Théorème d'Hermite-Lindeman

20 mars 2014

1 Enoncé

Théorème 1 (Théorème d'Hermite-Lindeman)**.** *Si a est un nombre complexe algébrique non nul, alors e^a est transcendant.*

2 Pré-requis

Lemme 1 (Lemme 1)**.** *Soit $P \in \mathbb{C}[X]$ de degré k, $Q_P = \sum_{j=0}^{k} P^{(j)}$, où $P^{(j)}$ est la $j^{ième}$ dérivée de P et $\alpha \in \mathbb{C}$ alors :*

$$\int_0^1 \alpha e^{-\alpha x} P(\alpha x) dx = Q_P(0) - e^{-\alpha} Q_P(\alpha). \tag{1}$$

Démonstration. Par intégration par parties des parties réelles et imaginaires. □

Lemme 2 (Lemme 2)**.** *Soit $R \in \mathbb{Z}[X]$ et soit $P = \frac{X^{p-1}}{(p-1)!}[R(X)]^p$, où p est un entier non nul, alors :*

1. *$P^{(p-1)}(0) = [R(0)]^p$.*
2. *Pour tout $r \geq p$, $P^{(r)} \in \mathbb{Z}[X]$ et ses coefficients sont des multiples de p.*

Démonstration. On montre facilement que pour tout $r \in \mathbb{N}$ et tout $0 \leq i \leq r$, on a $(X^r)^{(i)} = i! \times C_r^i X^{r-i}$.
Ainsi $\left(\frac{X^{p-1}}{(p-1)!}\right)^{(i)} = \frac{X^{p-1-i}}{(p-1-i)!}$ pour tout $0 \leq i \leq p-1$. On a également $(R(X)^p)^{(i)} = \left[pR(X)^{p-1}R(X)'\right]^{(i-1)}$ pour tout $i \geq 1$. On en déduit :

$$P^{(p-1)}(X) = \sum_{i=0}^{p-2} C_{p-1}^i \frac{X^{p-1-i}}{(p-1-i)!} \left[pR(X)^{p-1}R(X)'\right]^{(p-2-i)} + R(X)^p,$$

d'où $P^{(p-1)}(0) = [R(0)]^p$.
De plus, on montre facilement pour $r \geq p$:

$$P^{(r)}(X) = \sum_{i=0}^{p-1} C_r^i \frac{X^{p-1-i}}{(p-1-i)!} \left[pR(X)^{p-1}R(X)'\right]^{(r-i-1)}.$$

D'après $\left(X^r\right)^{(i)} = i! \times C_r^i X^{r-i}$, on montre que $\left[pR(X)^{p-1}R(X)'\right]^{(r-i-1)}$ a ses coefficients multiples de $(r-i-1)!$ qui est divisible par $(p-1-i)!$ donc $P^{(r)} \in \mathbb{Z}[X]$ et ses coefficients sont des multiples de p. □

Definition 1. *Soit A anneau commutatif.*
Un polynôme $P \in A[X_1, \ldots, X_n]$ est dit symétrique si pour toute permutation $\sigma \in S_n$, $P(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) = P(X_1, \ldots, X_n)$.
Les polynômes symétriques élémentaires $\sigma_1, \ldots, \sigma_n$ sont définis par :

$$\sigma_k(X_1, \ldots, X_n) = \sum_{1 \leq i_1 < i_2 < \ldots < i_k \leq n} X_{i_1} \times X_{i_2} \times \ldots \times X_{i_k}. \tag{2}$$

Proposition 1. *A anneau commutatif. Si $P \in A[X_1, \ldots, X_n]$ est symétrique, alors il existe $S \in A[X_1, \ldots, X_n]$ tel que :*

$$P(X_1, \ldots, X_n) = S(\sigma_1(X_1, \ldots, X_n), \ldots, \sigma_n(X_1, \ldots, X_n)). \tag{3}$$

Definition 2 (Entier algébrique)**.** *Un nombre algébrique est un entier algébrique s'il est racine d'un polynôme de $\mathbb{Z}[X]$ dont le coefficients dominant est* 1*.*

Lemme 3. *Soit $\beta_1, \ldots, \beta_n$ des entiers algébriques. Pour tout $1 \leq k \leq n$ et $(i_1, \ldots, i_k)$ un k-uplet d'entiers tels que $1 \leq i_1 < i_2 < \ldots < i_k \leq n$, on définit $\alpha_{k,(i_1,\ldots,i_k)} = \beta_{i_1} + \ldots + \beta_{i_k}$. Alors le polynôme :*

$$\Lambda(X) = \prod_{k=1}^{n} \prod_{1 \leq i_1 < \ldots < i_k \leq n} (X - \alpha_{k,(i_1,\ldots,i_k)}),$$

est à coefficients entiers.

