UFR de mathématique et d'informatique
Université de Strasbourg

Mémoire de L3 Magistère

Critères de rationalité de séries formelles : applications à l'arithmétique et à la géométrie algébrique

par
Damien Junger

encadré par
Arthur-César Le Bras

2025

Je souhaite remercier M. Le Bras d'avoir encadré ce mémoire. Ses conseils ont été précieux à chaque rencontre, et il a toujours su me pousser plus loin dans mes retranchements. Je retiens de nos conversations et des conférences et séminaires auxquels il m'a invité une belle image du merveilleux monde de l'arithmétique et de la géométrie algébrique, quoique parfois floue, mais que j'espère clarifier dans les années à venir.
Je remercie également M. Frățilă de m'avoir introduit au p-adique, qui a orienté mes recherches de sujet, et M. Charles d'avoir définie une partie abordable dans l'article [CDT24], traitée dans la dernière partie.

« Là-haut, la terre est bleue comme une orange »
Livre ancien, *Mur de la tour d'Ær*

Table des matières

I Introduction

L'objet principal de ce mémoire est l'étude des séries formelles dans leur relation avec la théorie des nombres.
Il ne semble pas *a priori* exister de liens très étroits entre ces deux branches des mathématiques. Nous pouvons déjà évoquer les nombreux ponts qui ont été créés entre l'arithmétique et l'analyse complexe pendant les deux derniers siècles : théorème des nombres premiers, fonctions L de Dirichlet, formes modulaires, et peut être le plus célèbre d'entre tous, l'hypothèse de Riemann.
L'introduction des séries formelles s'est alors faite par analogie avec les polynômes : nous dirons que les séries formelles sont aux séries entières ce que les polynômes sont aux fonctions polynômiales. Il existe en plus un avantage supplémentaire : nous nous affranchissons des problèmes de convergence. Nous ne nous intéressons plus qu'à leurs propriétés algébriques, dans un premier temps du moins. Nous développerons en série de Taylor formellement, et écrirons par exemple :

$$\frac{1}{1-X} = \sum_{n=0}^{\infty} X^n,$$

sans préciser quoi que ce soit sur un potentiel domaine de validité de cette formule. L'exemple de fonctions les plus simples à développer en série sont les fractions rationnelles. Réciproquement, on peut se demander si une série formelle est le développement de Taylor d'une fraction rationnelle. Ce n'est pas toujours le cas (par exemple, la série $\exp(X) = \sum_{n=0}^{\infty} \frac{X^n}{n!}$ n'est pas rationnelle ; elle n'a pas de pôle, par exemple).

Le centre de ce mémoire est l'étude de *critères de rationalité* de séries formelles. Le théorème de Kronecker III.1 nous offre déjà une caractérisation algébrique de rationalité en fonction de relations entre les coefficients (décrites sous forme de déterminants).
D'un point de vue plus analytique, l'approche « naïve » est celle de se ramener aux séries entières : où ma série converge t-elle dans le plan complexe ? Commençons par supposer que les coefficients de la série sont entiers, pour nous ramener à des considérations arithmétiques. Le théorème III.5 donne immédiatement une réponse favorable si elle converge dans un disque de rayon $R > 1$, et Borel énonce même qu'il suffit la méromorphie (plus précisément, qu'elle se prolonge en une fonction méromorphe dans un tel disque) : théorème III.6.
Cela reste tout de même assez contraignant : nous voulons étendre la classe de domaines considérés. Même dans les fonctions usuelles (racine carrée ou un logarithme par exemple) le domaine peut être le plan privé de certaines branches, voir un demi plan entier etc. Mais comment mesurer ces parties aussi efficacement que le fait le rayon pour le disque ? C'est la notion de *diamètre transfini* (§III.2.2) qui le permet le plus fidèlement. On peut étendre le théorème de Borel à des parties du plan sous une condition similaire à « $R > 1$ » (théorème III.13 de Pólya).
D'un autre côté, nous voulons étendre les critères à des séries formelles à coefficients disons rationnels. Il va alors falloir prendre du recul, et ne plus considérer la convergence sur $\mathbb{C}$, mais aussi sur les $\mathbb{C}_p$, qui sont des analogues (dans un sens défini §II.2.2) pour des complétions de $\mathbb{Q}$ par rapport aux autres valeurs absolues, les valeurs absolues p-adiques (§II.1). Nous pouvons alors énoncer des analogues aux théorèmes de Borel et Pólya : ce sont les théorèmes de Dwork III.14 et Bertrandias III.15.

Une fois ces outils en main, nous nous attaquons à des problèmes concrets d'arithmétique.

Dans la partie IV, nous examinerons une propriété générale sur les racines de polynômes à coefficients entiers, unitaires et irréductibles. Un théorème dû à Kronecker (IV.4) traite le cas où toutes les racines sont de module inférieure à 1. Le théorème central de cette partie examine le cas général : c'est le théorème de Schinzel-Zassenhaus. Dans le cas d'un polynôme de degré $n > 1$, ou il s'agit d'un polynôme cyclotomique (on se ramène au cas du théorème de Kronecker), où l'on a une borne sur la plus grande racine de ce polynôme, ne dépendant **que** de son degré ! L'utilisation de l'un de nos critères de rationalité trouve sa justification dans le lemme IV.7, qui offre une caractérisation de la cyclotomie *via* la rationalité d'une série dérivant du polynôme de départ : terrain d'entraînement par excellence pour nos critères !

Ensuite, dans la partie V, nous nous occuperons d'un critère de transcendance sur les nombres complexes, le théorème de Lindemann-Weierstrass. L'énoncé uniquement arithmétique dans un premier temps, trouve une formulation équivalente dans le langage des séries formelles (V.9), où le problème est ramené à montrer la rationalité d'un certain type de séries. Le point délicat de cette preuve repose sur le contrôle du diamètre transfini sur les places p-adiques, voir V.3.

Finalement, nous étudierons une propriété plus faible que le transcendance : l'irrationalité. Nous essaierons de tirer de la preuve d'Apéry sur l'irrationalité de $\zeta(3)$ une méthode généralisable pouvant s'appliquer à d'autres nombres, en particulier des valeurs de séries L de Dirichlet. C'est dans cette optique de systématisation que nous trouverons pertinente l'usage de séries formelles. Nous tenterons alors de développer de nouveaux outils, plus généraux que les théorèmes de rationalité, que nous appellerons théorèmes de *bornes holonomiques* (*holonomy bound* en anglais). Nous mettrons en pratique ces résultats sur une application assez modeste VI.3. Nous évoquerons tout de même en conclusion des résultats inédits, qui sont l'aboutissement (pour le moment du moins) de ces nouveaux outils.

Nous citerons aussi l'application du critère de Dwork dans la résolution de la première hypothèse de Weil sur la rationalité des fonctions ζ sur les corps finis (voir l'article de Serre [Ser60] à ce propos), qui donne un exemple d'usage de ces théories en géométrie algébrique.
Nous recommandons également au lectorat curieux le document de Chambert-Loir [CN23] sur les extensions récentes des théorèmes de rationalité sur d'autres types d'espaces, conjointement au développement de la théorie d'Arakelov.

II Notions préliminaires

« Toutes les lois des nombres dépendent du système de base adopté et sont déterminées par lui. »
Friedrich Engels, notes sur la *Dialectique de la Nature*

II.1 Valeurs absolues et corps valués

II.1.1 Valeurs absolues et valuations

Définition II.1.

Soit $\mathbb{K}$ un corps.
On appelle *valeur absolue* sur $\mathbb{K}$ toute application $|\cdot| : \mathbb{K} \to \mathbb{R}^+$ vérifiant :
(VA1) $\forall x \in \mathbb{K}, |x| = 0 \Leftrightarrow x = 0$
(VA2) $\forall (x, y) \in \mathbb{K}^2, |xy| = |x||y|$
(VA3) $\forall (x, y) \in \mathbb{K}^2, |x + y| \leq |x| + |y|$.

La valeur absolue est dite *ultramétrique* si de plus on a la condition :
(VA3') $\forall (x, y) \in \mathbb{K}^2, |x + y| \leq \max(|x|, |y|)$.

Remarque II.1.

Il existe une valeur absolue $|\cdot|_0$, dite triviale, que l'on peut définir sur tout corps par $|0|_0 = 0$ et $|x|_0 = 1$ si $x \neq 0$.

Définition II.2.

Soit $\mathbb{K}$ un corps.
On appelle *valuation* sur $\mathbb{K}$ toute application $v : \mathbb{K} \to \mathbb{R} \cup \{+\infty\}$ vérifiant :
(V1) $\forall x \in \mathbb{K}, v(x) = +\infty \Leftrightarrow x = 0$
(V2) $\forall (x, y) \in \mathbb{K}^2, v(xy) = v(x) + v(y)$
(V3) $\forall (x, y) \in \mathbb{K}^2, v(x + y) \geq \min(v(x), v(y))$.

On déduit de (V2) que $v(\mathbb{K}^*)$ est un sous-groupe additif de $\mathbb{R}$. On dira que v est discret ou dense selon si $v(\mathbb{K}^*)$ est discret ou dense.

Remarque II.2.

Se donner une valuation revient à se donner une valeur absolue ultramétrique sur un corps $\mathbb{K}$:

— Si v est une valuation sur $\mathbb{K}$ et $a \in]0, 1[$, alors $x \mapsto \begin{cases} 0 \text{ si } x = 0 \\ a^{v(x)} \text{ si } x \neq 0 \end{cases}$ est une valeur absolue ultramétrique sur $\mathbb{K}$.

— Si $|\cdot|$ est une valeur absolue ultramétrique sur $\mathbb{K}$ et $b \in]0, +\infty[$, alors $x \mapsto \begin{cases} +\infty \text{ si } x = 0 \\ -b \ln(|x|) \text{ si } x \neq 0 \end{cases}$ est une valuation sur $\mathbb{K}$.

On peut dans un tel cas associer une distance sur $\mathbb{K}$ définie par $d(x, y) = |x - y|$. On dira dans un tel cas que $(\mathbb{K}, v)$, ou $(\mathbb{K}, |\cdot|)$, ou bien $(\mathbb{K}, d)$ est un *corps valué ultramétrique* ou *corps valué non-archimédien*.

On pourra alors jongler entre valeur absolue ultramétrique et valuation selon les convenances.

II.1.2 Notions algébriques sur les corps valués

Lemme II.1.

Soit (K, v) un corps valué.
L'ensemble $\mathscr{O}_K := \{x \in K, v(x) \geq 0\}$ est un anneau local, d'idéal maximal $\mathfrak{m}_K := \{x \in K, v(x) > 0\}$.

Démonstration

On ne montre que le caractère maximal (le reste est clair). Si $x \in \mathscr{O}_K \backslash \mathfrak{m}_K$, alors $v(x) = 0$, et $v(x^{-1}) = -v(x) = 0$, donc $\mathscr{O}_K \backslash \mathfrak{m}_K = \mathscr{O}_K^\times$, c'est donc l'unique idéal maximal de l'anneau $\mathscr{O}_K$. □

Définition II.3.

$\mathscr{O}_K$ est appelé l'*anneau des entiers de* K, et le corps $k_K := \mathscr{O}_K/\mathfrak{m}_K$ est le corps résiduel de K.

II.1.3 Propriétés métriques des corps valués ultramétriques

Dans ce paragraphe, $(\mathbb{K}, d)$ désigne un corps valué ultramétrique muni de sa distance.

Proposition II.2.

(1) Soit $(x, y, z) \in \mathbb{K}^3$ tels que $d(x, y) \neq d(y, z)$. Alors $d(x, z) = \max(d(x, y), d(y, z))$.
(2) Tout point d'une boule de $\mathbb{K}$ en est un centre.
(3) Deux boules de $\mathbb{K}$ sont disjointes ou comparables (*ie* l'une est incluse dans l'autre).
(4) Toute boule ouverte de $\mathbb{K}$ est fermée.

Démonstration (II.2)

(1) On peut supposer $d(x, y) < d(y, z)$. Alors :

$$d(x, z) \leq \max(d(x, y), d(y, z)) = d(y, z) \text{ et } d(y, z) \leq \max(d(y, x), d(x, z)) = d(x, z),$$

donc $d(x, z) = d(y, z) = \max(d(x, y), d(y, z))$.
(2) Soient $x \in \mathbb{K}$ et $r > 0$. On note $\mathbb{B}(x, r) := \{y \in \mathbb{K}, d(x, y) < r\}$ la boule de centre x et de rayon r. Soient $y, z \in \mathbb{B}(x, r)$. Alors :

$$d(y, z) \leq \max(d(y, x), d(x, z)) < r,$$

donc $\mathbb{B}(x, r) \subseteq \mathbb{B}(y, r)$ et l'autre inclusion est semblable, donc y est bien un centre de $\mathbb{B}(x, r)$.
(3) Soient $x, y \in \mathbb{K}$ et $r, r' > 0$ tels que $\mathbb{B}(x, r) \cap \mathbb{B}(y, r') \neq 0$. Alors il existe un point commun z aux deux boules. D'après (2), c'est un centre de chacune d'elles, donc l'une est incluse dans l'autre (en fonction de si $r > r'$ ou $r \leq r'$).
(4) Soit $\mathbb{B}$ une boule ouverte de rayon r. Alors $\mathbb{B}^c = \bigcup_{x \in \mathbb{B}^c} \mathbb{B}(x, r)$ d'après (3), donc $\mathbb{B}^c$ est ouvert, donc $\mathbb{B}$ est fermée.

□

Définition II.4.

Soit $(a_n)_{n\in\mathbb{N}}$ une suite d'éléments de $\mathbb{K}$.
On dit que $(a_n)_{n\in\mathbb{N}}$ est une suite de Cauchy si :

$$\forall \varepsilon > 0, \exists N \in \mathbb{N}, \forall (m,n) \in \mathbb{N}^2, (m > n > N) \Rightarrow d(a_m, a_n) < \varepsilon$$

Définition II.5.

Soit $(\mathbb{K}, d)$ un corps valué ultramétrique.
On dit que $(\mathbb{K}, d)$ est complet si toute suite de Cauchy de $\mathbb{K}$ admet une limite dans $\mathbb{K}$.

Proposition II.3.

Soit $(a_n)_{n\in\mathbb{N}}$ une suite d'éléments de $\mathbb{K}$.
Alors $(a_n)_{n\in\mathbb{N}}$ est de Cauchy si, et seulement si, $d(a_n, a_{n+1}) \underset{n\to+\infty}{\longrightarrow} 0$.

Démonstration (II.3)

Le sens direct est clair.
Pour le sens réciproque : soit $\varepsilon > 0$. Il existe $N \in \mathbb{N}$ tel que pour tout entier et $n > N$, $d(a_n, a_{n+1}) < \varepsilon$. Soient m et n des entiers tels que $m > n > N$. Alors :

$$d(a_m, a_n) \leq \max(d(a_m, a_{m+1}), d(a_{m+1}, a_n)) \leq \cdots \leq \max_{m\leq k\leq n-1}(d(a_k, a_{k+1})) \leq \varepsilon.$$

Donc $(a_n)_{n\in\mathbb{N}}$ est de Cauchy.

□

Corollaire II.4.

Soit $(u_n)_{n\in\mathbb{N}}$ une suite d'éléments de $\mathbb{K}$. On suppose $\mathbb{K}$ complet.
Alors $\sum_{n\geq 0} u_n$ converge si, et seulement si, $(u_n)_{n\in\mathbb{N}}$ converge vers 0.

Démonstration (II.4)

Le sens direct est clair.
Pour le sens réciproque, notons $a_n := \sum_{k=0}^{n} u_k$. Avec le lien suite-série, $(u_n)_{n\in\mathbb{N}}$ et $(a_{n+1} - a_n)_{n\in\mathbb{N}}$ ont même nature, donc si la première converge vers 0, il en est de même pour la deuxième, et donc de la suite $d(a_n, a_{n+1})$. Donc $(a_n)_{n\in\mathbb{N}}$ est une suite de Cauchy d'après la proposition précédente, donc converge car $\mathbb{K}$ est complet.

□

À un corps valué, on peut associer la topologie définie par sa valeur absolue. On peut s'intéresser aux différentes topologies induites :

Définition II.6.

Soit $|\cdot|_1$ et $|\cdot|_2$ deux valeurs absolues sur $\mathbb{K}$.
On dit que $|\cdot|_1$ et $|\cdot|_2$ sont *équivalentes* si elles définissent la même topologie.
On appelle *places du corps* $\mathbb{K}$ les classes d'équivalence pour cette relation.

On peut définir la même notion dans des espaces métriques, mais les relations supplémentaires qu'imposent les valeurs absolues permettent une meilleure compréhension de ces places :

Proposition II.5.

Soit $|\cdot|_1$ et $|\cdot|_2$ deux valeurs absolues sur $\mathbb{K}$.
$|\cdot|_1$ et $|\cdot|_2$ sont équivalentes si, et seulement s'il existe $b > 0$ tel que $|\cdot|_1 = |\cdot|_2^b$.

Démonstration (II.5)

$\Rightarrow$: On pose $M := \{x \in \mathbb{K}, |x|_1 < 1\}$. Or $(x^n \underset{n\to\infty}{\longrightarrow} 0) \Leftrightarrow (|x|_i < 1)$ (pour $i = 1, 2$), donc par hypothèse, $M = \{x \in \mathbb{K}, |x|_2 < 1\}$. Si $M = 0$, alors $|\cdot|_1 = |\cdot|_2 = |\cdot|_0$ est la valeur absolue triviale : si $x \neq 0$, $|x|_i \geq 1$ et $|x^{-1}|_i \geq 1$, donc $|x|_i = 1$. Sinon, il existe $a \in M\backslash\{0\}$. Posons $b := \frac{\ln(|a|_1)}{\ln(|a|_2)} > 0$ (c'est le quotient de deux nombres négatifs). Soit $x \in \mathbb{K}$. Pour tout couple d'entiers (m, n),

$$\frac{n}{m}\frac{\ln(|x|_1)}{\ln(|a|_1)} > 1 \Leftrightarrow |x|_1^n < |a|_1^m \Leftrightarrow \frac{x^n}{a^m} \in M \Leftrightarrow |x|_2^n < |a|_2^m \Leftrightarrow \frac{n}{m}\frac{\ln(|x|_2)}{\ln(|a|_2)} > 1.$$

Donc $\frac{\ln(|x|_1)}{\ln(|a|_1)} = \frac{\ln(|x|_2)}{\ln(|a|_2)}$ (ces nombres définissent la même coupure de Dedekind), *ie* $|x|_1 = |x|_2^b$.
$\Leftarrow$: S'il existe $b > 0$ tel que $|\cdot|_1 = |\cdot|_2^b$, alors pour un point $x \in \mathbb{K}$, $\{\mathbb{B}_1(x, r), r > 0\} = \{\mathbb{B}_2(x, r), r > 0\}$ ($|x - y|_1 < r \Leftrightarrow |x - y|_2 < r^b$) donc les topologies sont les mêmes.

□

II.1.4 Complétion de corps valués ultramétriques

Rappelons un résultat général sur la complétion d'espace métrique dans notre cas particulier d'un corps valué ultramétrique $(\mathbb{K}, |\cdot|)$.

Théorème II.6.

Soit $(\mathbb{K}, |\cdot|)$ un corps valué ultramétrique. Alors :

(*i*) Il existe un corps valué ultramétrique complet $(\mathbb{K}', |\cdot|')$ et une injection canonique $\iota : \mathbb{K} \to \mathbb{K}'$ telle que $\iota(\mathbb{K})$ est dense dans $\mathbb{K}'$.

(*ii*) Le couple $(\mathbb{K}', |\cdot|')$ est unique à isomorphisme isométrique près, on l'appelle le *complété de* $\mathbb{K}$ pour la valeur absolue $|\cdot|$.

Lemme II.7.

Soient $a = (a_n)_{n\in\mathbb{N}}$ et $b = (b_n)_{n\in\mathbb{N}}$ une suite d'éléments de Cauchy d'éléments de $\mathbb{K}$. Alors :

(*a*) $(|a_n|)_{n\in\mathbb{N}}$ converge dans $\mathbb{R}^+$

(*b*) Si a ne converge pas vers 0, $(|a_n|)_{n\in\mathbb{N}}$ est stationnaire

(*c*) Si $a - b$ converge vers 0, $(|a_n|)_{n\in\mathbb{N}}$ et $(|b_n|)_{n\in\mathbb{N}}$ admettent la même limite.

Démonstration (II.7)

(*a*) Avec l'inégalité triangulaire « renversée », pour tous entiers m et n, $||a_{m+n}| - |a_m|| \leq |a_{m+n} - a_m|$, donc $(|a_n|)_{n\in\mathbb{N}}$ est de Cauchy, donc converge car $\mathbb{R}^+$ est complet.
(*b*) Il existe $\delta > 0$ et $N \in \mathbb{N}$ tel que pour tout $m > N$ et tout $n \in \mathbb{N}$, $|a_m| > \frac{2}{3}\delta$ (limite non nulle) et $|a_{m+n} - a_m| < \frac{1}{2}\delta$ (est de Cauchy). Donc $|a_{m+n} - a_m| < |a_m|$. Par l'inégalité ultramétrique, on a alors $|a_{m+n}| = |a_m|$ pour tout entier n, d'où le résultat.

(c) Encore une fois par inégalité triangulaire renversée.

