Les nombres transcendants

Gaëtan Bayle des Courchamps

Janvier 2003
(révision 17 Mars 2003)

Table des matières

1 Introduction

Cet article couvre les principaux résultats sur les nombres transcendants, d'où nous pourrons déduire aisément, en particulier, que π et e sont transcendants.
Nous utiliserons pour cela le théorème de Lindemann, qui est démontré dans la section 3 page 3.

Définition 1.1 (Nombre algébrique, nombre transcendant) *Soit* $\mathbf{K}$ *un sous-corps de* $\mathbf{C}$. *On dit qu'un complexe* $x \in \mathbf{C}$ *est* algébrique *sur* $\mathbf{K}$ *(en abrégé* $\mathbf{K}$*-algébrique) s'il existe un polynôme non-constant* $P \in \mathbf{K}[X]$ *tel que* $P(x) = 0$.
En général, si un nombre est $\mathbf{Q}$*-algégrique on dit qu'il est* algébrique*, tout court.*
On appelle nombre transcendant *tout élément de* $\mathbf{C}$ *qui n'est pas algébrique sur* $\mathbf{Q}$.

Définition 1.2 (Extension de corps; degré d'une extension) *Soit* $\mathbf{K}$ *un sous-corps de* $\mathbf{C}$*, et* A *une partie de* $\mathbf{C}$. *On note* $\mathbf{K}(A)$ *l'intersection de tout les sous-corps de* $\mathbf{C}$ *qui incluent* $\mathbf{K}$ *et* A*, i.e. le plus petit de ces sous-corps au sens de l'inclusion.*
Si $\mathbf{K}$ *et* $\mathbf{L}$ *sont deux sous-corps de* $\mathbf{C}$ *tels que* $\mathbf{K} \subset \mathbf{L}$*, on note* $[\mathbf{L} : \mathbf{K}]$ *la dimension (éventuellement* $+\infty$*) de* $\mathbf{L}$ *considéré comme un* $\mathbf{K}$*-espace vectoriel.*

Proposition 1.3 (Multiplicativité du degré) *Si* $\mathbf{K}$*,* $\mathbf{L}$*,* $\mathbf{M}$ *sont trois sous-corps de* $\mathbf{C}$ *tels que* $\mathbf{K} \subset \mathbf{L} \subset \mathbf{M}$*, alors :*

$$[\mathbf{M} : \mathbf{K}] = [\mathbf{M} : \mathbf{L}][\mathbf{L} : \mathbf{K}]$$

Proposition 1.4 (Commutativité des extensions de corps) *Pour tout sous-corps* $\mathbf{K}$ *de* $\mathbf{C}$*, pour toutes parties* A *et* B *de* $\mathbf{C}$ *:*

$$\mathbf{K}(A)(B) = \mathbf{K}(B)(A) = \mathbf{K}(A \cup B)$$

Preuve : $\mathbf{K}(A)(B)$ inclue $A \cup B$, donc $\mathbf{K}(A \cup B) \subset \mathbf{K}(A)(B)$, par définition.
On a aussi $\mathbf{K}(A) \subset \mathbf{K}(A \cup B)$ et $B \subset \mathbf{K}(A \cup B)$, donc par définition de $\mathbf{K}(A)(B)$: $\mathbf{K}(A)(B) \subset \mathbf{K}(A \cup B)$.
Par double inclusion, on en déduit l'égalité recherchée. ∎

Exercice 1.5 (Le corps des nombres K-algébriques) *Nous allons montrer successivement que :*
- *pour tout sous-corps* $\mathbf{K}$ *de* $\mathbf{C}$*, si* $x \in \mathbf{C}$ *est algébrique sur* $\mathbf{K}$*, alors il existe un unique polynôme unitaire* $P \in \mathbf{K}[X]$*, de degré minimal* $n \geq 1$*, tel que* $P(x) = 0$*.*
- *et que* P *est alors irréductible.*
- *alors* $\mathbf{K}(x) = E$ *avec* $E = \{A(x) \mid A \in \mathbf{K}[X], \text{degre}(A) < n\}$
- *et de plus* $[\mathbf{K}(x) : \mathbf{K}] = n$*.*
- *pour tout sous-corps* $\mathbf{K}$ *de* $\mathbf{C}$*,* x *est algébrique sur* $\mathbf{K}$ *ssi* $[\mathbf{K}(x) : \mathbf{K}] < +\infty$*.*
- k *nombres* $\alpha_1, \ldots, \alpha_k$ *sont* $\mathbf{K}$*-algébriques ssi* $[\mathbf{K}(\alpha_1, \ldots, \alpha_k) : \mathbf{K}] < +\infty$*.*
- *l'ensemble des nombres* $\mathbf{K}$*-algébriques est un corps.*
- *ce corps est algébriquement clos.*

