Les nombres de Pisot

Guillaud Maxence [1]

Sous la direction de Johannes Kellendonk [2]

Semestre de Printemps 2011 - 2012

1. maxence.guillaud@etu.univ-lyon1.fr
2. Professeur à l'Institut Camille Jordan : kellendonk@math.univ-lyon1.fr

Table des matières

Introduction

Les nombres de Pisot sont nommés d'après Charles Pisot (1910-1984), un mathématicien français qui travaillaient surtout dans la théorie des nombres. Il existe beaucoup de résultat sur cet ensemble, qu'il soit algébrique, topologique et même physique !
Nous souhaitons donc offrir une petite introduction accessible avec un bagage mathématiques réduit et permettant quand même d'apercevoir leurs richesses mathématique. Que le lecteur avisé ne s'étonne pas de ne trouver ni une liste exhaustive de résultats les concernant, ni quelque chose de nouveau, ce n'est pas le but.
Cependant, avant d'en arriver là , nous devrons passer par différentes phases. La philosophie de ce travail est d'être accessible à tout élève de deuxième année, c'est pourquoi, nous l'avons organisé ainsi :

– Le premier chapitre sera essentiellement des rappels et des compléments. Il servira à donner une certaine familiarité avec des concepts qui m'ont été nécessaire et d'autres dans lesquelles j'ai dû me plonger totalement étant donné la nouveauté de ceux-ci pour moi. Mais je n'ai pas cédé à la tentation de ne faire que de l'utile et je n'ai pas pu résister à y développer des résultats "inutiles" pour la suite, mais que j'ai trouvé personnellement intéressant. Il ne faut donc pas voir cette partie comme une boite à outil de résultat utile, mais comme de brèves incursions en dépassant la simple utilité. Cette partie se base essentiellement sur [1], [2], [3].

– Le deuxième chapitre s'appuie directement sur la partie précédente et est en sorte une charnière entre une première partie posant des bases et un troisième chapitre en lien direct avec le sujet de ce document. Nous utiliserons la plupart des objets introduits et des résultats de cette partie dans les parties suivantes. Cette partie se basera sur le premier chapitre de [5] et [4].

– Le troisième chapitre qui se base sur le cinquième chapitre de [5] et sur[6] est une première approche des nombres de Pisot en travaillant sur un surensemble de ceux-ci.

– Le quatrième et dernier chapitre, lui, traite uniquement des nombres de Pisot. Nous y développerons quelques résultats sur ceux-ci et tenterons une petite excursion vers le monde de la recherche.Pour plus de détails, on consultera [5] et [6]

Nous avons tenté de démontrer tout ce qu'il nous était possible de démontrer. Mais une volonté de ne pas trop charger cette étude nous a obligé de passer sous silence quelques démonstrations exclusivement algébriques qui auraient nécessité de longs compléments.

Enfin, je remercie Johannes Kellendonk qui a guidé ce TIPE, du choix du sujet, jusqu'à sa rédaction et a su m'aider à surmonter les difficultés que j'ai pu rencontrer en prenant sur son temps pour me conseiller.

Chapitre 1

Pré-requis

1.1 Introduction

Dans cette partie, vous trouverez quelques rappels de notions nécessaires à la poursuite de votre lecture. Bien entendu, une lecture linéaire de cette partie n'est pas nécessaire. Les rappels se structureront sur trois grands thèmes : de l'algèbre générale, une introduction aux séries formelles et enfin des rudiments d'analyse complexe. Pour la partie sur l'analyse complexe, nous ne résisterons pas à l'envie d'aller un peu plus loin...

1.2 Rappel d'algèbre

Nous donnerons ici quelques définitions d'algèbre générale (anneau, corps, etc.)

Définition : Un ensemble G muni d'une loi $\times$ est un groupe si :
- $\times$ est une loi de composition interne associative sur G
- $(G, \times)$ possède un élément neutre
- Pour chaque élément de G, il existe un inverse.

G sera dit abélien si $\times$ est commutative.

