)$ on note $I(X)$ l'idéal homogène formé des polynômes qui s'annulent en tout point de X. On rappelle le théorème suivant.

Théorème 5.1. *(Nullstellensatz). Pour tout idéal J de A, $I(\mathfrak{Z}(J)) = \sqrt{J}$.*

Définition 5.2. *Soit n un entier. On appelle variété projective de $\mathbb{P}_n(K)$ tout sous-ensemble X de $\mathbb{P}_n(K)$ tel qu'il existe un idéal premier homogène I de $K[X_0, \ldots, X_n]$ avec $X = \mathfrak{Z}(I)$.*

On appelle hypersurface toute variété V qui s'écrit $V = \mathfrak{Z}(I)$ avec I un idéal homogène principal. Si $I = (F)$, on notera également $X = \mathfrak{Z}(F)$.
On va définir la dimension d'une variété de manière analogue à la dimension de Krull d'un anneau A :

Définition 5.3. *Soit V une variété. On définit la dimension de V comme le plus grand entier n tel qu'il existe une chaîne $Z_0 \subset Z_1 \subset \ldots \subset Z_n$ de sous-ensembles fermés de V (pour la topologie de Zariski) irréductibles (i.e. qui ne s'écrivent pas comme union de deux sous-ensembles fermés propres) distincts.*

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

Proposition 5.4. *Pour tout idéal premier I de A, on a*

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

Démonstration. On trouvera une preuve dans [6], Chapitre 5, paragraphe 14. □

Dans toute la suite, on se fixe un entier h, un h-uplet d'entiers strictement positifs $d \in (\mathbb{N}^*)^h$ et une variété projective V de dimension $h-1$. L'idéal $I = I(V)$ est donc de hauteur $n-h+1$, et $\mathfrak{E}_d(p)$ est principal (Théorème 4.9).

Notation. *On garde celles des parties précédentes, et on pose en plus $\mathbf{u} = (u^{1,d_1}, \ldots, u^{h,d_h})$. On notera $f_{V,d}$ la forme éliminante d'indice d associée à la variété V : $f_{V,d} = \mathrm{élim}_d(I(V))$. Si $d = \mathbf{1} = (1, \ldots, 1)$, on dira que $f_{V,d}$ est une forme de Chow de V.*

Pour $i = 1, \ldots, h$ on note N_i le cardinal de $\mathfrak{M}_{d_i}$. On définit la variété caractéristique $C(V)$ de V par :

$$C(V) = \{(x, u) \in \mathbb{P}_n(K) \times \mathbb{P}_{N_1}(K) \times \ldots \times \mathbb{P}_{N_h}(K) \,|\, x \in V \text{ et } U_{1,d_1}(x) = \ldots = U_{h,d_h}(x) = 0\}$$

On a alors $I(C(V)) = I(V)\ A[\mathbf{u}] + U_{1,d_1}\ A[\mathbf{u}] + \ldots + U_{h,d_h}\ A[\mathbf{u}]$. En reprenant les notations de la partie précédente, cela nous donne $I(C(\mathfrak{Z}(J))) = J[\mathbf{u}]$, pour J idéal premier homogène de A.

Donnons deux exemples d'utilisation du théorème d'élimination (TE), avec $d = (1, \ldots, 1)$.
Si $V = \{x\}$, alors $h = 1$, et $U = U_{1,1} = u_0 X_0 + \ldots + u_n X_n$. $f_{V,1}$ est un polynôme de $K[\mathbf{u}] = K[u_0, \ldots, u_n]$. Comme K est algébriquement clos, $f_{V,1}$ a toutes ses racines dans K^{n+1}.
Appliquons maintenant (TE) : pour tout morphisme de K-algèbres $\rho : K[\mathbf{u}] \to K$, on a l'équivalence

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

Or, $I(C(V)) = I(V) \cdot K[X][\mathbf{u}] + U \cdot K[X][\mathbf{u}]$. Pour que tout $P \in \rho(I(C(V)))$ s'annule en y, il faut donc que $(\rho(U))(y) = 0$, et que tout $P \in \rho(I(V))$ s'annule en y. Comme $I(V) = (X - x)$, on a nécessairement $y = \rho(x) = x$.

On a donc montré que pour tout morphisme $\rho : K[\mathbf{u}] \to K$, on avait $\rho(f_{V,1}) = 0$ si et seulement si $(\rho(U))(\rho(x)) = \rho(U(x)) = 0$. En prenant pour ρ le morphisme qui envoie $\mathbf{u}$ sur une racine de $f_{V,1}$, on voit que $U(x)$ et $f_{V,1}$ ont exactement les mêmes racines, et sont donc proportionnels. Toute forme de Chow de V est donc proportionnelle à $U(x)$.

Si $V = \mathfrak{Z}(F)$ est une hypersurface, par le même raisonnement on montre que $\rho(\mathbf{u})$ est racine de $f_{V,1}$ si, et seulement si, il existe x dans V tel que $\rho(\mathbf{u})$ soit racine de tous les $U_{i,1}(x)$. Fixant ρ, on a n équations linéaires en n inconnues (les coordonnées homogènes de x). La solution du système est donnée par

$$x_i = \Delta_i = \det(u_\alpha^{j,1})_{\substack{j=1,\dots,n \\ 0 \le \alpha \le n, \alpha \neq i}}$$

Toute forme de Chow de V est donc proportionnelle à la forme multi-homogène

$$F(\Delta_0, \dots, \Delta_n).$$

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

5.1 Degré

On définit le degré de la variété V à partir de sa forme de Chow, en posant :

$$d(V) \;=\; d^\circ_{u^{i,d_i}} f_{V,(1,\dots,1)}$$

Comme $f_{V,1}$ est symétrique en chaque ensemble de variables $u^{i,1}$, cette définition ne présente pas d'ambiguité.

Remarque. *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 h hypersurfaces dont les positions sont* suffisamment générales. *Pour plus de détails, on se reportera à [7], chapitre 6.*

On veut maintenant caractériser le degré de V en fonction du degré d'une forme éliminante d'indice d quelconque de V.

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

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

L'idéal $\mathfrak{U}_{(d_1,\dots,d_{h-1})}(I)$ est un idéal premier de $A[(d_1, \dots, d_{h-1})]$ associé à une variété W. Par (TE) appliqué à l'extension L de K et à la projection canonique, $f_{V,d} = f_{W,d_h}$ 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 L^*.

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

$$\rho' : K[\mathbf{u}] \to K[\mathbf{u}']$$

qui envoie U_{h,d_h} sur $(U_{h,1})^{d_h}$.
Ce qui précède montre que $\rho(f_{V,d})$ est proportionnel à $(f_{V,d'})^{d_h}$, où $d' = (d_1, \dots, d_{h-1}, 1)$, le facteur de proportionnalité étant a priori dans L^*. Grâce au lemme suivant, qui découle de (TE), on déduit que le facteur de proportionnalité est en fait dans K^* :

Lemme 5.5. *Si P est un élément de $K[u^{1,d_1},\dots,u^{h-1,d_{h-1}}]$ qui divise $f_{V,d}$ alors $P \in K^*$.*

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

Le lemme montre de même qu'aucun élément de $K[u^{1,d_1},\dots,u^{h-1,d_{h-1}}]$ ne peut diviser $(f_{V,d'})^{d_h}$; donc le facteur de proportionnalité est dans K^*. En itérant, on montre que $\rho(f_{V,d})$ est proportionnel à $(f_{V,1})^{d_1\dots d_h}$, où ρ envoie tous les U_{i,d_i} sur $(U_{i,1})^{d_i}$. Comme ρ préserve l'homogénéité et est de degré d_i en u^{i,d_i}, et $f_{V,1}$ est symétrique en chaque ensemble de variables $u^{i,1}$, on a montré :

$$d^o_{u^{i,d_i}} f_{V,d} \;=\; d(V)\frac{d_1 \dots d_h}{d_i}.$$

5.2 Hauteur

On veut définir la hauteur $h(V)$ de toute variété V définie sur un corps de nombres. Dans la même logique que ce qui précède, on va poser $h(V) = h(f_{V,1})$ pour h une hauteur convenable sur $K[\mathbf{u}]$.

