Annexe : démonstration simplifiée de la transcendance de e[1]

On note D la dérivation d/dz. Pour une fonction f, on écrit aussi $f' = Df$ pour la dérivée de f, $f'' = D^2 f$ pour la dérivée seconde et $D^n = f^{(n)}$ pour la dérivée d'ordre n. Quand $n = 0$ on convient que $D^0 f = f$.

Soient N un entier positif et $f \in \mathbb{C}[z]$ un polynôme de degré $\leq N$. Le polynôme

$$F = \sum_{n\geq 0} D^n f = f + f' + f'' + \cdots + f^{(N)}$$

a le même degré que f et vérifie $F - DF = f$, ce qui peut être écrit

$$F = (1-D)^{-1} f \quad \text{où} \quad (1-D)^{-1} = \sum_{k\geq 0} D^k.$$

La dérivée de $e^{-z}F(z)$ est $-e^{-z}f(z)$, ce qui donne une des formes de ce qu'on appelle *l'identité d'Hermite* :

Lemme 1. *Pour $z \in \mathbb{C}$,*

$$\int_0^z e^{-t} f(t)dt = F(0) - e^{-z}F(z).$$

En utilisant le lemme 1 on peut écrire, pour $z \in \mathbb{C}$,

$$e^z F(0) = F(z) + e^z \int_0^z e^{-t} f(t)dt.$$

En choisissant convenablement le polynôme f, et en substituant à z un entier rationnel j, nous allons voir que $F(j)/F(0)$ est une bonne approximation rationnelle de e^j. Le polynôme f que l'on choisit est

$$f(t) = \frac{1}{(p-1)!} t^{p-1}(t-1)^p \cdots (t-m)^p,$$

où m et p sont deux entiers positifs. Ce polynôme f a pour degré $N = mp+p-1$, il a un zéro en chacun des points $1, \ldots, m$ de multiplicité p et il a un zéro en $t = 0$ de multiplicité $p-1$. Cela signifie que les nombres $f^{(n)}(j)$ sont nuls pour les couples (n, j) avec $0 \leq n \leq p-2$ et $j = 0$, et aussi pour ceux avec $0 \leq n \leq p-1$ et $1 \leq j \leq m$. On note aussi que $f^{(p-1)}(0) = (-1)^p m!^p$.

Nous allons vérifier que les nombres $F(0), \ldots, F(m)$ sont entiers (comme ci-dessus, F est la somme des dérivées de f).

La dérivée d'un polynôme de $\mathbb{Z}[X]$ est encore dans $\mathbb{Z}[X]$. En dérivant on peut faire apparaître des facteurs communs aux coefficients, comme le montre le lemme suivant.

[1] Michel Waldschmidt – Annexe au texte BibNum

Lemme 2. *Soit g un polynôme à coefficients entiers et soit k un entier ≥ 0. Alors les coefficients du polynôme $(1/k!)D^k g$ sont des entiers.*

Démonstration. Si on écrit $g(X) = \sum_{n\geq 0} a_n X^n$, alors

$$\frac{1}{k!}D^k g = \sum_{n\geq 0} a_n \binom{n}{k} X^n \quad \text{avec} \quad \binom{n}{k} = \frac{n!}{k!(n-k)!},$$

et les coefficients du binôme sont des entiers.

Du lemme 2 on déduit que pour tout polynôme $g \in \mathbb{Z}[X]$, pour tout entier $k \geq 0$ et pour tout entier $n \geq k$, le polynôme $(1/k!)D^n g$ est aussi dans $\mathbb{Z}[X]$.

Quand on utilise cela pour le polynôme

$$g(t) = (p-1)!f(t) = t^{p-1}(t-1)^p \cdots (t-m)^p$$

avec $k = p-1$, on en déduit $f^{(n)}(j) \in \mathbb{Z}$ pour tout $n \geq 0$ et tout $j \in \mathbb{Z}$ dans l'intervalle $0 \leq j \leq m$.