Définition : Soit A un ensemble muni de deux lois de composition interne $+$ et $\times$. On dit que $(A, +, \times)$ est un anneau si :
- $(A, +)$ est un groupe commutatif
- $\times$ est associative
- A possède un élément neutre pour $\times$
- $\times$ est distributive par rapport à $+$

Un anneau unitaire est un anneau possédant un élément neutre pour $\times$. Par convention, on écrira "anneau" pour "anneau unitaire" dans la suite.

Définition : Un anneau intègre est un anneau commutatif, diffèrent de $\{0\}$, et sans diviseur de 0.

Pour rappel, un diviseur de 0 dans A est un élément $a \in A, a \neq 0$ tel qu'il existe un $x \in A, x \neq 0$ tel que $ax = 0$.
Enfin, nous appellerons domaine d'intégrité un anneau commutatif unitaire intègre.

Définition : On dit que $(\mathbb{K}, +, \times)$ est un corps si $(\mathbb{K}, +, \times)$ est un anneau commutatif non réduit à $\{0\}$ et dont tous les éléments non nuls sont inversibles.

Définition : Soit A un anneau intègre. Il existe un sous-corps $\mathbb{K}$, unique à un isomorphisme près, tel que A soit un sous-anneau de $\mathbb{K}$ et que tout élément de $\mathbb{K}$ soit de la forme $\frac{a}{b}$, avec $(a, b) \in A^2$ et $b \neq 0$. Ce corps est appelé corps des fractions de l'anneau A.

1.3 Séries

On peut voir les séries formelles comme des analogues aux polynômes formels. Ainsi, il est, ici, sous-entendu que les notions de série numérique, de série entière, de polynôme formel et de fractions rationnelles, tout du moins les bases, sont acquises.

1.3.1 Notation

Dans tout le reste de ce chapitre, nous noterons $\mathbb{K}$ un corps quelconque (commutatif) et $\mathbb{A}$ un anneau. On note $\mathbb{K}[X]$ l'ensemble des polynômes formels à coefficients dans $\mathbb{K}$ où X est une indéterminée. De même, nous noterons $\mathbb{A}[X]$ l'ensemble des polynômes sur un anneau. Nous rappelons que l'ensemble des fractions rationnelles sur un corps $\mathbb{K}$ (respectivement sur un anneau $\mathbb{A}$) est noté $\mathbb{K}(X)$ (respectivement $\mathbb{A}(X)$).
Nous allons voir que la définition d'une série formelle est un prolongement naturel des polynômes formels.

1.3.2 Séries formelles

Définition

Définition : Une série entière formelle en une indéterminée X est une expression formelle $\sum_{n\geq 0} a_n X^n$ où les coefficients $(a_0, ... a_n, ...)$ ne sont plus supposés nuls à partir d'un certain rang.

Remarque : Pour les polynômes formels, la suite des coefficients est supposé nulle à partir d'un certain rang.
On note $\mathbb{K}[[X]]$ (respectivement $\mathbb{A}[[X]]$) l'ensemble des séries formelles à coefficients dans $\mathbb{K}$ (respectivement $\mathbb{A}$). On remarque que :
- $\sum_{n\geq 0} a_n X^n \quad + \quad \sum_{n\geq 0} b_n X^n = \sum_{n\geq 0} (a_n + b_n) X^n$
- $\lambda \sum_{n\geq 0} a_n X^n = \sum_{n\geq 0} \lambda a_n X^n$
- $(\sum_{n\geq 0} a_n X^n)(\sum_{n\geq 0} b_n X^n) = \sum_{n\geq 0} c_n X^n$ avec $c_n = \sum_{p+q=n} a_p b_q$

Si de plus, on note 0 la série formelle tel que $\forall n \in \mathbb{N}, \quad a_n = 0$, alors on a que $\mathbb{K}[[X]]$ est une algèbre sur $\mathbb{K}$ et que $\mathbb{K}[X]$ est une sous-algèbre de $\mathbb{K}[[X]]$.