□

Démonstration (II.6)

(i) L'ensemble $\mathcal{C}$ des suites de Cauchy est un sous-anneau de $\mathbb{K}^{\mathbb{N}}$. Notons $\mathcal{I}$ le sous-ensemble de $\mathcal{C}$ constitué des suites convergentes vers 0. Montrons que c'en est un idéal maximal.
C'est clairement un sous-groupe additif, et si $x \in \mathcal{C}$, $a \in \mathcal{I}$, alors x est bornée, donc ax converge bien vers 0 ; c'est donc un idéal.
Soit $a \in \mathcal{C}\backslash\mathcal{I}$. D'après le lemme, il existe $\delta > 0$ et $N \in \mathbb{N}$ tels que pour tout $n > N$, $|a_n| \geq \delta$. Alors on définit $(b_n)_{n\in\mathbb{N}}$ par $b_n = 0$ si $n \leq N$ et a_n^{-1} si $n > N$. Alors $(b_n)_{n\in\mathbb{N}}$ est une suite de Cauchy et $ab - 1$ converge vers 0. Donc la classe de a est inversible dans l'anneau $\mathcal{C}/\mathcal{I}$, donc c'est un corps, donc $\mathcal{I}$ est maximal.
On définit alors

$$\mathbb{K}' := \mathcal{C}/\mathcal{I},\ \iota : \begin{array}{ccc} \mathbb{K} & \hookrightarrow & \mathbb{K}' \\ x & \mapsto & [(x)_{n\in\mathbb{N}}]. \end{array}$$

On peut aussi poser (sans ambiguïté d'après le (c) du lemme) pour tout $x \in \mathbb{K}'$, $|x|' := \lim\limits_{n\to\infty} |x_n|$ si x_n converge vers x. La vérification des axiomes de valeur absolue ultramétrique est laissée à la sagacité du lecteur, en utilisant la continuité de $|\cdot|$. On note aussi que cette définition rend ι isométrique.
Montrons que $\iota(\mathbb{K})$ est dense dans $\mathbb{K}'$. Soit $a = (a_n)_{n\in\mathbb{N}} \in \mathcal{C}$. Alors $|a - a_n|' \leq \sup_{p>0}(|a_{n+p} - a_n|)$ (où $a_n := \iota(a_n)$ est la suite constante égale à a_n dans le terme de gauche). Le terme de gauche converge vers 0 car a est une suite de Cauchy, donc $a = \lim\limits_{n\to\infty} \iota(a_n)$, donc $\iota(\mathbb{K})$ est dense dans $\mathbb{K}'$.
Enfin, montrons que $\mathbb{K}'$ est bien complet. Soit $a = (a_n)_{n\in\mathbb{N}}$ une suite de Cauchy de $\mathbb{K}'$. $\iota(\mathbb{K})$ est dense dans $\mathbb{K}'$, donc pour tout $n \in \mathbb{N}$, il existe $b_n \in \mathbb{K}$ tel que $|a_n - \iota(b_n)|' \leq 2^{-n}$. Alors :

$$|b_{n+p} - b_n| = |\iota(b_{n+p}) - \iota(b_n)|' \leq \max(|\iota(b_{n+p}) - a_{n+p}|', |a_{n+p} - a_n|', |a_n - b_n|'),$$

donc $b = (b_n)_{n\in\mathbb{N}}$ est une suite de Cauchy (dans $\mathbb{K}$). Donc $(\iota(b_n))_{n\in\mathbb{N}}$ converge dans $\mathbb{K}'$. Il en est donc de même pour a, ce qui montre bien que $\mathbb{K}'$ est complet pour $|\cdot|'$.
(ii) Soit $(\mathbb{K}'', |\cdot|'', j)$ un autre triplet vérifiant (i). Alors on a un isomorphisme isométrique $\alpha = i \circ j : j(\mathbb{K}) \to i(\mathbb{K})$. Or $j(\mathbb{K})$ est dense dans $\mathbb{K}''$, donc il admet un unique prolongement continu sur $\mathbb{K}''$ (défini par $\alpha(x) = \lim\limits_{n\to\infty} \alpha(x_n)$ si $x \in \mathbb{K}''$ et $x_n \underset{n\to\infty}{\longrightarrow} x$). Par continuité + et $\times$, on vérifie qu'il s'agit aussi d'un isomorphisme algébrique.

□

Remarque II.3.

Deux valeurs absolues équivalentes donnent le même complété.

II.2 Nombres p-adiques

II.2.1 L'espace métrique $\mathbb{Q}_p$

a. Valeurs absolues sur $\mathbb{Q}$

Examinons le cas particulier de $\mathbb{K} = \mathbb{Q}$. On est déjà habitué à la valeur absolue dite *infinie* et notée $|\cdot|_\infty$, définie par $|x|_\infty = \max(x, -x)$ pour tout rationnel x. Nous en cherchons d'autres ici.

Dans la suite de la partie, p désignera un nombre premier (positif).

Définition II.7.

Soit $x \in \mathbb{Z}\backslash\{0\}$.
On définit l'entier naturel noté $v_p(x)$ suivant :

$$v_p(x) := \max\{m \in \mathbb{N},\ p^m | x\}.$$

On posera $v_p(0) = +\infty$.
Si $x = a/b \in \mathbb{Q}^*$, on définit de même dans $\mathbb{Z}$:

$$v_p(x) := v_p(a) - v_p(b).$$

Ce nombre ne dépend pas du représentant de x.

Proposition II.8.

v_p est une valuation sur $\mathbb{Q}$, et on l'appelle *valuation p-adique*.

Démonstration (II.8)

— (V1) est claire.
Pour des entiers a et b non nuls, on note $a = p^{v_p(a)}h$ et $b = p^{v_p(b)}h'$ avec $p \nmid h$, $p \nmid h'$.

— (VA2) On a :

$$ab = p^{v_p(a)+v_p(b)}hh' \text{ et } p \nmid hh',$$

donc $v_p(ab) = v_p(a) + v_p(b)$.

— (V3) On suppose $v_p(a) \geq v_p(b)$ sans perte de généralité :

$$a + b = p^{v_p(b)}(p^{v_p(a)-v_p(b)}h + h'),$$

donc $v_p(a + b) \geq \min(v_p(a), v_p(b))$.
Ces expressions restent valables pour a et b rationnels.

□

Corollaire II.9.

L'application :

$$\begin{array}{rl} \mathbb{Q} \to & \mathbb{R}^+ \\ x \mapsto & \begin{cases} 0 \text{ si } x = 0 \\ p^{-v_p(x)} \text{ sinon} \end{cases} \end{array}$$

est une valeur absolue ultramétrique sur $\mathbb{Q}$, appelée *valeur absolue p-adique* et notée $|\cdot|_p$.

On peut exhaustivement classifier les valeurs absolues sur $\mathbb{Q}$:

Théorème II.10 (Ostrowski).

Soit $|\cdot|$ une valeur absolue non triviale sur $\mathbb{Q}$. Alors on est dans l'un des cas (exclusifs) suivants :

(1) Il existe p premier et $b > 0$ tel que $|\cdot| = |\cdot|_p^b$,

(2) Il existe $\alpha \in]0, 1]$ tel que $|\cdot| = |\cdot|_\infty^\alpha$.

La disjonction de cas se fait selon s'il existe $n \in \mathbb{N}$ tel que $0 < |n| < 1$.
On n'étudie que la restriction à $\mathbb{N}$ de la valeur absolue car elle se prolonge de manière unique sur $\mathbb{Q}$ (en posant $|x| := |-x|$ si $x < 0$ est entier et $|\frac{a}{b}| = \frac{|a|}{|b|}$ si $a, b \in \mathbb{Z}\backslash\{0\}$).
On montre le lemme suivant :

Lemme II.11.

S'il existe un nombre premier p tel que $|p| < 1$,

(i) Pour tout $b \in \mathbb{N}, |b| \leq 1$

(ii) Pour tout entier q premier avec $p, |q| = 1$.

Démonstration (II.11)

(i) Soit $b \in \mathbb{N}$. Pour tout entier $k > 0$, on écrit $b^k = \sum_{i=0}^{h_k} b_{i,k} p^i$ (avec $0 \leq b_{i,k} < p$ et $b_{h_k,k} \neq 0$) en base p. Alors on obtient la majoration :

$$|b|^k = |b^k| \leq \sum_{i=0}^{h_k} |b_{i,k}||p|^i \leq (h_k + 1)M, \qquad (\dagger)$$

où $M = \max_{0 \leq l \leq p-1}(|l|)$. Or on a aussi

$$h_k \leq \frac{\ln(b^k)}{\ln(p)} < h_k + 1.$$

Posons $B := \frac{\ln(b)}{\ln(p)}$, de sorte que

$$|b| \leq M^{1/k}(Bk + 1)^{1/k},$$

d'où le résultat en passant à la limite en k.
(ii) Soit q premier avec p. Alors pour tout entier $n > 0$, p^n et q^n sont premiers entre eux, donc il existe u_n et v_n tels que :

$$u_n p^n + v_n q^n = 1.$$

Si on suppose que $|q| < 1$,

$$1 = |1| \leq |u_n p^n| + |v_n q^n| \overset{(i)}{\leq} |p|^n + |q|^n,$$

ce qui aboutit à une contradiction pour n assez grand.

□

Démonstration (II.10)

(1) Supposons qu'il existe $n \in \mathbb{N}$ tel que $0 < |n| < 1$. Alors il existe un facteur premier p de n tel que $|p| < 1$. Alors en posant $b := -\frac{\ln(|p|)}{\ln(p)}$. Tout entier m s'écrit (de manière unique) $m = p^{v_p(m)}m'$, avec $p \nmid m'$. Donc $|m| = |p^{v_p(m)}||m'| = |p|^{v_p(m)} = |m|_p^b$.

(2) Supposons que pour tout entier $n, |n| \geq 1$. $|\cdot|$ est non triviale, donc il existe $a \in \mathbb{N}$ tel que $|a| > 1$. Posons $\alpha := \frac{\ln(|a|)}{\ln(a)}$. On a $0 < \alpha < 1$. En effet, avec l'inégalité triangulaire :

$$|a| \leq 1 + |a-1| \leq \cdots \leq a.$$

On procède comme précédemment, avec cette fois-ci une majoration dans (†) par somme des termes d'une suite géométrique, ce qui nous donne en reprenant les notations, (avec p remplacé par a) :

$$|b| \leq M^{1/k} \left(\frac{|a|^{kB+1} - 1}{|a| - 1} \right)^{1/k},$$

d'où $|b| \leq |a|^B = b^\alpha$. Donc $\frac{\ln(|b|)}{\ln(b)} \leq \frac{\ln(|a|)}{\ln(a)} \leq \alpha$. En échangeant le rôle de a et b, si $|b| > 1$, alors $\frac{\ln(|b|)}{\ln(b)} = \alpha$.
Or tout entier $b > 1$ vérifie $|b| > 1$ (sinon, avec les calculs de (i), on aurait $|c| \leq 1$ pour tout entier c). Donc $|\cdot| = |\cdot|_\infty^\alpha$, ce qui assure le résultat.

□

Ce théorème apporte une condition nécessaire sur les valeurs absolues. Réciproquement :

Proposition II.12.

Soient $b > 0$, $\alpha \in]0, 1]$ et p un nombre premier. Alors $|\cdot|_p^b$ et $|\cdot|_\infty^\alpha$ sont des valeurs absolues sur $\mathbb{Q}$.

Démonstration (II.12)

Comme précédemment, on ne montre le résultat que pour des entiers naturels. (VA1) et (VA2) sont clairs. Soient $x, y \in \mathbb{N}\backslash\{0, 1\}$. Alors :

— $|x+y|_p^b \leq \max(|x|_p, |y|_p)^b = \max(|x|_p^b, |y|_p^b)$

— $|x+y|_\infty^\alpha \leq (|x|_\infty + |y|_\infty)^\alpha = e^{\alpha \ln(|x|_\infty + |y|_\infty)}) \overset{(\diamondsuit)}{\leq} e^{\alpha(\ln(|x|_\infty) + \ln(|y|_\infty))} \leq |x|_\infty^\alpha + |y|_\infty^\alpha$,

$(\diamondsuit)$ étant obtenue car $|x|_\infty + |y|_\infty \leq |x|_\infty |y|_\infty$.

□

Corollaire II.13.

Les places sur $\mathbb{Q}$ sont exactement la place infinie, les places p-adiques (pour tout p premier) et la place triviale.

Il s'avère qu'une formule lie toutes ces valeurs absolues :

Proposition II.14 (Formule du produit).

Pour tout $x \in \mathbb{Q}$,

$$|x|_\infty \prod_{p \text{ premier}} |x|_p = |x|_0$$

Remarque II.4.

Le produit ci-dessus est bien défini car $\{p \text{ premier}, |x|_p \neq 1\}$ est fini.

Démonstration (II.14)

Pour 0, la formule est claire. Si $x \neq 0$ est un entier, on écrit sa décomposition en produit de premiers :

$$x = \prod_{p \text{ premier}} p^{v_p(x)}$$

qui assure le résultat en mettant les termes du même côté, et on étend la formule aux rationnels. □

b. Complétions de $\mathbb{Q}$

On peut alors compléter $\mathbb{Q}$ avec ces valeurs absolues :

Définition II.8.

- On appelle *corps des nombres réels* et on note $\mathbb{R}$ le complété de $\mathbb{Q}$ pour la place infinie.
- Soit p un nombre premier. On appelle *corps des nombres p-adiques* et on note $\mathbb{Q}_p$ le complété de $\mathbb{Q}$ pour la place p-adique.

Remarque II.5.

On identifiera souvent places, valeurs absolues et leur indice, c'est-à-dire qu'on notera parfois « ∞ » la place infinie par exemple. On peut faire une telle identification car il y a une valeur absolue « canonique » pour chaque place, qui est normée pour la formule du produit.

Remarque II.6.

Notre approche des nombres p-adiques est purement analytique et ne nous intéresse uniquement comme outil pour la suite.
Il existe d'autres approches, plus algébriques, à la construction de $\mathbb{Q}_p$, et à son étude en soi. Nous recommandons la lecture du travail de notre prédécesseur [Gir24].

II.2.2 Le corps des nombres complexes p-adiques $\mathbb{C}_p$

On cherche ici à construire un sur-corps $\mathbb{C}_p$ de $\mathbb{Q}_p$, analogue à $\mathbb{C}$ pour $\mathbb{R}$.
On souhaiterait alors prendre comme définition, par analogie avec le cas archimédien, « $\mathbb{C}_p := \overline{\mathbb{Q}}_p$ » la clôture algébrique de $\mathbb{Q}_p$. Cependant, cette clôture algébrique n'est pas d'indice fini sur $\mathbb{Q}_p$ (là où $\mathbb{C}$ est d'indice 2 sur $\mathbb{R}$), et apparaît donc un phénomène peu souhaitable : ce corps n'est pas complet

pour la valeur absolue qu'il hérite de QQ_p. Heureusement, compléter ce corps permet d'obtenir un corps à la fois complet et algébriquement clos : voilà donc notre analogue à $\mathbb{C}$.
La construction étant un peu fastidieuse, on reportera le lectorat curieux à l'annexe A.

II.3 Séries formelles

Grossièrement, une série formelle est une série entière dont la convergence n'est pas importante dans un premier temps. On pourra ensuite choisir un espace dans lequel on examinera la convergence (en général, $\mathbb{C}$ ou les $\mathbb{C}_p$).
Ce paragraphe donne les rudiments pour la compréhension de la suite. Une étude plus approfondie peut être trouvée dans [[Cal06], VII].

A désignera un anneau commutatif unitaire.

Définition II.9.

On appelle anneau des séries formelles en une indéterminée X, noté $A[[X]]$, le triplet $(A^{\mathbb{N}}, +, \times)$, où $A^{\mathbb{N}}$ est l'ensemble des suites de termes de A, dont les éléments $(a_n)_{n\geq 0}$ seront notés $\sum_{n\geq 0} a_n X^n$, et où les lois $+$ et $\times$ sont définies comme suit :

$$\left(\sum_{n\geq 0} a_n X^n\right) + \left(\sum_{n\geq 0} b_n X^n\right) := \sum_{n\geq 0} (a_n + b_n) X^n$$
$$\left(\sum_{n\geq 0} a_n X^n\right) \times \left(\sum_{n\geq 0} b_n X^n\right) := \sum_{n\geq 0} \left(\sum_{k=0}^{n} a_k b_{n-k}\right) X^n.$$

Définition II.10.

On définit l'*opérateur de dérivation formel* D de $A[[X]]$ comme l'opérateur suivant :

$$\begin{array}{rccc} D : & A[[X]] & \longrightarrow & A[[X]] \\ & \sum_{n\geq 0} a_n X^n & \longmapsto & \sum_{n\geq 1} a_n n X^{n-1} \end{array}.$$

Remarque II.7.

Cet opérateur est linéaire et vérifie la règle de Liebniz : $D(f \times g) = D(f) \times g + f \times D(g)$.

Proposition II.15.

Soit $f \in A[[X]]$.
f est inversible si, et seulement si $f(0)$ est inversible.

Démonstration

Voir [[Cal06], Théorème 7.23]

□

Dans la suite, on suppose que $A = K$ est un corps, et on note $K(X)$ le corps des fractions rationnelles à coefficients dans K.

Remarque II.8.

Une série formelle alors est inversible si, et seulement si son coefficient constant est non nul. On peut alors associer à une fraction rationnelle irréductible $\frac{p}{q} \in K(X)$ une série formelle $pq^{-1} \in K[[X]]$ si $q(0) \neq 0$.
On notera $K(X)_0$ l'ensemble des fractions rationnelles donc 0 n'est pas un pôle.

Proposition II.16.

Il existe un unique morphisme de K-algèbres $\psi : K(X)_0 \to K[[X]]$ dont la restriction à $K[X]$ est l'identité.

Démonstration

Voir [[Cal06], Proposition 7.36]

□

Définition II.11.

Soit $f \in K[[X]]$.
On dit que f est une *fonction rationnelle* si f est dans l'image de ψ.

Remarque II.9.

Toutes les séries formelles ne sont pas des fonctions rationnelles (*ie* ψ n'est pas un isomorphisme), c'est tout l'objet du présent mémoire. On peut s'en convaincre assez simplement en considérant le développement des séries entières usuelles sur $\mathbb{R}$.

III Critères de rationalité sur les séries formelles

« Les mathématiques consistent à prouver une chose évidente par des moyens complexes. »
George Pólya

III.1 Critère algébrique

Dans cette partie, on se donne un corps $\mathbb{K}$ de caractéristique 0.

On cherche dans un premier temps une méthode pour déterminer si une série formelle est rationnelle à l'aide de relations entre ses coefficients.
On peut en effet trouver un tel critère en exprimant ces relations sous la forme d'un certain déterminant :

Définition III.1.

Soient $a = (a_n)_{n\in\mathbb{N}}$ une suite d'éléments de $\mathbb{K}$, k et n des entiers.
On appelle déterminant de Hankel de rang k et d'ordre n, et on note $D_n^k(a)$, le déterminant de la matrice $(a_{n+i+j})_{0\leq i,j\leq k}$.

On notera $M_n^k(a)$ cette dernière matrice.
Le lemme suivant est essentiel : c'est de lui dont on se servira pour démontrer les critères plus importants par la suite.

Lemme III.1 (Kronecker).

Soit $f(X) = \sum_{n=0}^{\infty} a_n X^n$ une série formelle à coefficients dans $\mathbb{K}$.
$f(X)$ est une fonction rationnelle si, et seulement s'il existe des entiers k et n_0 tels que pour tout entier $n \geq n_0$, $D_n^k(a) = 0$.

Démonstration (III.1)

$\Rightarrow$: Il existe un polynôme $Q = \sum_{n=0}^{k} q_i X^i \in \mathbb{K}[X]$ tel que $P = \sum_{i=0}^{k} p_i X^i := Qf$ est un polynôme. Donc pour tout entier l, $p_l = \sum_{i=0}^{l} q_i a_{l-i}$. Donc pour $n > \deg(P)$, $\sum_{i=0}^{n} q_i a_{n-1} = 0$. Donc pour k, n entiers tels que $k + n > \deg(P) + \deg(Q)$,

$$\begin{pmatrix} a_n & a_{n+1} & \cdots & a_{n+k-1} & a_{n+k} \\ a_{n+1} & a_{n+2} & \cdots & a_{n+k} & a_{n+k+1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{n+k-1} & a_{n+k} & \cdots & a_{n+2k-2} & a_{n+2k-1} \\ a_{n+k} & a_{n+k+1} & \cdots & a_{n+2k-1} & a_{n+2k} \end{pmatrix} \begin{pmatrix} q_0 \\ q_1 \\ \vdots \\ q_{k-1} \\ q_k \end{pmatrix} = 0$$

Donc cette matrice n'est pas inversible car $Q \neq 0$, ce qui assure le résultat.
$\Leftarrow$: Montrons l'existence d'une suite $(b_0, \ldots, b_k) \in \mathbb{K}^{k+1}$ telle que pour tout n assez grand, $\sum_{i=0}^{k} b_i a_{n+i}$. On pourra conclure en exhibant un polynôme Q tel que Qf est aussi un polynôme, de manière analogue à la démonstration du sens direct.
Déjà, quitte à diminuer k, on peut supposer celui-ci minimal, au sens où $D_n^{k-1}(a) \neq 0$ pour une infinité de n.
On démontre un résultat intermédiaire :

Lemme III.2.

Si $D_{n_0}^{k-1}(a) = 0$, alors pour tout entier $n \geq n_0$, $D_n^{k-1}(a) = 0$.

Démonstration (III.2)

Si $D_{n_0}^{k-1}(a) = 0$, il existe une relation de liaison entre les lignes $(L_i)_{0\leq i\leq k-1}$ de la matrice $M_{n_0}^{k-1}(a)$: $\sum_{i=0}^{k-1} \lambda_i L_i = 0$.