Commençons quelques rappels sur les valeurs absolues d'un corps de nombres. Pour de plus amples détails, on pourra se référer à [18].

Définition 5.6. *Soit K un corps. Une valeur absolue de K est une fonction non nulle $|.|$ définie sur K et à valeurs dans les réels positifs telle que, pour tous $(x,y) \in K^2$,*

1. $|x| = 0 \iff x = 0$
2. $|xy| = |x|\,|y|$
3. $|x+y| \leq |x| + |y|$

Une valeur absolue est dite *non-archimédienne* si la distance associée est ultramétrique, c'est-à-dire si on a, pour tous $(x,y) \in K^2$, l'inégalité

$$|x+y| \leq \max(|x|,|y|).$$

Deux valeurs absolues sont dites *équivalentes* si elles se déduisent l'une de l'autre par élévation à la puissance d'un nombre réel positif. Une valeur absolue est dite *archimédienne* si elle n'est équivalente à aucune valeur absolue non-archimédienne.

Définition 5.7. *On appelle* valuation discrète *d'un corps K toute fonction de K dans $\mathbb{Z} \cup \{-\infty\}$ telle que v soit surjective, et telle que, pour tous $x, y \in K$ on ait :*

$$v(xy) = v(x) + v(y) \qquad \text{et} \qquad v(x+y) \;\geq\; \min(v(x), v(y)).$$

Sur tout corps K muni d'une valuation discrète v, on construit une valeur absolue associée comme suit. On choisit $a \in]0,1[$; la valeur absolue de x est $|x|_v = a^{v(x)}$. Cette valeur absolue est ultramétrique.

Si p est un entier premier, on définit la valuation p-adique sur $\mathbb{Q}$ qui à tout x non nul associe l'entier $v_p(x)$ tel que $x = p^{v_p(x)}\ a/b$ avec a et b non divisibles par p. C'est une valuation discrète. La valeur absolue associée est notée $|.|_p$.

Théorème 5.8. *Toute valeur absolue ultramétrique de K, lorsqu'on la restreint à $\mathbb{Q}$, est équivalente à une valuation p-adique pour un certain nombre premier p.*

Démonstration. On pourra consulter [18], Chapitre 6, paragraphe 9. □

On dit alors que p est *le nombre premier sous* $|.|_v$.

Définition 5.9. *On appelle place de K toute classe d'équivalence de valeurs absolues sur K.*

Si v est une place de K, on note K_v le complété de K pour une valeur absolue $|.|_v$ associée à v.

Pour chaque place, on fixe une valeur absolue représentant v, dans le cas archimédien cela revient à fixer un plongement $\sigma_v : K \to \mathbb{C}$ tel que la valeur absolue normalisée soit simplement $|\sigma_v(.)|$, et dans le cas ultramétrique on impose $|p|_v = p^{-1}$ pour le nombre premier p sous v. Pour $x \in K^l$ on pose $| x |_v = \sqrt{|x_1|^2 + \ldots + |x_l|^2}$ si v est archimédienne et $| x |_v = Max(|x_1|_v, \ldots, |x_l|_v)$ si v est ultramétrique. Finalement, pour $f \in K[\mathbf{u}]$ on pose :

$$h(f) = \sum_v \frac{[K_v : \mathbb{Q}_v]}{[K : \mathbb{Q}]} \log(M_v(f))$$

où v parcourt toutes les places de K, $M_v(f)$ est le maximum des valeurs absolues v-adiques des coefficients de f si v est ultramétrique et, si $\sigma_v : K \to \mathbb{C}$ est le plongement associé à σ dans le cas archimédien :

$$\log(M_v(f)) = \int_{S_{N_1+1} \times \ldots \times S_{N_h+1}} \log |\sigma_v(f)| \ \eta_{N_1+1} \wedge \ldots \wedge \eta_{N_h+1} + \sum_{i=1}^{h} d^\circ_{i,d_i} f \ \sum_{j=1}^{N_i} \frac{1}{2j}$$

où S_{N+1} est la sphère unité de S^{N+1} et η_{N+1} la mesure de Haar sur la sphère S_{N+1} de masse totale 1 (rappel : pour $i = 1, \ldots, h$, N_i est le cardinal de $\mathfrak{M}_{d_i}$).

On a $h(\lambda f) = h(f)$ pour tout $\lambda \in K^*$ et $h(f) \geq 0$ pour tout f dans $K[\mathbf{u}]$ ([7], chapitre 6, paragraphe 4). Un calcul montre que pour tout $i = 1, \ldots, h$, $\log(M_v(U_{i,d_i}(x))) = d_i \ \log \|x\|_v$. On peut alors montrer, par les mêmes arguments que dans la section précédente, que

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

5.3 Les théorèmes de Bézout géométrique et arithmétique

On voudrait caractériser le degré et la hauteur d'une intersection $V \cap W$ de variétés. Pour simplifier, on va supposer dans la suite que $W = \mathfrak{Z}(F)$ est une hypersurface.

Définition 5.10. *On appelle cycle une combinaison linéaire formelle Z de variétés, à coefficients dans $\mathbb{N}$: $Z = \sum_{j=1}^{s} m_j \ V_j$. On dira qu'un cycle est équidimensionnel de dimension $h-1$ si toutes les variétés concernées sont de dimension $h-1$.*

En général, si ρ est un morphisme de $K[u^{h,d_h}]$ dans K, il n'est pas vrai que $\rho(f_{V,d})$ est une forme éliminante de $\rho(I[u^{h,d_h}])$. Cependant, le lemme suivant nous permet de caractériser $\rho(f_{V,d})$ comme une forme d'-éliminante associée à un cycle ($d' = (d_1, \ldots, d_{h-1})$) :

Lemme 5.11. *Soit $\rho : K[u^{h,d_h}] \to K$ un morphisme tel que $\rho(f_{V,d}) \neq 0$ (c'est-à-dire $\rho(U_{h,d_h}) \notin I(V)$ par (TE)). Appelons $f_1, \ldots, f_t$ les formes éliminantes d'indice $(d_1, \ldots, d_{h-1})$ des idéaux premiers minimaux associés à l'idéal $\rho(I(C(V)))$. Il existe alors des entiers naturels non nuls $l_1, \ldots, l_t$ et un élément $\lambda \in K$ tels que*

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

On dira alors que $\rho(f_{V,d})$ est une forme éliminante d'indice $(d_1, \ldots, d_{h-1})$ associée au cycle $Z = \sum_{j=1}^{t} l_j \ V_j$, où V_j est la variété associée à f_j.

Démonstration. Pour tout homomorphisme $\rho' : K[\mathbf{u}] \to K$ prolongeant ρ, par (TE) on a :

$$\begin{aligned}\rho'(f) = 0 &\Longleftrightarrow \rho'((I(V))[\mathbf{u}])) \text{ a un zéro non trivial dans } K^{n+1}\\ &\Longleftrightarrow \rho'((I(V), \rho(U_{h,d_h}))[(u^{1,d_1}, \ldots, u^{h-1,d_{h-1}})]) \text{ a un zéro non trivial dans } K^{n+1}\\ &\Longleftrightarrow \exists i \in \{1, \ldots, t\} \text{tel que } \rho'(f_i) = 0,\end{aligned}$$

car une forme éliminante d'indice d de $\sqrt{(I(V), \rho(U_{h,d_h}))}$ est $f_1 \ldots f_t$ d'après la proposition 4.6. Ceci signifie que l'hypersurface $\mathfrak{Z}(\rho(f))$ a les mêmes points définis sur K que la réunion des hypersurfaces $\bigcup_{h-1}^{t} \mathfrak{Z}(f_h)$, d'où le lemme. □

On considère l'intersection $V \cap W$ comme une intersection ensembliste. En général, $V \cap W$ n'est pas une variété. On peut quand même lui associer une forme éliminante de la manière suivante : 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 $d' = (d_1, \ldots, d_{h-1})$, et

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

On peut ainsi définir le degré de $V \cap W$ de manière analogue à celui de V, comme on l'a fait plus haut.