Ordre, intégrité

Définition : On note $ord(S)$ ou $\omega(S)$, avec $S \in \mathbb{K}[[X]]$ le nombre : $ord(S) = \omega(S) = min\{n | a_n \neq 0\}$. Dans le cas où $S = 0$, on peut soit ne pas définir $ord(S)$ soit le définir comme étant $+\infty$.

On a alors la proposition suivante :

Propriété : $\mathbb{K}[[X]]$ est un anneau intègre. ($ST = 0 \Longrightarrow S = 0$ ou $T = 0$)

Preuve : Supposons $S(X) = \sum_p a_p X^p$ et $T(X) = \sum_q b_q X^q$ non nulles. Notons $s = \omega(S)$ et $t = \omega(T)$. Considérons le produit : $S(X)T(X) = \sum_{n\geq 0} c_n X^n$. On a $c_n = 0$ pour $n < t + s$ et $c_{t+s} = a_t b_s$. $\mathbb{K}$ étant un corps, $(a_t \neq 0, b_s \neq 0) \Longrightarrow c_{t+s} \neq 0$. Donc ST n'est pas nulle.

Ce résultat nous permet en même temps de montrer que $\omega(ST) = \omega(S) + \omega(T)$.
Enfin, si on se place sur A un anneau commutatif unitaire, on a l'implication : $\mathbb{A}$ intègre $\Longrightarrow \mathbb{A}[[X]]$ intègre.

Inverse d'une série formelle

Définition : Soit $S \in \mathbb{K}[[X]]$, on dit que S est inversible s'il existe $T \in \mathbb{K}[[X]]$ tel que $ST = 1$.

Remarque : $(1 - X)$ possède une inverse dans $\mathbb{K}[[X]]$. En effet, on a :

$$(1 - X)(1 + X + ... + X^n + ...) = 1$$

Propriété : $S(X) = \sum_{n\geq 0} a_n X^n$ possède une inverse pour la multiplication de $\mathbb{K}[[X]]$ si et seulement si $a_0 \neq 0$ (ie $S(0) \geq 0$).

Preuve : Notons $T(X) = \sum_{n\geq 0} b_n X^n$ tel que $S(X)T(X) = 1$. Alors $a_0 b_0 = 1$ d'où $a_0 \neq 0$. Supposons maintenant que $a_o \neq 0$. Considérons alors $S_1(X) = (a_0)^{-1} S(X)$. On peut écrire $S_1(X) = 1 - U(X)$ où $U(X) = (-\frac{a_1}{a_0} X - ... - \frac{a_n}{a_0} X^n - ...)$. D'après la remarque, $S_1(X)$ possède un inverse $T_1(X)$ et donc $S(X)$ possède un inverse et :

$$(S(X))^{-1} = (a_0)^{-1} T_1(X)$$

1.4 Analyse complexe

1.4.1 Définition

Définition : On dit qu'une fonction f, définie au voisinage de x_0 est développable en série entière au point x_0 s'il existe une série entière formelle $S(X) = \sum_{n\geq 0} a_n X^n$ dont le rayon de convergence ne soit pas 0 satisfaisant la relation : $f(x) = \sum_{n\geq 0} a_n (x - x_0)^n$ pour $|x - x_0|$ assez petit.

Définition : Une fonction f à valeurs réelles ou complexes, définie dans un ouvert D est dite analytique dans D si, en tout point z_0 de D, la fonction f est développable en série entière au point z_0. Autrement dit, il existe un nombre $r_{z_0} \geq 0$ et une série entière formelle $S(X) = \sum_{n\geq 0} a_n X^n$ de rayon de convergence plus grand que r_{x_0} tel que :

$$f(x) = \sum_{n\geq 0} a_n (z - z_0)^n \quad \text{pour} |z - z_0| < r_{z_0}$$

1.4.2 Critère d'analycité

Propriété : Soit $S(X) = \sum_{n\geq 0} a_n X^n$ une série entière dont le rayon de convergence r n'est pas 0. Soit $S(z) = \sum_{n\geq 0} a_n z^n$ sa somme pour $|z| < r$. Alors $S(z)$ est une fonction analytique dans le disque $|z| < r$.

