

Transcendance de e et π pour les nuls.

Avissa Hedayati Dezfouli Marc Laly Sheedy Shiwpursad

Mai 2009

Mémoire de Licence 1^{ère} année.
Réalisé sous la direction d'Alain Prouté
Université Denis Diderot-Paris 7

Table des matières

1	Introduction.	2
1.1	La quadrature du cercle.	2
1.2	Nombres transcendants.	2
1.3	L'essentiel de la méthode.	3
2	Quelques outils.	3
2.1	Une intégration par parties.	3
2.2	Polynômes symétriques.	4
2.2.1	Définition et théorème fondamental.	4
2.2.2	Familles d'entiers algébriques.	5
2.3	Un lemme sur la dérivation.	6
3	Transcendance de e.	7
3.1	Une égalité qui s'avèrera impossible.	7
3.2	Une question d'intégralité.	8
3.3	Une majoration.	9
4	Transcendance de π.	9
4.1	Préliminaires.	9
4.2	Intervention de la formule d'Euler $1 + e^{i\pi} = 0$	11
4.3	Un polynôme canonique.	11
4.4	Une égalité qui s'avèrera impossible.	11
4.5	Une question d'intégralité.	12
4.6	Une majoration.	13

1 Introduction.

1.1 La quadrature du cercle.

La quadrature du cercle est un problème classique de géométrie. Il fait partie des trois grands problèmes de l'Antiquité, avec la trisection de l'angle et la duplication du cube. Le problème consiste à construire un carré de même aire (ou de même périmètre) qu'un cercle donné à l'aide d'une règle et d'un compas.

Il remonte à l'invention de la géométrie et a occupé de nombreux mathématiciens au cours des siècles. C'est en 1837 que Pierre-Laurent Wantzel démontre un théorème qui permet d'exhiber la forme des équations dont sont solutions les nombres constructibles à la règle et au compas. Puis en 1844, Joseph Liouville met en évidence l'existence des nombres transcendants. Mais il faudra attendre jusqu'en 1882 pour que le mathématicien allemand Ferdinand von Lindemann démontre la transcendance de π pour appliquer le théorème de Wantzel au problème de la quadrature du cercle et ainsi démontrer qu'elle est impossible à réaliser.

La quadrature du cercle nécessite la construction à la règle et au compas de la racine carrée de π , ce qui est impossible en raison de la transcendance de π : les nombres constructibles sont les rationnels et les racines de certains polynômes de degré 2^n à coefficients entiers, ce sont des nombres algébriques ce qui n'est pas le cas de π .

1.2 Nombres transcendants.

DÉFINITION 1 *On définit les expressions « nombre algébrique », « entier algébrique », « polynôme normalisé », « polynôme canonique », et « nombre transcendant », comme suit :*

- *Un nombre complexe a est dit « algébrique » s'il existe un polynôme $\varphi(x)$ non constant à coefficients entiers (c'est-à-dire dont les coefficients appartiennent à \mathbb{Z}) tel que $\varphi(a) = 0$.*
- *Si de plus le polynôme $\varphi(x)$ peut être choisi « normalisé », c'est-à-dire tel que le coefficient de son terme de plus haut degré soit 1, on dit que a est un « entier algébrique ».*
- *Un nombre qui n'est pas algébrique est dit « transcendant ».*
- *Un polynôme qui est à la fois à coefficients entiers et normalisé est dit « canonique ».*

Par exemple, $\sqrt{2}$ est un entier algébrique car il est racine du polynôme canonique $x^2 - 2$. De même, i est un entier algébrique car il est racine de $x^2 + 1$. Un nombre rationnel $\frac{p}{q}$, où p et q sont des entiers, est algébrique car il est racine du polynôme

$qx - p$, et est un entier algébrique si et seulement si il est entier.

L'objet de ce texte est de montrer que e et π sont transcendants.

1.3 L'essentiel de la méthode.

Aussi bien pour e que pour π , on construit une égalité particulière $E = F$ à partir de l'hypothèse que ce nombre est algébrique. Cette égalité dépend d'un entier premier p , qu'on peut choisir aussi grand qu'on veut. Puis, on prouve d'une part que le membre de gauche E est un entier non nul dès que p est assez grand, et d'autre part que le membre de droite F tend vers 0 quand p tend vers l'infini. On a bien sûr une contradiction, ce qui prouve la transcendance de notre nombre.