Théorème 5.12. *(Bézout Géométrique). Si $V \cap W \neq \emptyset$, alors*

$$d(V \cap W) \leq d(V)\, d(W) = d(V)\, d^{\circ} F.$$

Démonstration. Considérons l'homomorphisme de K-algèbres $\rho_F : K[\mathbf{u}] \to K[\mathbf{u'}]$ défini par $\rho_F(U_{h,d_h}) = F$, où $\mathbf{u}' = (u^{1,d_1}, \ldots, u^{h-1,d_{h-1}})$. Par le lemme 5.11, on peut associer un cycle $Z = \sum_{j=1}^{s} m_j V_j$ à $\rho_F(f_{V,d})$, de telle sorte que $\rho_F(f_{V,d}) = \lambda \prod_{j=1}^{s} f_{V_j,d'}^{m_j}$. Dans toute la suite, on notera $V.W$ ce cycle.

Or, d'après ce qui précède il est clair que $f_{V \cap W, d'}$ divise $\rho_F(f_{V,d})$ (car les m_i sont non nuls). En prenant $d = (1, \ldots, 1, d^o F)$ on a, en utilisant la caractérisation du degré que l'on a donnée plus haut :

$$d(V)\, d(W) = d(V) d^o F = d^o_{u^{1,1}} f_{V,d} = d^o_{u^{1,1}} \rho_F(f_{V,d}) \geq d^o_{u^{1,1}} f_{V \cap W, d'} = d(V \cap W).$$

□

On s'intéresse ensuite au comportement de la hauteur que l'on a définie à la section précédente par rapport à l'intersection.

Si $\alpha \in \mathbb{N}^{n+1}$ est un multi-indice, et k un entier, on note $C_k^{\alpha} = C_{k!}^{\alpha_0! \ldots \alpha_n!}$.

On définit une hauteur légèrement modifiée h_1 sur les polynômes $P \in K[X_0, \ldots, X_n]$ en posant

$$h_1(P) = \sum_v \frac{[K_v : \mathbb{Q}_v]}{[K : \mathbb{Q}]} \log |P|_v,$$

où $|F|_v$ est le maximum des valeurs absolues des coefficients P_α de P si v est ultramétrique, et $(\sum_{|\alpha| = d^\circ F} (C^{\alpha}_{d^\circ F})^{-1} |\sum_v (F_\alpha)|^2)^{1/2}$ sinon.

On a alors le théorème suivant :

Théorème 5.13. *(Bézout Arithmétique). Avec les mêmes notations que ci-dessus, si $V \cap W \neq \emptyset$ alors*

$$h(V \cap W) \leq h(V)\, d^{\circ} F \; + \; h_1(F)\, d(V).$$

Démonstration. On pourra se référer à [7], Chapitre 6, p.87. □

5.4 Distance d'un point à une variété

On se restreint dans cette section au cas d'une variété définie sur $K = \mathbb{C}$.
Pour $x = (x_0, \ldots, x_n) \in \mathbb{P}_n^*(\mathbb{C})$, on va introduire des formes générales qui s'annulent en x. Considérons le morphisme de K-algèbres :

$$\mathfrak{d}_x \ : \ \mathbb{C}[\mathbf{u}] \to \mathbb{C}[\mathbf{s}]$$

défini par $\mathfrak{d}_x(u_{\mathfrak{m}}^{i,d_i}) = \sum_{\mathfrak{m}' \in \mathfrak{M}_{d_i}} s_{\mathfrak{m},\mathfrak{m}'}^{i,d_i}\, \mathfrak{m}'(x)$, où les $s_{\mathfrak{m},\mathfrak{m}'}^{i,d_i}$ sont des nouvelles variables liées par les seules relations $s_{\mathfrak{m},\mathfrak{m}'}^{i,d_i} + s_{\mathfrak{m}',\mathfrak{m}}^{i,d_i} = 0$. Grâce à ces relations d'antisymétrie, les formes $\mathfrak{d}_x(U_{i,d_i})$ s'annulent en x et on déduit de (TE) que x est dans V si, et seulement si, $\mathfrak{d}_x f = 0$ (on note $f = f_{V,d}$). La taille de $\mathfrak{d}_x$ va mesurer la distance de x à V, de la manière suivante :

$$\mathrm{Dist}_d(x, V) = \frac{M(\mathfrak{d}_x f)}{M(f) \prod_{i=1}^{h} \|x\|^{d_i d^\circ_{u^{i,d_i}} f}}$$

où si $P = \sum\ a_{i_1,\ldots,i_n} X^{i_1} \ldots X^{i_n}$, on a noté $M(P) = \max\{|a_{i_1,\ldots,i_n}|\}$, et $|\,.\,|$ est la norme euclidienne. Si $\mathbb{Z} = \Sigma_i m_i V_i$ est un cycle équidimensionnel de dimension $h-1$, on définit

$$\mathrm{Dist}_d(x, Z) \ = \ \prod_i \mathrm{Dist}_d(x, V_i)^{m_i}.$$

Remarque : si $V = \mathfrak{Z}(F)$ est une hypersurface, alors $\mathrm{Dist}(x, V) = \dfrac{|F(x)|}{M(F)\ |\,x\,|^{\,d^\circ F}}$, ce qui découle de l'expression de $f_{V,d}$ en fonction de F que l'on a donnée au début de la section 5.

Proposition 5.14. *(Propriété du point le plus proche). Avec les notations ci-dessus, si $d_1 = \ldots = d_h = 1$, alors il existe $y \in V$ tel que*

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

Démonstration. On pourra se reporter à [7], Chapitre 6, pp. 89-90. □

5.5 Théorèmes métriques de Bézout

Les deux théorèmes qui suivent vont jouer un rôle fondamental dans la démonstration du critère d'indépendance algébrique de Philippon. Une démonstration en est donnée dans [7], Chapitre 6, pp. 90-94.

Théorème 5.15. *(Premier théorème de Bézout métrique).*
Soit V une variété projective de $\mathbb{P}_n(\mathbb{C})$ définie sur un corps de nombres K, F un polynôme de degré d dans $K[X_0, \ldots, X_n]$, $x \in \mathbb{P}_n(\mathbb{C})$ et $T \in \mathbb{N}^*$. Fixons un plongement $K \to \mathbb{C}$, $\Delta = [K : \mathbb{Q}]$ si K est réel ou $[K : Q]/2$ si K est imaginaire, et posons $W = V.\mathfrak{Z}(F)$. Alors

$$\begin{aligned}\frac{1}{\Delta}\ \log \mathrm{Dist}(x, W) + h(W) \leq \ & \frac{1}{\Delta} \log(\mathrm{Dist}(x, V)^T + \sum_{t=0}^{T-1} \frac{|\,F^{(t)}(x)\,|}{|\,F\,|}\, \mathrm{Dist}(x, V)^t) \\ & + d\,h(V) + d(V)\,(h_1(F) + \frac{(T+3d)h}{\Delta} \log(n+1)).\end{aligned}$$

Théorème 5.16. *(Deuxième théorème de Bézout métrique).*
Soit $\sigma \leq 1$ un réel, V une variété projective de $\mathbb{P}_n(\mathbb{C})$ définie sur un corps de nombres K, F un polynôme de degré d dans $K[X_0, \ldots, X_n]$, $x \in \mathbb{P}_n(\mathbb{C})$ et $T \in \mathbb{N}^*$. Fixons un plongement

$K \to \mathbb{C}$, $\Delta = [K:\mathbb{Q}]$ *si* K *est réel ou* $[K:Q]/2$ *si* K *est imaginaire, et posons* $W = V.\mathfrak{Z}(F)$. *En supposant que*

$$\frac{\|F^{(t)}(x)\|}{\|F\|} \leq \min_{y \in V(\mathbb{C})} (\mathrm{Dist}(x,y)^{(T-t)/\sigma})$$

pour tout $t = 0, \ldots, T-1$, *on a la majoration :*

$$\frac{1}{\Delta} \log \mathrm{Dist}(x,W) + h(W) \leq \frac{T}{\sigma\Delta} \log \mathrm{Dist}(x,V) + d\, h(V) + d(V)\,(h_1(F) + (\frac{Th}{\sigma} + 3d)\log(n+1)).$$

6 Indépendance algébrique de π, e^π, *et* $\Gamma(1/4)$

6.1 Quelques corollaires du théorème de Nesterenko

Nous allons donner trois corollaires du théorème suivant, montré par Yu.V. Nesterenko [8] en 1996 :

Théorème 6.1. *Soit* $q \in \mathbb{C}$ *satisfaisant* $0 < |q| < 1$. *Alors le degré de transcendance sur* $\mathbb{Q}$ *du corps*

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

est supérieur ou égal à 3.