Propriété : Sous les mêmes hypothèses, soit z_0 tel que $|z_0| < r$. Alors la série entière $\sum_{n\geq 0} \frac{1}{n!} S^{(n)}(z_0) X^n$ a un rayon de convergence $\geq r - |z_0|$ et l'on a :

$$S(z) = \sum_{n\geq 0} \frac{1}{n!} S^{(n)}(z_0)(z-z_0)^n \quad \text{pour} |z-z_0| < r$$

Preuve (de la deuxième propriété) : Posons $r_0 = |z_0|$, $\alpha_n = |a_n|$ et $q = n-p$. On a $S^{(p)}(z_0) = \sum_{q\geq 0} \frac{(p+q)!}{q!} a_{p+q}(z_0)^q$. Donc : $|S^{(p)}(z_0)| \leq \sum_{q\geq 0} \frac{(p+q)!}{q!} \alpha_{p+q}(r_0)^q$. Pour $r_0 \leq \rho < r$:

$$\begin{aligned}
\sum_{p\geq 0} \frac{1}{p!} |S^{(p)}(z_0)|(\rho - r_0)^p &\leq \sum_{p,q} \frac{(p+q)!}{p!q!} \alpha_{p+q}(r_0)^q (\rho - r_0)^p \\
&\leq \sum_{n\geq 0} \alpha_n \Big(\sum_{0\leq p\leq n} (\rho - r_0)^p (r_0)^{n-p} \Big) \\
&\leq \sum_{n\geq 0} \alpha_n \rho^n < +\infty
\end{aligned}$$

Donc le rayon de convergence de $\sum_{n\geq 0} \frac{1}{n!} S^{(n)}(z_0) X^n$ est $\geq \rho - r_0$. Puisque ρ est quelconque et proche de r, on a alors que le rayon de convergence de la série est $\geq r - r_0$.
Considérons maintenant z tel que $|z - z_0| \leq r - r_0$, la série :

$$\sum_{p,q} \frac{(p+q)!}{p!q!} a_{p+q}(z_0)^q (z-z_0)^p$$

converge absolument. On peut donc changer l'ordre des termes de la somme en ayant toujours le bon résultat.
On a alors :

$$\sum_{n\geq 0} a_n \Big(\sum_{0\leq p\leq n} \frac{n!}{p!(n-p!)} (z-z_0)^p (z_0)^{n-p} \Big) = \sum_{n\geq 0} a_n z^n = S(z)$$

et
$$\sum_{p\geq 0}\frac{(z-z_0)^p}{p!}(\sum_{q\geq 0}\frac{(p+q)!}{q!}a_{p+q}(z_0)^q)=\sum_{p\geq 0}\frac{(z-z_0)^p}{p!}S^{(p)}(z_0)$$
D'où : $S(z)=\sum_{p\geq 0}\frac{(z-z_0)^p}{p!}S^{(p)}(z_0)$
La première propriété s'en déduit alors facilement.

1.4.3 Principe du prolongement analytique

La lecture de cette partie n'est pas nécessaire pour continuer à avancer. Néanmoins, c'est un résultat assez emblématique de l'analyse complexe, montrant la puissance de celle-ci.

Propriété : Soit f une fonction analytique dans un ouvert convexe D et soit $z_0\in D$. Les conditions suivantes sont équivalentes :

1. $f^{(n)}(z_0)=0 \quad \forall n\in\mathbb{N}^*$
2. f est identiquement nulle sur un voisinage de z_0
3. f est identiquement nulle dans D

