Bibnum
Textes fondateurs de la science
Mathématiques | 2018

La méthode de Charles Hermite en théorie des nombres transcendants

Michel Waldschmidt

Édition électronique
URL : https://journals.openedition.org/bibnum/893
DOI : 10.4000/bibnum.893
ISSN : 2554-4470

Éditeur
FMSH - Fondation Maison des sciences de l'homme

Référence électronique
Michel Waldschmidt, « La méthode de Charles Hermite en théorie des nombres transcendants », *Bibnum* [En ligne], Mathématiques, mis en ligne le 01 avril 2009, consulté le 04 février 2023. URL : http://journals.openedition.org/bibnum/893 ; DOI : https://doi.org/10.4000/bibnum.893

La méthode de Charles Hermite
en théorie des nombres transcendants

par Michel Waldschmidt, professeur à l'Université Pierre et Marie Curie

Contexte historique

Quand Hermite publie en 1873 son mémoire, la démonstration par Liouville de l'existence de nombres transcendants remonte à moins de trente ans[1]. La théorie de l'irrationalité est bien maîtrisée, grâce à l'outil fondamental constitué par le développement en fractions continues. Euler avait développé cette théorie et explicité un certain nombre de tels développements, comme celui du nombre *e* en 1737. C'est la théorie des fractions continues qui permet à Johann Heinrich Lambert (1728-1777) de démontrer en 1761 l'irrationalité du nombre π — ses recherches sont explicitement motivées par la question de la quadrature du cercle, mais il ne prétend pas la résoudre et se contente d'une magnifique démonstration de *l'irrationalité de quantités circulaires et logarithmiques*[2]. Une autre approche de l'irrationalité est enseignée par Joseph Fourier[3] dans ses cours à l'École polytechnique en 1815 pour le nombre *e*, utilisant le développement de Taylor de la fonction exponentielle – cette méthode a été développée par Liouville trente ans avant qu'il n'exhibe les premiers exemples de nombres transcendants : par la méthode de Fourier, Liouville démontre l'irrationalité de e^2, puis il montre que ce nombre n'est pas quadratique, c'est-à-dire qu'il n'est pas solution d'une équation du second degré à coefficients rationnels. D'une certaine manière, on peut voir la démonstration de Hermite en 1873 comme une vaste généralisation de celles de Fourier et Liouville : au lieu d'approcher la fonction exponentielle par des polynômes, obtenus en tronquant le développement de la fonction exponentielle, Hermite va considérer des approximations par des fractions rationnelles.

C'est seulement un an après la publication du mémoire de Hermite que Georg Cantor introduira des arguments différents pour démontrer l'existence de

[1] Cette démonstration date de 1844 (voir texte BibNum correspondant à http://www.bibnum.education.fr/mathematiques/propos-de-lexistence-des-nombres-transcendants).
[2] Voir ce texte de Lambert commenté sur BibNum http://www.bibnum.education.fr/mathematiques/lambert-et-l%E2%80%99irrationalite-de-p-1761
[3] Cette démonstration de Fourier a été reprise par Janot de Stainville en 1812, voir le texte BibNum correspondant http://www.bibnum.education.fr/mathematiques/melange-danalyse-algebrique-et-de-geometrie.

nombres transcendants, basés sur sa théorie de l'infini. L'approche de Cantor connaîtra d'autres développements, conduisant à la théorie métrique de l'approximation diophantienne, dans laquelle on s'intéresse au comportement, du point de vue de l'approximation par des nombres rationnels, de "presque tous les nombres" (au sens de la mesure de Lebesgue – cela revient en quelque sorte à se demander ce qui se passe pour un nombre "pris au hasard").