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

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

Nous donnerons une preuve directe du corollaire 6.3 ci-dessous dans la section 6.3, qui elle n'utilise pas de lemme de zéros mais passe par une mesure d'indépendance algébrique de ω/π et η/π, due à Philibert [9], que l'on exposera en 6.2.

Corollaire 6.2. *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)
Les fonctions J et Δ sont liées aux fonctions P, Q, R par les relations (cf 1.3 et 1.4) :

$$\Delta = \frac{1}{1728}(Q^3 - R^2) \text{ et } J = \frac{Q^3}{\Delta}.$$

Si on suppose $J(q)$ algébrique, alors $Q(q)$ et $R(q)$ sont algébriquement dépendants, et donc les 3 nombres algébriquement indépendants donnés par le théorème sont soit q, $P(q)$, $R(q)$, soit q, $P(q)$, $Q(q)$. Dans les deux cas, on obtient l'indépendance de q, $P(q)$ et $\Delta(q)$. □

Les deux corollaires suivants se déduisent du corollaire 6.2 :

Corollaire 6.3. *Soit* $\wp$ *la fonction elliptique de Weierstrass attachée au réseau* Ω, *d'invariants* g_2 *et* g_3 *algébriques. Alors les trois nombres*

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

sont algébriquement indépendants.

Démonstration. On note $q = e^{2i\pi\tau}$ et on utilise les formules démontrées à la section 1.3 :

$$\frac{1}{(2i\pi)^4}\, g_2\, \omega_1^4 = \frac{1}{12}\left(1 + 240 \sum_{n=1}^{\infty} \frac{n^3 q^n}{1-q^n}\right),$$
$$\frac{1}{(2i\pi)^6}\, g_3\, \omega_1^6 = \frac{1}{6^3}\left(-1 + 504 \sum_{n=1}^{\infty} \frac{n^5 q^n}{1-q^n}\right).$$

On a besoin d'une formule similaire pour η_1, qui est démontrée dans [3], (chapitre 18, p.249) :

$$\frac{1}{(2i\pi)^2}\omega_1\, \eta_1 = \frac{1}{12}\left(-1 + 24 \sum_{n=1}^{\infty} \frac{n q^n}{1-q^n}\right).$$

On a alors

$$\begin{aligned} P(q) &= -\omega_1\, \eta_1\ \frac{12}{(2\mathrm{i}\pi)^2} \\ &= 3\frac{\omega_1 \eta_1}{\pi^2}, \end{aligned}$$

$$\begin{aligned} Q(q) &= \frac{12}{(2\mathrm{i}\pi)^4}\ \omega_1^4\, g_2 \\ &= \frac{3}{4}\left(\frac{\omega_1}{\pi}\right)^4\ g_2, \end{aligned}$$

$$\begin{aligned} R(q) &= -\frac{6^3}{(2\mathrm{i}\pi)^6}\ \omega_1^6\, g_3 \\ &= \frac{27}{8}\left(\frac{\omega_1}{\pi}\right)^6\ g_3. \end{aligned}$$

On en déduit facilement

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

Comme les nombres algébriques forment un corps, le théorème 6.2 montre alors que q, $\dfrac{\omega}{\pi}$ et $\dfrac{\eta}{\pi}$ sont algébriquement indépendants. □

Corollaire 6.4. *Les trois nombres*

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

sont algébriquement indépendants. En particulier les deux nombres π et e^{π} sont algébriquement indépendants.

L'indépendance π et de e^{π} n'était pas connue. Par contre, celle de π et de $\Gamma(1/4)$ a été montrée en 1976 par G.V. Chudnovsky.
On utilise le lemme suivant ([5], lemme 3.1).

Lemme 6.5. *Si la fonction de Weierstrass $\wp$ (attachée au réseau Ω) a multiplication complexe, alors il existe $k \in K(g_2, g_3)$ (où $K = \mathbb{Q}(\tau)$) et des entiers A et C tels que*

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

Démonstration. Comme $\wp$ a multiplication complexe, K est une extension quadratique de $\mathbb{Q}$ et donc il existe des entiers A, B, C non tous nuls tels que $A + B\tau + C\tau^2 = 0$.

Soit f la fonction méromorphe sur $\mathbb{C}$ définie par :

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

où k est le nombre défini par l'énoncé du lemme (i.e. on pose $k = (A\eta_1 - C\tau\eta_2)/\omega_2$). On veut montrer que k est bien dans $K(g_2, g_3)$. Pour $i = 1, 2$, on a : $\zeta(z+\omega_i) = \zeta(z)+\eta_i$, d'où :

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

par définition de k. De même, de $C\tau\omega_2 = -A\omega_1 - B\omega_2$ on tire

$$f(z+\omega_2) - f(z) = -AC\eta_2 + C\tau(-A\eta_1 - B\eta_2) + C\tau k\omega_2 = 0.$$

Donc f a les mêmes périodes que la fonction $\wp$ de Weierstrass : c'est donc une fonction rationnelle de $\wp$ et de $\wp'$.

Soit σ un automorphisme de $K(g_2, g_3, k)$ qui fixe $K(g_2, g_3)$, et f^σ la fonction obtenue en appliquant σ au développement de Laurent de f à l'origine. σ fixe alors $\wp$ et $\wp'$, car leur développement de Laurent à l'origine a ses coefficients dans $\mathbb{Q}(g_2, g_3)$ (remarque précédent le théorème 2.15) ; donc f^σ est encore une fonction rationnelle de $\wp$ et de $\wp'$. ζ étant également fixée par σ, on a :

$$f(z) - f^\sigma(z) = C\tau(k - k^\sigma)z.$$

Or $f - f^\sigma$ est une fonction elliptique, d'où $f - f^\sigma$=0 et $k = k^\sigma$. Comme σ est quelconque, k est fixé par tout automorphisme d'extensions, et donc $k \in K(g_2, g_3)$. □

Démonstration. (du Corollaire 6.4) En utilisant la relation de Legendre

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

on déduit immédiatement que les trois nombres ω/π, η/π et $1/\omega$ sont liés par une relation linéaire à coefficients algébriques sur $\mathbb{Q}$.