Preuve :
3) $\Longrightarrow$ 1) : Évident.
1) $\Longrightarrow$ 2) : On a $f^{(n)}(z_0)=0$. f est analytique donc au voisinage de z_0, on peut écrire : $f(z)=\sum_{n\geq 0}\frac{1}{n!}f^{(n)}(z_0)(z-z_0)^n$. Les dérivées de f étant toutes nulles sur un voisinage de z_0, on a le résultat.
2) $\Longrightarrow$ 3) : f est identiquement nulle sur un voisinage de z_0. Pour démontrer cette assertion, nous allons essayer de montrer que $D'=\{z\in D|f(z)=0\}$ est à la fois ouvert et fermé. (Et si c'est vrai, alors $D'=D$ car D est connexe et D' est un sous-ensemble de D). On a, par définition d'un voisinage, que D' est ouvert. Soit $z_0\in D$ adhérent à D'. Pour chaque $n\geq 0$, $f^{(n)}(z)=0$ en des points voisins de z_0 (donc des points de D'). Or $f^{(n)}$ est continue, on a alors $f^{(n)}(z_0)=0$. Et c'est vrai pour tout $n\geq 0$. On vient donc de démontrer que $f(z)$ est identiquement nulle sur un voisinage de z_0, donc que $z_0\in D'$. Ainsi, D' est fermé et ouvert, on a donc le résultat voulu.

De ce résultat, on en tire deux corollaires intéressant :

Corollaire 1 : L'anneau des fonctions analytiques dans un ouvert connexe D est un anneau d'intégrité.

Et le corollaire beaucoup plus intéressant qui est le principe du prolongement analytique et qui est le but de cette partie.

Corollaire 2 : Si deux fonctions analytiques f et g dans un ouvert connexe D coïncident au voisinage d'un point D, elles sont identiques dans D.

Preuve : Il suffit de considérer la fonction analytique $h = f - g$ et de voir que les hypothèses sur f et g permettent d'appliquer la propriété précédente et donc de montrer que $h = 0$, ce qui nous donne le résultat.

1.4.4 Fonction holomorphe

Définition : Une fonction $f : \Omega \to \mathbb{C}$ est dite $\mathbb{C}$-dérivable en un point $a \in \Omega$ si la limite :

$$f'(a) = \lim_{h \to 0} \frac{f(a+h) - f(a)}{h}$$

existe dans $\mathbb{C}$.

Une fonction $\mathbb{C}$-dérivable sur un ensemble est bien entendu une fonction $\mathbb{C}$-dérivable en tout point de l'ensemble.

Il peut être intéressant de se poser la question suivante : $\mathbb{C}$ et $\mathbb{R}^2$ sont isomorphe, on peut définir la notion de différentiabilité sur les deux ensembles, on ne peut définir la notion de dérivabilité que sur $\mathbb{C}$. Existe-il un lien entre dérivabilité et différentiabilité ?

Nous rappelons d'abord la définition de différentiabilité :

Définition : Une fonction $f : \Omega \to \mathbb{C}$ est dite différentiable en un point a s'il existe une application $\mathbb{R}$-linéaire $T : \mathbb{C} \to \mathbb{C}$ telle qu'au voisinage de $h = 0$, on ait :

$$f(a+h) = f(a) + T(h) + o(h)$$

Maintenant, nous allons démontrer une propriété qui répond à la question posée.

Propriété : Soit $f : \Omega \to \mathbb{C}$, les propriétés suivantes sont équivalentes :

1. f est $\mathbb{C}$-dérivable en un point $a \in \Omega$

2. f est différentiable en a et df_a est une similitude directe (i.e $df_a(h) = \lambda h$ pour un certain $\lambda \in \mathbb{C}$)
3. f est différentiable en a et $df_a : \mathbb{C} \to \mathbb{C}$ est $\mathbb{C}$-linéaire.

On a de plus que $df_a(h) = f'(a)h$.

Preuve :
Supposons (2) : On a alors $df_a(h) = \lambda h$. Au voisinage de 0, on peut donc écrire :

$$f(a+h) - f(a) = \lambda h + o(h)$$

En divisant le résultat, on obtient (1).
Supposons (1) : Si on prend $\lambda = f'(a)$, on a bien : $f(a+h) - f(a) = f'(a)h + o(h)$, ce qui prouve (2).
Maintenant, prouvons l'équivalence entre (2) et (3). On a bien évidemment que $df_a(h) = \lambda h$ est $\mathbb{C}$-linéaire. Inversement, si $T : \mathbb{C} \to \mathbb{C}$ est $\mathbb{C}$-linéaire alors $T(h) = hT(1)$, ce qui prouve le résultat.