Démonstration. Les coefficients de $\Lambda(X)$ sont des polynômes symétriques en les $\alpha_{k,(i_1,\ldots,i_k)}$, on remarque de plus que les $\alpha_{k,(i_1,\ldots,i_k)}$ sont invariants par permutation des $\beta_1, \ldots, \beta_n$, donc les coefficients de $\Lambda(X)$ sont des polynômes symétriques en $\beta_1, \ldots, \beta_n$. On en déduit que les coefficients de $\Lambda(X)$ sont de la forme $S(\sigma_1(\beta_1, \ldots, \beta_n), \ldots, \sigma_n(\beta_1, \ldots, \beta_n))$ et comme les $\sigma_k(\beta_1, \ldots, \beta_n)$ sont entiers alors les coefficients sont entiers. □

Lemme 4. *Si a est un nombre algébrique alors il existe un entier c non nul tel que ca soit un entier algébrique.*

Démonstration. Si a_n est le coefficient dominant du polynôme minimal sur $\mathbb{Z}$ de a, prendre $c = a_n$. □

3 Théorème d'Hermite-Lindeman

Théorème 2 (Théorème d'Hermite-Lindeman)**.** *Si a algébrique non nul, alors e^a est transcendant.*

Démonstration. On va montrer que si e^a est algébrique différent de 1, alors a est transcendant.
Soit e^a algébrique et $f(X) = a_m X^m + \ldots + a_0 \in \mathbb{Z}[X]$ son polynôme minimal. Supposons que a est algébrique, alors il existe c entier non nul tel que ca soit un entier algébrique. Soit alors $\varphi(X) = X^n + b_{n-1}X^{n-1} + \ldots + b_0$ son polynôme minimal (sur $\mathbb{Z}$) et $c\beta_i$ pour $1 \leq i \leq n$ ses racines (un résultat connu nous dit que les racines d'un polynôme irréductibles sont distinctes). Il existe un q tel que $\beta_q = a$, et comme $f(e^a) = 0$, on en déduit :

$$\prod_{j=1}^{n} f(e^{\beta_j}) = 0. \tag{4}$$

Le produit précédent peut être développé en une somme du type :

$$0 = a_0^n + \sum \lambda_j e^{\alpha_j},$$

où α_j est de la forme $\mu_1\beta_1 + \ldots + \mu_n\beta_n$ avec $1 \leq \mu_k \leq m$. Pour $1 \leq l \leq m$, soit $\#l$ le nombre de μ_k égaux à l. On montre facilement que $\lambda_j = a_m^{\#m} \ldots a_1^{\#1} a_0^{n-\sum_{l=1}^{m} \#l}$.
Ainsi le produit (4) se développe en une somme du type :

$$a_0^n + \sum_{i=1}^{s} \lambda_i \sum_{j=1}^{r_i} e^{\alpha_{i,j}} = 0, \tag{5}$$

où pour un i donné, tous les $\alpha_{i,j}$ ont la même composition en termes de $\#l$. On remarque facilement que $\displaystyle\sum_{j=1}^{r_i} e^{\alpha_{i,j}}$ est un polynôme symétrique des β_i. Cette remarque nous sera d'une grande utilité.
Soit $\Lambda(X) = \displaystyle\prod_{i=1}^{s}\prod_{j=1}^{r_i}(X - c\alpha_{i,j})$. Les coefficients de $\displaystyle\prod_{j=1}^{r_i}(X - c\alpha_{i,j})$ sont des polynômes symétriques en $c\alpha_{i,j}$ et donc sont des polynômes en $c\beta_i$. D'après la remarque précédente, ils sont symétriques en $c\beta_i$ donc les coefficients de $\displaystyle\prod_{j=1}^{r_i}(X - c\alpha_{i,j})$ sont fonctions polynômiales des polynômes symétriques pris en $c\beta_i$. Comme les $c\beta_i$ sont racines d'un polynômes de $\mathbb{Z}$ à coefficients dominant 1, alors les coefficients de $\displaystyle\prod_{j=1}^{r_i}(X - c\alpha_{i,j})$ sont entiers. On en déduit que $\Lambda(X) \in \mathbb{Z}[X]$ et comme c est entier, $\Lambda(cX) \in \mathbb{Z}[X]$.
Posons $P(X) = \dfrac{X^{p-1}}{(p-1)!}\left[\Lambda(cX)\right]^p$ et Q_P la somme de ses dérivées comme con-

struite dans le Lemme 1. De :

$$\int_0^1 \alpha e^{-\alpha x} P(\alpha x) dx = Q_P(0) - e^{-\alpha} Q_P(\alpha),$$

on en déduit :

$$Q_P(\alpha) + R_P(\alpha) = e^{\alpha} Q_P(0),$$

avec :