- Si $\lambda_0 = 0$, on a directement une relation de liaison non triviale dans les lignes de sur $M_{n_0+1}^{k-1}(a)$, ce qui assure le résultat.
- Sinon, on peut écrire $L_0 = -\frac{1}{\lambda_0}\sum_{i=1}^{k-1} \lambda_i L_i$. En notant $(L'_i)_{0\leq i\leq k}$ les lignes de $M_{n_0}^{k}(a)$, $L'_0 = -\frac{1}{\lambda_0}\sum_{i=1}^{k} \lambda_i L'_i + (0,\dots,0,\beta)$.

  - Si $\beta = 0$, on a alors une relation de liaison non triviale parmi les k premières lignes de $M_{n_0}^{k}(a)$, ce qui assure aussi une telle relation de liaison sur les lignes de $M_{n_0+1}^{k-1}(a)$ en supprimant la première colonne.
  - Si $\beta \neq 0$: on a

$$D_{n_0}^k(a) = \det\begin{pmatrix} a_{n_0} & \cdots & a_{n_0+k} \\ \vdots & \ddots & \vdots \\ a_{n_0+k} & \cdots & a_{n_0+2k} \end{pmatrix} \overset{(\dagger)}{=} \det\left(\begin{array}{c|c} 0\dots0 & \beta \\ \hline & * \\ M_{n_0+1}^{k-1} & \vdots \\ & * \end{array}\right) = \pm\beta D_{n_0+1}^{k-1}(a),$$

  où $(\dagger)$ est obtenue par l'opération de Gauss $L'_0 \leftarrow L'_0 + \frac{1}{\lambda_0}\sum_{i=1}^{k} \lambda_i L'_i$.
  Donc $D_{n_0+1}^{k-1}(a) = 0$, ce qui assure le résultat.

On a donc montré que $D_{n_0+1}^{k-1}(a) = 0$, et on conclut le lemme par récurrence.

□

On a donc pour tout $n \geq n_0$, $\mathrm{rg}(M_n^k(a)) = k$. De plus, $\mathrm{Vect}\left((a_{i+j+n})_{\substack{0\leq i\leq k-1\\0\leq j\leq k}}\right) = \mathrm{Vect}\left((a_{i+j+n})_{\substack{1\leq i\leq k\\0\leq j\leq k}}\right)$ engendrent le même espace noté H (c'est le même pour toutes les matrices $M_n^k(a)$ pour $n \geq n_0$). H est un hyperplan de $\mathbb{K}^{k+1}$, donc le noyau d'une forme linéaire non nulle, que l'on peut donc écrire :

$$H = \left\{(x_0,\dots,x_k) \in \mathbb{K}^{k+1}, \sum_{i=0}^{k} b_{k-i}x_i = 0\right\}.$$

On a donc bien pour tout $n \geq k + n_0$, $b_0a_n + \cdots + b_ka_{n-k}$.
Posons alors $Q = \sum_{i=0}^{k} b_nX^n$, de sorte que :

$$Q(X)\left(\sum_{n=0}^{\infty} a_nX^n\right) = \sum_{n=0}^{\infty}\left(\sum_{m=0}^{n} b_ma_{n-m}\right)X^n = \sum_{n=0}^{n_0-1}\left(\sum_{m=0}^{n} b_ma_{n-m}\right)X^n + \cancel{\sum_{n=n_0+1}^{\infty}\left(\sum_{m=0}^{n} b_ma_{n-m}\right)X^n}.$$

Finalement, f est bien une fonction rationnelle.

□

Il s'agira alors dans la suite de majorer les déterminants de Hankel. Une méthode est d'utiliser le résultat suivant et d'étudier à la place la norme des vecteurs colonnes :

Théorème III.3 (Hadamard).

Supposons que $\mathbb{K} = \mathbb{C}$ ou l'un des $\mathbb{C}_p$, avec la valeur absolue canonique $|\cdot|$. Nous noterons $\|\cdot\|$ la norme euclidienne dans le premier cas, infinie dans le deuxième [a]. Soit $A \in \mathcal{M}_n(\mathbb{K})$ dont on note $F = (C_1, \dots, C_n)$ les vecteurs colonnes.
Alors :

$$|\det(A)| \leq \prod_{i=1}^{n} \|C_i\|.$$

a. On rappelle que $\|(x_1, \dots, x_n)\|_2 = \sqrt{\sum_{k=1}^{n} |x_k|^2}$ est la norme euclidienne et $\|(x_1, \dots, x_n)\|_\infty = \max_{1 \leq k \leq n} |x_k|$ est la norme infinie.

Lemme III.4.

Dans le cas ultramétrique, si les coefficients de A sont dans l'anneau de valuation $\mathcal{O}_{\mathbb{C}_p}$, alors il en est de même pour $|\det(A)|$.

Démonstration (III.4)

Le déterminant est polynômial en les coordonnées de A, et $\mathcal{O}_{\mathbb{C}_p}$ est un anneau.

□

Démonstration (III.3)

Le résultat est clair si A est inversible. Supposons alors qu'elle ne le soit pas.
Dans le premier cas, on utilise la décomposition $O - T$.
Notons B la base canonique sur $\mathbb{K}$ et . Notons $G = (V_1, \dots, V_n)$ la famille de vecteurs orthogonaux formant une base obtenue avec l'algorithme de Gram-Schmidt appliqué à F.
Alors $O := \mathrm{Mat}_B(G)$ est orthogonale et $A = \mathrm{Mat}_B(F) = \mathrm{Mat}_B(G)\mathrm{Mat}_G(F) = OT$ avec $T = \mathrm{Mat}_G(F)$.
Or l'algorithme de Gram-Schmidt assure que pour tout entier $1 \leq i \leq n$, $C_i \in \mathrm{Vect}(V_1, \dots, V_{i-1})$, donc T est triangulaire (supérieure) et ces coefficients diagonaux sont $\langle C_i, V_i \rangle$. Alors :

$$|\det(A)| \leq \underbrace{|\det(O)|}_{=1 \text{ car orthogonale}} |\det(T)| = \prod_{i=1}^{n} \langle C_i, V_i \rangle \underset{\text{Cauchy-Schwarz}}{\leq} \prod_{i=1}^{n} \|C_i\|^2.$$

Dans le second, posons $B := (\frac{1}{\|C_i\|} C_i)_{1 \leq i \leq n}$. Alors on sait que toutes les colonnes de B sont normalisées, donc tous les coefficients de B sont dans l'anneau de valuation $\mathcal{O}_{\mathbb{C}_p}$, donc $|\det(B)|$ aussi d'après le lemme, *ie* $|\det(B)| \leq 1$, et on retrouve l'inégalité voulue sur A.

□

III.2 Critères analytiques

III.2.1 Premiers théorèmes

Dans un premier temps, nous nous restreignons à des séries formelles à coefficients **entiers**. Nous verrons par la suite comment relâcher légèrement cette hypothèse.

Théorème III.5.

Soit $f(X) = \sum_{n\geq 0} a_n X^n$ une série formelle à coefficients entiers.
Si $f(X)$ converge dans $\mathbb{C}$ sur un disque de rayon $R > 1$ centré en 0, $f(X)$ est un polynôme.

Démonstration (III.5)

$1 < R$ donc $\sum_{n\geq 0} a_n$ converge. En particulier, $(a_n)_{n\geq 0}$ converge vers 0, donc il existe un rang n_0 tel que pour tout $n \geq n_0$, $|a_n| < \frac{1}{2}$. Or a_n est entier, donc $a_n = 0$, donc $f(X)$ est un polynôme. □

Borel a amélioré ce résultat en ne supposant que la méromorphie :

Théorème III.6 (Borel).

Soit $f(X) = \sum_{n\geq 0} a_n X^n$ une série formelle à coefficients entiers.
Si $f(X)$ est le développement de Taylor en $X = 0$ d'une fonction méromorphe sur un disque D de rayon $R > 1$ centré en 0, alors $f(X)$ est une fonction rationnelle.

Démonstration (III.6)

Elle est une copie simplifiée de la démonstration du théorème de Dwork, voir III.2.3. □

III.2.2 Au delà des disques

Les critères précédents sont restrictifs par le fait que la partie du plan complexe étudiée est toujours un disque centré en 0. Une généralisation possible serait de l'étendre à une réunion de disques non nécessairement centrés en 0. Mais comment remplacer efficacement l'hypothèse (essentielle !) $R > 1$? La notion de diamètre transfini est une bonne notion dans ce cas-là, et elle peut même être définie pour toute partie du plan.

a. Généralités sur le diamètre transfini

Proposition III.7.

Soit (E, d) un espace métrique, $B \subseteq E$ et $n \geq 2$.
Posons $D_n(B) := \sup \left\{ \prod_{i\neq j} d(x_i, x_j), (x_1, \ldots, x_n) \in B^n \right\} \in [0, +\infty]$ et $d_n(B) := D_n(B)^{\frac{1}{n(n+1)}}$.
Alors $(d_n(B))_{n\geq 2}$ admet une limite.

Démonstration (III.7)

Considérons le diamètre dans son sens usuel : $D(B) = \sup\{d(x,y), (x,y) \in B^2\}$. Alors on a $D_2(B) = D(B)^2$, et si $n \geq 2$, $D_n(B) \leq D(B)^{2n}$, d'où $d_n(B) \leq D(B)$.
Pour tout $(x_1, \ldots, x_n) \in B^n$, on pose $g_n(x_1, \ldots, x_n) := \prod_{i \neq j} d(x_i, x_j)$ et pour tout entier $1 \leq j \leq n+1$, $h_j := g_n(x^j)$ avec $x^j := (x_1, \ldots, x_{j-1}, \check{x}_j, x_{j+1}, \ldots, x_{n+1})$ (c'est-à-dire que g_n est évalué sur $(x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_{n+1})$). Alors un simple calcul nous donne $g_{n+1}(x_1, \ldots, x_{n+1})^n = \prod_{j=1}^{n+1} h_j(x_1, \ldots, x_{n+1})$.
En passant au supremum, $D_{n+1}(B)^n \leq D_n(B)^{n+1}$, donc $d_{n+1}(B) \leq d_n(B)^{1+\frac{1}{n}} \leq d_n(B) D(B)^{\frac{1}{n}}$.
De plus, si $r > 0$, la distance $d' := rd$, on a $d'_n(B) = r d_n(B)$, donc quitte à faire une telle homothétie, on peut supposer $D(B) < 1$.
Alors $d_n(B)$ est décroissante et minorée, donc converge.

□

Définition III.2.

Le nombre défini ci-dessus est noté $\delta_\infty(B) := \lim_{n \to \infty} d_n(B)$ et est appelé *diamètre transfini* de B.

Quelques propriétés qui suivent la définition :

Proposition III.8.

- $(\delta_\infty(A) < \infty) \Leftrightarrow (A$ est bornée$)$,
- $(A \subseteq B) \Rightarrow (\delta_\infty(A) \leq \delta_\infty(B))$,
- $(A \subseteq B$ et A est dense dans $B) \Rightarrow (\delta_\infty(A) = \delta_\infty(B))$,
- $\forall (x_1, \ldots, x_n) \in E^n, \delta_\infty(\{x_1, \ldots, x_n\}) = 0$.

Cette définition peut paraître un peu barbare. En fait, il s'agit d'une généralisation de la notion de diamètre pour des parties quelconques d'un espace métrique, comme on le verra plus tard.
Dans un premier temps, on donne une définition équivalente lorsque $E = K$ est un corps valué, qui va être une première occasion de manipuler le diamètre transfini.
Nous noterons $K'_n[X]$ les polynômes de degré exactement n et pour tout $P \in K'_n[X]$, $\|P\|_B := \sup_{x \in B} |P(x)|$.

Proposition III.9.

Soient K un corps valué, B une partie bornée de K.
Notons $S_n(B) := \inf_{P \in K'_n[X]} \|P\|_B$, et $s_n(B) := S_n(B)^{\frac{1}{n}}$.
Alors $(s_n(B))_{n \geq 1}$ admet une limite, et cette limite est égale à $\delta_\infty(B)$.

Démonstration (III.9)

La définition avec des limites et des bornes inférieures/supérieures nous incite à raisonner par doubles inégalités.

$\underline{s_n \leq d(B)}$: Pour tout $y = (y_1, \ldots, y_n) \in B^n$, notons $P_y(X) := \prod_{i=1}^n (X - y_i)$.
Soit $x \in B$. Alors $g_{n+1}(x, y_1, \ldots, y_n) = P_y(x)^2 g_n(y_1, \ldots, y_n)$.

Or $D_{n+1} \geq g_{n+1}(x, y_1, \ldots, y_n)$, donc en passant au supremum en x,

$$D_n(B)\|P_y\|_B^2 \leq D_{n+1}(B),$$

puis en passant à l'infimum sur y (et donc la même inégalité sur $P \in K_n'[X]$) :

$$D_n(B)S_n(B)^2 \leq D_{n+1}(B).$$

Donc on a :

$$s_n(B) \leq \left(\frac{D_{n+1}(B)}{D_n(B)}\right)^{\frac{1}{2n}} = \sqrt{\frac{d_{n+1}(B)^{n+1}}{d_n(B)^{n-1}}} = \sqrt{\left(\frac{d_{n+1}(B)}{d_n(B)}\right)^n d_{n+1}(B)d_n(B)} = \sqrt{(1+o(1))^n(d(B)+o(1))^2} = d(B)+o(1).$$

Finalement, $\limsup s_n(B) \leq d(B)$.

$\underline{s_n \geq d(B)}$: On remarque que $g_n(x_1, \ldots, x_n) = \det(V(x_1, \ldots, x_n))^2$ avec

$$V(x_1, \ldots, x_n) = \begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{pmatrix}$$

Donc pour tout $P \in K_{n-1}'[X]$, des opérations élémentaires de Gauss nous donnent :

$$\det(V(x_1, \ldots, x_n)) = \det \begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & P(x_1) \\ 1 & x_2 & x_2^2 & \cdots & P(x_2) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \cdots & P(x_n) \end{pmatrix}$$

En développant par rapport à la dernière colonne,

$$\det(V(x_1, \ldots, x_n)) = \pm \sum_{i=1}^{n} \det(V(x^i))P(x_i).$$

Donc, $g_n(x_1, \ldots, x_n) \leq n^2\|P\|_B^2 D_{n-1}(B)$, d'où $D_n(B) \leq n^2\|P\|_B^2 D_{n-1}(B)$.
En passant à l'infimum sur P, $\dfrac{D_n(B)}{n^2 D_{n-1}(B)} \leq S_{n-1}(B)^2$.
Or par les mêmes calculs que précédemment, $\left(\dfrac{D_n(B)}{n^2 D_{n-1}(B)}\right)^{\frac{1}{2n}} \underset{n\to\infty}{\longrightarrow} d(B)$, et finalement $\liminf s_n(B) \geq d(B)$.
Les deux inégalités impliquent le résultat.

□

b. Particularités dans le cas du plan complexe

Le diamètre transfini est bien connu dans le cadre de l'analyse dans le plan complexe, souvent trouvé sous le nom de *rayon conforme*.
Nous nous inspirons de [Hil02] dans ce paragraphe.
Nous noterons $\hat{\mathbb{C}} := \mathbb{C} \cup \{\infty\}$ la sphère de Riemann. Quelques rappels préliminaires :

Théorème III.10 (Théorème de l'application conforme).

Soient $U \subset \hat{\mathbb{C}}$ un ouvert simplement connexe non vide, dont le complémentaire contient au moins deux points, et $z_0 \in U$.
Alors il existe une bijection holomorphe, de réciproque holomorphe f de U dans le disque unité $D(0,1)$, telle que $f(z_0) = 0$.
Cette application est unique à rotation près. En particulier, le nombre $|f'(z_0)|$ est indépendant du choix d'une telle f.

Démonstration

Voir [[Hil02], Théorème 17.1.1]

□

Remarque III.1.

En composant deux telles applications, on en déduit que pour deux ouverts U et V de $\mathbb{C}$ contenant au moins deux points, tels que leur complémentaires sont simplement connexe, alors il existe une application bijective holomorphe f, d'inverse holomorphe, de $\hat{\mathbb{C}}\backslash U$ dans $\hat{\mathbb{C}}\backslash V$ telle que $f(\infty) = \infty$ (unique à rotation près).

Définition III.3.

Soient $U \subset \hat{\mathbb{C}}$ un ouvert simplement connexe non vide, dont le complémentaire contient au moins deux points, et $z_0 \in U$.
On appelle *rayon conforme de U relativement à z_0* le nombre

$$\mathrm{rad}(z_0, U) := \frac{1}{|f'(z_0)|},$$

où f est une application du théorème III.10.

Nous travaillerons désormais sur des parties E du plan complexe dont le complémentaire $\hat{\mathbb{C}}\backslash E$ est simplement connexe. Une raison est que l'on a un point « canonique » depuis lequel observer la taille sur ce complémentaire, qui est ∞, mais pas sur la partie en elle-même.
On peut s'inspirer de la définition précédente pour évaluer la taille depuis l'infini :

Définition III.4.

Soit $U \subset \mathbb{C}$ une partie simplement connexe contenant au moins deux points telle que $\hat{\mathbb{C}}\backslash U$ est un ouvert simplement connexe.
On appelle *rayon conforme de U relativement à l'infini*, ou *rayon conforme extérieur* de U, le nombre

$$\mathrm{rad}(\infty, U) := \left| \lim_{z \to \infty} \frac{z}{f(z)} \right|,$$

où $f : \hat{\mathbb{C}}\backslash U \to \hat{\mathbb{C}}\backslash \overline{D(0,1)}$ est une application de la remarque III.1.

Remarque III.2.

Notons que pour tout complexe z_0, $\mathrm{rad}(\infty, z_0 U) = |z_0| \mathrm{rad}(\infty, U)$.

Proposition III.11.

Soit $U \subset \mathbb{C}$ une partie simplement connexe telle que $\hat{\mathbb{C}} \backslash U$ est un ouvert simplement connexe, et U contient au moins deux points.
Alors :

$$\delta_\infty(U) = \mathrm{rad}(\infty, U).$$

Démonstration

Voir [[Hil02], Théorème 17.3.1]

□

Cette égalité permet de calculer bien plus simplement certains diamètres transfinis :

Proposition III.12.

Disque	Soient $z_0 \in \mathbb{C}$ et $r > 0$. Alors $\delta_\infty(D(z_0, r)) = r$.
Segment	Soit $(a, b) \in \mathbb{C}^2$. Alors $\delta_\infty([a, b]) = \frac{1}{4}\lvert b - a \rvert$.
Plan privé d'une demi-droite	Soit $a \in \mathbb{R}^{+*}$. Alors $\delta_\infty(\mathbb{C} \backslash [a, +\infty[) = \frac{1}{4a}$.

Démonstration (III.12)

Disque : Clair d'après III.2

Segment : On peut se limiter au segment $[-1, 1]$ d'après III.2. On considère alors l'application, dite de Joukowski :

$$\begin{array}{rccc} f : & \hat{\mathbb{C}} \backslash \overline{D(0,1)} & \longrightarrow & \hat{\mathbb{C}} \backslash [-1,1] \\ & z & \longmapsto & \frac{1}{2}(z + \frac{1}{z}) \end{array},$$

qui est clairement holomorphe et envoie ∞ sur lui-même.
Montrons la bijectivité, en s'intéressant à l'équation $w = \frac{1}{2}(z + \frac{1}{z})$. Si une solution est sur le cercle unité, alors elle s'écrit $z = e^{i\theta}$, et $w = \cos(\theta)$, ce qui contredit $w \notin [-1, 1]$. Sinon, les deux solutions de cette équation sont inverses l'une de l'autre, donc il n'existe qu'une solution hors du disque. On calcule alors, en notant que f^{-1} est la fonction qui nous intéresse et $\lim_{z \to \infty} \frac{z}{f^{-1}(z)} = \lim_{y \to \infty} \frac{f(y)}{y}$, $\mathrm{rad}(\infty, [-1, 1]) = \frac{1}{2}$, d'où le résultat voulu.

Plan privé d'une demi-droite : On peut encore une fois se restreindre au cas $a = 1$. On considère l'application

$$\begin{array}{rccc} f : & \hat{\mathbb{C}} \backslash \overline{D(0,1)} & \longrightarrow & [1, +\infty[\cup \{\infty\} \\ & z & \longmapsto & \frac{(1+z)^2}{4z} \end{array}.$$

Elle est holomorphe et envoie ∞ sur lui-même. Raisonnons comme précédemment sur l'équation $w = \frac{(1+z)^2}{4z}$. Si une solution est sur le cercle unité $z = e^{i\theta}$, alors $w = \cos^2(\theta/2)$, ce qui contredit $w \in [1, +\infty[$. Sinon, l'équation admet deux solutions inverses l'une de l'autre, donc seule l'une d'elle est hors du disque. Enfin, on calcule $\mathrm{rad}(\infty, [1, +\infty[) = \frac{1}{4}$, ce qui conclut.

□

Remarque III.3.

Nous retombons bien sur le rayon pour le disque !
On voit que pour calculer le diamètre transfini de cette manière, il « suffit » de trouver la bonne fonction, alors que par la définition, il faut trouver un ensemble de points maximisants la quantité $D_n(U)$ [a], montrer sa maximalité et calculer la limite.
Par exemple, dans le cas du disque unité, il faut trouver l'ensemble de points $\{e^{\frac{2i\pi k}{n}}, 1 \leq k \leq n\}$, trouver la quantité associée avec le calcul d'un déterminant de Vandermonde, puis déduire qu'il s'agit d'un ensemble maximisant avec l'inégalité d'Hadamard.
On pourra se référer à [[68], Question V] pour la démonstration dans le cas d'un segment.

a. qu'on appelle parfois *points de Fekete*

c. Amélioration du théorème de Borel

Le critère de Borel s'étend donc avec la notion de diamètre transfini au résultat suivant, dû à Pólya. On utilisera une série de Laurent $\frac{1}{X}f(\frac{1}{X})$ car l'on préfère travailler sur le *complémentaire* d'une partie bornée (dont le diamètre transfini nous intéresse).