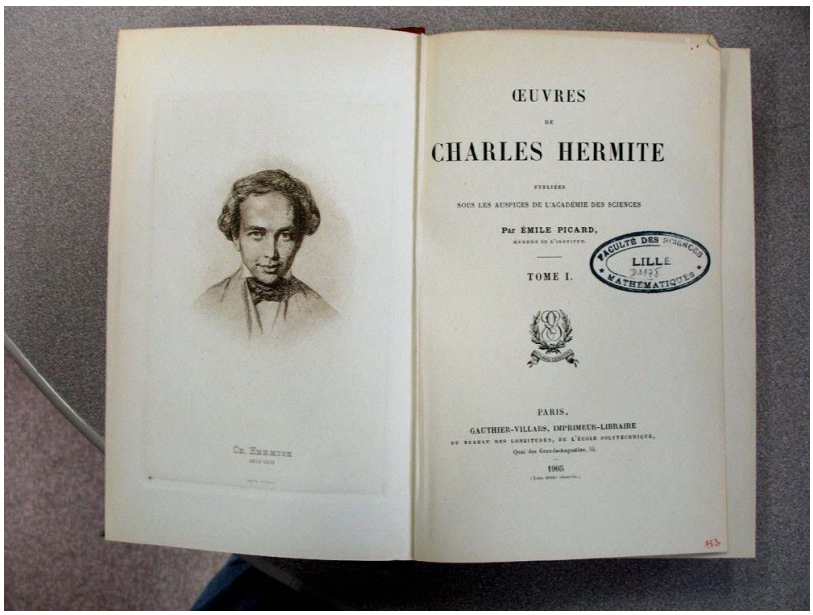

Figure 1 : Un portrait de Charles Hermite (1822-1901) jeune, sur l'édition de ses œuvres complètes. *Ces œuvres ont été éditées sous l'auspice de l'Académie des sciences, de 1905 à 1917, par son gendre Émile Picard, mathématicien, secrétaire perpétuel de l'Académie (cliché Alain Juhel).*

État de la question en 1873

– Irrationalité de e : L. Euler (1737)

– Irrationalité de e^r pour r nombre rationnel non nul, de log s pour s rationnel positif, de la tangente d'un nombre rationnel non nul, ce qui donne notamment l'irrationalité du nombre π : J.H. Lambert (1761)

– Démonstration de l'irrationalité de e par J. Fourier (1815), de e^2 par J. Liouville (1840) ; e^2 n'est pas quadratique.

– Existence de nombres transcendants par J. Liouville (1844, 1852)

- Le problème de la quadrature du cercle reste posé (les résultats de Wantzel sur les nombres constructibles datent de 1837).

Le mémoire de Hermite en 1873

Le résumé du texte de Hermite fait par le Dr Felix Müller[4] de Berlin dans le *Jahrbuch der Mathematik* (JFM 05.0248.01) est instructif. Il présente un problème qui peut être considéré comme une généralisation de la question de l'approximation diophantienne simultanée de nombres réels ou complexes : étant données des fonctions analytiques, on veut les approcher simultanément par des fractions rationnelles, ayant toutes le même dénominateur. L'approximation ici signifie que les développements de Taylor à l'origine auront les mêmes premiers termes. Müller poursuit en expliquant comment l'algèbre linéaire permet de s'assurer de l'existence d'une solution, sous des conditions naturelles concernant la qualité de l'approximation désirée, puis indique que l'auteur (Hermite) donne une solution explicite à ce problème dans le cas où les fonctions analytiques considérées sont des exponentielles. Dans ce résumé, Müller n'indique pas le résultat fondamental de l'article, qui est le fait que le nombre *e* est transcendant. Il est vrai que cet énoncé n'est formulé par Hermite qu'après 5 pages d'introduction (texte p. 22):

> *Je vais maintenant tenter d'aller plus loin à l'égard du nombre e, en établissant l'impossibilité d'une relation de la forme*
>
> $$N+ e^a N_1 + e^b N_2 +\ldots+ e^h N_n =0,$$
>
> *a, b, …, h étant des nombres entiers, ainsi que les coefficients N, N_1, …, N_n.*

Avant de formuler cet énoncé, il a indiqué comment il allait procéder, et mis en lumière que cela lui fournissait aisément une nouvelle démonstration du résultat de Lambert, selon lequel l'exponentielle d'un nombre rationnel non nul est un nombre irrationnel. L'approche de Hermite est novatrice, même s'il fait preuve, dans une lettre datée de 1873 adressée à Borchardt[5], d'une modestie exemplaire :

> *Tout ce que je puis, c'est de refaire ce qu'a déjà fait Lambert, seulement d'une autre manière.*

[4] Félix Müller (1843-1928) était un mathématicien et historien des mathématiques allemand.
[5] Karl Wilhelm Borchardt (1817-1880) était un mathématicien allemand, éditeur du *Journal de Crelle* à partir de 1856. La lettre de Hermite à Borchardt paraît dans cette revue lors du n°76, en 1873 (pp. 342-344) ; elle peut être vue en ligne dans la bibliothèque numérique de l'université de Göttingen http://gdz.sub.uni-goettingen.de/no_cache/dms/load/img/?IDDOC=266226.