L'égalité $E = F$ est construite à partir du polynôme $\varphi(x)$ dont l'existence résulte de l'hypothèse que e ou π est algébrique. Pour montrer que le membre de gauche E de notre égalité est entier, on manipule des dérivées de polynômes. Dans le cas de e , on utilise surtout le fait que quand on dérive un monôme de la forme ax^n avec a entier, on récupère le monôme anx^{n-1} dont le coefficient est toujours entier et de plus divisible par n . Dans le cas de π , il faut aussi utiliser les propriétés des polynômes symétriques. On verra les détails plus loin.

Pour montrer que le second membre F de notre égalité tend vers 0 quand p tend vers l'infini, on exprime ce second membre sous forme de somme d'intégrales, ce qui permet une majoration facile. L'essentiel de la technique se limite à des intégrations par parties à établir par récurrence.

2 Quelques outils.

2.1 Une intégration par parties.

Le lemme établi dans cette section servira pour e et pour π . Soit $k \in \mathbb{N}$, et P un polynôme de degré k . On pose :

$$Q_P(x) = P(x) + P'(x) + \dots + P^{(k)}(x)$$

Remarque : $Q_P(x) = P(x) + Q_{P'}(x)$.

LEMME 1 *On a, pour tout nombre complexe α :*

$$\int_0^1 \alpha e^{-\alpha x} P(\alpha x) dx = [-e^{-\alpha x} Q_P(\alpha x)]_0^1 = -e^{-\alpha} Q_P(\alpha) + Q_P(0)$$

Démonstration : Par récurrence sur le degré k de P . Si $k = 0$, on a $P(x) = a$ (P est constant), donc le membre de gauche est $\int_0^1 \alpha e^{-\alpha x} a dx$, qui vaut $[-e^{-\alpha x} a]_0^1$,

qui est aussi le membre de droite, puisque $Q_P(x) = a$. Supposons maintenant $k > 0$. Par hypothèse de récurrence on a :

$$\int_0^1 \alpha e^{-\alpha x} P'(\alpha x) dx = [-e^{-\alpha x} Q_{P'}(\alpha x)]_0^1$$

puisque P' est de degré $k - 1$. Par ailleurs,

$$\begin{aligned} \int_0^1 \alpha e^{-\alpha x} P(\alpha x) dx &= [-e^{-\alpha x} P(\alpha x)]_0^1 + \int_0^1 e^{-\alpha x} \alpha P'(\alpha x) dx \\ &= [-e^{-\alpha x} P(\alpha x)]_0^1 + [-e^{-\alpha x} Q_{P'}(\alpha x)]_0^1 \\ &= [-e^{-\alpha x} Q_P(\alpha x)]_0^1 \blacksquare \end{aligned}$$

2.2 Polynômes symétriques.

Les résultats de cette section ne sont utiles que pour la transcendance de π .

2.2.1 Définition et théorème fondamental.

Si on développe l'expression :

$$(x + \beta_1) \dots (x + \beta_p)$$

on obtient un polynôme normalisé de degré p :

$$x^p + b_1 x^{p-1} + b_2 x^{p-2} + \dots + b_{p-1} x + b_p$$

avec $b_1 = \beta_1 + \dots + \beta_p, \dots, b_p = \beta_1 \dots \beta_p$. Les coefficients b_i de ce polynôme sont eux-mêmes des polynômes en β_1, \dots, β_p , et on écrira :

$$b_i = \sigma_i(\beta_1, \dots, \beta_p)$$

Les polynômes $\sigma_i(\beta_1, \dots, \beta_p)$ sont appelés les « fonctions symétriques élémentaires » des p variables β_1, \dots, β_p .