Solution : • Comme x est algébrique, l'existence de P est immédiate. Soit n le plus petit entier ≥ 1 tel qu'il existe un polynôme $P \in \mathbf{K}[X]$ dont x est racine (P et n existent puisque x est algébrique).
Soit $A \in \mathbf{K}[X]$, unitaire et de degré n, tel que $A(x) = 0$. La division euclidienne de A par P donne $A = PQ + R$ avec $\text{degre}(R) < n$. Or $P(x) = A(x) = 0$ donc $R(x) = 0$; alors par définition de n : $\text{degre}(R) \leq 0$; or $R(x) = 0$ donc $R = 0$. Finalement $B = PQ$ est multiple de P.
Or A est unitaire et de degré n, donc $A = P$, d'où l'unicité.
• Si $P = AB$ avec $(A, B) \in \mathbf{K}[X] \times \mathbf{K}[X]$, $\text{degre}(A) \geq 1$ et $\text{degre}(B) \geq 1$, alors $A(x) = 0$ ou $B(x) = 0$, donc P ne serait pas de degré minimal : absurde. Donc P est irréductible dans $\mathbf{K}[X]$.
• Comme $\mathbf{K}(x)$ est un corps on a clairement $E \subset \mathbf{K}(x)$.
Remarquons que, pour tout polynôme $A \in \mathbf{K}[X]$, $A(x) \in E$. En effet, $P(x) = 0$ entraîne $A(x) = R(x)$, où R est le reste de la division euclidienne de A par P. Or $\text{degre}(R) < n$ donc $R(x) \in E$, d'où $A(x) \in E$. Pour tout $(a, b) \in E \times E$, il existe $(A, B) \in \mathbf{K}[X] \times \mathbf{K}[X]$ tels que $a = A(x)$ et $b = B(x)$. Alors $(A - B)(x) \in E$ et $(AB)(x) \in E$ donc $a - b \in E$ et $ab \in E$.
D'autre part, $\text{degre}(A) < \text{degre}(P) = n$ et P est irréductible, donc $A \wedge P = 1$ et, d'après le théorème de Bézout, il existe $(U, V) \in \mathbf{K}[X] \times \mathbf{K}[X]$ tels que $UP + VA = 1$. Or $P(x) = 0$ et $A(x) = a$ donc $V(x)a = 1$ i.e. $a^{-1} = V(x) \in E$.
Enfin on a $0 \in E$ et $1 \in E$, donc E est bien un sous-corps de $\mathbf{C}$ contenant x. La définition de $\mathbf{K}(x)$ donne alors $\mathbf{K}(x) \subset E$.
Par double inclusion on a bien $\mathbf{K}(x) = E$.
• $\mathbf{K}(x) = E$ est engendré par $x^0, \ldots, x^{n-1}$, donc $[\mathbf{K}(x) : \mathbf{K}] \leq n$. Si l'on avait $[\mathbf{K}(x) : \mathbf{K}] < n$, alors $x^0, \ldots, x^{n-2}$ serait $\mathbf{K}$-liée, ce qui contredirait le fait que P est de degré minimal. Donc $[\mathbf{K}(x) : \mathbf{K}] = n$.
• Si $[\mathbf{K}(x) : \mathbf{K}] = n < +\infty$, alors $x^0, \ldots, x^n$, qui compte $(n + 1)$ éléments, est $\mathbf{K}$-liée, donc x est racine d'un polynôme à coefficients dans $\mathbf{K}$.
La réciproque dérive du point précédents.
• Si $[\mathbf{K}(\alpha_1, \ldots, \alpha_n) : \mathbf{K}] < +\infty$, alors pour tout $i \in \{1, \ldots, k\}$, $[\mathbf{K}(\alpha_i) : \mathbf{K}] < +\infty$, donc α_i est $\mathbf{K}$-algébrique.
Réciproquement, si $\alpha_1, \ldots, \alpha_k$ sont algébriques sur K, on note $A_i = \{\alpha_1, \ldots, \alpha_i\}$, avec $A_0 = \emptyset$. Or, d'après la proposition 1.4 page 1, $\mathbf{K}(A_i) = \mathbf{K}(A_{i-1})(\alpha_i)$ pour $i \geq 1$; or α_i est $\mathbf{K}$-algébrique et a fortiori algébrique sur $\mathbf{K}(A_{i-1})$, donc $[\mathbf{K}(A_i) : \mathbf{K}(A_{i-1})] < +\infty$. Or par multiplicativité des degrés : $\mathbf{K}(A_k) = \prod_{i=1}^{k} [\mathbf{K}(A_i) : \mathbf{K}(A_{i-1})]$, donc $[\mathbf{K}(A_k) : \mathbf{K}] < +\infty$. CQFD.
• Soient x et y algébriques sur $\mathbf{K}$. Le point précédent entraîne $[\mathbf{K}(x, y) : \mathbf{K}] < +\infty$.
Or xy^{-1} et $x - y$ appartiennent à $\mathbf{K}(x, y)$ et sont donc algébriques[1] sur $\mathbf{K}$. L'ensemble des nombres $\mathbf{K}$-algébriques est donc un sous-corps de $\mathbf{C}$. CQFD.
• Soit $\mathbf{L}$ le corps des nombres $\mathbf{K}$-algébriques, et soit $P = \sum_{i=0}^{n} p_i X^i \in \mathbf{L}[X]$. Notons $\mathbf{M} = \mathbf{K}(p_0, \ldots, p_n)$. Alors $[\mathbf{M} : \mathbf{K}] < +\infty$. Toute racine x de P est alors algébrique sur $\mathbf{M}$ donc $[\mathbf{M}(x) : \mathbf{M}] < +\infty$.
Or $[\mathbf{M}(x) : \mathbf{K}] = [\mathbf{M}(x) : \mathbf{M}][\mathbf{M} : \mathbf{K}]$ donc $[\mathbf{M}(x) : \mathbf{K}] < +\infty$ et, en particulier, x est $\mathbf{K}$-algébrique donc $x \in \mathbf{L}$.
Or P, comme tout élément de $\mathbf{C}[X]$, peut s'écrire $P(X) = p_n \sum_{i=1}^{n} (X - x_1)$ où les x_i sont ses racines. Comme on vient de le dire, toutes ces racines sont dans $\mathbf{L}$, donc P est scindé sur $\mathbf{L}[X]$.
C'est vrai pour tout P de degré ≥ 1, donc $\mathbf{L}$ est algébriquement clos. CQFD. ∎