La manière est en effet bien différente, et la voie ouverte par Hermite conduit à des énoncés que la méthode de Lambert ne permet pas d'atteindre. Pour sa démonstration de l'irrationalité de l'exponentielle d'un nombre rationnel non nul, Hermite approxime la fonction exponentielle par une fraction rationnelle. L'existence de polynômes A et B, de degrés contrôlés tels que les développements de Taylor à l'origine des deux fonctions e^z et A(z)/ B(z) aient les mêmes premiers termes, est facile à établir (voir encadré ci-après). Le premier tour de force de Hermite est de donner des formules explicites pour de tels polynômes. L'irrationalité de e^a quand a est un nombre rationnel non nul découle facilement de ces formules, en utilisant un critère d'irrationalité très simple : *soit x un nombre réel ; on suppose que pour tout $\varepsilon > 0$, il existe deux nombres entiers p et q avec $q > 0$ tels que $0 < |qx-p| < \varepsilon$. Alors x est irrationnel.*

Figure 2 : Cour d'honneur de la Sorbonne *(à gauche) et médaillon consacré à Charles Hermite, au-dessus d'une des portes (à droite). Hermite y fut titulaire de la chaire d'algèbre de 1871 à 1898 (cliché Alain Juhel).*

Approfondissement : les polynômes de degré contrôlé

L'existence de polynômes A et B, de degrés contrôlés, tels que les développements de Taylor à l'origine de e^z et $A(z)/B(z)$ aient les mêmes premiers termes, est facile à établir. Plus précisément, si n_0 et n_1 sont deux entiers positifs, l'algèbre linéaire montre qu'il existe deux polynômes A et B, de degrés majorés par n_0 et n_1 respectivement, tels que $B(0)$ ne soit pas nul et que les n_0+n_1+1 premiers termes du développement de Taylor à l'origine de e^z soient les mêmes que ceux de $A(z)/B(z)$.

Le premier tour de force de Hermite est de donner des formules explicites pour de tels polynômes, de contrôler les coefficients du point de vue arithmétique, et de contrôler le reste en valeur absolue. Le dénominateur B peut être écrit de plusieurs manières (équivalentes) légèrement différentes, avec $N = n_0 + n_1$:

$$\begin{aligned} B(z) &= \sum_{\ell=0}^{n_1} (-1)^\ell \binom{n_0+\ell}{\ell} \frac{n_1!}{(n_1-\ell)!} z^{n_1-\ell} \\ &= (-1)^{n_1} \frac{n_1!}{n_0!} \sum_{h=0}^{n_1} (-1)^h \frac{(N-h)!}{(n_1-h)!h!} z^h \\ &= \sum_{k=n_0}^{N} z^{N-k} D^k f(0), \end{aligned}$$

où

$$f(t) = \frac{1}{n_0!} t^{n_0} (t-1)^{n_1}.$$

Le reste $R(z) = B(z)e^z - A(z)$ est donné par

$$R(z) = \sum_{k \geq N+1} \frac{(k-n_0-1)!}{(k-N-1)!k!} z^k = z^{N+1} e^z \int_0^1 e^{-tz} f(t) dt.$$

On déduit une formule explicite pour A à partir de celle pour B, en écrivant $A(-z)e^z - B(-z) = -e^z R(-z)$:

$$A(z) = (-1)^{n_1} \sum_{h=0}^{n_0} \frac{(N-h)!}{(n_0-h)!h!} \cdot z^h.$$

Comme nous l'avons dit, après ce brillant début, Hermite annonce son intention d'aller plus loin en montrant que le nombre *e* ne vérifie aucune relation polynomiale – autrement dit *le nombre* e *est transcendant*. Il s'agit donc de montrer que les puissances consécutives de *e* sont des nombres linéairement indépendants sur le corps $\mathbb{Q}$ des nombres rationnels. Le critère d'indépendance linéaire que va utiliser Hermite est simple : soient $x_1,\ldots,x_n$ des nombres réels ; par définition, dire que les nombres $1,x_1,\ldots,x_n$ sont linéairement indépendants sur $\mathbb{Q}$ signifie que si a_0, $a_1,\ldots$, a_n sont des nombres entiers non tous nuls, alors le nombre