DÉFINITION 2 *Un polynôme de p variables $P(x_1, \dots, x_p)$ est dit « symétrique » si pour toute permutation τ des entiers $1, \dots, p$, on a :*

$$P(x_{\tau(1)}, \dots, x_{\tau(p)}) = P(x_1, \dots, x_p)$$

Les polynômes σ_i des p variables β_1, \dots, β_p sont clairement symétriques. On va utiliser le théorème suivant (qu'on admettra, voir Serge Lang [2], page 132) :

THÉORÈME 1 Soit \mathcal{A} un anneau commutatif unitaire,⁽¹⁾ et soit $P(x_1, \dots, x_p)$ un polynôme symétrique à coefficients dans \mathcal{A} . Alors il existe un polynôme

$$S(u_1, \dots, u_p)$$

à coefficients dans \mathcal{A} , tel que :

$$P(x_1, \dots, x_p) = S(\sigma_1(x_1, \dots, x_p), \dots, \sigma_p(x_1, \dots, x_p))$$

Par exemple, $\beta_1^2\beta_2 + \beta_1\beta_2^2$ est symétrique en β_1, β_2 , et on a $\beta_1^2\beta_2 + \beta_1\beta_2^2 = (\beta_1\beta_2)(\beta_1 + \beta_2) = \sigma_2(\beta_1, \beta_2)\sigma_1(\beta_1, \beta_2)$. On a dans ce cas $S(u_1, u_2) = u_1u_2$.⁽²⁾

2.2.2 Familles d'entiers algébriques.

LEMME 2 Soit β_1, \dots, β_n la famille de toutes les racines (complexes, non nécessairement distinctes) d'un polynôme canonique. Alors, la famille obtenue en faisant toutes les sommes possibles d'éléments de la famille β_1, \dots, β_n est la famille des racines d'un polynôme canonique.

Par hypothèse, le polynôme :

$$(x - \beta_1) \dots (x - \beta_n)$$

est canonique. Notons S la famille de toutes les sommes possibles d'éléments de la famille β_1, \dots, β_n . On a :

$$S = \left\{ \begin{array}{l} 0, \\ \beta_1, \dots, \beta_n, \\ \beta_1 + \beta_2, \dots, \beta_{n-1} + \beta_n, \\ \beta_1 + \beta_2 + \beta_3, \dots \\ \dots \\ \beta_1 + \dots + \beta_n \end{array} \right\}$$

Notons α_i ($1 \leq i \leq s$) les éléments de la famille S . Noter que $s = 2^n$, puisqu'il y a exactement un élément dans S pour chaque partie de l'ensemble $\{1, \dots, n\}$, 0 correspondant à la partie vide, chaque β_i à un singleton, etc... et la dernière somme $\beta_1 + \dots + \beta_n$ à la partie pleine.

Il s'agit de montrer que le polynôme :

$$(x - \alpha_1) \dots (x - \alpha_s)$$

est à coefficients entiers. Quand on développe ce polynôme, on obtient un polynôme en x dont les coefficients sont, aux signes près, les fonctions symétriques

¹Par exemple l'anneau \mathbb{Z} des entiers relatifs, ou l'anneau $\mathbb{Z}[X]$ des polynômes à coefficients entiers.

²Le polynôme S n'a aucune raison d'être symétrique.

élémentaires des α_j . Ces coefficients sont donc invariants par permutation des α_j . Toute permutation des β_i , c'est-à-dire toute bijection de $\{1, \dots, n\}$ vers lui-même induit une bijection de l'ensemble des parties $\mathcal{P}(\{1, \dots, n\})$ vers lui-même. Il en résulte que toute permutation des β_i induit une permutation des α_j . Les coefficients de notre polynôme, que l'on peut voir comme des polynômes à coefficients entiers en β_1, \dots, β_n sont donc invariants par permutation des β_i . Ces coefficients sont donc des polynômes à coefficients entiers en les fonctions symétriques élémentaires des β_1, \dots, β_n , et sont donc des entiers. ■

LEMME 3 *Si une famille $S = \{\alpha_1, \dots, \alpha_s\}$ de nombres complexes est la famille de toutes les racines d'un polynôme canonique, il en est de même de la famille obtenue en retirant de S tous les éléments égaux à 0.*

En effet, par hypothèse, $\alpha_1, \dots, \alpha_s$ sont les racines d'un polynôme canonique qui a 0 pour racine avec pour multiplicité le nombre k d'éléments nuls dans la famille S . Ce polynôme est donc le produit de x^k par un polynôme canonique dont les racines sont les éléments de la nouvelle famille. ■