Ainsi, pour ce choix de f, les nombres $F(0)$ et $F(j)$ sont des entiers. Majorons maintenant le reste

$$e^j F(0) - F(j) = e^j \int_0^j e^{-t} f(t) dt$$

pour j entier dans l'intervalle $1 \leq j \leq m$. On combine l'inégalité

$$\sup_{0\leq t\leq m} |f(t)| < \frac{m^N}{(p-1)!}$$

avec l'encadrement

$$0 < \int_0^j e^{-t} dt = 1 - e^{-j} < 1,$$

ce qui donne

$$\left| \int_0^j e^{-t} f(t) dt \right| < \frac{m^N}{(p-1)!}.$$

Le théorème de Hermite sur la transcendance de e signifique que si $c_0, c_1, \ldots, c_m$ sont des nombres entiers rationnels, avec $c_0 \neq 0$, alors le nombre

$$C = c_0 + c_1 e + \cdots + c_m e^m$$

n'est pas nul. On choisit un entier p (qui sera supposé suffisamment grand en fonction de m, $c_0, \ldots, c_m$). On a donc

$$CF(0) = c_0 F(0) + c_1 F(1) + \cdots + c_m F(m) + \sum_{j=0}^m c_j e^j \int_0^j e^{-t} f(t) dt.$$

et

$$\left| \sum_{j=0}^m c_j e^j \int_0^j e^{-t} f(t) dt \right| < \sum_{j=0}^m |c_j| e^m \frac{m^N}{(p-1)!}.$$

L'entier m a été fixé au début, de même que les entiers $c_0, \dots, c_m$. Quand p tend vers l'infini, $m^{mp+p-1}/(p-1)!$ tend vers 0, donc pour p suffisamment grand on a

$$|c_0 F(0) + c_1 F(1) + \cdots + c_m F(m) - CF(0)| < 1.$$

Rappelons que le but est de démontrer $C \neq 0$. Il suffit pour cela de vérifier que l'entier $c_0 F(0) + c_1 F(1) + \cdots + c_m F(m)$ n'est pas nul, et la démonstration de ce fait pose des problèmes à Hermite : c'est pour cela qu'il fait intervenir des déterminants. Au lieu de prendre comme système d'exposants $(n_0, n_1, \dots, n_m)$ le $(m+1)$-uplet $(p-1, p, \dots, p)$ comme nous venons de le faire, il prend $m+1$ uplets distincts $(n_0, n_1, \dots, n_m)$ bien choisis qui lui donnent $m+1$ combinaisons linéaires à coefficients entiers de $c_0, \dots, c_m$ dont il montre qu'elles sont linéairement indépendantes. Comme l'un au moins des nombres $c_0, \dots, c_m$ n'est pas nul (on a même supposé $c_0 \neq 0$), ces $m+1$ combinaisons linéaires ne peuvent pas être toutes nulles.

Un argument de divisibilité a été introduit par Hilbert pour simplifier cette partie de la démonstration. Prenons maintenant pour p un nombre premier, suffisamment grand. On a

$$F(j) = f^{(p)}(j) + f^{(p+1)}(j) + \cdots + f^{(N)}(j) \in \mathbb{Z} \quad \text{pour } 1 \leq j \leq m$$

et

$$F(0) = f^{(p-1)}(j) + f^{(p)}(j) + \cdots + f^{(N)}(j) \in \mathbb{Z}.$$

De plus $f^{(k)}(j)$ est multiple de p pour $1 \leq j \leq m$ et $k \geq p$, tandis que $f^{(p-1)}(0) = (-1)^p m!^p$ n'est pas multiple de p. Par conséquent, puisque p est assez grand, le nombre

$$c_0 F(0) + c_1 F(1) + \cdots + c_m F(m),$$

qui est congru à $(-1)^p m!^p c_0$ modulo p, n'est pas multiple de p , donc n'est pas nul. Ceci complète la démonstration du théorème de Hermite sur la transcendance de e.

$\blacksquare$