Pour finir la démonstration, on considère la courbe elliptique $\wp$ donnée par l'équation $y^2 = 4x^3 - 4x$. On a alors $g_2 = 4$ et $g_3 = 0$, qui sont bien algébriques. On a vu dans la section 2 que les racines de l'équation $4\wp(z)^3 - 4\wp(z) = 0$ étaient $\wp(\omega_1/2)$, $\wp(\omega_2/2)$ et $\wp((\omega_1+\omega_2)/2)$. En appliquant éventuellement une transformation unimodulaire, on se ramène au cas où $\wp(\omega/2) = 1$. $\wp$ prend des valeurs réelles sur $]0, \omega/2]$, et est monotone décroissante positive car $\wp'$ ne s'annule pas, et $\wp(0) = +\infty$. En posant $u = \wp^{-1}(t)$, $t = \wp(u)$ et

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

En intégrant cette équation, on obtient

$$u = \wp^{-1}(t) = \frac{1}{2}\int_t^\infty (s(s+1)(s-1))^{-1/2} ds, \quad t \geq 1$$

Si $t = 1$, $u = \omega/2$, d'où :

$$\omega \ = \ 2\int_1^\infty \frac{ds}{\sqrt{4s^3 - 4s}}.$$

Pour calculer cette intégrale, on effectue le changement de variable $s = x^{-1/2}$, on obtient alors

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

où

$$B(a,b) \ = \ \int_0^1 t^{a-1}(1-t)^{b-1}\,\mathrm{d}t \ = \ \frac{\Gamma(a)\Gamma(b)}{\Gamma(a+b)}$$

est l'intégrale d'Euler du premier type. On conclut en appliquant la formule des compléments

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

avec $x = 1/4$, et on en déduit finalement l'expression de ω

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

Le réseau $\mathrm{i}\Omega$ a mêmes invariants g_2 et g_3 que Ω : c'est toujours vrai pour g_2, et $g_3(\mathrm{i}\Omega) = -g_3(\Omega) = 0$. Donc $\mathrm{i}\Omega = \Omega$, ce qui montre que la multiplication par i est un endomorphisme de Ω, et $\wp$ a donc multiplication complexe. En particulier, il existe $(a, b) \in \mathbb{Q}^2$ tels que $\tau = a + \mathrm{i}b$.

On peut alors appliquer le Corollaire 6.3, dont on déduit l'indépendance algébrique des trois nombres $e^{2i\pi\tau}$, ω/π et η/π. Comme on a montré plus haut que ω/π, η/ω et $1/\omega$ étaient linéairement dépendants, on obtient l'indépendance algébrique de $e^{2i\pi\tau}$, ω et π, soit de $e^{-2\pi}$, $\Gamma(1/4)^2/2\sqrt{2\pi}$ et π. Pour obtenir l'indépendance de π, $e^{\pi\sqrt{3}}$ et $\Gamma(1/3)$, on procède de même avec la courbe elliptique $y^2 = 4x^3 - 4$. □

6.2 La mesure d'indépendance algébrique de Philibert

Nous introduisons dans cette section une mesure d'indépendance algébrique des deux nombres ω/π et η/π établie par Philibert [9], c'est-à-dire une minoration de la valeur de tout polynôme $P \in \mathbb{Z}[X_1, X_2]$ en $x = (\omega/\pi, \eta/\pi)$ en fonction de la taille du polynôme P, que l'on va mesurer de la manière suivante :

Définition 6.6. *On appelle* longueur *de P, et on note $L(P)$, la somme des valeurs absolues des coefficients de P.*

On définit alors la taille *de P par*

$$t(P) \;=\; d^\circ P \;+\; \log L(P),$$

où $d^\circ P$ désigne le degré total de P.

On donne d'abord l'énoncé d'un critère d'indépendance algébrique établi par Philippon ([7], Chapitre 8). On appliquera ensuite ce critère aux deux nombres ω/π et η/π, suivant une démonstration de Philibert [9].

On suppose dans toute la suite que les invariants g_2 et g_3 du réseau Ω sont algébriques.

On rappelle que pour tout polynôme $Q \in \mathbb{Z}[X_0, \ldots, X_n]$, on note $\|Q\| = \sqrt{\left(\sum_\alpha \frac{|Q_\alpha|^2}{C^\alpha_{d^\circ Q}}\right)}$, $h_1(Q) = \log \|Q\|$ et $\|Q(x)\| = \frac{|Q(x)|}{\|x\|^{d^\circ Q}}$. Ces définitions ont été données en 5.3.

On suppose que

(H). Soit $x \in \mathbb{P}_n(\mathbb{C})$, $k \in \{0, \ldots, n\}$ et δ, τ, σ et U des réels tels que

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

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

1. $d^\circ Q_i \leq \delta$ et $h_1(Q_i) \leq \tau$
2. $\frac{\|Q_i(x)\|}{\|Q_i\|} \leq \exp(-S\sigma^{k+1})$

3. les polynômes Q_i n'ont pas de zéro commun dans la boule fermée $B(x, \exp(-S\sigma^{k+2}))$

Lemme 6.7. *(Critère d'indépendance algébrique) Sous les hypothèses* (H)*, soit V une sous-variété projective de $\mathbb{P}_n$ définie sur $\mathbb{Q}$ de dimension d telle que*

$$(\delta h(V) + ((k+1)\tau + 3\delta\log(n+1))d(V))\delta^k < \frac{U}{(k+1)\sigma^{k+1}} \qquad (\star)$$

Alors, si $d \leq k$, $\log(\mathrm{Dist}(x, V)) \geq -U$.

La preuve de ce résultat passe par le lemme suivant.

Lemme 6.8. *Sous les hypothèses* (H)*, soit V une variété définie sur $\mathbb{Q}$ de dimension d satisfaisant $(\star)$ et $\log \mathrm{Dist}(x, V) < -U$. Alors pour $h = d+1, \ldots, \max(0, d-k)$, il existe une variété projective Z_h définie sur $\mathbb{Q}$ et de dimension $h-1$ telle que, si $h' = h + k - d$*

1. $d(Z_h) \leq \delta^{d-h+1} d(V)$
2. $h(Z_h) \leq (\delta h(V) + (d-h+1)\tau d(V))\delta^{d-h}$
3. $\log(\mathrm{Dist}(x, Z_h)) < -h'\sigma^{h'}(\delta h(Z_h) + (h'\tau + 3\delta\log(n+1))d(Z_h))\delta^{h'-1}$

Démonstration. La preuve fait intervenir l'ensemble des outils que nous avons 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. Nous allons donc simplement donner une idée de la preuve en montrant comment sont utilisés les théorèmes de la section 5, et le lecteur pourra se référer à [7], pp.133-135 pour les détails.

On le fait par récurrence (descendante) sur h. Pour $h = d+1$, $Z_{d+1} = V$ convient. On suppose donc que Z_h est construit, et l'on veut construire Z_{h-1}.

Par la propriété du point le plus proche, il existe $y \in Z_h$ tel que

$$\log \mathrm{Dist}(x, y) \ \leq \ -\frac{\sigma\tau}{\mu}.$$

Il existe donc $\tau/\sigma^{k+1} < S' < U/\sigma^{k+1}$ tel que y soit dans la boule

$$B_{S'} = B(x, \exp(-S'\sigma^{k+2})).$$

On prend pour S la borne supérieure des S' dans cet intervalle tels que l'intersection de Z_h et de $B_{S'}$ soit non vide. Par (H3), un des polynômes Q_i correspondants n'est pas nul sur Z_h. On peut alors considérer le cycle $W = Z_h.\mathfrak{Z}(Q_i)$ qui est équidimensionnel de dimension $h-2$, et grâce aux théorèmes de Bézout géométrique et arithmétique, on obtient des majorations convenables de son degré et de sa hauteur.

Il reste à majorer $\mathrm{Dist}(x, W)$, pour cela on distingue deux cas :

Premier cas : $S = U/\sigma^{k+1}$. Par (H2) et $(\star)$, on peut appliquer le premier théorème de Bézout métrique pour majorer $\mathrm{Dist}(x, W)$.

Deuxième cas : $S < U/\sigma^{k+1}$. Par maximalité de S,

$$Z_h \cap B(x, \exp(-S'\sigma^{k+2})) \ = \ \emptyset$$

pour tout $S' > S$ et

$$\frac{1}{\sigma} \cdot \min_{y \in Z_h} \log \mathrm{Dist}(x, y) \ \geq \ -S\sigma^{k+1} \ \geq \ \log(\frac{\|Q_i(x)\|}{\|Q_i\|}).$$

On peut donc appliquer le deuxième théorème de Bézout métrique pour majorer $\mathrm{Dist}(x, W)$.