2.3 Un lemme sur la dérivation.

LEMME 4 *Soit $Q(x)$ un polynôme à coefficients entiers, et p un entier naturel au moins égal à 1. On pose :*

$$P(x) = \frac{x^{p-1}}{(p-1)!} (Q(x))^p$$

Alors pour tout entier $r \geq p$, le polynôme $P^{(r)}(x)$ est à coefficients entiers et ses coefficients sont divisibles par p . De plus :

$$P^{(p-1)}(0) = Q(0)^p.$$

Démonstration : Si on dérive r fois le monôme x^n , on obtient pour $r \leq n$:

$$(x^n)^{(r)} = n(n-1) \dots (n-r+1)x^{n-r} = \frac{n!}{(n-r)!} x^{n-r} = r! C_n^r x^{n-r}$$

et cette égalité reste vraie pour $r > n$, puisqu'on a alors $(x^n)^{(r)} = 0$ et $C_n^r = 0$. Elle est donc vraie pour tous entiers naturels n et r . $(x^n)^{(r)}$ est donc le produit de $r!$ par un monôme dont le coefficient est entier. Il en résulte que si on dérive r fois un polynôme à coefficients entiers, on obtient le produit de $r!$ par un polynôme à coefficients entiers.

Posons $R(x) = Q(x)^p$. On a $R'(x) = pQ'(x)Q(x)^{p-1}$. On voit donc que pour $i > 0$, $R(x)^{(i)} = p(Q'(x)Q(x)^{p-1})^{(i-1)}$, et donc que $R(x)^{(i)}$ est le produit de

$p(i-1)!$ par un polynôme à coefficients entiers. Par ailleurs, la formule de dérivation de Leibniz donne :

$$P^{(r)}(x) = C_r^0 \frac{x^{p-1}}{(p-1)!} R^{(r)}(x) + C_r^1 \frac{x^{p-2}}{(p-2)!} R^{(r-1)}(x) + \dots + C_r^{p-1} R^{(r-p+1)}(x) \quad (1)$$

puisqu'on obtient 0 quand on dérive p fois le monôme x^{p-1} . L'équation (1) s'écrit encore :

$$P^{(r)}(x) = C_r^0 \frac{x^{p-1}}{(p-1)!} p(r-1)! S_r(x) + C_r^1 \frac{x^{p-2}}{(p-2)!} p(r-2)! S_{r-1}(x) + \dots + C_r^{p-1} p(r-p)! S_{r-p+1}(x)$$

où les $S_i(x)$ sont des polynômes à coefficients entiers. Par ailleurs, comme $r \geq p$, $(p-1)!$ divise $(r-1)!$, $(p-2)!$ divise $(r-2)!$ etc..., ce qui prouve la première assertion du lemme. La seconde assertion du lemme résulte immédiatement de l'équation (1). ■

3 Transcendance de e .

Supposons que e soit algébrique, et donc racine d'un polynôme à coefficients entiers :

$$\varphi(x) = a_0 + a_1 x + \dots + a_n x^n$$

avec $n \geq 1$ et $a_n \neq 0$.

3.1 Une égalité qui s'avèrera impossible.

Soit p un nombre premier. Introduisons le polynôme :

$$P(x) = \frac{x^{p-1}}{(p-1)!} (x-1)^p \dots (x-n)^p$$

qui est de degré $np + p - 1$. À ce polynôme est associé le polynôme $Q_P(x)$ défini précédemment au début de la section 2.1. En multipliant $\varphi(e)$ et $Q_P(0)$, on obtient l'égalité :

$$\sum_{j=0}^n a_j e^j Q_P(0) = 0 \quad (2)$$

puisque $\varphi(e) = 0$. On a vu (lemme 1) que :

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

En multipliant par e^α , on obtient :

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

On pose enfin $R_P(\alpha) = \alpha e^\alpha \int_0^1 e^{-\alpha x} P(\alpha x) dx$, et on a finalement :

$$Q_P(\alpha) + R_P(\alpha) = Q_P(0) e^\alpha \quad (3)$$

L'égalité (2) peut donc être réécrite :

$$\sum_{j=0}^n a_j (Q_P(j) + R_P(j)) = 0$$

c'est-à-dire :

$$a_0 Q_P(0) + \sum_{j=1}^n a_j Q_P(j) = - \sum_{j=1}^n a_j R_P(j) \quad (4)$$

On va montrer que pour p assez grand le membre de gauche de (4) est un entier non nul et que le membre de droite a un module strictement plus petit que 1.