$$L = a_0+a_1x_1+\ldots+a_nx_n$$

n'est pas nul. Pour cela, on cherche à approcher simultanément les nombres x_1, $\ldots,x_n$ par des nombres rationnels : si on montre l'existence de nombres entiers rationnels b_0, $b_1,\ldots$, b_n tels que les quantités

$$\varepsilon_i = b_0x_i - b_i \quad (i=1,\ldots n) \quad \text{et} \quad R = a_1\varepsilon_1+\ldots+a_n\varepsilon_n$$

vérifient $0<|R|<1$, alors $L \neq 0$. Cela résulte de l'observation que le nombre

$$A= a_0b_0+a_1b_1+\ldots+a_nb_n$$

est un entier rationnel satisfaisant $b_0L= A+R$.

Pour Hermite, les x_i sont des puissances entières de *e*. Afin de les approcher simultanément par des nombres rationnels, Hermite recherche des approximations simultanées, par des fractions rationnelles, des puissances entières de la fonction exponentielle, puis substitue z = 1 dans ses formules analytiques.

Ainsi, une étape essentielle de la démonstration d'Hermite consiste à expliciter des fractions rationnelles, ayant le même dénominateur, qui approchent les fonctions exponentielles. La solution qu'il apporte à ce problème original est admirable : ce qu'il obtient est le premier exemple de ce qu'on appelle maintenant *approximants de Padé*, du nom de son disciple Henri Eugène Padé (1863-1953), qui développera systématiquement la théorie de l'approximation de fonctions analytiques par des fractions rationnelles. Les formules intégrales que produit Hermite sont maintenant classiques, elles ont de multiples applications.

Approfondissement : les approximations de l'exponentielle par des fractions rationnelles

Ainsi, une étape essentielle de la démonstration d'Hermite consiste à expliciter des fractions rationnelles, ayant le même dénominateur, qui approchent les fonctions exponentielles. On veut approcher simultanément les fonctions $e^z, e^{2z}, \ldots, e^{mz}$ par des fractions rationnelles

$$\frac{\Phi_1(z)}{\Phi(z)}, \frac{\Phi_2(z)}{\Phi(z)}, \ldots, \frac{\Phi_m(z)}{\Phi(z)}$$

On choisit des entiers $n_0, n_1, , \ldots, n_m$ et on introduit le polynôme

$$f(t) = \frac{1}{n_0!} t^{n_0} (t-1)^{n_1} \cdots (t-m)^{n_m}$$

dont le degré est $N = n_0 + n_1 + \cdots + n_m$. Alors le polynôme

$$\Phi(z) = \sum_{k=n_0}^{N} z^{N-k} D^k f(0),$$

a pour degré $N - n_0$, pour $1 \leq j \leq m$ le polynôme

$$\Phi_j(z) = \sum_{k=n_j}^{N} z^{N-k} D^k f(j),$$

a pour degré $N - n_j$, tandis que les restes

$$R_j(z) = \Phi(z)e^z - \Phi_j(z) \quad (1 \leq j \leq m)$$

sont donnés par

$$R_j(z) = z^{N+1} e^{jz} \int_0^j e^{-tz} f(t) dt.$$

Une fois que Hermite dispose de ces approximations par des fractions rationnelles et qu'il substitue z = 1 dans ces formules de façon à exhiber des approximations numériques, il lui reste une étape qui lui demande encore des efforts : dans le critère d'indépendance linéaire que nous avons énoncé, il est crucial de vérifier que le reste R n'est pas nul[6]. On lit dans le texte (p. 77):

> *… on ne peut, en général, admettre que le déterminant Δ proposé s'annule,…*

puis, quelques lignes plus loin :

[6] En effet, même si la démonstration conduit au fait que |R| < 1, on doit aussi vérifier R ≠ 0, car sinon la relation $b_0 L = A + R$ ne permet pas de conclure.

Mais une autre voie conduira à une démonstration plus rigoureuse…

Ainsi Hermite n'arrive pas à démontrer que son déterminant Δ n'est pas nul : cela lui suffirait pour conclure, mais il y a là une vraie difficulté. Pour la contourner, il lui faut développer de nouveaux arguments pour lesquels il cite le travail de Liouville en 1844, où l'existence de nombres transcendants a été démontrée.