Théorème III.13 (Pólya).

Soit $g(X) = \sum_{n\geq 0} \frac{a_n}{X^{n+1}}$ une série de Laurent à coefficients entiers qui peut être prolongée en une fonction méromorphe sur le complémentaire d'une partie bornée $0 \in A \subset \mathbb{C}$ de diamètre transfini strictement inférieur à 1.
Alors $g(X)$ est une fonction rationnelle.

Démonstration

Admis. C'est un corollaire du théorème de Bertrandias III.15, voir [Pól28] pour une démonstration « directe ».

□

Remarque III.4.

L'inégalité stricte est nécessaire ! Voici un contre-exemple pour le cas d'égalité.
Définissons la fonction d'une variable complexe

$$f(z) = \frac{1}{\sqrt{1-\frac{4}{z}}}.$$

C'est une fonction analytique sur $\mathbb{C}\backslash[0,4]$, qui se développe sous la forme :

$$f(z) = \sum_{n=0}^{\infty} \binom{2n}{n} \frac{1}{z^n}.$$

qui est une série à coefficients entiers. Or $[0,4]$ a comme diamètre transfini 1 d'après III.12 ; mais $f(z)$ n'est pas rationnelle.

III.2.3 Du local au global

Les deux critères précédents n'ont fait apparaître que des conditions sur le plan complexe. Il n'y a pas *a priori* de raison de privilégier la place infinie (donc $\mathbb{C}$) aux places p-adiques (donc $\mathbb{C}_p$) [1]. Le théorème qui suit permet d'étendre la condition un peu restrictive $R > 1$ dans $\mathbb{C}$ en compensant potentiellement avec le comportement dans les places p-adiques. Ce point de vue global permet également de considérer des séries formelles à coefficients rationnels plutôt que simplement entiers [2].

Théorème III.14 (Dwork).

Soit $f(X) = \sum_{n=0}^{\infty} a_n X^n$ une série formelle à coefficients dans $\mathbb{Q}$. Soit $\mathcal{S}$ un ensemble fini de places de $\mathbb{Q}$, contenant ∞, telle que :

(D1) Pour tous $p \notin \mathcal{S}, n \in \mathbb{N}, |a_n|_p \leq 1$ (*ie* $a_n \in \mathbb{Z}_p$),

(D2) Pour tout $p \in \mathcal{S}$, $f(z)$ se prolonge en une fonction méromorphe sur un disque $D_p \subset \mathbb{C}_p$ de rayon R_p,

(D3) $\prod_{p \in \mathcal{S}} R_p > 1$.

Alors $f(X)$ est une fonction rationnelle.

Sous la même justification que le paragraphe précédent, Bertrandias a étendu le critère de Dwork à des parties quelconques avec la notion de diamètre transfini.

Théorème III.15 (Bertrandias).

Soit $g(X) = \sum_{n \geq 0} \frac{a_n}{X^{n+1}}$ une série formelle à coefficients rationnels. Soit $\mathcal{S}$ un ensemble fini de places de $\mathbb{Q}$, contenant ∞, telle que :

(B1) Pour tous $p \notin \mathcal{S}, n \in \mathbb{N}, |a_n|_p \leq 1$ (*ie* $a_n \in \mathbb{Z}_p$),

(B2) Pour tout $p \in \mathcal{S}$, $g(z)$ se prolonge en une fonction méromorphe sur le complémentaire d'une partie bornée $K_p \subset \mathbb{C}_p$,

(B3) $\prod_{p \in \mathcal{S}} \delta_\infty(K_p) < 1$.

Alors $g(X)$ est une fonction rationnelle.

Pour résumer schématiquement :

	Disques centrés en 0	Parties bornées
$\mathbb{C}$	Borel	Pólya
$\mathbb{C}$ et $\mathbb{C}_p$	Dwork	Bertrandias

Nous allons passer à la démonstration du critère de Dwork et omettre celle de Bertrandias, bien que le second implique le premier. En effet, l'idée de la preuve est la même (un lemme de majoration des déterminants de Kronecker puis une application selon les hypothèses), les éléments pour Bertrandias sont d'un niveau bien supérieur, autant en analyse complexe standard qu'en analyse p-adique. On redirigera le lectorat curieux vers [[Ami75], §5.4] pour une telle preuve.
Comme annoncé, voici le lemme de majoration dont il est question :

1. si ce n'est que l'on est généralement, et historiquement, plus familier avec l'analyse complexe classique
2. voire même dans des corps de nombres, c'est à dire des extensions algébriques finies sur $\mathbb{Q}$. Ce cas ne nous sera pas utile dans la suite ; le lectorat intéressé pourra se référer à [[Ami75], 1§8, 5§3 et 5§4].

Lemme III.16.

Notons $\mathbf{C} = \mathbb{C}$ ou un des $\mathbb{C}_p$, avec la valeur absolue canonique $|\cdot|$.
Soit $f(X) = \sum_{n\geq 0} a_n X^n$ une série formelle à coefficients dans $\mathbf{C}$, définissant une fonction méromorphe dans un disque ouvert de centre 0 et de rayon $R > 0$. Soient $r < R$ et Q un polynôme de degré s tel que $g := Qf$ converge sur $D(0, r)$. Soit enfin $k \geq s$.
Alors il existe une constante $M > 0$ telle que :

$$\forall n \in \mathbb{N}, |D_n^k(a)| \leq M b^{-ns} r^{-n(k-s)},$$

où l'on a noté $b := \inf_{Q(z)=0} |z|$.

Démonstration (III.16)

Nous prendrons la norme infinie dans le cas ultramétrique, la norme euclidienne pour le cas archimédien. Notons $Q(X) = \sum_{i=0}^{s} q_i X^i$, c_i les coefficients de g, et $A_n^k(f)$ le vecteur colonne $(a_n, \ldots, a_{n+k})^T$, de sorte qu'avec ces notations :

$$D_n^k := D_n^k(a) = \det(A_n^k(f), \ldots, A_{n+k}^k(f)),$$

et, pour $m \geq s$:

$$A_m^k(g) = \sum_{i=0}^{s} q_i A_{m-i}^k.$$

Donc avec des opérations élémentaires de Gauss :

$$D_n^k = \det(A_n^k(f), \ldots, A_{n+s-1}^k(f), A_{n+s}^k(g), \ldots, A_{n+k}^k(g)).$$

Or f (respectivement g) définit une fonction holomorphe bornée dans le disque $D(0, b)$, *ie* là où $Q(x) \neq 0$ (respectivement dans le disque $D(0, r)$), donc d'après les inégalités de Cauchy (on l'admettra dans le cas ultramétrique, voir [[Ami75], Corollaire 4.1.11]), il existe deux constantes L et L' telles que :

$$\forall n \in \mathbb{N}, |a_n| \leq L b^{-n} (\text{respectivement, } |c_n| \leq L' r^{-n}).$$

Avec le théorème de Hadamard III.3, on a pour tout $k \geq s$ et $n \geq 0$,

$$|D_n^k| \leq M b^{-ns} r^{-n(k-s)},$$

avec $M = L^s L'^{k-s+1} b^{-s(s-1)/2} r^{-(k-s+1)(k-s+2)/2}$ une constante indépendante de n.

□

Démonstration (III.14)

Comme l'inégalité (D3) est stricte, pour tout $p \in \mathcal{S}$, il existe $0 < r_p < R_p$ tel que $r := \prod_{p\in\mathcal{S}} r_p > 1$. Notons alors Q_p un polynôme de degré d_p vérifiant : $Q_p(0) \neq 0$ et $Q_p f$ converge dans le disque fermé $\overline{D}(0, r_p)$ dans $\mathbb{C}_p$ (hypothèse de méromorphie).
Notons $b_p := \min\{z \in \mathbb{C}_p, Q_p(z) = 0\}$ et $d := \max_{p\in\mathcal{S}} d_p$.
Par le lemme III.16, il existe des constantes $(M_{k,p})_{\substack{k\in\mathbb{N},k\geq s \\ p\in\mathcal{S}}}$ telles que pour tout entier $k \geq s$:

$$\prod_{p\in\mathcal{S}} |D_n^k|_p \leq \prod_{p\in\mathcal{S}} M_{k,p} b_p^{-ns} r_p^{-n(k-d_p)}.$$

Notons $\Delta_k := \prod_{p\in\mathcal{S}} b_p^{-ns} r_p^{-n(k-d_p)}$ et $M := \prod_{p\in\mathcal{S}} M_{k,p}$. On calcule alors directement que $\Delta_k \underset{k\to\infty}{\longrightarrow} \frac{1}{r}$, donc par construction de r, il existe un $k_0 \geq s$ tel que $\Delta := \Delta_{k_0} < 1$.
Or par (D1), on a $|D_n^k(a)|_p \leq 1$ pour tout $p \notin \mathcal{S}$ d'après III.4. Alors si $D_n^k \neq 0$, par la formule du produit II.14, on a $1 \leq \Delta^n M$ pour tout n, ce qui est impossible car $\Delta < 1$, d'où le résultat par le lemme III.1.

□

Remarque III.5.

Notons l'importance de toutes les hypothèses dans les théorèmes. Par exemple, pour Dwork, il existe des contre exemples pour chaque :

— Si (D1) seule n'est pas vérifiée : On considère la série

$$f(X) = \sum_{n=0}^{\infty} \frac{2^n}{q_n} X^n,$$

où $q_n := \min\{q \text{ premier tel que } q > 2^n\}$ est le plus petit premier supérieur à 2^n. On notera $a_n := \frac{2^n}{q_n}$.
Notons au préalable que la suite (q_n) est strictement croissante.

- $\neg$ (D1) : La contraposée de (D1) est : $\forall \mathcal{S}$ finie, $\exists p \notin \mathcal{S}, \exists n \in \mathbb{N}, |a_n|_p > 1$. Ceci est vérifié, car si $\mathcal{S}$ est un ensemble fini de places, alors $\{q \text{ premier}, q > \max(\mathcal{S})\} \cap \{q_n, n \in \mathbb{N}\} \neq \emptyset$, et en un de ces n particuliers, $|a_n|_{q_n} > 1$.
- (D2),(D3) On peut poser $R_2 = 2$ et $R_p = 1$ pour $p \neq 2$ premier pour vérifier ces hypothèses (on se souviendra de II.4 pour montrer la convergence).
- f non rationnelle : par la caractérisation avec la relation de récurrence, supposons qu'il existe deux entiers positifs k et n_0, des entiers [a] $b_0, \ldots, b_k$ (avec $b_0 \neq 0$) tels que :

$$\text{pour tout } n \geq n_0, b_0 a_n + \cdots + b_k a_{n+k} = 0.$$

Alors la relation équivaut à :

$$b_0 \prod_{j\neq 0} q_{n+j} = -q_n \left(b_1 \prod_{j\neq 1} q_{n+j} + \cdots + b_k 2^k \prod_{j\neq k} q_{n+j} \right).$$

Donc q_n divise $b_0 \prod_{j\neq 0} q_{n+j}$ et est premier avec $\prod_{j\neq 0} q_{n+j}$ (car les q_i sont distincts et premiers), donc par le lemme de Gauss, q_n divise b_0, et ce pour une infinité de q_n, donc $b_0 = 0$, ce qui contredit l'hypothèse.

— Si (D3) seule n'est pas vérifiée : On considère la série

$$f(X) = \sum_{n=0}^{\infty} X^{n!},$$

et l'on notera $a_n := \begin{cases} 1 \text{ s'il existe } k \text{ tel que } n = k! \\ 0 \text{ sinon.} \end{cases}$

- (D1) Clair

- $\neg$ (D3) Pour toute place, le rayon de convergence de la série est exactement 1 (le terme général de la série ne tend pas vers 0), donc on a $\prod_p R_p = 1$.

- f non rationnelle : on reprend les mêmes notations qu'avant. Alors ici, pour $m = \max(3, n_0, k)$ et $n = m!$, on a $n \geq n_0$, $n + k < (m+1)!$, donc la relation de récurrence donne en cet indice n : $b_0 = 0$, ce qui contredit l'hypothèse, donc f n'est pas rationnelle.

a. on peut se restreindre aux entiers, quitte à multiplier par les dénominateurs.

Il existe des généralisations de ces théorèmes.
La première étape est de considérer (comme pour les nombres !) non plus la rationalité, mais l'algébricité des séries formelles,

Définition III.5.

Soit $f(X) = \sum_{n=0}^{\infty} a_n X^n$ une série formelle à coefficients dans un corps K.
On dit que f est algébrique s'il existe un polynôme non nul $P \in K[X, Y]$ tel que $P(X, f(X)) = 0$.

ou encore de considérer une série formelle à plusieurs variables. Les applications de tels théorèmes sont hors de portée de ce mémoire. On pourra en trouver dans [CN23]. On peut aussi réduire légèrement les hypothèses (par exemple, prendre une inégalité large au lieu d'une inégalité stricte pour la condition sur $\prod R_p$ sous certaines conditions, c'est le théorème de Harbeter [[Har88], Proposition 2.1].
Dans la partie VI, nous donnerons une esquisse des applications récentes de ces généralisations.

IV Conjecture de Schinzel-Zassenhaus

« Dieu a créé les nombres naturels ; le reste, c'est le travail de l'homme. »
Leopold Kronecker

IV.1 Rappels sur les pôlynomes

Nous ne faisons que rappeler des résultats sur les polynômes qui nous seront utiles dans la suite. Nous recommandons au lectorat voulant se remémorer la théorie générale les sources suivantes : [[Cal06], VIII] pour les polynômes symétriques et [[Per96], III§4] pour les polynômes cyclotomiques.

IV.1.1 Autour des polynômes symétriques

On note dans cette partie A un anneau commutatif unitaire.

Définition IV.1.

Soit $P \in A[X_1, \dots, X_n]$.
On dit que P est un polynôme symétrique si, pour toute permutation $\rho \in \mathfrak{S}_n$,

$$P(X_1, \dots, X_n) = P(X_{\rho(1)}, \dots, X_{\rho(n)}).$$

Définition IV.2.

Soient deux entiers $n > 0$ et $0 \leq k \leq n$.
On appelle k-ième polynôme symétrique élémentaire en n et on note $\sigma_k(X_1, \dots, X_n)$ le polynôme (symétrique) suivant :

$$\sigma_k(X_1, \dots, X_n) := \sum_{1 \leq i_1 < \dots < i_k \leq n} \prod_{j=1}^{k} X_{i_j}.$$

Théorème IV.1 (Théorème fondamental des polynômes symétriques).

Soit $P \in A[X_1, \dots, X_n]$ un polynôme symétrique.
Alors il existe un unique $Q \in A[X_1, \dots, X_n]$ tel que :

$$P(X_1, \dots, X_n) = Q(\sigma_1(X_1, \dots, X_n), \dots, \sigma_n(X_1, \dots, X_n)).$$

Démonstration

Voir [[Cal06], Théorème 8.14]

□

Théorème IV.2 (Relations coefficients-racines).

On suppose que A est un corps.
Soit $P = \sum_{k=0}^{n} a_k X^k$ un polynôme unitaire scindé à coefficients dans A. Notons $\alpha_1, \dots, \alpha_n$ ses n racines.
Alors pour tout $k \in [\![0, n]\!]$,

$$a_k = (-1)^{n-k}\sigma_{n-k}(\alpha_1, \ldots, \alpha_n)$$

Démonstration

Voir [[Cal06], VIII§3]

□

IV.1.2 Autour des polynômes cyclotomiques

Définition IV.3.

Soit $n \geq 1$ un entier.
On appelle n-ième polynôme cyclotomique, et on note Φ_n l'élément de $\mathbb{C}[X]$ défini par :

$$\Phi_n(X) := \prod_{\zeta \in \mu_n^*} (X - \zeta),$$

où μ_n^* désigne les racines primitives n-ième de l'unité : $\mu_n^* = \{e^{\frac{2i\pi k}{n}}, 0 \leq k \leq n-1, \text{pgcd}(n,k) = 1\}$.

Proposition IV.3.

Pour tout entier $n \geq 1$,

(a) $X^n - 1 = \prod_{d|n} \Phi(X)$,

(b) $\Phi_n \in \mathbb{Z}[X]$,

(c) Φ_n est irréductible sur $\mathbb{Z}$.

Démonstration

(a) Voir [[Per96], Proposition 4.5]
(b) Voir [[Per96], Proposition 4.8,1)]
(c) Voir [[Per96], Théorème 4.10]

□

IV.2 Une première approche : le théorème de Kronecker

On étudie dans un premier temps le théorème de Kronecker car il possède des similitudes avec la conjecture de Schinzel-Zassenhaus sur deux plans : le résultat, qui porte sur la localisation des zéros d'un polynôme à coefficients entiers, et des arguments dans les preuves.

Théorème IV.4 (Kronecker).

Soit $n > 1$ un entier. Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire, de degré n. On suppose que les racines de P dans $\mathbb{C}$ sont contenues dans le disque unité et que 0 n'est pas racine.
Alors les racines de P sont situées sur le cercle unité.

Démonstration (IV.4)

Notons Ω_n l'ensemble des polynômes unitaires de degré n à coefficients entiers dont les racines sont dans le disque unité.
Montrons qu'il n'existe qu'un nombre fini de complexes du disque unité qui annulent un polynôme de Ω_n. Pour ça, sachant qu'un polynôme de degré n a au plus n racines complexes distinctes, il suffit de montrer que Ω_n est fini.
Soit $Q = \sum_{k=0}^{n} a_k X^k \in \Omega_n$. Montrons qu'il n'existe qu'un nombre fini de choix de ses coefficients. Notons $z_1, \dots, z_n$ ses racines dans $\mathbb{C}$ et $\sigma_0, \dots, \sigma_n$ les polynômes symétriques élémentaires en n, évalués en $(z_1, \dots, z_n)$. Alors d'après les relations coefficients-racines, pour tout $k \in [\![0, n]\!]$,

$$\sigma_k = (-1)^k a_{n-k},$$

donc les σ_k sont entiers et par la définition de σ_k :

$$|a_{n-k}| \leq \sum_{1 \leq i_1 < \dots < i_k \leq n} \overbrace{\prod_{j=1}^{k}}^{\leq 1} |z_{i_j}| \leq \binom{n}{k}.$$

Les a_k étant entiers, ils ne peuvent prendre qu'un nombre fini de valeurs, d'où le résultat.
Revenons maintenant à notre polynôme particulier P, dont on notera aussi $z_1, \dots, z_n$ ses racines et $\sigma_0^1, \dots, \sigma_n^1$ les polynômes symétriques élémentaires associés. Construisons alors, pour tout entier $m > 1$, les polynômes

$$P_m(X) := \prod_{k=1}^{n} (X - z_k^m).$$

Alors les polynômes symétriques élémentaires associés, notés $\sigma_0^m, \dots, \sigma_n^m$, sont des polynômes de $\mathbb{Z}[X_1, \dots, X_n]$. Soit $k \in [\![1, n]\!]$. D'après IV.1, il existe $Q_{k,m} \in \mathbb{Z}[X_1, \dots, X_n]$ tel que

$$\sigma_k^m(X_1, \dots, X_n) = \sigma_k^1(X_1^m, \dots, X_n^m) = Q_{k,m}(\sigma_1^1(X_1, \dots, X_n), \dots, \sigma_n^1(X_1, \dots, X_n)).$$

Alors sachant que $\sigma_k^1(z_1, \dots, z_n)$ sont entiers, il en est de même pour les $\sigma_k^m(z_1, \dots, z_n)$, et subséquemment des coefficients de P_m.
Or on a également que les racines de P_m sont situées dans le disque unité. Donc $P_m \in \Omega_n$.
On en déduit que la famille $(P_m)_{m \geq 1}$ est finie, donc pour tout $k \in [\![1, n]\!]$, il existe deux entiers $r > 0$ et $s > 0$ tels que $z_k^r = z_k^s$. Sachant que $z_k \neq 0$, c'est une racine de l'unité, d'où le résultat souhaité.

□

On s'approche encore un peu de la conjecture de Schinzel-Zassenhaus avec le résultat qui suit, faisant appel à des polynômes cyclotomiques :

Corollaire IV.5.

Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire et irréductible sur $\mathbb{Q}$ tel que toutes ses racines complexes sont dans le disque unité. Alors $P = X$ ou P est un polynôme cyclotomique.

Démonstration (IV.5)

Si 0 est racine de P, $X|P$, et P est unitaire et irréductible, donc $P = X$.
Sinon, d'après le théorème de Kronecker, toutes ses racines sont de module 1. Il existe donc un entier $N > 0$ tel que pour toute racine α de P, $\alpha^N = 1$ (on peut prendre le PPCM des ordres des racines). Donc $P \mid X^N - 1$. Or $X^N - 1 = \prod_{d|n} \Phi_d(X)$ et les Φ_d sont irréductibles (par IV.3), donc par irréductibilité de P, $P = \Phi_d$ pour un certain d.

□

IV.3 Théorème de Schinzel-Zassenhaus

L'objectif de cette partie est de montrer, entre autres à l'aide d'un théorème de rationnalité, le résultat qui suit. Il donne une minoration du module de la plus grande racine d'un polynôme à coefficients entiers unitaire, **determinée uniquement par le degré** de ce polynôme (quand celui-ci n'est pas cyclotomique).

Théorème IV.6 (Schinzel-Zassenhaus, Dimitrov).

Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire, irréductible de degré $n > 1$.
Alors on est dans un des deux cas (exclusifs) suivants :

— P est cyclotomique

— $\max_{P(\alpha)=0} |\alpha| \geq 2^{\frac{1}{4n}} = 1 + \frac{\ln(2)}{4n} + O\left(\frac{1}{n^2}\right)$.