Dans les deux cas, on a vérifié que W vérifiait les assertions du lemme. Comme les fonctions degré, hauteur et log Dist sont additives sur les cycles, on en déduit qu'au moins une des composantes irréductibles de W satisfait ces mêmes assertions, et on définit Z_{h-1} comme étant égale à cette composante, ce qui conclut la récurrence et la preuve du lemme. □

Démonstration. (du critère d'indépendance algébrique) Lorsque $d \leq k$, la conclusion du lemme 6.8 est fausse. En effet, Z_0 doit être le cycle vide (de dimension -1) pour lequel $\mathrm{Dist}(x, Z_0) = 1$, et donc $\log(\mathrm{Dist}(x, Z_0))$ ne peut être < 0. Ainsi, les hypothèses du lemme 6.8 sont contradictoires quand $d \leq k$ et, sous (H), on doit donc avoir $\log(\mathrm{Dist}(x, V)) \leq -U$ pour toute variété V définie sur $\mathbb{Q}$, de dimension $d \leq k$, satisfaisant $(\star)$. □

Théorème 6.9. *(Mesure d'indépendance algébrique de Philibert). Pour tout $\varepsilon > 0$, il existe une constante c dépendant de ω, Ω et ε telle que pour tout polynôme P de $K[X, Y]$ on ait :*

$$\left| P(\frac{\omega}{\pi}, \frac{\eta}{\pi}) \right| \geq exp(-(ct(P))^{3+\varepsilon}).$$

Remarque. *Ce résultat contient en particulier l'indépendance algébrique de π et de $\Gamma(1/4)$.*

Démonstration. La preuve est donnée dans [9]. Le but est d'appliquer le critère d'indépendance algébrique de Philippon. On veut donc contruire une famille $(Q_i)_{i \in I}$ de polynômes de $K[X, Y]$ dont on contrôle le degré, la taille, la valeur en $x = (\omega/\pi, \eta/\pi)$ et qui n'ont pas de zéros dans une petite boule centrée en x. Pour mesurer la taille de ces polynômes, on utilise la hauteur h introduite dans la section 5.2 (on prend $h = 2$, $N_1 = N_2 = 1$ dans la définition).

On montre alors l'existence de constantes A_1, A_2, A_3, A_4, A_5 telles que pour tout $N > 0$, il existe une famille de polynômes $(Q_i)_{i \in I_n}$ tels que :

1. $d^o Q_i \leq A_2 N$
2. $h(Q_i) \leq A_3 N log(N)$
3. $Q_i(x) \leq exp(-A_4 N^3)$
4. Les Q_i n'ont pas de zéro dans la boule de centre x et de rayon $e^{-A_5 N^3}$

Le critère d'indépendance algébrique de Philippon (Lemme 6.7) permet alors à Philibert de conclure (la variété V est le lieu des zéros du polynôme P ; dans ce cas la distance du point $x = (\eta/\pi, \omega/\pi)$ à V s'exprime simplement en fonction de la taille de P et de sa valeur en x, comme on l'a vu dans la section 5.4. Il suffit alors de vérifier les hypothèses du lemme pour un bon choix des paramètres.).

□

6.3 Une démonstration directe de l'indépendance algébrique

Montrons tout d'abord un résultat préliminaire, dont nous nous sommes déjà servis pour démontrer le théorème Stéphanois, et qui va nous être utile pour démontrer la Proposition 6.11.

Lemme 6.10. *(Thue-Siegel). Soit $G = (g_{ij})$ une matrice à coefficients dans $\mathbb{Z}$ possédant M lignes et N colonnes, avec $N > M$. Il existe $X = \begin{pmatrix} x_1 \\ \vdots \\ x_N \end{pmatrix} \in \mathbb{Z}^N$ non nul tel que $GX = 0$ et*

$$\max_{1 \leq j \leq N} |x_j| \leq (\prod_{i=1}^{M} G_i)^{1/(N-M)}$$

où $G_i = \max\{1, \sum_{j=1}^{N} |g_{ij}|\}$.

Démonstration. Posons $G = [(G_1 \dots G_M)^{1/(N-M)}]$ (où $[.]$ désigne la partie entière). Il y a alors $(G+1)^N$ vecteurs distincts $x = (x_1, \dots, x_N)$ à coordonnées entières vérifiant

$$0 \leq x_j \leq G \ (j = 1, 2, \dots, N).$$

A chaque tel vecteur on associe un deuxième vecteur à coordonnées entières $y = (y_1, \dots, y_M)$ défini par

$$y_i = \sum_{j=1}^{N} g_{ij} x_j \ (i = 1, 2, \dots, M).$$

On définit de plus, pour tout $i = 1, 2, \dots, M$ deux entiers positifs n_i et p_i par

$$n_i = \sum_{j=1, g_{ij}<0}^{N} |g_{ij}|, \ p_i = \sum_{j=1, g_{ij}>0}^{N} |g_{ij}|.$$

Alors il est clair que pour tout $i = 1, 2, \dots, M$, et pour tous les vecteurs y, on a :

$$G_i = n_i + p_i \text{ et } -n_i G \leq y_i \leq p_i G.$$

Ceci montre que chaque coordonnée y_i peut prendre au plus $n_i G + p_i G + 1 = G_i G + 1$ valeurs distinctes, et donc qu'il y a au plus $(G_1 G + 1) \dots (G_M G + 1)$ vecteurs y distincts. Mais

$$(G+1)^N = (G+1)^M (G+1)^{N-M} > (G+1)^M G_1 \dots G_M \geq (G_1 G + 1) \dots (G_M G + 1)$$

Il existe donc deux vecteurs distincts x et x' qui ont le même vecteur associé. Le vecteur $x - x'$ est alors non nul, et vérifie $G(x - x') = 0$; de plus les coordonnées $x_1, \dots, x_N$ de x sont comprises entre $-G$ et G, donc x a les propriétés voulues. □

Nous pouvons désormais montrer la proposition suivante.

Proposition 6.11. *Soit $q \in \mathbb{C}$, tel que $0 < |q| < 1$. Il existe 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 $A_N \in \mathbb{Z}[z, X_1, X_2, X_3]$ tel que*

1. $\deg A_N \leq cN \log M$
2. $\log H(A_N) \leq cN(\log M)^2$
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 [8]. En fait, la démonstration qui suit permet essentiellement à Yu.V. Nesterenko de réduire le Théorème 6.1 à un lemme de zéros qui constitue la partie difficile de sa preuve, et que nous esquivons. C'est M. Waldschmidt, dans [17], qui a repris ces arguments pour démontrer directement le Corollaire 6.2.

On commence par montrer deux lemmes :

Lemme 6.12. *Soit $N \in \mathbb{N}$. Alors 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 des quatre variables, tel que la fonction*

$$F(z) = A(z, P(z), Q(z), R(z))$$

ait, à l'origine, un zéro de multiplicité $\geq L = [(N+1)^4/2]$, et dont la longueur soit majorée par : $L(A) \leq N^{85N}$.

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 $\sum a_n z^n \ll \sum b_n z^n$ singifie que que $|a_i| \leq |b_i|$ pour tout i ; on a donc :

$$P(z) \ll \frac{24.2!}{(1-z)^3},\ Q(z) \ll \frac{240.4!}{(1-z)^5},\ R(z) \ll \frac{504.6!}{(1-z)^7},\ z \ll \frac{1}{1-z}.$$

En effet, $P(z) = 1 - 24 \sum_{n=1}^{\infty} \sigma_1(n) z^n$; expression qui s'obtient facilement à partir de celle donnée à la section 1.3, et il y a des expressions similaires pour Q et R.