Impact du mémoire de Hermite

Une des motivations principales des travaux d'irrationalité et de transcendance jusqu'au XIXè siècle était le problème de la quadrature du cercle : on savait que, pour le déclarer insoluble, il suffisait de démontrer la transcendance du nombre π, et c'est F. Lindemann qui parviendra à ce résultat en 1882. Hermite avait écrit à Borchardt en 1873 (lettre déjà mentionnée, 1873) :

> *Je ne me hasarderai point à la recherche d'une démonstration de la transcendance du nombre π. Que d'autres tentent l'entreprise. Nul ne serait plus heureux que moi de leur succès. Mais, croyez m'en, mon cher ami, il ne laissera pas que de leur en coûter quelques efforts.*

Avec le recul du temps, on peut considérer que toutes les idées nécessaires pour parvenir à ce résultat étaient pourtant en germe dans le mémoire de Hermite. Cependant, il ne faut pas oublier qu'il a quand même fallu près de dix ans pour que la méthode de Hermite soit généralisée de façon à s'adapter au nombre π, et plus généralement à la démonstration du théorème de Hermite-Lindemann : *si γ est un nombre algébrique non nul, alors e^{γ} est un nombre transcendant.* De façon équivalente, *si α est un nombre algébrique non nul* et si log α est une détermination quelconque[7] (mais non nulle au cas où $\alpha = 1$) du logarithme de α, *alors log α est un nombre transcendant.*

Cet énoncé a été encore généralisé par Lindemann et Weierstrass en un résultat d'indépendance algébrique pour des valeurs de la fonction exponentielle en des points algébriques linéairement indépendants. La recherche de simplifications des démonstrations de Hermite et Lindemann occupera de brillants mathématiciens comme Adolf Hurwitz (1859-1919), Paul Gordan (1837-

[7] Un nombre complexe t est un logarithme d'un nombre complexe non nul z si $e^t = z$. Tout nombre complexe non nul z admet une infinité de logarithmes, si l'un est t, les autres sont de la forme $t + 2ik\pi$ avec k entier rationnel (positif, négatif ou nul). Comme $e^0 = 1$, le seul nombre admettant t = 0 comme logarithme est z = 1.

1912), David Hilbert (1862-1943) : en 1932, Henri Lebesgue fera une analyse pertinente de leurs apports respectifs. On peut maintenant donner des démonstrations très courtes de la transcendance de *e* (comme par exemple celle qui est donnée en annexe) et de π, mais on ne comprendra vraiment ce qui se passe qu'en se référant au texte de Hermite.

Figure 3 : Charles Hermite (1822-1901), en 1887. *Hermite était ancien élève de l'École polytechnique. Il avait épousé la soeur du mathématicien Joseph Bertrand (1822-1900), secrétaire perpétuel de l'Académie des sciences de 1874 à sa mort, et sa fille épousera le mathématicien Émile Picard (1856-1941), secrétaire perpétuel de l'Académie des sciences de 1917 à sa mort.*

La méthode de Hermite, Lindemann et Weierstrass a été enrichie par les travaux de C.L. Siegel en 1929, avant que A.O. Gelfond et Th. Schneider ne démontrent la transcendance de nombres de la forme a^b ou de la forme $\log a_1 / \log a_2$ pour a, b, a_1, a_2 nombres algébriques, résolvant ainsi le septième des problèmes de Hilbert (anticipé par Euler qui avait suggéré un tel énoncé – voir la fin de l'*Introductio in Analysin Infinitorum*[8]). La théorie des nombres transcendants s'est considérablement développée au XX^{è} siècle, donnant lieu à de nombreuses applications, notamment par ses liens avec d'autres questions diophantiennes (approximation, géométrie, équations). D'une certaine manière, on peut considérer que toutes les méthodes de transcendance qui ont été développées après Hermite ont leurs racines dans son mémoire fondamental de

[8] On peut se référer à http://www.math.dartmouth.edu/~euler/pages/E101.html pour ce texte.

1873 : les idées essentielles s'y trouvent. Les outils élaborés ensuite font appel à de nombreuses branches des mathématiques, mais la stratégie de base est celle qui a été proposée par Hermite.