On remarque alors immédiatement que la $\mathbb{C}$-dérivabilité implique la différentiabilité et que si f est $\mathbb{C}$-dérivable alors $df = f'dz$.

Maintenant, définissons une fonction holomorphe :

Définition : On dit qu'une fonction $f : \Omega \to \mathbb{C}$ est holomorphe dans Ω si f est de classe C^1 et $\mathbb{C}$-dérivable en tout point.

Remarque : De ce qui précède, si f est $\mathbb{C}$-dérivable, il est équivalent de dire que f est holomorphe ou que f est $\mathbb{C}$-dérivable à dérivée continue.

Remarque : On remarque facilement qu'une fonction développable en série entière est holomorphe sur son disque de convergence. En fait, on pourrait démontrer qu'il y a équivalence des deux notions !

1.4.5 Résidu d'une fonction

Nous allons maintenant nous atteler à quelque chose qui sera beaucoup plus utile pour la suite, qui est la notion de résidu d'une fonction (complexe). Nous allons seulement donner le nécessaire pour pouvoir l'utiliser dans un cas particulier.
On note $\mathscr{H}(U)$ l'ensemble des fonctions holomorphe sur U un ouvert de $\mathbb{C}$.

Définition : Soit U un ouvert de $\mathbb{C}$, $a \in \mathbb{U}$ et $f : \mathbb{U} \setminus \{a\} \to \mathbb{C}$ une fonction holomorphe. S'il existe une fonction $g : \mathbb{U} \setminus \{a\} \to \mathbb{C}$ et $n \in \mathbb{N}$ tel que :

$$g(a) \neq 0 \qquad \text{et} \quad f(z) = \frac{g(z)}{(z-a)^n} \quad \forall z \in \mathbb{U} \setminus \{a\}$$

alors a est un pôle de f et n est l'ordre du pôle.

Définition : Soit U un ouvert de $\mathbb{C}$. Une fonction f sur U est dite méromorphe dans U s'il existe une partie localement finie A de U telle que $f \in \mathscr{H}(U \setminus A)$ et telle que tout point de A soit un pôle de f. On note $\mathscr{M}(U)$ l'ensemble des fonctions méromorphes dans U.

Autrement dit, une fonction méromorphe sur U est une fonction holomorphe sur U, sauf éventuellement sur un ensemble de points isolés dont chacun est un pôle pour la fonction.

Admettons que nous pouvons écrire $f = \dfrac{g}{h}$ ou f et g sont des fonctions holomorphe sur U non nulles et telle que l'ensemble de points A soit l'ensemble des 0 de h. Supposons de plus que g ne s'annule pas sur A
Soit $a \in A$ un zéro de h de multiplicité p (on dit que a est un pôle d'ordre p) on a $h(z) = (z-a)^p h_1(z)$ avec $h_1(a) \neq 0$ et h holomorphe sur U.

Théorème 1 *Soient U un ouvert de $\mathbb{C}$, $a \in U$, et $f \in \mathscr{H}(U \setminus \{a\})$. Si f admet un pôle d'ordre p alors :*
$\exists!(a_{-1}, \ldots, a_{-p}), \quad p \geq 1, \quad a_{-p} \neq 0$ *tel que*

$$z \mapsto f(z) - \sum_{k=1}^{p} \frac{a_{-k}}{(z-a)^k}$$

se prolonge en une fonction holomorphe au voisinage de a. On appelle le polynôme $\sum_{k=1}^{p} a_{-k}(z-a)^{-k}$ la partie principale de f en a.

Définition : Soient U un ouvert de $\mathbb{C}$, $f \in \mathscr{M}(U)$, et $a \in U$ un pôle d'ordre p de f. La partie principale de f en a est :

$$P(z) = \sum_{k=1}^{m} \alpha_{-k}(z-a)^{-k}$$

On dit que α_{-1} est le résidu de f en a, et on note $\alpha_{-1} = Res(f, a)$.