Pour tout vecteur $k = (k_0, k_1, k_2, k_3)$, $k_i \in \mathbb{Z}$, $0 \leq k_i \leq N$, $i = 0, 1, 2, 3$, on a :

$$z^{k_0} P(z)^{k_1} Q(z)^{k_2} R(z)^{k_3} = \sum_{n=0}^{\infty} d(k,n) z^n \ll \frac{c_1^{3N}}{(1-z)^{16N}}, \tag{2}$$

où $c_1 = 504.6!$ et $d(k,n) \in \mathbb{Z}$. De (1) et (2) on déduit que

$$|d(k,n)| \leq c_1^{3N}(n+16N)^{16N} \leq (c_2 nN)^{16N} \leq (nN)^{17N}\ (n \geq 1), \tag{3}$$

si N est suffisamment grand, et $|d(k,0)| \geq 1$.

Posons $A = \sum_{0 \leq k_i \leq N} a(k) z^{k_0} x_1^{k_1} x_2^{k_2} x_3^{k_3}$, où les entiers $a(k)$ sont choisis comme étant une solution non triviale du système d'équations linéaires

$$\sum_{0 \leq k_i \leq N} d(k,n) a(k) = 0.\ \ (n = 0, 1, \ldots, [\frac{(N+1)^4}{2}] - 1).$$

Ici le nombre de variables est $u = (N+1)^4$ et le nombre d'équations est $v = [(N+1)^4/2]$. Si on utilise (3) et le lemme de Thue et Siegel, on voit donc que le système a une solution entière non triviale vérifiant l'inégalité

$$\max_k |a(k)| \leq (N+1)^4 (\frac{(N+1)^4}{2} N)^{17N} \leq N^{85N}.$$

□

Soit N un entier assez grand. On considère le polynôme A donné par le lemme précédent. Soit $M = \mathrm{ord}_0 F$ l'ordre de F en 0. La construction de A donne $M \geq L \geq N^4/2$.

Posons $r = \min\{\frac{(1+|q|)}{2}, 2|q|\}$ (on a alors $|q| < r < 1$) et montrons un deuxième lemme :

Lemme 6.13. *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. Soit

$$F(z) \ = \ \sum_{n=M}^{\infty} b_n z^n$$

le développement de Taylor de F à l'origine. Alors, $b_n = \sum_{0 \geq k_i \geq N} d(k,n) a(k) \in \mathbb{Z}$ et, par (3),

$$|b_n| \leq \sum_{0 \leq k_i \leq N} (nN)^{17N} N^{85N} \leq n^{17N} N^{103N}\ (n \geq M).$$

Pour $|z| \leq r$ on a

$$\begin{aligned}
|F(z)| &\leq \sum_{n=M}^{\infty} |b_n|\,|z|^n = \sum_{n=0}^{\infty} |b_{n+M}|\,|z|^{n+M} \\
&\leq |z|^M N^{103N} \sum_{n=0}^{\infty} (n+M)^{17N} |z|^n \\
&\leq |z|^M N^{103N} (M+1)^{17N} (1 + \sum_{n=1}^{\infty} n^{17N} |z|^n) \\
&\leq |z|^M N^{103N} (M+1)^{17N} \frac{(17N)!}{(1-r)^{17N+1}} \\
&\leq |z|^M N^{103N} (M+1)^{17N} N^{17N} \leq |z|^M M^{48N}
\end{aligned}$$

si N est assez grand. □

L'étape suivante consiste à montrer que $\mathrm{ord}_q F = T \leq \alpha N \log M$, avec $\alpha = \left(\log \frac{r}{|q|}\right)^{-1}$. On applique pour cela le principe du maximum à la fonction

$$H(z) = \frac{F(z)}{z^M} \left(\frac{r^2 - \bar{q}z}{r(z-q)}\right)^T$$

On obtient alors

$$|H(0)| \leq |H|_r \tag{2}$$

Or le nombre $G(0) = \frac{1}{M!} F^{(M)}(0)$ est entier et non nul. On minore sa valeur absolue par 1 et on trouve

$$|H(0)| \geq \left(\frac{r}{|q|}\right)^T \tag{3}$$

Finalement,

$$\begin{aligned}
\left(\frac{r}{|q|}\right)^T &\leq |H|_r \\
&\leq r^{-M} |F|_r \\
&\leq M^{48N}
\end{aligned}$$

On en déduit la majoration de T.

En 1916 Ramanujan [13] a été le premier à définir les fonctions P, Q et R (par leur développement en série entière), et il a montré en particulier qu'elles vérifiaient les équations différentielles

$$\theta P = \frac{1}{12}(P^2 - Q),\ \theta Q = \frac{1}{3}(PQ - R),\ \theta R = \frac{1}{2}(PR - Q^2),$$

où $\theta = z\dfrac{\partial}{\partial z}$.

On introduit, sur l'anneau $\mathbb{C}[z, X_1, X_2, X_3]$ l'opérateur de dérivation correspondant à ce système d'équations différentielles :

$$D = z\frac{\partial}{\partial z} + \frac{1}{12}(X_1^2 - X_2)\frac{\partial}{\partial X_1} + \frac{1}{3}(X_1 X_2 - X_3)\frac{\partial}{\partial X_2} + \frac{1}{2}(X_1 X_3 - X_2^2)\frac{\partial}{\partial X_3}$$

de sorte que pour tout polynôme $B \in \mathbb{C}[z, X_1, X_2, X_3]$, on ait l'égalité :

$$z\frac{d}{dz} B(z, P(z), Q(z), R(z)) = (DB)(z, P(z), Q(z), R(z)). \tag{4}$$

On définit le polynôme A_N (pour N suffisamment grand) 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 à la Proposition 6.11 et T est l'entier défini ci-dessus. On vérifie par une récurrence immédiate sur T que

$$(z^{-1}D)^T = z^{-T}\prod_{k=0}^{T-1}(D-k), \tag{5}$$

ce qui montre que $A_N \in \mathbb{Z}[z, X_1, X_2, X_3]$. Par (4), on voit que

$$A_N(z, P(z), Q(z), R(z)) = (12z)^T F^{(T)}(z)$$

Pour obtenir la majoration annoncée on utilise la formule

$$F^{(T)}(q) = \frac{T!}{2\pi i}\int_{C_2}\frac{F(z)}{(z-q)^{T+1}}dz,$$

où C_2 est le cercle $\{z \in \mathbb{C} \mid |z-q| = r - |q|\}$. En utilisant l'inégalité $|z| \leq |z-q| + |q| = r$, ansi que le Lemme 6.12 et la majoration de T que l'on a établie plus haut, on obtient

$$|A_N(q, P(q), Q(q), R(q))| \leq 12^T \cdot T! \cdot (r-|q|)^{-T} r^M \cdot M^{48N} \leq e^{-\kappa M}$$

On va maintenant montrer les majorations sur le degré et la longueur, en utilisant (5). Si $B \in \mathbb{C}[z, X_1, X_2, X_3]$ et $B \ll G(1+z+X_1+X_2+X_3)^S$, alors pour tout entier k on a :

$$\begin{aligned}(D+k)B &\ll |k|G(1+z+X_1+X_2+X_3)^S + GS(1+z+X_1+X_2+X_3)^{S-1}\\ &\quad\times(z+(X_1^2+X_2)+(X_1X_2+X_3)+(X_1X_3+{X_2}^2))\\ &\ll |k|G(1+z+X_1+X_2+X_3)^S + GS(1+z+X_1+X_2+X_3)^{S+1}\\ &\ll G(S+|k|)(1+z+X_1+X_2+X_3)^{S+1}.\end{aligned}$$

D'où

$$12^T\prod_{k=0}^{T-1}(D-k)B(z, X_1, X_2, X_3) \ll 12^T G(S+2T)^T(1+z+X_1+X_2+X_3)^{S+T}.$$

Par la lemme 6.12 on a

$$A \ll N^{85N}(1+z+X_1+X_2+X_3)^{4N}$$

d'où

$$A_N(z, X_1, X_2, X_3) \ll N^{85N}(48N+24T)^T(1+z+X_1+X_2+X_3)^{4N+T}.$$

Ceci implique que

$$\begin{aligned}&\deg A_N \leq 4N+T \leq (\alpha+1)N\log M,\\ &L(A_N) \leq N^{85N}5^{4N+T}(48N+24T)^T \leq \exp(2\alpha N(\log M)^2),\end{aligned}$$

ce qui achève la démonstration. □

On peut désormais montrer le Corollaire 6.4, énoncé dans la section 6.1.