3.2 Une question d'intégralité.

Nous montrons dans cette section que le premier membre de (4) :

$$a_0 Q_P(0) + \sum_{j=1}^n a_j Q_P(j)$$

est un entier non nul pour p assez grand. Rappelons que :

$$P(x) = \frac{x^{p-1}}{(p-1)!} (x-1)^p (x-2)^p \dots (x-n)^p$$

Comme les entiers $1, \dots, n$ sont tous racine d'ordre p de $P(x)$, ils sont tous racine $P^{(r)}(x)$ pour $r < p$. De même, $P^{(r)}(0) = 0$, mais seulement pour $r < p-1$. Il en résulte que pour $j = 1, \dots, n$, on a :

$$Q_P(j) = P^{(p)}(j) + \dots + P^{(np+p-1)}(j)$$

et donc d'après le lemme 4 que $Q_P(j)$ est un entier multiple de p .

Par ailleurs, en ce qui concerne $Q_P(0)$, on a :

$$Q_P(0) = P^{(p-1)}(0) + P^{(p)}(0) + \dots + P^{(np+p-1)}(0)$$

c'est-à-dire toujours par le lemme 4 :

$$Q_P(0) = (-1)^{pn} (n!)^p + \text{multiple de } p$$

Il suffit que p soit premier et supérieur à $|a_0|$ et à n pour que $a_0 Q_P(0)$ ne soit pas multiple de p , donc pour que le premier membre de (4) soit un entier non nul.

3.3 Une majoration.

Nous majorons maintenant le second membre de (4). On a :

$$|R_P(j)| = je^j \left| \int_0^1 e^{-jx} P(jx) dx \right|$$

donc :

$$|R_P(j)| \leq je^j \sup_{0 \leq t \leq j} |P(t)|$$

Pour $0 \leq t \leq n$, on a tout de suite d'après la définition de $P(x)$:

$$|P(t)| \leq \frac{n^{p-1}}{(p-1)!} (n!)^p$$

Ainsi, on obtient (pour $j = 1, \dots, n$) :

$$|R_P(j)| \leq \frac{n^p e^n (n!)^p}{(p-1)!}$$

D'autre part, posons :

$$M = \sup_{j=1, \dots, n} |a_j|$$

On a alors :

$$\left| \sum_{j=1}^n a_j R_P(j) \right| \leq \frac{M n^{p+1} e^n (n!)^p}{(p-1)!} = M n^2 e^n (n!) \frac{(nn!)^{p-1}}{(p-1)!}$$

En prenant p assez grand, on peut rendre le rapport :

$$\frac{(nn!)^{p-1}}{(p-1)!}$$

aussi petit qu'on veut (puisque le terme général de la série définissant l'exponentielle tend vers 0).

On a donc prouvé la transcendance de e .

4 Transcendance de π .

4.1 Préliminaires.

Soit γ un nombre algébrique, qui est donc racine d'un polynôme à coefficients entiers :

$$\varphi(z) = a_n z^n + a_{n-1} z^{n-1} + \dots + a_0$$

tel que $a_n \neq 0$ et $n \geq 1$. On a : $\varphi(\gamma) = 0$.

LEMME 5 *Si γ est algébrique, $i\gamma$ est lui aussi algébrique.*

On pose $\gamma' = i\gamma$, ce qui donne $\gamma = -i\gamma'$, et on a :

$$\varphi(-i\gamma') = 0$$

d'où :

$$\varphi(-i\gamma') \cdot \varphi(i\gamma') = 0$$

On pose $Q(x) = \varphi(-ix) \cdot \varphi(ix)$ et on va démontrer que $\overline{Q(x)} = Q(x)$ pour x réel.