On peut caractériser les polynômes cyclotomiques qui apparaissent dans IV.5, par l'intermédiaire des polynômes P_m (P_2 et P_4 notamment) déjà introduits précédemment : si $P(X) = \prod_{k=1}^{n}(X - \alpha_k)$ est la décomposition de P dans $\mathbb{C}$,

$$P_m(X) := \prod_{k=1}^{n}(X - \alpha_k^m).$$

Lemme IV.7.

Soit $P \in \mathbb{Z}[X]$ irréductible, de degré $n > 1$ tel que P_2 est irréductible. Alors les propositions suivantes sont équivalentes :

(*i*) P est cyclotomique de rang impair

(*ii*) $P_2 = P_4$

(*iii*) P_2P_4 est un carré parfait

(*iv*) $\sqrt{P_2P_4}$ est rationelle.

Démonstration (IV.7)

On a déjà $(ii) \Rightarrow (iii) \Rightarrow (iv)$, et $(iv) \Rightarrow (iii)$ du fait que si $\sqrt{P_2P_4}$ est rationnelle, c'est en fait un polynôme.

$(i) \Rightarrow (ii)$: Soit N impair tel que $P(X) = \Phi_N(X)$. Alors $\{\alpha_k, 1 \leq k \leq n\} = \{e^{\frac{2i\pi k}{N}}, 1 \leq k \leq n\}$. Donc $\{\alpha_k^2, 1 \leq k \leq n\} = \{\alpha_k^4, 1 \leq k \leq n\}$ (N est impair), donc $P_2 = P_4$.

$(iii) \Rightarrow (i)$: On note $P_2P_4 = Q^2$. Soit α une racine de P. P_2 est irréductible, donc P_2 et P_2' sont premiers entre eux, et par le théorème de Bézout, on en déduit que α^2 est racine simple de P_2, donc annule aussi P_4 (*via* son ordre de multiplicité dans Q). Il existe alors $\sigma \in \mathrm{Gal}(P)$ tel que $\alpha^2 = \sigma(\alpha)^4$. Notons k l'ordre de σ. De la suite d'égalité :

$$\alpha^2 = \sigma(\alpha^2)^2 = \sigma(\sigma(\alpha^2)^2)^2 = \sigma^2(\alpha^2)^{2^2} = \cdots = \sigma^{k-1}(\alpha^2)^{2^{k-1}} = \sigma^k(\alpha)^{2^{k+1}} = \alpha^{2^{k+1}},$$

on tire $\alpha^{2(2^k-1)} = 1$, donc α est une racine de l'unité. Nous admettrons que son ordre est impair.

□

Or P_2 et P_4 sont liés par la proposition suivante :

Proposition IV.8.

$P_2 \equiv P_4[4\mathbb{Z}[X]]$.

Démonstration (IV.8)

Examinons les congruences (mod 4) des coefficients de ces polynômes.
Commençons par le coefficient devant X^{n-1}. Notons $s_m = s_m(\alpha_1, \ldots, \alpha_n) = \sum_{i_k}^n \alpha_k^m$ la m-ième somme de Newton et $\sigma_m = \sigma_m(\alpha_1, \ldots, \alpha_n)$ la m-ième fonction élémentaire. Par les relations coefficients-racines, les deuxième et quatrième sommes de Newton correspondent (au signe près) au coefficient devant X^{n-1} de P_2 et P_4 respectivement. Or par les identités de Newton,

$$s_2 = \sigma_1^2 - 2\sigma_2 \text{ et } s_4 = \sigma_1^4 + 2\sigma_2^2 - 4(\sigma_1^2\sigma_2 - \sigma_4 - \sigma_1\sigma_3).$$

Donc, sachant que les σ_i sont entiers, $s_2 \equiv s_4[4]$ (on pourra faire des tables de congruences de σ_1 et σ_2 (mod 4) pour s'en convaincre).
Pour les autres coefficients, la méthode est la même, en changeant le polynôme dont les sommes de Newton et les fonctions élémentaires sont associées : on prendra en effet pour tout $2 \leq k \leq n-1$ les polynômes $R_k(X) = \prod_{1 \leq i_1 < \cdots < i_k \leq n} \left(X - \prod_{j=1}^k \alpha_{i_j} \right)$. Alors les sommes de Newton associées sont :

$$s_2 = \sum_{1 \leq i_1 < \cdots < i_k \leq n} \prod_{j=1}^k \alpha_{i_j}^2 \text{ et } s_4 = \sum_{1 \leq i_1 < \cdots < i_k \leq n} \prod_{j=1}^k \alpha_{i_j}^4.$$

Ce sont exactement les k-ièmes fonctions symétriques de P_2 et P_4 respectivement (donc les coefficients devant X^{n-k} au signe près) ; et ces sommes sont congrues (mod 4) par le calcul juste au-dessus ! Le résultat est donc démontré.

□

On a alors l'existence d'un polynôme T tel que $P_2 = P_4 + 4T$, d'où $P_2P_4 = P_4^2 + 4TP_4$, donc P_2P_4 est un carré parfait (mod 4). Il s'avère que dans ce cas, on arrive à contrôler le développement de $\sqrt{P_2P_4}$ de IV.7 :

Proposition IV.9.

Soit $Q \in \mathbb{Z}[X]$ tel que $Q(0) = 1$. Supposons que Q est un carré parfait dans $(\mathbb{Z}[X])/(4)$,

c'est-à-dire qu'il existe $U, V \in \mathbb{Z}$ tel que $Q = U^2 + 4V$.
Alors $\sqrt{Q(X)}$ se développe en série de Taylor avec des coefficients entiers : $\sqrt{Q(X)} \in 1+\mathbb{Z}[[X]]$.

Démonstration (IV.9)

Étudions le développement en série de Taylor de $\sqrt{1+4Y}$ (au voisinage de 0) :

$$\sqrt{1+4Y} = 1 + \sum_{k=1}^{\infty} \binom{1/2}{k} \frac{4^k}{k!} Y^k = 1 + \sum_{k=1}^{\infty} \left(\prod_{i=0}^{k-1} \left(\frac{1}{2} - i \right) 4^k \right) Y^k =$$
$$1 + \sum_{k=1}^{\infty} (-1)^{k+1} \left(\frac{\prod_{i=1}^{k-1}(2i-1) \prod_{i=1}^{k-1}(2i)}{k! \prod_{i=1}^{k-1}(2i)} 2^k \right) Y^k = 1 + \sum_{k=1}^{\infty} 2(-1)^{k+1} \frac{(2k-2)!}{(k-1)!k!} Y^k.$$

On reconnaît ici le $(k-1)$-ième nombre de Catalan :

$$C_{k-1} = \frac{(2k-2)!}{(k-1)!k!} = \frac{1}{k}\binom{2k-2}{k-1} = \binom{2k-2}{k-1} - \binom{2k-2}{k} \in \mathbb{Z},$$

Donc en l'appliquant à $Q = U^2 + 4V$ (sachant que $Q(0) = 1$, donc $U(0) = \pm 1$ et $V(0) = 0$) :

$$\sqrt{Q(X)} = U(X) \sqrt{1 + 4\frac{V(X)}{U(X)^2}} \in \mathbb{Z}[[X]].$$

□

Le polynôme P_2P_4 ne vérifie pas $P_2P_4(0) = 1$, mais on sait qu'il est unitaire. Il est convenable de travailler plutôt avec le polynôme réciproque $P^\star$ de P défini par

$$P^\star(X) := X^n P\left(\frac{1}{X}\right).$$

(C'est le polynôme dont le coefficient devant X^k est celui de P devant X^{n-k}.)
On notera l'égalité $(P_m)^\star = (P^\star)_m$.

Nous sommes donc ramenés à étudier la rationalité d'une série formelle ! On utilisera $f(X) := \sqrt{P_2^\star\left(\frac{1}{X}\right) P_4^\star\left(\frac{1}{X}\right)}$ dans l'application du théorème de Bertrandias [3].
Il nous reste toutefois à trouver une partie de $\mathbb{C}$ sur laquelle f est analytique. Les seuls problèmes de l'analycité de f se présentent sur les branches de la racines carrées, entre les racines de $P_2^\star(1/X)$ et $P_4^\star(1/X)$, *ie* l'ensemble $\{\alpha_k^2, \alpha_k^4, 1 \le k \le n\}$, et 0. Pour en faire une partie convenable (et connexe), on relie chacun de ces racines à l'origine.

Définition IV.4.

Soient $\alpha_1, \ldots, \alpha_n$ des complexes non nuls.
On appelle *hérisson* [a] de $\alpha_1, \ldots, \alpha_n$, et on note $\mathcal{K}(\alpha_1, \ldots, \alpha_n)$ la partie de $\mathbb{C}$ définie par :

$$\mathcal{K}(\alpha_1, \ldots, \alpha_n) := \bigcup_{i=1}^{n} [0, a_i],$$

3. en fait, ici, il s'agira plutôt de la version faible : le théorème de Pólya

où $[0, \alpha_i] = \{t\alpha_i, t \in [0,1]\}$ est le segment reliant 0 à α_i.

a. en anglais, *hedgehog*

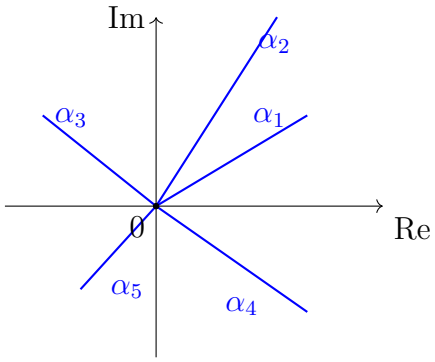


FIGURE 1 – Hérisson de $(\alpha_1, \ldots, \alpha_5)$

Les travaux du mathématicien Dubinin (sur les mesures harmoniques) permettent de connaître une majoration fine du diamètre transfini d'un tel hérisson (on admettra ce résultat) :

Théorème IV.10 (Dubinin).

Le diamètre transfini d'un hérisson $\mathcal{K} = \mathcal{K}(\alpha_1, \ldots, \alpha_n) \subset \mathbb{C}$ vérifie :

$$\delta_\infty(\mathcal{K}) \leq \left(\frac{b_n}{4}\right)^{\frac{1}{n}},$$

où $b_n := \max\limits_{1\leq k\leq n} |\alpha_k|^n$; avec égalité si, et seulement si les α_k sont les sommets d'un n-gone régulier centré en 0, *ie* s'il existe un complexe non nul z tel que pour tout entier $1 \leq k \leq n, \alpha_k = ze^{\frac{2i\pi k}{n}}$ (à permutation des racines près).

DÉMONSTRATION (IV.6)

On est donc en mesure d'appliquer le théorème de Bertrandias. Notons $\mathcal{K} := \mathcal{K}(\alpha_1^2, \ldots, \alpha_n^2, \alpha_1^4, \ldots, \alpha_n^4)$. Alors f est analytique sur $\hat{\mathbb{C}}\backslash\mathcal{K}$, et on a la majoration :

$$\delta_\infty(\mathcal{K}) \leq \left(\tfrac{b_n}{4}\right)^{\frac{1}{2n}}$$

avec ici $b_n = \max\limits_{1\leq k\leq n} |\alpha_k^4|^{2n} = \max\limits_{1\leq k\leq n} |\alpha_k|^{8n}$. En effet, la plus grande racine est de module au moins 1 (on peut le voir comme une conséquence du théorème de Kronecker), donc pour ce α_k, $|\alpha_k^4| \geq |\alpha_k^2|$.
Supposons alors que $\max\limits_{1\leq k\leq n} |\alpha_k| < 2^{\frac{1}{4n}}$.
D'après le théorème de Bertrandias, f est rationnelle.

- Supposons P_2 irréductible. Donc d'après IV.7, P est cyclotomique.
- Sinon, on peut raisonner par récurrence sur n, en supposant le résultat acquis pour tout polynôme de degré $m < n$. Notons Q_i le polynôme minimal de α_i^2. P étant irréductible et unitaire, c'est le polynôme minimal de α_i. Or α_i est racine de $Q_i(X^2)$, donc $P \mid Q_i(X^2)$,

donc $\deg(P) \mid 2\deg(Q_i)$. Or $\deg(Q) < \deg(P)$, ce qui assure $\deg(Q_i) = \deg(P)/2$. Donc par hypothèse, toutes les racines de Q_i sont de module 1, en particulier α_i l'est, et ce pour tout i. Le résultat est donc prouvé au rang n.

□

V Transcendance de nombres

« Arithmétique ! algèbre ! géométrie !
trinité grandiose ! triangle lumineux !
Celui qui ne vous a pas connues est un insensé ! »
Comte de Lautréamont, *Les chants de Maldoror.*

V.1 Introduction

On s'intéresse dans cette partie à une propriété arithmétique des nombres complexes : leur caractère algébrique ou transcendant.

Définition V.1.

Soit $z \in \mathbb{C}$.
On dit que z est *algébrique* (sur $\mathbb{Q}$) s'il existe un polynôme $P \in \mathbb{Q}[X]$ non nul tel que $P(z) = 0$.
On note $\overline{\mathbb{Q}}$ l'ensemble des nombres complexes algébriques sur $\mathbb{Q}$.
Un nombre complexe qui n'est pas algébrique est dit *transcendant* (sur $\mathbb{Q}$).

Un argument de dénombrement de l'ensemble des polynômes $\mathbb{Q}_m[X]$ de degré exactement m de $\mathbb{Q}[X]$ permet de déduire la dénombrabilité de $\mathbb{Q}[X] = \bigcup_{m\in\mathbb{N}} \mathbb{Q}_m[X]$ et celle de $\overline{\mathbb{Q}}$. La mesure de $\overline{\mathbb{Q}}$ est donc nulle, donc presque-tout complexe est transcendant. Il est cependant difficile de montrer qu'un nombre est transcendant (c'est une propriété de *non-existence*).
On cherche dans cette partie à prouver un théorème donnant un critère de transcendance.

Théorème V.1 (L-W [a],1885).

Soient $\alpha_1, \dots, \alpha_m$ des nombres algébriques deux à deux distincts.
Alors $e^{\alpha_1}, \dots, e^{\alpha_m}$ sont linéairement indépendants sur $\overline{\mathbb{Q}}$, *ie* :

$$\forall\, (\lambda_1, \dots, \lambda_m) \in \overline{\mathbb{Q}}^m, \left(\sum_{i=1}^{m} \lambda_i e^{\alpha_i} = 0\right) \Rightarrow (\lambda_1, \dots, \lambda_m) = (0, \dots, 0).$$

a. pour *Lindemann-Weierstrass*

On en déduit un résultat un peu plus faible, démontré avant, donnant un critère direct :

Corollaire V.2 (H-L [a],1882).

Soit $z \in \mathbb{C}$ algébrique non nul.
Alors e^z est transcendant.

a. Pour *Hermite-Lindemann*

Démonstration (V.2)

En supposant (LW), e^z et $e^0 = 1$ sont linéairement indépendants sur $\overline{\mathbb{Q}}$, donc e^z est transcendant.

□

Corollaire V.3.

π et $e = e^1$ sont transcendants.

Démonstration (V.3)

Si π est algébrique, $i\pi$ l'est aussi ($\overline{\mathbb{Q}}$ est un anneau) donc $-1 = e^{i\pi}$ est transcendant, ce qui est absurde.

□

V.2 Reformulation en langage de séries formelles

On voit que l'étude se porte donc sur l'évaluation en 1 d'une fonction du type $\sum_{i=1}^{m} \lambda_i(z)e^{\alpha_i z}$, et il est naturel d'introduire la transformée de Laplace pour passer d'exponentielles à fractions rationnelles. Pour un corps $\mathbb{K}$, on notera $\mathscr{F}_{\mathbb{K}} := \frac{1}{X}\mathbb{K}[[\frac{1}{X}]]$ l'anneau des séries entières en $\frac{1}{X}$ nulle en l'infini.

Définition V.2.

Soient $f : U \subseteq \mathbb{C} \to \mathbb{C}$ et $\mathbb{K}$ un sous-corps de $\mathbb{C}$.
On dit que f est un *polynôme exponentiel* à coefficients dans $\mathbb{K}$ s'il existe un entier $r > 0$, des polynômes $p_1, \dots, p_r \in \mathbb{K}[X]$ et des nombres $\alpha_1, \dots, \alpha_r \in \mathbb{K}$ tels que pour tout $z \in U$,

$$f(z) = \sum_{i=0}^{r} p_i(z)e^{\alpha_i z}.$$

Définition V.3.

On appelle transformée de Laplace formelle l'application :

$$\begin{array}{rccc} \mathscr{L} : & \mathbb{C}[[z]] & \to & \mathscr{F}_{\mathbb{C}} \\ & \sum_{n=0}^{\infty} a_n z^n & \mapsto & \sum_{n=0}^{\infty} \frac{n! a_n}{z^{n+1}}. \end{array}$$

Remarque V.1.

La définition ci-dessus s'inspire de la transformée de Laplace sur les fonctions complexes f suffisamment régulières :

$$\mathscr{L}(f)(p) = \int_0^{+\infty} e^{-tp} f(t)dt.$$

Proposition V.4.

$\mathscr{L}$ est une bijection.

On peut caractériser des propriétés de $\mathscr{L}(f)$ à partir de celles de f : c'est l'objet des deux prochains résultats.

Lemme V.5.

Soit $f \in \mathbb{C}[[z]]$. Les propositions suivantes sont équivalentes :

(*i*) f est entière et f est à croissance exponentielle, *ie* il existe deux constantes C_1 et C_2 telles que pour tout $z \in \mathbb{C}$, $|f(z)| \leq C_1 e^{C_2|z|}$.

(*ii*) $\mathscr{L}(f)$ est analytique en $+\infty$.

Démonstration (V.5)

$(i) \Rightarrow (ii)$: Montrons que $\mathscr{L}(f)(\frac{1}{z}) = \sum_{n=0}^{+\infty} a_n n! z^{n+1}$ a un rayon de convergence strictement positif en $z = 0$.
Soit $r > 0$ un nombre réel. En utilisant la transformée de Laplace sous forme intégrale :

$$\left|\mathscr{L}(f)\left(\frac{1}{r}\right)\right| \leq \int_0^{+\infty} |f(t)|\, e^{-t/r} dt \leq C_1 \int_0^{+\infty} e^{C_2 t} e^{-t/r} dt = C_1 \left[\frac{e^{(C_2 - \frac{1}{r})t}}{C_2 - \frac{1}{r}}\right]_0^{+\infty}.$$

Si $C_2 - \frac{1}{r} < 0$, *ie* $r < 1/C_2 \neq 0$, le membre de droite est fini. Donc le rayon de convergence de $\mathscr{L}(f)\left(\frac{1}{z}\right)$ est supérieur à $1/C_2$, le résultat est donc assuré.

$(ii) \Rightarrow (i)$: Par hypothèse, il existe $R > 0$ tel que pour tout $0 < r < R$, $\sum_{n=0}^{\infty} a_n n! r^{n+1}$ converge. En particulier, il existe un entier $N > 0$ tel que pour tout $n \geq N$, $|a_n| n! r^{n+1} < 1$. Donc $|a_n||z|^n < \frac{|z/r|^n}{n!}$ d'où $\sum_{n=N}^{\infty} |a_n z^n| \leq \sum_{n=N}^{\infty} \frac{|z/r|^n}{n!} \leq e^{|z|/r}$. Donc on a bien l'inégalité $|f(z)| \leq C_1 e^{C_2|z|}$ pour de certaines constantes C_1 et C_2.

□

Lemme V.6.

Soit $f \in \mathbb{C}[[z]]$. Les propositions suivantes sont équivalentes :

(*i*) f est le développement en série entière autour de $z = 0$ d'un polynôme exponentiel.

(*ii*) $\mathscr{L}(f)$ est une fonction rationnelle.

Cette équivalence donne une bijection entre l'ensemble des polynômes exponentiels et les fonctions rationnelles nulles en $+\infty$.

Démonstration (V.6)

Examinons dans un premier temps l'action de la transformation de Fourier (intégrale) sur un polynôme exponentiel. Par linéarité, il suffit de l'examiner sur une fonction du type $u : z \mapsto z^k e^{\alpha z}$: pour tout p complexe tel que $\mathfrak{Re}(p) > \alpha$,

$$\mathscr{L}(u)(p) = \int_0^{+\infty} e^{-tp} t^k e^{\alpha t} dt \overset{\text{I.P.P.}}{=} \frac{k!}{(\alpha - p)^{k+1}}.$$

$(i) \Rightarrow (ii)$: Avec la précédente remarque, ce sens est clair.
$(ii) \Rightarrow (i)$: $\mathscr{L}(f)(z) = R(z) + \frac{P(z)}{Q(z)}$ avec P, Q, R des polynômes et $\deg(P) \geq \deg(Q)$. En décomposant en éléments simples, $\frac{P(z)}{Q(z)} = \sum_{i=1}^{r} \sum_{j=1}^{d_i} \frac{\alpha_{i,j}}{(z-\beta_i)^j}$.
Notons $R(X) = \sum_{i=0}^{d} a_i X^i$. Alors on a : $\frac{P(z)}{Q(z)} = \mathscr{L}(\sum_{i=1}^{r} \sum_{j=1}^{d_i} \frac{-\alpha_{i,j} e^{\beta_i} (-z)^{j-1}}{j!})$.
Par injectivité de $\mathscr{L}$, $f(z) = \sum_{i=0}^{d} a_i \frac{i!}{(-s)^{i+1}} + \sum_{i=1}^{r} \left(\sum_{j=1}^{d_i} \frac{-\alpha_{i,j}(-z)^{j-1}}{j!}\right) e^{\beta_i}$.