Remarque : Comme il existe des nombres $\mathbf{Q}$-transcendants (cf π), le sous-corps des nombres $\mathbf{Q}$-algébriques est strictement plus petit que $\mathbf{C}$. D'après la dernière question, c'est alors un exemple de sous-corps de $\mathbf{C}$ algébriquement clos et strictement plus petit que $\mathbf{C}$.
D'autre part, en notant $\mathbf{L}$ l'ensemble des nombres $\mathbf{K}$-algébriques, tout nombre $\mathbf{L}$-algébrique est aussi $\mathbf{K}$-algébrique; de même, tout nombre $\mathbf{K}$-transcendant est $\mathbf{L}$-transcendant.

[1] par exemple, $xy^{-1} \in \mathbf{K}(x, y)$ donc $\mathbf{K}(xy^{-1}) \subset \mathbf{K}(x, y)$ et par conséquent $\mathbf{K}(xy^{-1}) \leq \mathbf{K}(x, y) < +\infty$

2 Théorèmes auxiliaires

La démonstration du théorème de Lindemann comporte un certain nombre de prérequis, dont les plus importants suivent. Quelques-uns sont redémontrés; pour les autres il vous faudra ressortir vos vieux cours sur les polynômes.

Théorème 2.1 (Les nombres algébriques forment un sous-corps de C) *Pour tout sous corps* $\mathbf{K}$ *de* $\mathbf{C}$*, l'esemble des nombres* $\mathbf{K}$*-algébriques est un sous-corps de* $\mathbf{C}$*.*

Preuve : cf l'exercice 1.5 page 2 ∎

Théorème 2.2 (Racines rationnelles d'un polynôme) *Soit* $A \in \mathbf{Z}[X]$*, de degré* ≥ 1*. Si* $A(p/q) = 0$*, (avec* $(p,q) \in \mathbf{Z} \times \mathbf{N}^*$ *et* $p \wedge q = 1$*) alors* q *divise le coefficient dominant de* A*, et* p *divise son coefficient constant.*

Preuve : Notons $A(X) = \sum_{k=0}^{n} a_k X^k$. Comme $A(p/q) = 0$, on a $a_0 q^n = -\sum_{k=1}^{n} a_k p^k q^{n-k}$. Donc $a_0 q^n = -p \sum_{k=1}^{n} a_k p^{k-1} q^{n-k}$ est multiple de p, et comme $p \wedge q = 1$, le théorème de Gauss dit que a_0 est multiple de p.
De même, $a_n p^n = -q \sum_{k=0}^{n-1} a_k p^k q^{n-1-k}$ est multiple de q donc a_n l'est. CQFD. ∎

Corollaire 2.3 *Les racines rationnelles d'un polynôme unitaire* [2] *de degré* ≥ 1 *à coefficients entiers sont entières.*

Théorème 2.4 (Waring) *Soient un corps commutatif* $\mathbf{K}$*,* $\mathbf{A}$ *un sous-anneau de* $\mathbf{K}$*, et* P *un polynôme unitaire de degré* n *à coefficients dans* $\mathbf{A}$*, possédant* n *racines* $\omega_1, \ldots, \omega_n$ *dans* $\mathbf{K}$*.*
Soit Q *un polynôme symétrique à* n *indéterminées et à coefficients dans* $\mathbf{A}$*.*
Alors $Q(\omega_1, \ldots, \omega_n) \in \mathbf{A}$*.*