Nous allons maintenant nous consacrer au calcul pratique du résidu en un pôle simple de f.
Si a un pôle simple ($p=1$), on a :

$$f(z) = \frac{g(z)}{(z-a)h_1(z)} = \frac{\alpha_{-1}}{z-a} + l(z)$$

Donc :

$$Res(f,a) = \alpha_{-1} = \lim_{z\to a}(z-a)f(z) = \lim_{z\to a}\frac{g(z)}{h_1(z)} = \frac{g(a)}{h_1(a)}$$

Or de $h(z) = (z-a)h_1(z)$ on obtient : $h_1(a) = h'(a)$.
On obtient finalement : $Res(f,a) = \dfrac{g(a)}{h'(a)}$.

Chapitre 2

Séries rationnelles

Dans cette partie, nous noterons $\mathbb{A}$ un domaine d'intégrité, $\mathbb{K}$ le corps des fractions de $\mathbb{A}$. Nous remarquerons que les résultats seront presque toujours appliqués avec $\mathbb{A} = \mathbb{Z}$ et $\mathbb{K} = \mathbb{Q}$

2.1 Définition :

Définition : Une série formelle F est dite série rationnelle ou série fractionnaire si et seulement si il existe 2 polynômes P et Q dans $\mathbb{K}[X]$, Q inversible dans $\mathbb{K}[[X]]$ tel que $F = \dfrac{P}{Q} = PQ^{-1}$

Nous observons encore une fois une ressemblance forte entre les fractions rationnelles et les séries rationnelles. Nous allons maintenant nous intéresser à quelques critères de rationalité, critères qui seront purement algébrique.

2.2 Critère de rationalité

2.2.1 Quelques critères

Propriété : Une série formelle $F = \sum_{n\geq 0} a_n X^n \quad \in \mathbb{K}[[X]]$ est une série rationnelle si et seulement si il existe 2 entiers (s, n_0) et $(q_0, ..., q_s) \quad \in \mathbb{K}^{s+1} \quad (s+1)$ éléments de $\mathbb{K}$ tous différents de 0 tel que :

$$\forall n \geq n_0, \quad q_0 a_n + q_1 a_{n-1} + ... + q_s a_{n-s} = 0$$

Preuve : Si F est une série rationnelle, on peut écrire : $F = \sum_{n\geq 0} a_n X^n = \frac{P}{Q}$ avec $Q = \sum_{0\leq i\leq s} q_i X^i, \quad (P,Q) \in \quad \mathbb{K}[X]^2$ et $deg(P) = r$. On a égalité entre les deux séries formelles : $QF = P$.
Prenons $n_0 = sup(r+1, s)$ et soit $n \geq n_0$ alors le coefficient devant chaque X^n de QF sera nul, et en faisant le calcul, on obtient donc :

$$q_0 a_n + q_1 a_{n-1} + ... + q_s a_{n-s} = 0$$

et ce $\forall n \geq n_0$. Réciproquement, posons $Q = \sum_{0\leq i\leq s} q_i X^i$, la relation donnée dans la propriété montre que QF est de degré $\leq n_0 - 1$, donc F est une série rationnelle.

Il existe d'autres critères de rationalités, nous allons en donner un autre, sans démonstration. Mais avant, une petite définition :

Définition : Soit $F = \sum_{n\in\mathbb{N}} a_n X^n \in \mathbb{K}[[X]]$. On appelle déterminant de Kroenecker de F le déterminant :

$$D_n(F) = \begin{vmatrix} a_0 & a_1 & \dots & a_n \\ a_1 & a_2 & \dots & a_{n+1} \\ \vdots & \vdots & \dots & \vdots \\ a_n & a_{n+1} & \cdots & a_{2n} \end{vmatrix}$$

Propriété : $F \in \mathbb{K}[[X]]$ est une série rationnelle si et seulement si $D_n(F) = 0$ à partir d'un certains rang n.