□

Si $\mathscr{L}(f)$ est une fraction rationnelle, alors $\mathscr{L}(f)(1) = 0$ équivaut à $(z-1)|\mathscr{L}(f)$. D'où la définition suivante :

Définition V.4.

On définit les deux opérateurs suivants :

$$\delta : \begin{array}{ccc} \mathbb{C}[[z]] & \to \mathbb{C}[[z]] \\ f(z) & \mapsto (1-z)f(z) \end{array} \quad \text{et} \quad \mathcal{D} : \begin{array}{ccc} \mathscr{F}_{\mathbb{C}} & \to \mathscr{F}_{\mathbb{C}} \\ f & \mapsto f + f' \end{array} .$$

L'introduction de l'opérateur $\mathcal{D}$ est justifiée par le résultat suivant :

Proposition V.7.

Le diagramme suivant commute :

$$\begin{array}{ccc} \mathbb{C}[[z]] & \xrightarrow{\mathscr{L}} & \mathscr{F}_{\mathbb{C}} \\ \delta \downarrow & & \downarrow \mathcal{D} \\ \mathbb{C}[[z]] & \xrightarrow{\mathscr{L}} & \mathscr{F}_{\mathbb{C}} \end{array}$$

Proposition V.8.

δ et $\mathcal{D}$ sont des opérateurs bijectifs.

Démonstration (V.8)

On note que les opérateurs :

$$\tilde{\delta} : \begin{array}{ccc} \mathbb{C}[[z]] & \to \mathbb{C}[[z]] \\ f(z) & \mapsto \frac{f(z)}{1-z} \end{array} \quad \text{et} \quad \tilde{\mathcal{D}} : \begin{array}{ccc} \mathscr{F}_{\mathbb{C}} & \to \mathscr{F}_{\mathbb{C}} \\ f & \mapsto \sum_{k=0}^{\infty} (-1)^k \frac{d^k}{dx^k} \end{array} .$$

sont respectivement réciproques de δ et $\mathcal{D}$.

□

Remarque V.2.

Examinons l'action des opérateurs ci-dessus. Si on prend comme notation :

$$\begin{cases} \delta\left(\sum_{n=0}^{\infty} a_n z^n\right)(z) = a_0 + \sum_{n=1}^{\infty} (a_n - a_{n-1}) z^n =: \sum_{n=0}^{\infty} b_n z^n, \\ \mathcal{D}\left(\sum_{n=0}^{\infty} \frac{c_n}{z^{n+1}}\right)(z) = \frac{c_0}{z} + \sum_{n=1}^{\infty} \frac{c_n - n c_{n-1}}{z^{n+1}} =: \sum_{n=0}^{\infty} \frac{d_n}{z^{n+1}}. \end{cases}$$

Alors on a les relations entre les coefficients :

$$\begin{cases} b_0 = a_0, & \forall n \in \mathbb{N}\backslash\{0\},\ b_n = a_n - a_{n-1} \\ d_0 = c_0, & \forall n \in \mathbb{N}\backslash\{0\},\ d_n = c_n - n c_{n-1}, \end{cases}$$

que l'on peut « inverser » :

$$\begin{cases} \forall n \in \mathbb{N}, a_n = \sum_{k=0}^{n} b_k \\ \forall n \in \mathbb{N}, c_n = n! \sum_{k=0}^{n} \frac{d_k}{k!}. \end{cases}$$

Enfin, compte tenu de ces propriétés, Bezivin et Robba ont introduit en 1987 une formulation équivalente de (L-W) en termes de séries formelles :

Théorème V.9 (B-R [a]).

Si $v \in \mathscr{F}_{\mathbb{Q}}$ est analytique à l'infini telle que $\mathcal{D}(v)$ est une fonction rationnelle, alors v est une fonction rationnelle.

a. pour *Bezivin-Robba*

C'est (B-R) que l'on va montrer dans la partie suivante. Montrons d'abord l'équivalence.

Théorème V.10.

(L-W) $\Leftrightarrow$ (B-R).

Démonstration (V.10)

$\Rightarrow$: Soit $v \in \mathscr{F}_{\mathbb{Q}}$ analytique en $+\infty$, telle que $D(v)$ soit une fonction rationnelle.
Du lemme 2 et de la surjectivité de $\mathscr{L}$, il existe un polynôme exponentiel à coefficients dans $\overline{\mathbb{Q}}$: $f(z) = \sum_{i=1}^{r} p_i e^{\alpha_i z}$, tel que $\mathscr{L}(f) = \mathcal{D}(v)$.
Définissons g par $g(z) := \frac{f(z)}{1-z}$. g vérifie $\delta(g) = f$, donc par le lemme 3, $\mathcal{D}(\mathscr{L}(g)) = \mathscr{L}(\delta(f)) = \mathcal{D}(v)$. Par injectivité de $\mathcal{D}$, $\mathscr{L}(g) = v$. Par le lemme 1, g est entière. Donc 1 n'en est pas un pôle, donc $\sum_{i=0}^{r} p_i(1)e^{\alpha_i} = f(1) = 0$. Par (LW), on a donc pour tout $i \in [\![1, n]\!]$, $p_i(1) = 0$, donc $(1-z)|f(z)$. Finalement g est un polynôme exponentiel, donc par le lemme 2, v est bien une fonction rationnelle.

$\Leftarrow$: Supposons par l'absurde $\neg$(LW). Alors il existe $f(z) = \sum_{i=1}^{m} \beta_i e^{\alpha_i z}$, où les α_i et β_i sont algébriques, les α_i distincts deux à deux et les β_i non tous nuls ; tels que $f(1) = 0$
Quitte à remplacer f par le produit de ces conjugués de Galois $\sum_{i=1}^{m} \sigma(\beta_i) e^{\sigma(\alpha_i) z}$, on peut même supposer que les α_i et β_i sont rationnels.
Alors :

$$\mathscr{L}(f)(z) = \sum_{i=1}^{m} \frac{\beta_i}{1 - \alpha_i z},$$

les pôles étant tous simples.
De plus, $f(1) = 0$, donc $g(z) := \frac{f(z)}{1-z}$ est entière et de croissance exponentielle. Donc d'après le lemme 1, $v := \mathscr{L}(g)$ est analytique à l'infini. Les relations $v = \mathscr{L}(g)$ et $\delta(g) = f$, muni du lemme 3, nous assurent $\mathcal{D}(v) = \mathscr{L}(f)$, donc $\mathcal{D}(v)$ n'a que des pôles simples.
Supposons v rationnelle. On peut alors écrire $v = \frac{P}{Q}$ (avec Q non nul), et $\mathcal{D}(v) = \frac{PQ + P'Q + PQ'}{Q^2}$, et en comparant les ordres de multiplicités des racines, on remarque que cette fraction rationnelle ne peut avoir de pôles simples, donc v n'est pas rationnelle.

On a donc trouvé une fonction v qui n'est pas rationnelle et analytique à l'infini, mais telle que $\mathcal{D}(v)$ est rationnelle, ce qui contredit (B-R).

□

V.3 Démonstration de (B-R)

Soit $v \in \mathscr{F}_{\mathbb{Q}}$ analytique à l'infini telle que $w := \mathcal{D}(v)$ est une fonction rationnelle. On peut donc décomposer w en éléments simples dans $\mathbb{Q}$:

$$w(z) = \sum_{i=1}^{m} \sum_{j=1}^{d_i} \frac{\alpha_{i,j}}{(z-\gamma_i)^j}.$$

Or $\mathcal{D}^{-1} = \sum_{k=0}^{\infty} (-1)^k \frac{d^k}{dx^k}$, donc :

$$v(z) = \sum_{i=1}^{m} \sum_{j=0}^{d_i} \alpha_{i,j} \sum_{k=0}^{\infty} \binom{k+j-1}{j-1} \frac{k!}{(z-\gamma_i)^{j+k}}. \tag{1}$$

Notons :

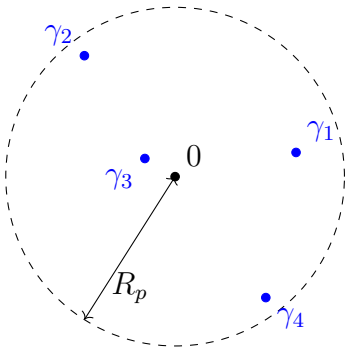
- Pour tout $i \in [\![1, m]\!]$, $\mathcal{U}_i = \{p \text{ premier}, |\gamma_i|_p = 1\}$
- Pour tous $i \in [\![1, m]\!]$, $j \in [\![1, d_i]\!]$, $\mathcal{V}_{i,j} = \{p \text{ premier}, |\alpha_{i,j}|_p = 1\}$
- Pour tous $i \neq j \in [\![1, m]\!]$, $\mathcal{W}_{i,j} = \{p \text{ premier}, |\gamma_i - \gamma_j|_p = 1\}$.

Alors tous ces ensembles sont de complémentaires finis (on utilise le fait que les $\alpha_{i,j}$ et γ_i sont des nombres rationnels), et posons $\mathcal{S}'$ l'union de tous les complémentaires, à laquelle on ajoute ∞ ($\mathcal{S}'$ est donc fini).
Écrivons :

$$v(z) = \sum_{n=0}^{\infty} \frac{a_n}{z^{n+1}}.$$

Soit $p \notin \mathcal{S}'$. Notons dans un premier temps que $k!$ et $\binom{k+j-1}{j-1}$ sont des entiers, donc de valeur absolue p-adique inférieure à 1. Alors en utilisant l'inégalité ultramétrique, la définition de $\mathcal{S}'$ et l'expression 1, on a, pour tout $n \in \mathbb{N}$, $|a_n|_p \leq 1$. Donc (B1) est vérifiée, et on peut même affirmer que pour tout ensemble de places contenant $\mathcal{S}'$, (B1) est toujours vérifiée.

Soit maintenant $p \in \mathcal{S}'$. Alors d'après 1, v converge en dehors d'un disque (connexe) $\mathcal{K}_p \subset \mathbb{C}_p$ de rayon $R_p > \max_{1 \leq i \leq m} (|\gamma_i|_p)$, d'où (B2).



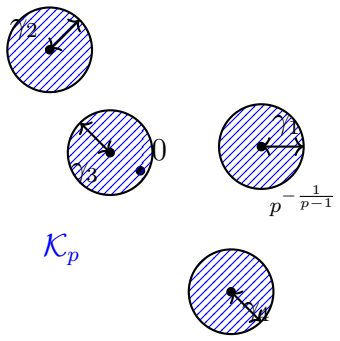
Pour raffiner cette condition et obtenir un contrôle du diamètre transfini nécessaire à (B3), observons le comportement de v pour $p \notin \mathcal{S}'$.
Soit alors $p \notin \mathcal{S}'$. v converge en dehors de disques de centre γ_i. Plus précisément, $|\cdot|_p$ étant ultramétrique, d'après II.4,

$$v(z) \text{ converge si, et seulement si pour tous } i \in [\![1,m]\!], j \in [\![1,d_i]\!], \ \frac{|(k+j-1)!|_p}{|z-\gamma_i|_p^k} \underset{k\to\infty}{\longrightarrow} 0.$$

Or cette dernière expression a le même comportement que la suite $(k!/z^k)_{k\geq 0}$, qui converge, d'après la formule de Legendre, pour tout $|z|_p > p^{\frac{-1}{p-1}}$.
Posons alors :

$$\mathcal{K}_p := \bigcup_{i=1}^{m} \underbrace{D(\gamma_i, p^{\frac{-1}{p-1}})}_{D_i},$$

de sorte que v converge sur le complémentaire de $\mathcal{K}_p$.



Calculons alors le diamètre transfini de $\mathcal{K}_p$.
Pour tout $i \neq j \in [\![1,m]\!], |\gamma_i - \gamma_j|_p = 1 > p^{\frac{-1}{p-1}}$ par définition de $\mathcal{S}'$, donc $D_i \cap D_j = \emptyset$. Notons que si deux points x et y sont dans deux disques, respectivement D_i et D_j avec $i \neq j$, leur distance est de 1. En effet :

$$|\gamma_i - y| = \max(|\gamma_i - \gamma_j|, |\gamma_j - y|) = 1$$

car $|\gamma_i - \gamma_j| = 1 \neq p^{\frac{-1}{p-1}} = |\gamma_j - y|$, donc :

$$|x - y| = \max(|x - \gamma_i|, |\gamma_i - y|) = 1.$$

De même, si deux points distincts appartiennent à la même boule, leur distance est au plus $p^{\frac{-1}{p-1}}$, et cette distance est atteinte au « bord » de cette boule, *ie* lorsque la distance à γ_i est $p^{\frac{-1}{p-1}}$.
On reprend les notations de III.2.2.
Soient un entier $n > 0$ et des points $x_1, \ldots, x_n$ de $\mathcal{K}_p$. Alors, pour maximiser $g(x_1, \ldots, x_n) = \prod_{i\neq j} |x_i - x_j|$, on place $\lfloor n/m \rfloor + \varepsilon$ points dans chacune des m boules, tous les points dans une même boule à distance $p^{\frac{-1}{p-1}}$ des autres (avec $\varepsilon = 0$ ou 1 décrivant les $n - m\lfloor n/m \rfloor$ points restants). On obtient alors l'encadrement :

$$p^{\frac{-1}{p-1} n \lfloor \frac{n}{m} \rfloor} \leq D_n(B) \leq p^{\frac{-1}{p-1} n (\lfloor \frac{n}{m} \rfloor + 1)},$$

d'où :

$$\delta_\infty(\mathcal{K}_p) = p^{\frac{-1}{m(p-1)}}$$

Donc :

$$\prod_{\substack{p\notin\mathcal{S}'\\ p\leq x}} \delta_\infty(\mathcal{K}_p) = \prod_{\substack{p\notin\mathcal{S}'\\ p\leq x}} p^{\frac{-1}{m(p-1)}} = \exp\left(\sum_{\substack{p\notin\mathcal{S}'\\ p\leq x}} \frac{-\ln(p)}{m(p-1)}\right).$$

Or $\sum_{p \text{ premier}} \frac{\ln(p)}{p}$ diverge vers $+\infty$ [4] et $\mathcal{S}'$ est fini, donc :

$$\prod_{\substack{p\notin\mathcal{S}'\\ p\leq x}} \delta_\infty(\mathcal{K}_p) \underset{x\to\infty}{\longrightarrow} 0.$$

En particulier, si l'on note $T := \prod_{p\in\mathcal{S}'} \delta_\infty(\mathcal{K}_p)$, il existe un certain x_0 tel que pour tout $x > x_0$, $\prod_{\substack{p\notin\mathcal{S}'\\ p\leq x}} \delta_\infty(\mathcal{K}_p) < 1/T$.
Posons alors $\mathcal{S} = \{p \notin \mathcal{S}',\ p \leq x_0\} \sqcup \mathcal{S}'$. Pour ce choix (fini, contenant ∞) de places, on a bien :

$$\prod_{p\in\mathcal{S}} \delta_\infty(\mathcal{K}_p) < 1,$$

donc (B3) vérifiée. On note aussi que (B2) est toujours vérifiée.
Donc d'après le théorème de Bertrandias, v est rationnelle. D'où (B-R).

Remarque V.3.

Notons l'importance de l'hypothèse que v est à coefficients rationnels dans la preuve. En effet, si v était à coefficients complexes, alors $\mathcal{S}'$ n'a pas de raison d'être fini, et (B1) ne pourrait être vérifiée *a priori*.
On peut d'ailleurs donner un contre-exemple à (B-R) dans le cas complexe. Reprenons les notations de la démonstration de théorème 3.10 et définissons :

$$f(z) = e^{i\pi z} + 1.$$

Cette fonction s'annule en 1, ce qui permet de définir $g(z) = \frac{f(z)}{z-1}$. On vérifie alors que

$$v(z) := \mathscr{L}(g)(z) = \mathscr{L}\left(\sum_{k=0}^{\infty} \frac{(i\pi)^{k+1}}{(k+1)!} z^k\right) = \sum_{k=1}^{\infty} \frac{1}{k+1}\left(\frac{i\pi}{z}\right)^k = -\log\left(1 - \frac{i\pi}{z}\right),$$

n'est pas rationnelle, mais est analytique à l'infini, et :

$$\mathcal{D}(v)(z) = \mathscr{L}(f)(z) = -\mathscr{L}\left(\sum_{k=1}^{\infty} \frac{(i\pi)^k}{k!} z^k\right) = -\frac{1}{z}\sum_{k=1}^{\infty}\left(\frac{i\pi}{z}\right)^k = \frac{1}{z}\left(1 - \frac{1}{1-\frac{i\pi}{z}}\right),$$

est rationnelle.

4. C'est même équivalent à $\ln(n)$: il s'agit du premier théorème de Martens.

VI Preuves d'irrationalité : vers de nouvelles méthodes au delà des critères d'algébrisation

« Oh ! chérubins. »
Évariste Galois, en marge d'une lettre de Siméon Denis Poisson

L'article au centre de cette section est [CDT24], dont l'objectif est de montrer l'irrationalité de la valeur de la fonction L de Dirichlet suivante :

$$L(2,\chi_{-3}) = \sum_{n=0}^{\infty}\left(\frac{1}{(3n+1)^2} - \frac{1}{(3n+2)^2}\right) \approx 0,7813.$$

Nous n'irons pas jusqu'à ce résultat, mais suivre la démarche des auteurs qui y mènent, pour s'arrêter sur une application, qui n'est certes pas une exclusivité, mais qui donne une bonne idée de comment la théorie s'applique.

Notons que le résultat de cet article est l'unique preuve de l'irrationalité explicite [5] de L-valeurs [6], en dehors de la constante d'Apéry $\zeta(3)$ [7]. C'est la preuve d'Apéry lui-même qui va inspirer la construction de la théorie exposé dans l'article.

VI.1 Une première approche : la preuve d'Apéry de l'irrationalité de $\zeta(3)$

Nous nous contenterons de donner une esquisse de la démonstration. Une preuve complète peut être trouvée en [Poo79].
Cette preuve repose sur un critère « élémentaire » d'irrationalité :

Lemme VI.1.

Soient β un réel, $\varepsilon > 0$ et $(p,q) \in (\mathbb{Z}\times\mathbb{N}\backslash\{0\})^{\mathbb{N}}$ tels que pour tout entier $n \geq 0, p_n/q_n \neq \beta$, et $\lim_{n\to\infty} q_n = +\infty$.

Supposons qu'il existe $n_0 \in \mathbb{N}$ tel que pour tout entier $n \geq n_0, \left|\beta - \dfrac{p_n}{q_n}\right| < \dfrac{1}{q_n^{1+\varepsilon}}$.

Alors β est irrationnel.

Démonstration (VI.1)

Si $\beta = \frac{a}{b}$ est rationnel, pour tout $n \geq n_0$, on a :

$$0 < |aq_n - p_n b| < \frac{|b|}{q_n^{\varepsilon}},$$

et $|aq_n - p_n b|$ est entier, d'où le résultat par l'absurde en sachant que le terme de droite

5. Il existe des résultats assez insolites sur ces valeurs. Par exemple, Zudilin a montré qu'au moins une valeur parmi $\zeta(5),\zeta(7),\zeta(9)$ et $\zeta(11)$ est irrationnelle

6. ou valeurs de fonctions L

7. ... et des valeurs $\zeta(2n)$ avec n entier positif, mais ce résultat est relativement simple à montrer, contrairement aux deux autres.

converge vers 0.

□

Remarque VI.1.

Grossièrement, ce résultat nous affirme que si un nombre peut être approximé de trop près par des rationnels sans être approximé exactement, c'est qu'il ne peut pas être lui aussi rationnel.

La première idée est de s'inspirer de la représentation suivante de $\zeta(3)$:

$$\zeta(3) = \frac{5}{2}\sum_{n=0}^{\infty} \frac{(-1)^{n-1}}{n^3\binom{2n}{n}},$$

qui converge « plus vite » que la représentation classique.
Ensuite sont introduits (de manière très astucieuse) deux suites (a_n) et (b_n) de rationnels, qui proviennent de la suite doublement indicée :

$$c_{n,k} := \sum_{m=1}^{n} \frac{1}{m^3} + \sum_{m=1}^{k} \frac{(-1)^{m-1}}{2m^3\binom{n}{m}\binom{n+m}{m}},$$

qui converge vers $\zeta(3)$ lorsque $n \to \infty$, uniformément en k. [8].
Il vérifie ensuite que les suites ainsi définies vérifient une même relation de récurrence :

$$\forall n \geq 2, n^3u_n - (34n^3 - 51n^2 + 27n - 5)u_{n-1} + (n-1)^3u_{n-2} = 0, \qquad (\dagger)$$

avec différentes conditions initiales.
Cela lui permet de déterminer deux éléments importants :

— pour tout entier $n \geq 0, a_n \in \mathbb{Z}$ et $[1, \ldots, n]^3 b_n \in \mathbb{Z}$,
— $a_n, b_n = O(\alpha^n)$ avec $\alpha = (1+\sqrt{2})^4$ [9].

Nous noterons dans la suite $[1, \ldots, n] := \text{ppcm}(1, \ldots, n)$ si n est entier [10], et $[1, \ldots, a] := [1, \ldots, \lfloor a \rfloor]$ si $a > 0$.