Théorème 2.5 (Combinaison polynomiale de racines) *Soit* $P \in \mathbf{Z}[X_1, \ldots, X_n]$*. Si* $x_1, \ldots, x_n$ *sont racines de polynômes unitaires de* $\mathbf{Z}[X]$*, alors* $P(x_1, \ldots, x_n)$ *est racine d'un tel polynôme.*

Preuve : Il suffit de montrer que c'est vrai pour $x_1 + x_2$, $x_1 x_2$ et pour ax_1, où $a \in \mathbf{Z}$ est quelconque. Le reste suit immédiatement, par récurrence sur le nombre de termes de P. Remarquons d'abord que, quitte à faire des produits de polynômes, on peut considérer que x_1, x_2 (distincts ou non) sont racines d'un certain polynôme unitaire $A \in \mathbf{Z}[X]$. Soit $m \geq 2$ son degré et notons $x_1, \ldots, x_m$ les racines (distinctes ou non) de A.
Considérons le polynôme $B(X) = \prod_{i<j} (X - x_i x_j)$. Il est unitaire, et tous ses coefficients sont les valeurs prises en $(x_1, \ldots, x_m)$ par des polynômes symétriques de $\mathbf{Z}[X_1, \ldots, X_m]$. Ils sont donc entiers d'après le théorème de Waring, et par conséquent, pour tout (i,j), le produit $x_i x_j$ est racine d'un certain polynôme unitaire de $\mathbf{Z}[X]$.
De même, considérer le polynôme $C(X) = \prod_{i<j} (X - (x_i + x_j))$ nous fait conclure que $x_i + x_j$ est aussi racine d'un polynôme unitaire de $\mathbf{Z}[X]$.
Enfin, tout $a \in \mathbf{Z}$ est racine de $X - a$ qui est unitaire, donc ax_1 est racine d'un polynôme unitaire de $\mathbf{Z}[X]$ d'après la remarque sur les produits. ∎

3 Démonstration du théorème de Lindemann

Théorème 3.1 (Théorème de Lindemann) *Soient* $A_1, \ldots, A_l$ *des nombres algébriques non-nuls et soient* $\alpha_1, \ldots, \alpha_l$ *des nombres algébriques distincts deux à deux. Alors :*

$$\sum_{i=1}^{l} A_i e^{\alpha_i} \neq 0$$

En 1873, le français Hermite avait prouvé les cas où A et α sont des nombres rationnels, et l'allemand Lindemann prouva le théorème en 1882.
Sa démonstration, extrêmement difficile, a ensuite été simplifiée, entre autres par Karl Weirstrass (1815-1897), puis par P.Gordan (1837-1912). Elle est maintenant très accessible.

[2] Rappel : c'est ainsi que l'on appelle les polynômes dont le coefficient de plus haut degré est 1.

La version présentée ici est adaptée de *100 Great Problems of Elementary Mathematics* [3] , avec une modernisation des notations et des rappels de certains théorèmes moins connus de nos jours.

La démonstration se fait par l'absurde : on commence donc par supposer $\sum_{i=1}^{l} A_i e^{\alpha_i} = 0$.

3.1 Les coefficients peuvent être supposés entiers

Les $A_1, \ldots, A_l$ sont racines d'un certain polynôme non-nul de $\mathbf{Z}[X]$, de degré $L \geq l$ et à racines simples. Notons ces racines $A_1, \ldots A_L$. Notons $S_{l,L}$ l'ensemble des applications injectives de $\{1, \ldots, l\}$ dans $\{1, \ldots, L\}$. Alors :

$$\prod_{\sigma \in S_{l,L}} \left(\sum_{i=1}^{l} A_{\sigma(i)} e^{\alpha_i} \right) = 0$$

En développant le produit et en regroupant les exponentielles de même exposant, on trouve m termes tels que :

$$\sum_{i=1}^{m} B_i e^{\beta_i} = 0$$

Comme les nombres algébriques forment un corps, les B_i sont algébriques. Ils sont de plus non-nuls : en effet, comme les exposants s'additionnent dans le produit, et que l'ordre lexicographique[4] est compatible avec l'addition, l'exposant β_{i_O} le plus petit parmi les β_i a pour coefficient B_{i_0} un unique produit de nombres choisis parmi les A_i, qui sont non-nuls. Il est donc non-nul.

D'autre part, le produit est indépendant d'une permutation des A_i (c'est fait exprès !). Par conséquent les B_i sont les valeurs prises en $(A_1, \ldots, A_L)$ par des polynômes symétriques à coefficients entiers. Ils sont donc rationnels d'après le théorème de Waring 2.4 page 3.