$$\begin{aligned} \overline{Q(x)} &= \overline{\varphi(-ix) \cdot \varphi(ix)} \\ &= \overline{\varphi(ix)} \cdot \overline{\varphi(-ix)} \\ &= \varphi(ix) \cdot \varphi(-ix) \\ &= Q(x) \end{aligned}$$

car φ est à coefficients entiers donc réels. Ceci prouve que les coefficients de Q sont réels. Par ailleurs, les coefficients de Q sont des sommes de produits d'entiers et de nombres parmi 1, -1 , i et $-i$. Les coefficients de Q sont donc entiers. De plus :

$$Q(i\gamma) = \varphi(-ii\gamma) \varphi(ii\gamma) = \varphi(\gamma) \varphi(-\gamma) = 0$$

On a ainsi démontré que si γ est algébrique $i\gamma$ l'est aussi. ■

LEMME 6 *Si z est algébrique, il existe un entier c tel que cz soit un entier algébrique.*

On a :

$$\varphi(z) = a_n z^n + a_{n-1} z^{n-1} + \dots + a_0 = 0$$

avec $n \geq 1$ et $a_n \neq 0$. On définit $\psi(z)$ par :

$$\psi(z) = a_n^{n-1} \varphi\left(\frac{z}{a_n}\right)$$

On a :

$$\psi(z) = a_n^{n-1} a_n \left(\frac{z}{a_n}\right)^n + a_n^{n-1} a_{n-1} \left(\frac{z}{a_n}\right)^{n-1} + \dots + a_n^{n-1} a_1 \left(\frac{z}{a_n}\right) + a_n^{n-1} a_0$$

Ce polynôme est à coefficients entiers et normalisé. Par ailleurs,

$$\psi(a_n z) = a_n^{n-1} \varphi\left(\frac{a_n z}{a_n}\right) = a_n^{n-1} \varphi(z) = 0$$

$a_n z$ est donc un entier algébrique, ce qui prouve le lemme avec $c = a_n$. ■

4.2 Intervention de la formule d'Euler $1 + e^{i\pi} = 0$.

Donc, si π est algébrique, $i\pi$ est lui aussi algébrique et $ci\pi$ est un entier algébrique pour un certain entier c . On a donc $\varphi(ci\pi) = 0$, où $\varphi(z)$ est un polynôme canonique :

$$\varphi(z) = z^n + a_{n-1}z^{n-1} + \dots + a_1z + a_0$$

On appelle $c\beta_1, c\beta_2, \dots, c\beta_n$ les racines du polynôme $\varphi(z)$. Il existe un entier q tel que $1 \leq q \leq n$ et $\beta_q = i\pi$, donc tel que (formule d'Euler) :

$$1 + e^{\beta_q} = 0$$

On a donc :

$$\prod_{i=1}^n (1 + e^{\beta_i}) = 0$$

Quand on développe ce produit, on obtient la somme de 1 et de produits d'exponentielles, c'est-à-dire des exponentielles de sommes de nombres pris parmi les β_i . Certaines de ces sommes sont nulles et ont donc des exponentielles égales à 1. On regroupe tous ces 1 sous la forme d'un entier $k > 0$, et on a :

$$k + e^{\alpha_1} + e^{\alpha_2} + \dots + e^{\alpha_s} = 0 \quad (5)$$

où les $\alpha_1, \dots, \alpha_s$ sont toutes les sommes non nulles de nombres pris parmi les β_i . Il y a juste à montrer que l'équation (5) est impossible.

4.3 Un polynôme canonique.

LEMME 7 *Le polynôme :*

$$\Lambda(x) = (x - c\alpha_1) \dots (x - c\alpha_s) = \prod_{j=1}^s (x - c\alpha_j)$$

est à coefficients entiers (et donc canonique).

Il s'agit de montrer que $c\alpha_1, \dots, c\alpha_s$ sont les racines d'un polynôme canonique. On sait que $c\beta_1, \dots, c\beta_n$ sont les racines du polynôme canonique $\varphi(z)$. Les lemmes 2 et 3 montrent qu'il en est de même de la famille $c\alpha_1, \dots, c\alpha_s$. ■

Remarque : Comme c est entier, $\Lambda(cx)$ est encore à coefficients entiers, mais n'est plus nécessairement normalisé.