Donc les séries $A(x) := \sum_{n=0}^{\infty} a_n x^n$ et $B(x) := \sum_{n=0}^{\infty} b_n x^n$ ont comme rayon de convergence commun $\frac{1}{(1+\sqrt{2})^4} = (1-\sqrt{2})^4$.
Avec la même relation, on peut montrer que la série $P(x) := B(x) - \zeta(3)A(x)$ a comme rayon de convergence $(1+\sqrt{2})^4$, ou autrement dit que :

$$\zeta(3) - \frac{b_n}{a_n} = O\left(\frac{1}{a_n^2}\right).$$

On ne peut cependant pas encore appliquer le lemme, car les b_n ne sont pas entiers, mais on peut essayer de l'appliquer à $p_n := [1, \ldots, n]^3 b_n$ et $q_n := [1, \ldots, n]^3 a_n$, qui eux, sont entiers.
Le théorème des nombres premiers nous donne l'estimation asymptotique $\ln([1, \ldots, n]) = n + o(n)$, donc la borne devient $q_n = O(\alpha^n e^{3n})$, et

8. Les suites (a_n) et (b_n) vont être des formes un peu modifiées du numérateur et dénominateurs, respectivement, de $(c_{n,n})$, dans un sens défini dans l'article.
9. c'est une racine du polynôme associé $X^2 - 34X + 1$
10. cette notation est utile pour regarder la « mise au même dénominateur » des premiers inverses d'entiers

$$\zeta(3) - \frac{p_n}{q_n} = O(\alpha^{-2n}) = O(q_n^{1-\varepsilon}),$$

avec $\varepsilon := \dfrac{\ln(\alpha) - 3}{\ln(\alpha) + 3} \approx 0,08 > 0$, d'où le résultat avec le lemme.

De nombreuses tentatives ont été entreprises afin de faire fonctionner cette idée de démonstration avec d'autres L-valeurs, sans vraiment aboutir (en dehors de $\zeta(2)$; la preuve se trouve aussi dans l'article de van der Poorten, et est aussi dûe à Apéry).
La suite de cette section a pour objectif d'évoquer des moyens d'améliorer qualitativement cette méthode.

VI.2 *Holonomy bound* et application à la rationalité de séries formelles

La démonstration d'Apéry utilise de façon essentielle la relation entre les coefficients (†), qui, dans le langage des séries formelles, signifie que $A(x)$ et $B(x)$ sont solutions d'une équation différentielle ordinaire (EDO dans la suite) à coefficients dans $\mathbb{Z}[X]$, avec des singularités en $0, \infty$ et $(\sqrt{2} \pm 1)^4$ (elles en forment même une base des solutions). La fonction $P(x)$ ainsi définie est l'unique (modulo la multiplication par un scalaire) solution de l'EDO qui soit holomorphe en 0 et en $(\sqrt{2} - 1)^4$: cette propriété caractérise $\zeta(3)$.
Le seul élément utilisé par Apéry est qu'elle est holomorphe sur le disque ouvert $D(0, \alpha)$, alors qu'elle est bien plus, puisqu'elle se prolonge en une fonction holomorphe sur $\mathbb{C}\backslash[\alpha, \infty[$, et cela à tout à voir avec nos théorèmes de la partie III.2 ! En effet, ce qu'a utiliser Apéry est un équivalent du théorème de Borel, alors que ce que nous suggérons est plutôt un équivalent du théorème de Pólya, c'est à dire s'appliquant à une partie simplement connexe du plan qui n'est pas un disque.

Dans le cas général, pour un certain nombre donné η [11] dont nous voulons montrer l'irrationalité, on trouve une série entière f à coefficients dans $\mathbb{Q}(\eta)$ qui le caractérise, comme étant unique solution d'une certaine EDO qui converge sur un domaine plus important que les séries qui forment une base des solutions. On suppose ensuite par l'absurde que η est rationnelle ; autrement dit que f est à coefficients rationnels.
L'idée maintenant est de considérer la forme des dénominateurs de f puisque ces coefficients sont rationnels, et de construire un $\mathbb{Q}(x)$-espace vectoriel engendré par les séries entières du même type. L'objectif est alors d'estimer la dimension de l'espace vectoriel ainsi engendré.
Pour déterminer un *minorant*, on souhaite trouver des fonctions « connues » qui sont dans cet espace (à coefficients rationnels !), puis de montrer l'indépendance linéaire sur $\mathbb{Q}(x)$ avec la fonction f (qui s'obtient par exemple par des considérations de monodromie).
De l'autre côté, il existe des résultats assez récents de *majorations* de telles dimensions. Nous espérons alors avoir trouver assez de fonctions pour que la minoration dépasse la majoration, ce qui aboutirait à une contradiction.
Ces théorèmes de majoration sont au centre de l'article [CDT24], et sont dénommés *arithmetic holonomy bound*.
Voici un exemple de telles majorations, qui nous sera utile dans la suite :

Théorème VI.2.

Soit $\mathbf{b} = (b_{i,j})$ une matrice de taille $m \times r$ de nombres positifs telle qu'il existe, pour tout

11. plus précisément une *période*, qui forment une classe de nombres particulière

$j \in [\![1, r]\!]$, des entiers $1 \leq u_j \leq m$ et des nombres $b_j > 0$ vérifiant

$$0 = b_{1,j} = \cdots = b_{u_j,j} < b_{u_j+1,j} = \cdots = b_{m,j} = b_j.$$

Pour tout $i \in [\![1, m]\!]$, notons $\sigma_i = \sum_{j=1}^{r} b_{i,j}$ la somme des termes de la ligne i, et notons :

$$\tau(\mathbf{b}) := \frac{1}{m^2} \sum_{i=1}^{m} (2i-1)\sigma_i.$$

Soit $\Omega \subset \mathbb{C}$ un ouvert simplement connexe contenant 0 de rayon conforme $\mathrm{rad}(0, \Omega) > e^{\tau(\mathbf{b})}$. Soient enfin $f_1, \ldots, f_m$ des séries formelles à coefficients dans $\mathbb{Q}$ linéairement indépendantes sur $\mathbb{Q}(x)$ de la forme

$$f_i(x) = \sum_{n=0}^{\infty} \frac{a_{i,n}}{[1, \ldots, b_{i,1}n] \ldots [1, \ldots, b_{i,r}n]} x^n,$$

où les $a_{i,n}$ sont entiers, méromorphes sur Ω.
Alors on a l'inégalité suivante :

$$m \leq \frac{\ln(\mathrm{rad}(0, \Omega))}{\ln(\mathrm{rad}(0, \Omega)) - \tau(\mathbf{b})}.$$

C'est en fait un corollaire d'un théorème central de l'article. On trouvera sa démonstration [[CDT24], Théorème 2.7.1].

Remarque VI.2.

Notons que le rayon conforme relativement à 0 prend ici la place du diamètre transfini (fidèlement à l'article). Ce ne sont pas les mêmes quantités, surtout que les auteurs de l'article ont défini le rayon conforme comme l'inverse de celui défini dans ce texte III.3 (voir en effet la remarque précédant le théorème 1.2.4 de l'article). Néanmoins les calculs sont similaires en prenant comme fonction du théorème de l'application conforme la fonction $g(w) = \frac{1}{f(\frac{1}{w})}$, avec f une fonction utilisée dans le calcul du diamètre transfini. Nous laisserons au lectorat le soin de se convaincre de cette traduction.

Une application de ce que l'on vient de développer :

Proposition VI.3.

Soit $f(x) = \sum_{n=0}^{\infty} a_n x^n$ une série entière à coefficients rationnels telle que :

(1) Pour tout $n \in \mathbb{N}, [1, \ldots, n] a_n \in \mathbb{Z}$

(2) $f(x)$ est holomorphe sur $\mathbb{C} \backslash [1, +\infty[$.

Alors il existe deux fractions rationnelles $P, Q \in \mathbb{Q}(x)$ telles que

$$f(x) = P(x) + Q(x) \ln(1 - x).$$

Démonstration (VI.3)

L'ouvert simplement connexe $\Omega := \mathbb{C}\backslash[1, +\infty[$ a comme rayon conforme $\mathrm{rad}(0, \Omega) = 4$ par III.12. Appliquons le théorème VI.2 à $m = 3, r = 1, \mathbf{b} = (0, 1, 1)^T$. On calcule

$$\tau(\mathbf{b}) = \frac{1}{3^2}((2 \times 1 - 1) \times 0 + (2 \times 2 - 1) \times 1 + (2 \times 3 - 1) \times 1 = \frac{8}{9}.$$

Or,

$$e^{\frac{8}{9}} < 4 \text{ et } \frac{\ln(4)}{\ln(4) - \frac{8}{9}} \approx 2,78 < 3,$$

qui contredit le théorème, donc il n'y a pas de fonction $\mathbb{Q}(x)$-linéairement indépendante de 1 et $\ln(1 - x)$ qui satisfait (1) et (2), d'où le résultat.

□

Remarque VI.3.

Ce résultat donne, comme le nomme les auteurs de l'article, une *caractérisation arithmétique* du logarithme, qui est, modulo la multiplication par des fractions rationnelles, la seule qui vérifie les hypothèses.
La question peut être posée pour d'autres types de dénominateurs ; c'est par exemple l'objet de la conjecture 2.8.1 de l'article pour les dénominateurs du type $[1, \ldots, n]^2$.

Un corollaire est le résultat suivant, qui traite à proprement parler de rationalité de séries formelles :

Théorème VI.4.

Soit $\Omega \subset \mathbb{C}$ un ouvert simplement connexe contenant 0. Soient r un entier, $b_1, \ldots, b_r \geq 0$ et $f(x)$ une série formelle du type :

$$f(x) = \sum_{n=0}^{\infty} \frac{a_n}{[1, \ldots, b_1 n] \ldots [1, \ldots, b_r n]} x^n,$$

où les a_n sont entiers. Supposons que $f(x)$ soit en $x = 0$ le germe d'une fonction méromorphe [a] sur Ω, et plaçons nous dans l'un des deux cas suivants :

(i) $\Omega = D(0, R)$ est un disque de rayon $R > e^{b_1 + \cdots + b_r}$ centré en 0,

(ii) son rayon conforme vérifie : $\mathrm{rad}(0, \Omega) > e^{\frac{3}{2}(b_1 + \cdots + b_r)}$.

Alors $f(x)$ est rationnelle.

a. *ie* qui coïncide avec une fonction méromorphe au voisinage de 0

Démonstration (VI.4)

Commençons par le cas (ii), qui est plus simple. En effet, il s'agit de la contraposée du théorème précédent. Posons $m = 2$ et

$$\mathbf{b} = \begin{pmatrix} 0 & \ldots & 0 \\ b_1 & \ldots & b_r \end{pmatrix}.$$

Alors on calcule $\tau(\mathbf{b}) = \frac{3}{4}\sigma$, où l'on notera $\sigma := \sum_{i=1}^{r} b_i$.

Par hypothèse, on a $\ln(\mathrm{rad}(0,\Omega)) > 2\tau(\mathbf{b})$, donc $2 > \frac{\mathrm{rad}(0,\Omega)}{\mathrm{rad}(0,\Omega)-\tau(\mathbf{b})}$, donc 1 et $f(x)$ sont liées sur $\mathbb{Q}(x)$, ce qui veut précisément dire que $f(x)$ est rationnelle.
Pour l'autre cas, le théorème VI.2 nous assure dans un premier temps que le $\mathbb{Q}(x)$-espace vectoriel engendré par les fonctions de ce type, noté $\mathcal{H}$, est de dimension finie. En effet, s'il y a m fonctions linéairement indépendantes avec ce type de dénominateurs, alors $\sigma \geq \frac{m}{m+1}\ln(\mathrm{rad}(0,\Omega))$, d'où la borne $e^{\tau(\mathbf{b})} < \mathrm{rad}(0,\Omega)$ pour m assez grand. Or si une fonction $f(x)$ est dans $\mathcal{H}$, alors il en est de même de ses dérivées. Donc $\mathcal{H}$ étant de dimension finie, f est solution d'une EDO à coefficients dans $\mathbb{Q}(x)$, ou autrement dit, il existe un entier r, des fractions rationnelles $c_0, \ldots, c_r$ (avec $c_r \neq 0$) telles que l'opérateur $A := \sum_{k=0}^{r} c_k D^k$ vérifie :

$$Af = 0.$$

Or, pour tout entier m, en posant $\zeta_m := e^{\frac{2i\pi}{m}}$, les fonctions

$$\frac{1}{m}\sum_{i=0}^{m-1} f(\zeta_m^i x)\zeta_m^{-ix} = \sum_{n=0}^{\infty} a_{mn+k}x^{mn+k},$$

(qui sont les transformées de Fourier de f), sont aussi méromorphes sur Ω, et ont des dénominateurs du même type ; autrement dit ils sont encore dans $\mathcal{H}$, et $\mathcal{H}$ est conservé sous l'action $x \mapsto \zeta_m x$, pour tout m. Donc si s est une singularité de A, il en est de même pour tout $\zeta_m s$. Donc $s = 0$ ou $s = \infty$. Il en découle que f est méromorphe sur $\mathbb{C}$ et par le théorème VI.2 de nouveau, avec R aussi grand que l'on veut, on a le résultat.

□

Remarque VI.4.

Ce résultat étend le théorème de Borel dans (i) et Pólya dans (ii), avec $b_1 = \cdots = b_r = 0$.

VI.3 Application : irrationalité de ln(3)

Nous mettons à l'épreuve le dernier résultat que nous venons d'évoquer, en démontrant que ln(3) est irrationnelle [12].
Pour cela, considérons la fonction :

$$f(x) := \frac{1}{\sqrt{1-4x+x^2}}\int_{2-\sqrt{3}}^{x} \frac{dt}{\sqrt{1-4t+t^2}}.$$

Notons que : $2-\sqrt{3}$ est un racine de X^2-4X+1, et l'on connaît une primitive de $t \mapsto \frac{1}{\sqrt{1-4t+t^2}}$, qui est $t \mapsto -\ln(2-t+\sqrt{1-4t+t^2})$ (d'où l'apparition du ln(3) en évaluant en $2-\sqrt{3}$).
On peut alors calculer le développement de Taylor de f. Le calcul explicite est fastidieux et peu utile. On ne veut que la forme des dénominateurs. On peut alors l'estimer :

$$f(x) = \frac{1}{2}\sum_{n=0}^{\infty}(b_n - a_n\ln(3))\frac{x^n}{2^n},$$

avec $a_n \in \mathbb{Z}$ et $[1,\ldots,n]b_n \in \mathbb{Z}$ (vient du développement de ln). Ici aussi, les fonctions $A(x)$ et $B(x)$ sont holomorphes en dehors de $\{2 \pm \sqrt{3}\}$, et $f(x)$ est l'unique combinaison linéaire (à multiplication

12. elle est même transcendante en vertu du théorème de Lindemann Weierstrass V.1 ; l'objectif est simplement d'appliquer la théorie.

par un scalaire près) des deux qui est holomorphe en $2-\sqrt{3}$ (comme on peut le voir sur la forme intégrale).
Pour simplifier les notations, nous travaillerons avec $g(x) := f(2x)$. Supposons maintenant $\ln(3) \in \mathbb{Q}$. Alors $g(x)$ est à coefficients dans $\mathbb{Q}$. On peut appliquer le théorème VI.4 avec $r = 1, b_1 = 1$, et $g(x)$ holomorphe sur $\Omega := \mathbb{C}\backslash[\frac{2+\sqrt{3}}{2}, +\infty[$, dont le rayon conforme $\mathrm{rad}(0, \Omega) = 2(2+\sqrt{3}) > e^{3/2}$, ce qui prouve la contradiction (f dérive d'un logarithme, donc n'est pas rationnelle).

Remarque VI.5.

Il est possible d'avoir, avec relativement peu d'efforts supplémentaires, un résultat inédit d'irrationalité, à savoir la linéaire indépendance sur $\mathbb{Q}$ entre les périodes suivantes :

$$1, \frac{\pi}{\sqrt{3}}, \pi^2 \text{ et } L(2, \chi_{-3}) - \tfrac{\pi \ln(3)}{3\sqrt{3}},$$

en travaillant sur les fonctions suivantes :

$$\frac{1}{\sqrt{1-4x}}, \frac{1}{\sqrt{1-4x}} \int_0^x \frac{dt}{(1-t)\sqrt{1-4t}}, \frac{1}{\sqrt{1-4x}} \int_0^x \frac{\ln(1-t)}{t\sqrt{1-4t}} dt, \text{ et}$$
$$\frac{1}{\sqrt{1-4x}} \int_0^x \frac{\ln(1-t)}{(1-t)\sqrt{1-4t}} dt,$$

le point critique 1/4, et des considérations de monodromie. C'est l'objet du §2.11 de l'article. Il faudra bien plus de travail pour montrer le résultat phare de l'article, à savoir la linéaire indépendance entre $1, \zeta(2)$ et $L(2, \chi_{-3})$.

A Construction du corps des nombres complexes p-adiques

« Le désert ne peut plus croître, il est partout.
Mais il peut encore s'approfondir »
Comité invisible, *L'insurrection qui vient*

A.1 Généralités sur les extensions de corps

A.1.1 Premières définitions

Définition A.1.

Soit $\mathbb{K}$ un corps.
On appelle extension de corps de $\mathbb{K}$ tout couple $(\mathbb{L}, \varphi)$, où $\mathbb{L}$ est un corps et $\varphi : \mathbb{K} \to \mathbb{L}$ est un morphisme de corps (nécessairement injectif).

Remarque A.1.

On notera abusivement $\mathbb{K} \subseteq \mathbb{L}$ pour signifier que $(\mathbb{L}, \varphi)$ est une extension de $\mathbb{K}$ pour un certain φ, et on identifiera les éléments de $\mathbb{K}$ avec leur image par φ.

Dans la suite de cette sous-section, on fixe $\mathbb{K} \subseteq \mathbb{L}$ une telle extension.

Proposition A.1.

$\mathbb{L}$ est un $\mathbb{K}$-espace vectoriel pour les opérations d'addition héritées de l'addition en tant qu'anneau et de multiplication par un scalaire de $\mathbb{K}$.

Définition A.2.

On appelle *degré de l'extension* de $\mathbb{L}$ sur $\mathbb{K}$ et on note $[\mathbb{L} : \mathbb{K}] \in \mathbb{N} \cup \{+\infty\}$ la dimension de $\mathbb{L}$ en tant que $\mathbb{K}$-espace vectoriel.
On dira que l'extension est *finie* si $[\mathbb{L} : \mathbb{K}] < +\infty$.

Proposition A.2 (Base téléscopique).

Soient $\mathbb{K} \subseteq \mathbb{L}$ et $\mathbb{L} \subseteq \mathbb{M}$ deux extensions finies de degré respectif d et d'. Alors $\mathbb{K} \subseteq \mathbb{M}$ est une extension finie, de degré dd'.

Démonstration (A.2)

Si $(a_i)_{1 \leq i \leq d}$ est une base de $\mathbb{L}$ en tant que $\mathbb{K}$-espace vectoriel et $(b_j)_{1 \leq j \leq d'}$ est une base de $\mathbb{M}$ en tant que $\mathbb{L}$-espace vectoriel, alors on montre que $(a_i b_j)_{\substack{1 \leq i \leq d \\ 1 \leq j \leq d'}}$ est une base de $\mathbb{M}$ en tant que $\mathbb{K}$-espace vectoriel.

□

A.1.2 Notion de polynôme minimal

On supposera l'extension finie.

Définition A.3.

Soit $a \in \mathbb{L}$.
On appelle *polynôme minimal* de a sur $\mathbb{K}$, et on note $\pi_{a,\mathbb{K}}$, l'unique polynôme unitaire irréductible à coefficients dans $\mathbb{K}$ qui admet a pour racine.

Remarque A.2.

Cette définition est valable car $\mathbb{K}[X]$ est principal, et le polynôme unitaire qui engendre l'idéal annulateur de a défini comme $\{P \in \mathbb{K}[X], P(a) = 0\}$ est unique : c'est le polynôme minimal de a.

Définition A.4.

Soit $a \in \mathbb{L}$.
On note $\mathbb{K}(a)$ le plus petit sous-corps de $\mathbb{L}$ qui contient a et $\mathbb{K}$.

Proposition A.3.

Soit $a \in \mathbb{L}$.
$\mathbb{K}(a)$ est une extension finie de $\mathbb{K}$ et son degré est le degré d du polynôme minimal de a sur $\mathbb{K}$.

Démonstration (A.3)

Il suffit de considérer $(1, a, \ldots, a^{d-1})$, qui est une base de $\mathbb{K}(a)$.

□

On supposera désormais que $\mathbb{K} \subseteq \mathbb{L}$ est finie.

Corollaire A.4.

Soit $a \in \mathbb{L}$.
Alors $\deg(\pi_{a,\mathbb{K}}) \mid [\mathbb{L}, \mathbb{K}]$.

Démonstration (A.4)

Par la formule de la base téléscopique, en considérant $\mathbb{K} \subseteq \mathbb{K}(a) \subseteq \mathbb{L}$.

□

Définition A.5.

Soit $a \in \mathbb{L}$.
On appelle *norme* de a relative à l'extension $\mathbb{L}/\mathbb{K}$ [a], l'élément de $\mathbb{K}$ noté $N_{\mathbb{L}/\mathbb{K}}(a)$, égal au déterminant de l'endomorphisme de $\mathbb{L}$ (en tant que $\mathbb{K}$-espace vectoriel) φ_a défini par $\varphi_a(x) = ax$ pour tout $x \in \mathbb{L}$.

a. ou simplement *norme* de α quand les circonstances sont évidentes

Proposition A.5.

Soit $a \in \mathbb{L}$. Notons $d := \deg(\pi_{a,\mathbb{K}})$ et $c := [\mathbb{L}/\mathbb{K}]/d$.

Alors $N_{\mathbb{L}/\mathbb{K}}(a) = ((-1)^d \pi_{a,\mathbb{K}}(0))^c$.