Quitte à multiplier les A_i par un nombre ad-hoc (le ppcm des dénominateurs des B_i fait l'affaire) on peut donc supposer les B_i entiers.

3.2 Des exposants très particuliers

Nous allons maintenant effectuer une manœuvre analogue sur les β_i. Comme ce sont des sommes de certains des α_i, ils sont algébriques. En particulier ils sont racines d'un certain polynôme de $\mathbf{Q}[X]$, à racines simples et de degré $M \geq m$, dont nous noterons les racines $\beta_1, \ldots, \beta_M$.
Considérons la fonction :

$$u(x) = \prod_{\sigma \in S_{m,M}} \left(\sum_{i=1}^{m} B_i e^{x\beta_{\sigma(i)}} \right)$$

En développant et en regroupant les exponentielles de même exposant, nous obtenons n termes tels que :

$$u(x) = \sum_{i=1}^{n} C_i e^{x\gamma_i}$$

où les C_i sont entiers non-nuls (même argument que pour les B_i). Développons en série entière :

$$u(x) = \sum_{j=1}^{\infty} a_j x^j \text{ où } a_j = \frac{1}{j!} \sum_{i=1}^{n} C_i \gamma_i^j$$

Or $u(x)$ est invariant par une permutation des β_i. Par unicité du développement en série entière, a_j l'est aussi. Donc a_j est la valeur prise par un certain polynôme symétrique à coefficients entiers en $\beta_1, \ldots, \beta_n$. Conformément au théorème de Waring 2.4 page 3, a_j est rationnel, ce qui entraîne : $\forall j \in \mathbf{N}$, $\sum_{i=1}^{n} C_i \gamma_i^j \in \mathbf{Q}$.
Alors pour tout polynôme $g \in \mathbf{Q}[X]$:

$$\sum_{i=1}^{n} C_i g(\gamma_i) \in \mathbf{Q} \quad (1)$$

[3] Traduction anglaise d'un livre écrit par Heinrich Dörrie en 1932. Dover Publications, 1965, ISBN 0-486-61348-8

[4] On dit, pour deux complexes, que $x \geq y$ pour l'ordre lexicographique ssi $\mathrm{Re}(x) < \mathrm{Re}(x)$ ou ($\mathrm{Re}(x) = \mathrm{Re}(y)$ et $\mathrm{Im}(x) \leq \mathrm{Im}(y)$).

D'autre part, $u(1)$ contient le facteur $\sum_{i=1}^{m} B_i e^{\beta_i} = 0$, donc $u(1) = 0$ i.e. :

$$\sum_{i=1}^{n} C_i e^{\gamma_i} = 0 \quad (2)$$

C'est déjà pas mal, mais on peut aller encore plus loin. Les γ_i sont racines d'un certain polynôme unitaire $R \in \mathbf{Q}[X]$, de degré $N \geq n$. En notant $R(X) = \sum_{j=0}^{N} r_j X^j$, avec $r_N = 1$, en appelant H le ppcm des dénominateurs des r_j et en posant $\delta_i = H\gamma_i$, il vient :

$$0 = H^N R(\gamma_i) = \sum_{j=0}^{N} (r_j H^{N-j})(H\gamma_i)^j = \sum_{j=0}^{N} (r_j H^{N-j})\delta_i^j$$

Le polynôme $f(X) = \sum_{j=0}^{N} r_j H^{N-j} X^j \in \mathbf{Z}[X]$ a donc pour racines les $(\delta_i)_{1\leq i\leq N}$.
De plus, il est unitaire car $r_N = 1$. Or pour tout polynôme $g \in \mathbf{Z}[X]$, $\sum_{i=1}^{n} C_i g(\delta_i)$ est une combinaison, polynômiale à coefficients entiers, des δ_i. C'est donc (d'après le théorème 2.5 page 3) une racine d'un certain polynôme *unitaire* de $\mathbf{Z}[X]$.
Or c'est aussi un nombre *rationnel* d'après (1), donc le théorème 2.2 page 3 nous dit que c'est un *entier* i.e. :

$$\forall g \in \mathbf{Z}[X], \quad \sum_{i=0}^{n} C_i g(\delta_i) \in \mathbf{Z} \quad (3)$$

Assez remarquable, non ?