$$R_P(\alpha) = \alpha e^{\alpha} \int_0^1 e^{-\alpha x} P(\alpha x) dx.$$

En utilisant l'égalité (5), on a alors :

$$a_0^n Q_P(0) + \sum_{i=1}^{s} \lambda_i \sum_{j=1}^{r_i} (Q_P(\alpha_{i,j}) + R_P(\alpha_{i,j})) = 0,$$

qui s'écrit :

$$a_0^n Q_P(0) + \sum_{i=1}^{s} \lambda_i \sum_{j=1}^{r_i} Q_P(\alpha_{i,j}) = -\sum_{i=1}^{s} \lambda_i \sum_{j=1}^{r_i} R_P(\alpha_{i,j}). \tag{6}$$

Nous allons montrer que cette dernière égalité est impossible.

Première étape : si p est un nombre premier suffisamment grand, alors le membre de gauche est non nul

Les $\alpha_{i,j}$ sont racines d'ordre au moins p de P, ainsi $Q_P(\alpha_{i,j}) = P^{(p)}(\alpha_{i,j}) + \ldots + P^{(\deg P)}(\alpha_{i,j})$, qui est un polynôme en $\alpha_{i,j}$ à coefficients entiers multiples de p. Le polynôme $\sum_{j=1}^{r_i} Q_P(\alpha_{i,j})$ est symétrique en $\alpha_{i,j}$. Comme pour i fixé, les $\alpha_{i,j}$ sont racines de $\prod_{j=1}^{r_i}(cX - c\alpha_{i,j}) \in \mathbb{Z}[X]$, alors $\sum_{j=1}^{r_i} Q_P(\alpha_{i,j})$ est un rationnel ainsi $\sum_{i=1}^{s} \lambda_i \sum_{j=1}^{r_i} Q_P(\alpha_{i,j})$ est également un rationnel $\frac{a}{b}$ avec a et b premiers entre eux. Mais $\sum_{i=1}^{s} \lambda_i \sum_{j=1}^{r_i} Q_P(\alpha_{i,j})$ est également de la forme px. Il s'ensuit que x est un rationnel $\frac{y}{z}$ avec y et z premier entre eux. On montre également que si p est premier, on peut choisir z premier avec p. En effet, si p est un nombre premier figurant dans la décomposition de z, alors px est de la forme $\frac{y}{z'}$, mais comme les $P^{(k)}(X)$ ont des coefficients multiples de p dès que $k \geq p$, alors px peut être choisi de la forme $p\frac{y'}{z'}$.

De même 0 est racine d'ordre au moins $p-1$ de P, on en déduit que $Q_P(0)$ est égal à la somme de $[\Lambda(0)]^p$ et le produit de p par un rationnel de dénominateur premier avec p. Ainsi :

$$a_0^n Q_P(0) + \sum_{i=1}^{s} \lambda_i \sum_{j=1}^{r_i} Q_P(\alpha_{i,j}) = a_0^n [\Lambda(0)]^p + p\frac{u}{v},$$

où u et v sont premiers entre eux et v premier avec p. Choisissant p nombre premier strictement plus grand que $|v|$, $|a_0|$ et les coefficients de $\Lambda(cX)$ et appliquant le théorème de Bezout à $va_0^n[\Lambda(0)]^p + pu$, on en déduit qu'il existe p nombre premier tel que :

$$a_0^n Q_P(0) + \sum_{i=1}^{s} \lambda_i \sum_{j=1}^{r_i} Q_P(\alpha_{i,j}) > 0. \tag{7}$$

Deuxième étape : le membre de droite tend vers 0 **lorsque** p **tend vers l'infini**
Par une simple majoration d'intégrale. On laisse au lecteur de vérifier le résultat.
Conclusion : Le membre de gauche est un entier positif pour p suffisamment grand tandis que le membre de droite tend vers 0 si p tend vers l'infini. Ceci est contradictoire donc a est transcendant. □

Corollaire 1 (Théorème d'Hermite)**.** *e est transcendant.*

Démonstration. 1 est évidemment un nombre algébrique non nul d'où le résultat. □

Remarque : Le théorème d'Hermite a été démontré en 1873 par Hermite 10 ans avant le théorème d'Hermite-Lindemann (1882). Historiquement, ce n'est donc pas un corrolaire du théorème d'Hermite-Lindemann. La démonstration du théorème d'Hermite est plus simple que celle du théorème d'Hermite-Lindemann et n'utilise que les 2 premiers lemmes.

Corollaire 2 (Théorème de Lindemann)**.** *π est transcendant.*

Démonstration. $e^{i\pi} = -1$ est évidemment algébrique différent de 1, ainsi $i\pi$ est transcendant. Comme i est algébrique et que l'ensemble des nombres algébriques est un corps, alors π est transcendant. □