Démonstration. On va le déduire du Théorème 6.9 et de la Proposition 6.11. Soit $q \in \mathbb{C}$ tel que $0 < |q| < 1$.

Comme dans ce qui précède, on suppose g_2 et g_3 algébriques. On raisonne par l'absurde, en supposant que $q = e^{2i\pi\tau}$, ω/π et η/π sont algébriquement liés. Les formules pour $P(q)$, $Q(q)$ et $R(q)$ qui ont été données dans la démonstration du Corollaire 6.3 montrent que chacun des quatre nombres q, $P(q)$, $Q(q)$ et $R(q)$ est racine d'un polynôme $A_i(X_i, \frac{\omega}{\pi}, \frac{\eta}{\pi})$ pour $i = 0, 1, 2, 3$ avec $A_i \in \mathbb{Z}[X_i, Y_1, Y_2]$. On va éliminer, dans l'anneau des polynômes

en 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, X_3 entre les cinq polynômes A, A_0, A_1, A_2, A_3 (où A est un des A_N donnés par la proposition 6.11, pour un N qui sera choisi ultérieurement).

On commence par calculer le résultant en X_0 de A et de A_0 :

$$\mathrm{Res}_{X_0}(A_0, A)(X_1, X_2, X_3, \frac{\omega}{\pi}, \frac{\eta}{\pi}) \ = \prod_{\alpha, A_0(\alpha, \omega/\pi, \eta/\pi)=0} A(\alpha, X_1, X_2, X_3).$$

On recommence en prenant le résultant du polynôme obtenu avec A_1, puis A_2 et A_3. On obtient ainsi un polynôme $P \in \mathbb{Z}(Y_1, Y_2)$ tel que, en notant

$$Z = \{(\alpha_0, \alpha_1, \alpha_2, \alpha_3) \mid A_i(\alpha_i, \omega/\pi, \eta/\pi) = 0 \ (i = 0, 1, 2, 3)\}$$

$$\begin{aligned} P(\omega/\pi, \eta/\pi) = & \prod_{(\alpha_0, \alpha_1, \alpha_2, \alpha_3) \in Z} A(\alpha_0, \alpha_1, \alpha_2, \alpha_3) \\ & = A(q, P(q), Q(q), R(q)) \prod_{\substack{(\alpha_0, \alpha_1, \alpha_2, \alpha_3) \\ \in Z - \{(q, P(q), R(q), Q(q))\}}} A(\alpha_0, \alpha_1, \alpha_2, \alpha_3) \end{aligned}$$

D'où, si C est une constante (plus grande que 1) qui majore le module de toutes les racines des $A_i(X_i, \omega/\pi, \eta/\pi)$ (dans une clôture algébrique) :

$$\begin{aligned} |P(\omega/\pi, \eta/\pi)| & \leq e^{-\kappa M} \left(C^{d^\circ A} L(A)\right)^{\sum_{i=0}^{3} d^\circ A_i} \\ & \leq e^{-\kappa M} \left(C^{cN \log M} e^{cN(\log M)^2}\right)^{\sum_{i=0}^{3} d^\circ A_i} \\ & \leq e^{-\kappa M + C' N (\log M)^2} \\ & \leq e^{-\kappa' N^4} \end{aligned}$$

pour N assez grand. Or, par le théorème 6.9, on a la minoration

$$|P(\omega/\pi, \eta/\pi)| \geq \exp(-c'(d^\circ P + \log L(P))^{3+\varepsilon}),$$

pour tout $\varepsilon > 0$ et où c' est une constante dépendant de ε. Par ailleurs, en écrivant le résultant comme un déterminant, on voit qu'il existe trois constantes B, B' et B'' telles que :

$$\begin{aligned} d^\circ(P) \ & \leq \ B d^\circ(A) \\ L(P) \leq \ & B'^{d^\circ(A)} L(A)^{B''}. \end{aligned}$$

D'où :

$$|P(\omega/\pi, \eta/\pi)| \geq e^{-c''(N \log M + N(\log M)^2)^{3+\varepsilon}}.$$

Cette minoration est incompatible avec la majoration établie plus haut : les estimations données par le Théorème 6.9 et la Proposition 6.11 ne sont pas compatibles. L'hypothèse faite (à savoir, $e^{2i\pi\tau}$, ω/π et η/π algébriquement liés) est donc contredite, ce qui termine la preuve. □

On peut remarquer, en conclusion, que la preuve de la Proposition 6.11 que nous avons donnée ressemble beaucoup à la preuve du théorème Stéphanois esquissée à la section 3. Dans les deux cas, on considère une fonction auxiliaire F ayant un ordre de multiplicité au moins L en l'origine, puis on essaie d'encadrer soit la valeur de F en un point α^S, soit la valeur d'une dérivée T-ième de F en un point q. Ce type de démonstration est essentiellement le seul dont on dispose actuellement pour des preuves d'indépendance algébrique. C'est Hermite qui a introduit ce type d'argument le premier, avec la démonstration de la transcendance de e en 1873.

Références

[1] K. Barré-Sirieix, G. Diaz, F. Gramain, G. Philibert. *Une preuve de la conjecture Mahler-Manin.* Invent. Math. 124, 1-9, 1996.

[2] K. Chandrasekharan. *Elliptic functions.* Grund. der math. Wiss. 281, Springer-Verlag, 1985.

[3] S. Lang. *Elliptic functions.* Springer-Verlag, 1973.

[4] K. Mahler. *On the coefficients of transformation polynomials for the modular function.* Bull. Austral. Math. Soc. 10, 197-218, 1978.

[5] D. Masser. *Elliptic Functions and Transcendance.* Lecture Notes in Mathematics, Springer-Verlag, 437.

[6] H. Matsumura. *Commutative Algebra.* W.A. Benjamin Co., New York (1970).

[7] Yu.V. Nesterenko. *Introduction to algebraic independence theory.* Lecture Notes in Mathematics, 1752, Ed. Yu.V. Nesterenko, P. Philippon.

[8] Yu.V. Nesterenko. *Modular functions and transcendance problems.* Math. Sb., 187 (1996), 65-96.

[9] G. Philibert. *Une mesure d'indépendance algébrique.* Ann. Inst. Fourier (Grenoble) 38, 85-103, 1988.

[10] P. Philippon. *Sur les mesures d'indépendance algébrique.* Séminaire de théorie des nombres, Paris (1983-1984), Birkäuser, Progress in Math., vol. 59, 219-233.

[11] P. Philippon. *Une approche méthodique pour la transcendance et l'indépendance algébrique de valeurs de fonctions analytiques.* http ://www.mathp6.jussieu.fr/~pph.

[12] P. Philippon. *Critères pour l'indépendance algébrique.* Publications mathématiques de l'I.H.E.S. 64 (1986), 5-52.

[13] S. Ramanujan. *On certain arithmetical functions.* Trans. Cambridge Philosoph. Soc. 22 :9 (1916), 159-184.

[14] M. Reid. *Undergraduate Commutative Algebra.* London Mathematical Society, Student Texts 29.

[15] Th. Schneider. *Introduction aux nombres transcendants.* Gauthier-Villars, 1959.

[16] J-P. Serre. *Cours d'arithmétique.* Coll. SUP, PUF, 1970.

[17] M. Waldschmidt. *Sur la nature arithmétique des valeurs des fonctions modulaires.* Séminaire BOURBAKI, 49^{e} année, 1996-1997, n°824.

[18] Zariski et Samuel. *Commutative Algebra.* Van Nostrand.