Passons à autre chose. Les $(\delta_i)_{1\leq i\leq N}$ sont tous distincts, donc la dérivée $\phi(X)$ de $f(X)$ n'est nulle en aucun d'entre eux. Alors il existe un entier h vérifiant $0 \leq h < n$ et :

$$\sum_{i=1}^{n} C_i \delta_i^h \phi(\delta_i) \neq 0 \quad (4)$$

En effet, si un tel h n'existait pas on aurait :

$$\begin{bmatrix} \delta_1^0 & \delta_2^0 & \dots & \delta_n^0 \\ \delta_1^1 & \delta_2^1 & \dots & \delta_n^1 \\ \vdots & \vdots & \dots & \vdots \\ \delta_1^{n-1} & \delta_2^{n-1} & \dots & \delta_n^{n-1} \end{bmatrix} \begin{bmatrix} C_1\phi(\delta_1) \\ C_2\phi(\delta_2) \\ \vdots \\ C_n\phi(\delta_n) \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

Or les $C_i\phi(\delta_i)$ sont non-nuls puisque $\phi(\delta_i) \neq 0$, donc le déterminant de la matrice carrée serait nul. Or il vaut[5] $\prod_{1\leq i<j<n}(\delta_j - \delta_i)$ qui est non-nul puisque les δ_i sont distincts deux-à deux. Absurde.

3.3 Torturons les exponentielles

Considérons l'application $\mathbf{C}$-linéaire $\mathcal{F} : \mathbf{C}[X] \to \mathbf{C}$ telle que pour tout $i \in \mathbf{N}$, on ait $\mathcal{F}(X^i) = H^i i!$.
Alors pour tout $x \in \mathbf{C}$, pour tout $i \in \mathbf{N}$:

$$e^x H^i i! = A_i(x) + B_i(x) \text{ avec } A_i(x) = \sum_{j=0}^{i} H^i i! \frac{x^j}{j!} \text{ et } B_i(x) = \sum_{j\geq i+1} H^i i! \frac{x^j}{j!}$$

Occupons-nous de $A_i(x) = \sum_{j=0}^{i} H^{i-j}(i-j)!\frac{i!}{j!(i-j)!}(Hx)^j$. Alors $A_i(x) = \sum_{j=0}^{i} \mathcal{F}(X^{i-j})\mathcal{C}_i^j (Hx)^j = \mathcal{F}\left(\sum_{j=0}^{i} X^{i-j}\mathcal{C}_i^j (Hx)^j\right)$.
La formule du binôme donne alors : $A_i(x) = \mathcal{F}((Hx+X)^i)$.
Passons à $B_i(x) = (Hx)^i \sum_{j\geq i+1} i!\frac{x^{j-i}}{j!}$. Comme $j > i \geq 0$, on a $1 \leq \mathcal{C}_j^i = \frac{j!}{i!(j-i)!}$ donc $\frac{i!}{j!} \leq \frac{1}{(j-i)!}$.
D'où $B_i(x) \leq |Hx|^i \sum_{j\geq i+1} \frac{|x|^{j-i}}{(j-i)!} < |Hx|^i \sum_{j\geq i} \frac{|x|^{j-i}}{(j-i)!} = |Hx|^i e^{|x|}$ puisque $\frac{|x|^0}{0!} = 1 > 0$.

[5] Vous aurez en effet reconnu un déterminant de Vandermonde.

Donc il existe $\varepsilon_i(x) \in \mathbf{C}$ tel que $|\varepsilon_i(x)| < 1$ et $B_i(x) = \varepsilon_i(x)\,|Hx|^i\, e^{|x|}$.
Finalement, en remarquant que $e^x H^i i! = e^x \mathcal{F}(X^i)$:

$$\forall i \in \mathbf{N}, \forall x \in \mathbf{C}, \quad e^x \mathcal{F}(X^i) = \mathcal{F}((Hx+X)^i) + \varepsilon_i(x)(Hx)^i e^{|x|} \text{ avec } |\varepsilon_i(x)| < 1$$

Par $\mathbf{C}$-linéarité de $\mathcal{F}$ on en tire pour tout polynôme $V(X) = \sum_{i=0}^{v} V_i X^i$:

$$\forall V \in \mathbf{C}[X], \forall x \in \mathbf{C}, \quad e^x \mathcal{F}(V(X)) = \mathcal{F}(V(Hx+X)) + W_V(Hx)e^{|x|}$$

avec $W_V(Hx) = \sum_{i=0}^{v} \varepsilon_i(x) V_i (Hx)^i$.
Supposons V unitaire et notons ses racines $\omega_1, \ldots, \omega_v$. En posant $d = \max_{1\le i\le v}\{|Hx| + |\omega_i|\}$, on a alors $|W_V(Hx)| < d^v$.
En effet, on a alors[6] $d^v \ge \prod_{i=1}^{v}(|Hx| + |\omega_i|) \ge \sum_{i=0}^{v} |V_i|\,|Hx|^i > \sum_{i=0}^{v} |\varepsilon_i(x)V_i|\,|Hx|^i \ge W_V(Hx)$.