Démonstration (A.5)

Notons χ_a le polynôme caractéristique de φ_a, et ψ_a la restriction de φ_a à $\mathbb{K}(a)$. Remarquons que le polynôme minimal de φ_a est aussi le polynôme minimal de a, à savoir $\pi_{a,\mathbb{K}}$. On sait alors déjà que $\pi_{a,\mathbb{K}} \mid \chi_a$, montrons que $\chi_a = (\pi_{a,\mathbb{K}})^c$.
On sait que $(1, a, \dots, a^{d-1})$ est une base de $\mathbb{K}(a)$ en tant que $\mathbb{K}$-espace vectoriel. La matrice $M_{\mathbb{K}(a)}$ de ψ_a dans cette base est la matrice compagnon de $\pi_{a,\mathbb{K}}$, donc son polynôme caractéristique est $\pi_{a,\mathbb{K}}$.
Maintenant, on sait que si $(l_1, \dots, l_c)$ est une base de $\mathbb{L}$ en tant que $\mathbb{K}(a)$-espace vectoriel, $(m^i l_j)_{\substack{1 \le i \le d \\ 1 \le j \le c}}$ est une base de $\mathbb{L}$ sur $\mathbb{K}$, et la matrice $M_{\mathbb{L}}$ de φ_a dans cette base est la matrice par blocs :

$$M_{\mathbb{L}} = \begin{pmatrix} M_{\mathbb{K}(a)} & 0 & \dots & 0 \\ 0 & M_{\mathbb{K}(a)} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & M_{\mathbb{K}(a)} \end{pmatrix},$$

d'où l'égalité $\chi_a = (\pi_{a,\mathbb{K}})^c$, et le résultat en évaluant en 0.

□

A.2 Un peu d'algèbre linéaire

Le résultat suivant est en fait une généralisation du théorème valable sur $\mathbb{R}$ ou $\mathbb{C}$: « En dimension finie, toutes les normes sont équivalentes ».

Proposition A.6.

Soit $\mathbb{K}$ un corps valué complet. Soit E un $\mathbb{K}$-espace vectoriel de dimension finie.
Alors toutes les normes sur E sont équivalentes. De plus, E est complet pour chacune d'entre elles.

Démonstration (A.6)

Nous allons raisonner avec comme norme de référence la norme infinie $\|\cdot\|_\infty : (x_1, \dots, x_n) \mapsto \max_{1 \le i \le n} |x_i|$ (n la dimension de E).
Notons déjà que la première conclusion implique la deuxième, car la norme infinie préserve la complétude.
Démontrons alors la première conclusion, et ce par récurrence sur $n = \dim_{\mathbb{K}}(E)$.
Si $n = 1$, il n'y a rien à démontrer.
Sinon, soit $(e_1, \dots, e_n)$ une base de E. Alors pour tout $x = (x_1, \dots, x_n) \in E$,

$$\|x\| = \left\| \sum_{i=1}^{n} x_i e_i \right\| \le \sum_{i=1}^{n} |x_i| \|e_i\| \le \|x\|_\infty \sum_{i=1}^{n} \|e_i\|,$$

d'où l'une des inégalités.
Pour l'autre, supposons par l'absurde que les topologies engendrées sont différentes. Alors il existe une suite $x = (x_{k,1}, \dots, x_{k,n})_{k \ge 0}$ qui converge vers 0 pour $\|\cdot\|$ mais pas pour $\|\cdot\|_\infty$. Il existe

donc une constante $c > 0$, un indice i et une extractrice φ telle que $x_{\varphi(k),i} > c$ pour tout $k \geq 0$. Alors la suite définie pour tout $k \geq 0$ par $u_k := \frac{1}{x_{\varphi(k),i}} x_{\varphi(k)}$ est bien définie et converge vers 0 pour $\|\cdot\|$, donc $(u_k - e_i)_{k\geq 0}$ est une suite d'éléments de $H := \mathrm{Vect}(e_1, \ldots, e_{i-1}, e_{i+1}, \ldots, e_n)$ qui converge vers e_i. Autrement dit, e_i est dans l'adhérence de H. Or, par hypothèse de récurrence, H est complet, donc $e_i \in H$, ce qui est absurde car $(e_1, \ldots, e_n)$ est une base de E, ce qui achève la démonstration.

□

Remarque A.3.

La démonstration n'utilise principalement que la complétude de $\mathbb{K}$. On pourra comparer avec les démonstrations dans le cas $\mathbb{R}$ ou $\mathbb{C}$, qui utilisent souvent la compacité locale de ces espaces.

A.3 Méthode de Newton dans le cas ultramétrique

Cette sous-section ne comporte pas de preuves, car la théorie développée n'a comme objectif (dans ce texte) qu'un corollaire utile pour la suite. Néanmoins, cette théorie est intéressante en elle-même, et nous conseillons au lectorat curieux le document de Chambert-Loir [Cha23] et celui de Colmez [Col05].

Rappelons rapidement le principe de la méthode de Newton dans le cas réel. L'idée est d'approximer, via une suite de réels, un zéro d'une fonction suffisamment régulière. On s'inspire en fait du développement de Taylor au voisinage d'un zéro x : $f(x) \approx f(x_0) + (x - x_0)f'(x_0)$ pour $x_0 \approx x$, pour construire une suite définie par x_0 proche de x et pour $k \geq 1, x_{k+1} = x_k - \frac{f(x_k)}{f'(x_k)}$. Cette suite converge sous les bonnes conditions, souvent même assez vite (quadratiquement).
Il existe un résultat similaire dans le cas ultramétrique.
On notera K un corps ultramétrique complet, dont on note $A = \mathscr{O}_K$ son anneau d'entiers et $k = k_K$ son corps résiduel.

Théorème A.7.

Soit $f \in A[T]$. Soit $a \in A$ tel que $|f(a)| < |f'(a)|^2$.
La méthode de Newton pour f issue du point a converge vers l'unique élément $x \in A$ tel que $f(x) = 0$ et $|x - a| < |f'(a)|$.

Démonstration

Voir [[Cha23], proposition 3.2]

□

Ce résultat s'énonce aussi dans le cas de plusieurs variables, où la norme retenue est la norme infinie, et la dérivée est remplacée par le jacobien (noté Jf) :

Théorème A.8.

Soit $f = (f_1, \ldots, f_n) \in A[T_1, \ldots, T_n]^n$. Soit $a \in A^n$ tel que $\|f(a)\| < |Jf(a)|^2$.
La méthode de Newton pour f issue du point a converge vers l'unique élément $x \in A^n$ tel que $f(x) = 0$ et $|x - a| < |Jf(a)|$.

Démonstration

Voir [[Cha23], proposition 3.6]

□

Le prochain résultat est essentiel en arithmétique des corps ultramétriques. Il énonce, pour faire simple, qu'une factorisation approchée d'un polynôme suffit pour avoir une factorisation exacte. C'est un corollaire du théorème précédent, avec l'application de multiplication de polynômes

$$f : \begin{array}{ccc} A_n[T]^2 & \longrightarrow & A_{2n}[T] \\ (P,Q) & \longmapsto & PQ \end{array}.$$

Le jacobien ici dérive alors du *résultant* des polynômes considérés g et h de degré respectifs p et q, noté $\mathrm{Res}_{p,q}(g,h)$; c'est le déterminant de l'application linéaire :

$$\varphi : \begin{array}{ccc} A_q[T] \times A_p[T] & \longrightarrow & A_{p+q}[T] \\ (U,V) & \longmapsto & Ug + Vh \end{array}.$$

Le résultant a été assez bien étudié, même en dehors de notre cadre, ce qui permet par exemple de savoir :

Lemme A.9.

Soient $g, h \in K[T]$, $p, q \in \mathbb{N}$.
Alors $\mathrm{Res}_{p,q}(f,g) = 0$ si, et seulement si, l'une des deux conditions suivantes est vérifiée :

— g et h ne sont pas premiers entre eux

— $\deg(g) < p$ ou $\deg(h) < q$.

Démonstration

Voir [[Cha23], §3.7]

□

Théorème A.10 (Lemme de Hensel).

Soit $f, g, h \in A[T]$ des polynômes de degré respectif n, p et q, de résultant noté $R = \mathrm{Res}_{p,q}(g,h)$, tels que $n = p + q$ et $\|f - gh\| < |R|^2$.
Alors il existe un unique couple $(g^*, h^*) \in A[T]^2$ tel que :

$$\begin{cases} f = g^* h^* \\ \deg(g - g^*) < p, \|g - g^*\| < |R| \\ \deg(h - h^*) < q, \|h - h^*\| < |R|. \end{cases}$$

Démonstration

Voir [[Cha23], §3.8]

□

Enfin nous arrivons au résultat qui nous importe dans la suite de la construction :

Corollaire A.11.

Soit $f = \sum_{k=0}^{n} a_k T^k \in K[T]$ irréductible, unitaire, et tel que $a_0 \in A$.
Alors $f \in A[T]$.

Démonstration (A.11)

On veut alors prouver que pour tout $0 \leq k \leq n, |a_k| \leq 1$. Notons p le plus grand indice tel que $|a_p| = \max_{0\leq k\leq n} |a_k|$. Les hypothèses assurent le résultat si $p = 0$ ou n.
Sinon, notons $b_k := a_p^{-1} a_k$ (ce sont les coefficients de $a_p^{-1} f$). Alors, par construction de p, pour tout $0 \leq k \leq p-1, |b_k| \leq 1$ et pour tout $p+1 \leq k \leq n, |b_k| < 1$.
Posons $g := b_n T^{n-p} + 1$ et $h := T^p + b_{p-1} T^{p-1} + \cdots + b_0$. Ce sont des polynômes à coefficients dans A et on a $\deg(a_p^{-1} f - gh) < n$, et les coefficients de $a_p^{-1} f - gh$ sont de valeur absolue inférieure strictement à 1 (en écrivant explicitement le polynôme).
Étudions alors $R := \mathrm{Res}_{n-p,p}(g, h)$. Sa projection dans le corps résiduel est $\overline{R} = \mathrm{Res}_{n-p,p}(\overline{g}, \overline{h}) = \mathrm{Res}_{n-p,p}(\overline{b_n} T^{n-p} + 1, T^p)$. Ces deux polynômes n'ont pas de racines communes et $p = \deg(\overline{h})$, donc d'après le lemme au dessus, ce résultant n'est pas nul, donc $R \notin \mathfrak{m}_K$, donc $|R| = 1$. Le lemme de Hensel assure donc une factorisation de $a_p^{-1} f$, donc de f, ce qui contredit l'hypothèse d'irréductibilité.

□

A.4 Sur les extensions de valuation

Cette sous-section sera en grande partie inspirée par [Col05].

Examinons maintenant comment se prolonge à une extension $\mathbb{K} \subseteq \mathbb{L}$ une valuation définie sur $\mathbb{K}$, dans un premier temps quand l'extension est finie :

Proposition A.12.

Soit $\mathbb{K}$ un corps complet pour une valuation v, et soit $\mathbb{L}$ une extension finie de $\mathbb{K}$.
Alors il existe une unique valuation v' sur $\mathbb{L}$ telle que $v'|_{\mathbb{K}} = v$. De plus,

$$\forall x \in \mathbb{L}, v'(x) = \frac{1}{[\mathbb{L} : \mathbb{K}]} v(N_{\mathbb{L}/\mathbb{K}}(x)).$$

Démonstration (A.12)

Vérifions que la formule ci-dessus définit bien une valuation.
(VA1) $v'(0) = \frac{1}{[\mathbb{L}:\mathbb{K}]} v(0) = +\infty$,
(VA2) Soient $a, b \in \mathbb{L}$. On a (en écrivant simplement la définition) $\varphi_{ab} = \varphi_a \circ \varphi_b$ et le déterminant est un morphisme, donc $v'(ab) = \frac{1}{[\mathbb{L}:\mathbb{K}]} v(N_{\mathbb{L}/\mathbb{K}}(a) N_{\mathbb{L}/\mathbb{K}}(b)) = v'(a) v'(b)$,
(VA3) Soit $a \in \mathbb{L}$. Quitte à utiliser la multiplicativité, il suffit de montrer que si a vérifie $v'(a) \geq 0$, alors $v'(1 + a) \geq 0$.
Soit $f(X) = X^d + \cdots + a_0$ le polynôme minimal de a sur $\mathbb{K}$. Alors d'après un A.5, $N_{\mathbb{L}/\mathbb{K}}(a) = ((-1)^d a_0)^{[\mathbb{L}:\mathbb{K}]/d}$. Donc, sachant $v(N_{\mathbb{L}/\mathbb{K}}(a)) \geq 0, v(a_0) \geq 0$, donc $a_0 \in \mathscr{O}_{\mathbb{K}}$. Or f est irréductible, donc avec le corollaire précédent, $f \in \mathscr{O}_{\mathbb{K}}[X]$. Or le polynôme minimal de $a + 1$ est $f(X - 1)$, donc $N_{\mathbb{L}/\mathbb{K}}(a + 1) = ((-1)^d f(-1))^{[\mathbb{L}:\mathbb{K}]/d} \in \mathscr{O}_{\mathbb{K}}$, ce qui assure $v'(a + 1) \geq 0$ et le résultat.
Pour l'unicité, si une autre valuation v'' sur $\mathbb{L}$ vérifie la même propriété, alors d'après A.6, elles sont multiples l'une de l'autre. En évaluant sur un élément de $\mathbb{K}$ distinct de 0 et 1, on trouve qu'elles sont en fait égales.

□

Corollaire A.13.

Soit $(\mathbb{K}, v)$ un corps valué complet. Notons $\overline{\mathbb{K}}$ sa clôture algébrique.
Alors il existe une unique manière de prolonger v à $\overline{\mathbb{K}}$.

Démonstration (A.13)

Il suffit de vérifier que le prolongement de v ne dépend pas de l'extension choisie dans laquelle on considère $x \in \overline{\mathbb{K}}$ dans la formule ci-dessus. On montre par exemple que pour toute extension $\mathbb{K} \subset \mathbb{L}$ qui contient x,

$$\frac{1}{[\mathbb{L} : \mathbb{K}]} v(N_{\mathbb{L}/\mathbb{K}}(x)) = \frac{1}{[\mathbb{K}(x) : \mathbb{K}]} v(N_{\mathbb{K}(x)/\mathbb{K}}(x)),$$

ce qui est vrai d'après A.5 et le théorème de la base téléscopique.

□

Il nous reste maintenant à montrer que cette clôture algébrique est bien complète ... ce qui n'est le cas en général. Néanmoins, une étape en plus donne fin au cycle. Nous repassons aux valeurs absolues pour clarifier les notations.

Théorème A.14.

Soit $(\mathbb{K}, |\cdot|)$ un corps valué complet. Notons $\overline{\mathbb{K}}$ sa clôture algébrique.
Alors la complétion $\mathbb{C}_{\mathbb{K}}$ de $\overline{\mathbb{K}}$ est algébriquement close.

Démonstration (A.14)

Soit $f = X^n + \sum_{i=0}^{n-1} a_i X^i$ un polynôme à coefficients dans $\mathbb{C}_{\mathbb{K}}$. Par II.6, $\overline{\mathbb{K}}$ est dense dans $\mathbb{C}_{\mathbb{K}}$, donc pour tout entier $0 \leq i \leq n-1$, il existe des coefficients $(a_{i,j})_{j \geq 0}$ de $\overline{\mathbb{K}}$ tels que pour tout indice i et tout entier j assez grand, $|a_{i,j} - a_i| < \min(|a_i|, \frac{1}{j})$. Par inégalité ultramétrique, on a déjà $|a_{i,j}| = |a_i|$. Nous noterons pour tout entier j,

$$f_j = X^n + \sum_{i=0}^{n-1} a_{i,j} X^i.$$

Ces polynômes sont à coefficients dans $\overline{\mathbb{K}}$, donc il existe une racine x_j à f_j dans $\overline{\mathbb{K}}$ pour tout j. On voudrait trouver, à partir de la suite x_j et d'une *potentielle limite*, une racine à f dans $\mathbb{C}_{\mathbb{K}}$.
Regardons d'abord le contrôle qu'impose les coefficients de f sur les x_j.
Notons que de $f_j(x_j) = 0$, on a l'inégalité

$$|x_j^n| = \left| \sum_{i=0}^{n-1} a_{i,j} x_j^i \right| \leq \max_{0 \leq i \leq n-1} |a_{i,j}||x_j^i| = \max_{0 \leq i \leq n-1} |a_i||x_j|^i.$$

Pour tout entier j, notons i_j un indice qui réalise ce maximum. Alors $|x_j| \leq |a_{i_j}|^{\frac{1}{n-i_j}}$, donc en notant $C := \max_{0 \leq i \leq n-1} |a_i|^{\frac{1}{n-i}}$, on a

$$|x_j| \leq C.$$

Ensuite, on peut regarder la « taille » de la valeur que prend f en la suite x_j :

$$|f(x_j)| = |f(x_j) - f_j(x_j)| = \left|\sum_{i=0}^{n-1}(a_i - a_{i,j})x_j^i\right| \leq \max_{0\leq i\leq n-1}|a_i - a_{i,j}||x_j|^i \leq$$
$$\max_{0\leq i\leq n-1}|a_i - a_{i,j}|\max(1, C^{n-1}) \leq \frac{\max(1, C^{n-1})}{j}$$

par construction des $a_{i,j}$. Ainsi, la suite $(f(x_j))_{j\geq 0}$ converge vers 0.
Enfin, notons $(\alpha_i)_{1\leq i\leq n}$ les racines de f dans un corps de décomposition $\mathbb{C}_\mathbb{K} \subset \mathbb{L}$. Alors l'égalité au dessus se réécrie :

$$\lim_{j\to\infty}\prod_{i=1}^{n}(x_j - \alpha_i) = 0.$$

Donc il existe un indice k tel que la suite $(x_j - \alpha_k)_{j\geq 0}$ admette une sous suite d'extractrice φ qui converge vers 0. En particulier, $(x_{\varphi(j)})_{j\geq 0}$ est de Cauchy dans $\mathbb{C}_\mathbb{K}$ donc converge dans $\mathbb{C}_\mathbb{K}$ par complétude, vers α_k, qui est une racine de f, ce qui achève la démonstration.

□

Une fois ce travail effectué, on peut se reconcentrer sur notre cas particulier $\mathbb{Q}_p$, et construire un tel surcorps :

Définition A.6.

On appelle *corps des nombres complexes p-adiques* et on note $\mathbb{C}_p$ la complétion d'une clôture algébrique de $\mathbb{Q}_p$ pour la valuation héritée canoniquement de $\mathbb{Q}_p$.

Références

[68] *Agrégation des sciences mathématiques*. 1968. URL : http://maths.rombaldi.free.fr/AgregExterne/SujetsAgreg/MathsGenes/mg_1968.pdf.

[Ami75] Y. Amice. *Les nombres p-adiques*. Presses universitaires de France, 1975.

[Bak15] M. Baker. *A p-adic proof that pi is transcendental*. Consulté le 10 mars 2025. 2015. URL : https://mattbaker.blog/2015/03/20/a-p-adic-proof-that-pi-is-transcendental/.

[Cal06] J. Calais. *Éléments de théorie des anneaux. Anneaux commutatifs*. Ellipses, 2006.

[CDT24] F. Calegari, V. Dimitov et Y. Tang. « The linear independance of $1, \zeta(2)$, and $L(2, \chi_{-3})$ ». In : *Arxiv* (2024). URL : https://arxiv.org/pdf/2408.15403.

[Cha23] A. Chambert-Loir. « Balade newtonienne entre analyse et arithmétique ». In : *Arxiv* (2023). URL : https://arxiv.org/pdf/2312.03380.

[CN23] A. Chambert-Loir et C. Noûs. « Potentiel et rationalité ». In : *Arxiv* (2023). URL : https://arxiv.org/pdf/2305.17210.

[Col05] P. Colmez. « Les nombres p-adiques, notes de cours de M2 ». In : (2005). URL : https://webusers.imj-prg.fr/~pierre.colmez/nombres-p-adiques.pdf.

[Dim19] V. Dimitrov. « A proof of the Schinzel-Zassenhaus conjecture on polynomials ». In : *Arxiv* (2019). URL : https://arxiv.org/pdf/1912.12545.

[Gir24] M. Girodon. « Les nombres p-adiques et les groupes profinis ». Université de Strasbourg, 2024.

[Har88] D. Harbeter. « Galois Covers of an Arithmetic Surface ». In : *The Johns Hopkins University Press* (1988). URL : https://www.jstor.org/stable/pdf/2374696.pdf.

[Hil02] E. Hille. *Analytic function theory, vol.2*. American Mathematical Society, 2002.

[Kob77] N. Koblitz. *p-adic Numbers, p-adic Analysis, and Zeta-Functions*. Springer, 1977.

[Per20] Persiflage. *Vesselin Dimitrov on Schinzel–Zassenhaus*. Consulté le 19 mars 2025. 2020. URL : https://www.galoisrepresentations.com/2020/02/10/vesselin-dimitrov-on-schinzel-zassenhaus/.

[Per96] D. Perrin. *Cours d'algèbre*. ellipses, 1996.

[Pól28] G. Pólya. « Über gewisse notwendige Determinantenkriterien für die Fortsetzbarkeit einer Potenzreihe ». In : *Mathematische Annalen* (1928). URL : https://doi.org/10.1007/BF01459120.

[Poo79] A. van der Poorten. « A Proof that Euler Missed ... Apéry's Proof of the Irrationality of $\zeta(3)$ ». In : (1979). URL : https://pracownicy.uksw.edu.pl/mwolf/Poorten_MI_195_0.pdf.

[Ser60] J.-P. Serre. « Rationalité des fonctions ζ des variétés algébriques ». In : *Séminaire Bourbaki* (1960). URL : https://www.numdam.org/item/SB_1958-1960__5__415_0.pdf.

[Tao14] T. Tao. *Dwork's proof of rationality of the zeta function over finite fields*. Consulté le 10 mars 2025. 2014. URL : https://terrytao.wordpress.com/2014/05/13/dworks-proof-of-rationality-of-the-zeta-function-over-finite-fields/#arch.