4.4 Une égalité qui s'avèrera impossible.

Pour démontrer que l'équation (5) est impossible, on considère le polynôme $P(x)$ suivant :

$$P(x) = \frac{x^{p-1}}{(p-1)!} \Lambda(cx)^p \quad (6)$$

où p est un nombre premier quelconque. Ce polynôme est de degré $ps + p - 1$.
On pose comme précédemment :

$$Q_P(x) = P(x) + P'(x) + \dots + P^{(ps+p-1)}(x)$$

Si on multiplie (5) par $Q_P(0)$ on obtient :

$$kQ_P(0) + \sum_{j=1}^s e^{\alpha_j} Q_P(0) = 0$$

Ou encore, d'après l'équation (3) (qui est valable pour tout polynôme $P(x)$, donc pour celui qui nous occupe ici) :

$$kQ_P(0) + \sum_{j=1}^s Q_P(\alpha_j) = - \sum_{j=1}^s R_P(\alpha_j) \quad (7)$$

On va montrer que pour p premier assez grand le membre de gauche de (7) est un entier non nul et que le membre de droite de (7) peut être rendu aussi petit qu'on veut.

4.5 Une question d'intégralité.

On a :

$$\begin{aligned} P^{(r)}(0) &= 0 && \text{si } r < p - 1 \\ P^{(r)}(\alpha_j) &= 0 && \text{si } r < p \end{aligned}$$

pour $j = 1, \dots, s$, puisque 0 est racine d'ordre $p - 1$ de $P(x)$ et α_j racine d'ordre p de $P(x)$.

D'après le lemme 4, $P^{(r)}(x)$ est le produit de p par un polynôme à coefficients entiers dès que $r \geq p$. On voit donc que :

$$\sum_{j=1}^s Q_P(\alpha_j)$$

est un polynôme symétrique en $\alpha_1, \dots, \alpha_s$ dont tous les coefficients sont des entiers divisibles par p . Cette expression est donc un entier divisible par p d'après le théorème 1 et le lemme 7.

De même, $Q_P(0)$ est la somme de $P^{(p-1)}(0)$ et d'un entier multiple de p , puisque $P^{(r)}(0)$ est un entier multiple de p dès que $r \geq p$.

Le membre de gauche de (7) se réduit donc à :

$$kP^{(p-1)}(0) + \text{multiple de } p$$

Pour en faire un entier non nul, il suffit de choisir p de telle sorte que $kP^{(p-1)}(0)$ soit premier à p . Or, on a :

$$P^{(p-1)}(0) = \Lambda(0)^p$$

d'après le lemme 4. On choisit donc p premier strictement plus grand que tous les facteurs de $kP^{(p-1)}(0)$, c'est-à-dire strictement plus grand que k et $|\Lambda(0)|$ (qui sont des entiers indépendants de p).

4.6 Une majoration.

On a, pour $j = 1, \dots, s$:

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

Comme s est indépendant de p , il suffit de majorer l'expression ci-dessus pour rendre $\sum_{j=1}^s R_P(\alpha_j)$ aussi petit qu'on veut.

Notons H un majorant des $|\alpha_j|$ ($j = 1, \dots, s$) et M le maximum du module de $P(x)$ pour les complexes x tels que $|x| \leq H$. On a alors $|\alpha_j| \leq H$, $|e^{\alpha_j}| \leq e^H$ et $|e^{-\alpha_j x}| \leq e^H$, puisque $x \in [0, 1]$. Noter que H et M sont indépendants de p . On a :

$$|R_P(\alpha_j)| \leq H e^{2H} M$$

Or, pour $|x| \leq H$, on a $|cx - c\alpha_j| < c(|x| + |\alpha_j|) < 2|c|H$. On a donc d'après la définition de $P(x)$:

$$M < \frac{H^{p-1} (2|c|H)^{ps}}{(p-1)!}$$

Si on pose $K = (2|c|H)^s$, on obtient :

$$M < K \frac{(HK)^{p-1}}{(p-1)!}$$

Comme H et K sont indépendants de p , on voit qu'en prenant p (premier) assez grand, on rend M aussi petit qu'on veut, ce qui termine la démonstration.

Références

- [1] **Georges Valiron** *Théorie des Fonctions*. (Troisième édition) Masson 1966.
- [2] **Serge Lang** *Algebra*. (Second edition) Addison-Wesley 1970.