Dans une notice nécrologique de Hermite, Paul Painlevé écrira :

Mais la découverte d'Hermite qui surpasse toutes les autres, c'est la démonstration de la transcendance du nombre e, démonstration qui, à peine modifiée, entraîne la transcendance du nombre π, c'est-à-dire l'impossibilité du fameux problème de la quadrature du cercle…

… sa méthode sera admirée tant que des hommes existeront capables de comprendre la notion de nombre.

Conclusion

Les méthodes de transcendance ont toutes leur fondement dans ces travaux de Charles Hermite en 1873. On connaissait alors depuis une trentaine d'années des exemples de nombres transcendants, grâce aux travaux de Joseph Liouville, mais ceux qu'il avait exhibés étaient artificiels, spécialement construits pour satisfaire des contraintes d'approximation diophantienne très strictes. La démonstration par Georg Cantor de l'existence de beaucoup de nombres transcendants était nettement moins explicite. Hermite est le premier à démontrer la transcendance d'une constante fondamentale de l'analyse. Sa démonstration allait être exploitée en 1881 par Ferdinand Lindemann, qui donnait ainsi la réponse définitive au problème de la quadrature du cercle. Parmi les mathématiciens de tous les temps, il en est peu qui aient ainsi exercé une influence directe comparable à celle d'Hermite ; il n'en est pas dont l'œuvre soit plus sûrement impérissable.

■

(Note de l'éditeur : le caractère assez ardu pour le grand public du texte de Hermite n'a pas permis d'en faire un commentaire pas à pas ; toutefois, nous avons souhaité faire figurer en complément, pour le lecteur BibNum, une démonstration simplifiée de la transcendance de e, ci-après, toujours par Michel Waldschmidt) (Nous remercions Alain Juhel, par ailleurs auteur BibNum, pour ses clichés photographiques http://home.nordnet.fr/~ajuhel/Hermite/Hermite.html)

Annexe : démonstration simplifiée de la transcendance de e

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 $f^{(p-1)}(0) = (-1)^{pm} m!^p$.

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.

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 $c_0, \ldots, c_m$. Quand p tend vers l'infini, $m^{mp+p-1}/(p-1)!$ tend vers 0, donc pour p suffisamment grand on a

$$|c_0F(0) + c_1F(1) + \cdots + c_mF(m) - CF(0)| < 1.$$

Rappelons que le but est de démontrer $C \neq 0$. Il suffit pour cela de vérifier que l'entier $c_0F(0) + c_1F(1) + \cdots + c_mF(m)$ 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 $(n_0, n_1, \ldots, n_m)$ le $(m+1)$-uplet $(p-1, p, \ldots, p)$ comme nous venons de le faire, il prend $m+1$ uplets distincts $(n_0, n_1, \ldots, n_m)$ bien choisis qui lui donnent $m+1$ combinaisons linéaires à coefficients entiers de $c_0, \ldots, c_m$ dont il montre qu'elles sont linéairement indépendantes. Comme l'un au moins des nombres $c_0, \ldots, c_m$ 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

$$c_0F(0) + c_1F(1) + \cdots + c_mF(m),$$

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.

■

Annexe : démonstration simplifiée de la transcendance de e

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 $f^{(p-1)}(0) = (-1)^{pm} m!^p$.

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.

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 $c_0, \ldots, c_m$. Quand p tend vers l'infini, $m^{mp+p-1}/(p-1)!$ tend vers 0, donc pour p suffisamment grand on a

$$|c_0F(0) + c_1F(1) + \cdots + c_mF(m) - CF(0)| < 1.$$

Rappelons que le but est de démontrer $C \neq 0$. Il suffit pour cela de vérifier que l'entier $c_0F(0) + c_1F(1) + \cdots + c_mF(m)$ 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 $(n_0, n_1, \ldots, n_m)$ le $(m+1)$-uplet $(p-1, p, \ldots, p)$ comme nous venons de le faire, il prend $m+1$ uplets distincts $(n_0, n_1, \ldots, n_m)$ bien choisis qui lui donnent $m+1$ combinaisons linéaires à coefficients entiers de $c_0, \ldots, c_m$ dont il montre qu'elles sont linéairement indépendantes. Comme l'un au moins des nombres $c_0, \ldots, c_m$ 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

$$c_0F(0) + c_1F(1) + \cdots + c_mF(m),$$

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.