Donc il existe $\varepsilon \in \mathbf{C}$ tel que :

$$e^x \mathcal{F}(V(X)) = \mathcal{F}(V(Hx+X)) + \varepsilon e^{|x|} d^v \quad \text{et} \quad |\varepsilon| \le 1 \quad (5)$$

Prenons maintenant un V bien choisi :

$$V(X) = F(X)^q \Phi(X) \text{ où } \left\{ \begin{array}{rcl} F(X) & = & X^h f(X) \\ \Phi(X) & = & X^h \phi(X) \end{array} \right.$$

où q est un entier que nous choisirons plus tard. Le degré v de V vaut alors $(h+N)q + h + N - 1$ puisque f est de degré N et que ϕ est sa dérivée.

Quand x prend les valeurs $\gamma_1, \ldots, \gamma_n$, Hx prend les valeurs $\delta_1, \ldots, \delta_n$, et d (qui dépend de x) prend les valeurs $d_1, \ldots, d_n$. Posons enfin :

$$D = \max_{1\le i\le n} \left\{ d_i^{N+h}, e^{|\gamma_i|} d_i^{2(N+h)-1} \right\}$$

Remarque : Pour $q \ge 1$, les racines de V sont celles de f, celles de ϕ et 0 (si $h \ge 1$). Elles ne dépendent pas de q, donc les d_i non plus, et D non plus.

Pour tout $i = 1, \ldots, n$ on a $D/d_i^{N+h} \ge 1$ et $D/d_i^{N+h} \ge e^{|\gamma_i|} d_i^{N+h-1}$, donc $(D/d_i^{N+h})^q \ge e^{|\gamma_i|} d_i^{N+h-1}$. Or $v = (h+N)q + h + N - 1$ donc $D^q \ge e^{|\gamma_i|} d_i^v$, d'où l'existence de $\eta_i \in \mathbf{C}$ tel que $|\eta_i| \le 1$ et que :

$$e^{\gamma_i} \mathcal{F}(V(X)) = \mathcal{F}(V(\delta_i + X)) + \eta_i D^q \text{ avec } |\eta_i| \le 1 \quad (6)$$

Prenons $q = p - 1$, où p est un certain nombre premier qui reste à choisir. Alors $V(\delta_i + X) = (\delta_i + X)^{hq} f^q(\delta_i + X)(\delta_i + X)^h \phi(\delta_i + X) = (\delta_i + X)^{hp} f^q(\delta_i + X)\phi(\delta_i + X)$.
Par définition de f, on a $f(\delta_i + X) = X \prod_{j=1;j\ne i}^{N}(X + \delta_i - \delta_j)$, donc $f(\delta_i + X)$ est multiple de X, et son coefficient de degé 1 est $\prod_{j=1;j\ne i}^{N}(\delta_i - \delta_j) = \phi(\delta_i)$ Donc V est multiple de X^q, et son coefficient de degré q est $\delta(i)^p \phi(\delta_i)^q \phi(\delta_i) = \delta_i^p \phi(\delta_i)^p = \Phi(\delta_i)^p$.

Donc $V(\delta_i + X) = \sum_{j=q}^{v} \psi_j(\delta_i) X^j$ où les ψ_j sont des polynôme à coefficients entiers (comme V), avec en particulier $\psi_q = \Phi^p$. Par linéarité de $\mathcal{F}$:

$$\forall i \in \{1, \ldots, n\}, \quad e^{\gamma_i} \mathcal{F}(V(X)) = \sum_{j=q}^{v} \psi_j(\delta_i) \mathcal{F}(X^j) + \eta_i D^q$$

donc $\left(\sum_{i=1}^{n} C_i e^{\gamma_i}\right) \mathcal{F}(V(X)) = \sum_{j=q}^{n} \left(\sum_{i=1}^{n} C_i \psi_j(\delta_i)\right)(F)(X^j) + \left(\sum_{i=1}^{n} C_i \eta_i\right) D^q$. Or d'après (2), $\sum_{i=1}^{n} C_i e^{\gamma_i} = 0$; d'après (3), $\sum_{i=1}^{n} C_i \psi_j(\delta_i)$ est un entier que nous noterons G_j; d'après (6), $|\eta_i| \le 1$ donc $|\sum_{i=1}^{n} C_i \eta_i| \le n \max_{1\le i\le n}\{|C_i|\}$. En bref :

$$0 = \sum_{j=q}^{v} G_j \mathcal{F}(X^j) - \lambda D^v \text{ où } \lambda = -\sum_{i=1}^{n} C_i \eta_i \text{ et } |\lambda| \le n \max_{1\le i\le n}\{|C_i|\} \quad (7)$$

[6] En effet, $V(X) = \prod_{i=1}^{v}(X - \omega_i)$. Chaque coefficient du polynôme $\prod_{i=1}^{v}(X + |\omega_i|)$ est alors supérieur à la valeur absolue du coefficient de V de même degré. En remplacant l'indéterminée X par Hx et en utilisant l'inégalité triangulaire, le tour est joué.

3.4 Contradiction finale

Comme $\mathcal{F}(X^j) = H^j j!$, tous les termes de la somme (7) sont multiples de H^q, et ceux de rang $j \geq p$ sont multiples de $H^p p!$, donc en posant $G' = \sum_{j=p}^{v} G_j \frac{H^j j!}{H^q p!}$ et $E = \frac{D}{H}$, (7) devient :

$$G_q q! + G' p! = \lambda E^q \quad \text{où } G_q \in \mathbf{Z}, \quad G' \in \mathbf{Z} \quad (8)$$

Exprimons $G_q = \sum_{i=1}^{n} C_i \Psi_q(\delta_i) = \sum_{i=1}^{n} C_i \Phi(\delta_i)^p$ en fonction de la quantité $G = \sum_{i=1}^{n} C_i \Phi(\delta_i) = \sum_{i=1}^{n} C_i \delta_i^h \phi(\delta_i)$ qui est non-nulle par choix de h fait en (4), et entière d'après (3).
En développant G^p, et en regroupant les termes apparaissant p (ou un multiple de p) fois dans μ, on obtient :

$$G^p = \sum_{i=1}^{n} C_i^p \Phi^p(\delta_i) + \mu p \quad (9)$$

En tant que combinaison polynômiale à coefficients entiers des δ_i, μ est, d'après le théorème 2.5 page 3, racine d'un polynôme unitaire de $\mathbf{Z}[X]$.

Comme p est premier, le petit théorème de Fermat dit que $C_i^p - C_i$ et $G^p - G$ sont multiples de p; il existe donc des entiers c_i et g tels que $C_i^p = C_i + c_i p$ et $G^p = G + gp$. Alors (9) devient :

$$G = \sum_{i=1}^{n} C_i \Phi(\delta_i)^p + \mu' p = G_q + \mu' p \text{ où } \mu' = \mu + \sum_{i=1}^{n} c_i \Phi(\delta_i)^p - g$$

où μ' est racine d'un polynôme unitaire de $\mathbf{Z}[X]$ pour la même raison que μ. Or on a aussi $\mu' = (G - G_q)/p$ donc $\mu' \in \mathbf{Q}$, et d'après le théorème 2.2 page 3 c'est un entier.
Alors $G' + \mu'$ est un entier noté g', et (8) devient :

$$G + g'p = \lambda \frac{E^{p-1}}{(p-1)!}$$

Or G est indépendant de p, E l'est aussi puisque D est indépendant de $q = p - 1$, et la majoration de λ dans (7) aussi[7]. On peut donc prendre p assez grand pour que $p > |G|$ et $\lambda \frac{E^{p-1}}{(p-1)!} < 1$.
Or G est non-nul donc $G + g'p$ n'est pas multiple de p, et est donc un entier non-nul. C'est incompatible avec la valeur absolue du membre de droite, qui est < 1 par choix de p. Donc la contradiction est trouvée et le théorème prouvé. Ouf !

4 Corollaires du théorème de Lindemann

4.1 Transcendance de e et de π

Exercice 4.1 (e et π sont transcendants)

En effet, si e était un nombre algébrique α on aurait $e^1 - \alpha e^0 = 0$, ce qui contredirait le théorème.
Si π était algébrique, alors $\mathbf{i}\pi$ le serait aussi et on aurait alors $e^{\mathbf{i}\pi} + e^0 = 0$ puisque $e^{\mathbf{i}\pi} = -1$.
Remarque : Ceux qui n'ont pas tout lu se demanderont peut-être si π n'est pas racine d'un polynôme dont les coefficients seraient, cette fois, $\mathbf{Q}$-algébriques. La réponse est NON ! Toujours sceptique ? Référez-vous à la remarque page 2 qui suit la correction de l'exercice 1.5.

4.2 Courbes transcendantes

Exercice 4.2 (Courbes transcendantes) *Montrer que les courbes $y = e^x$ et $y = \sin(x)$ passent par un unique point de coordonnées algébriques, et déterminer lequel.*

Solution : Aux points algébriques de la courbe exponentielle, on a $e^x - ye^0 = 0$ et le seul moyen de ne pas contredire le théorème de Lindemann consiste alors à prendre deux exposants égaux, i.e. $x = 0$. Alors $y = 1$. Réciproque immédiate.
De même pour le sinus : $\frac{1}{2\mathbf{i}} e^{\mathbf{i}x} - \frac{1}{2\mathbf{i}} e^{-\mathbf{i}x} - ye^0$. On prend alors $\mathbf{i}x = -\mathbf{i}x$ ou $\mathbf{i}x = 0$, ce qui dans les deux cas donne $x = 0$ et $y = 0$. Réciproque immédiate. ∎

[7] Par contre g' dépend de p, mais ça n'a pas d'importance du moment qu'il est entier