Preuve : La condition nécessaire utilise le premier critère et le fait que le déterminant est une forme multilinéaire alternée. On démontre facilement que pour $n \geq sup(n_0, s)$, la dernière colonne de $D_n(F)$ soit une combinaison linéaire des autres. La condition suffisante, quant à elle, se traite en travaillant directement sur les colonnes d'une matrice choisie spécifiquement. Pour plus de détails, voir chapitre 1 de [5].

2.2.2 Lemme de Fatou

Le lemme de Fatou est aussi une condition algébrique de rationalité. Bien qu'on puisse le trouver dans un cas plus général que celui annoncé (en remplaçant $\mathbb{Z}$ par anneau de Dedekind), nous nous contenterons de ce cas particulier.

Propriété : Lemme de Fatou : Soit $\mathbb{Z}$ muni de l'addition et de la multiplication, c'est à dire un anneau et F une série rationnelle dans $\mathbb{Z}[[X]]$. Alors il existe deux polynômes A et T dans $\mathbb{Z}[X]$ tel que $F = \frac{A}{T}$ où A et T sont premiers entre eux et $T(0) = 1$.

Preuve : Notons A et T dans $\mathbb{Z}[X]$. On les considère premier entre eux. (Sinon, on divise par leur facteur premier pour qu'ils le soient.)
On utilise le théorème de Bezout dans les polynômes :

$$\exists (A_1, T_1, n) \in \mathbb{Z}[[X]]^2 \times \mathbb{Z} \setminus \{0\}, \quad AA_1 + TT_1 = n$$

Divisons par T, on obtient : $A_1 \frac{A}{T} + T_1 = \frac{n}{T}$.
Par hypothèse : $\frac{A}{T} = F$ donc développable en série entière. On alors :

$$a_0 + a_1 z + \ldots + a_n z^n + \ldots = \frac{n}{\alpha + \ldots + \beta z + \ldots + \lambda z^q}$$

Le dénominateur étant T.
On va maintenant supposer que $(\alpha, \ldots, \lambda, n)$ sont premier entre eux dans $\mathbb{Z}$.
De l'égalité entre une fraction rationnelle et une série entière, on en tire :

$$n = a_0 \alpha$$

Soit p un diviseur premier de α (donc p divise n). Si p divise les a_n, on divise par p des deux côtés de l'égalité, on obtient une égalité similaire et on recommence. Ainsi, nous pouvons supposer que p ne divise pas tous les a_n.

Notons maintenant s l'indice du premier coefficient a_n non divisible par p.

On écrit alors :

$$n = (\alpha + \ldots + \lambda z^q)(a_0 + \ldots + a_{s-1} z^{s-1}) + (\alpha + \ldots + \lambda z^q)(a_s z^s + \ldots + a_n z^n + \ldots)$$

On a : p divise n, p divise le premier terme de l'addition (par construction de s), p doit donc diviser le deuxième terme.

Ainsi : p divise $(\alpha + \ldots + \lambda z^q)(a_s z^s + \ldots + a_n z^n + \ldots) = (\alpha a_s) z^s + (\alpha a_{s+1} + \beta a_s) z^{s+1} + \ldots$

On a donc : p divise chaque coefficient de la série obtenu. Mais p ne divise aucun $\{a_n, n \geq s\}$ et p divise α.
On en déduit alors, de proche en proche, que p divise tous les coefficients

$(\alpha, ..., \lambda, n)$. Ainsi, ils ne sont pas premier entre eux, comme supposé. Il y a donc une contradiction, on en conclut qu'il n'existe pas de nombre premier p divisant α et donc que $\alpha = 1$. On a ainsi $T(z) = 1 + \beta z + ... + \lambda z^q$. Donc $T(0) = 1$.

Ainsi, si on a $F \in \mathbb{Z}[[X]]$, on sait que $F = \dfrac{A}{B}$ avec A et B dans $\mathbb{Z}[X]$ et nous venons de prouver qu'on peut les trouver premiers entre eux et tel que $B(0) = 1$.

Chapitre 3

Caractérisation de $\mathbb{U}$

3.1 Introduction

Nous allons maintenant introduire un ensemble particulier de nombre. Pour cela, nous allons démontrer un théorème qui nous permettre de définir et caractériser cet ensemble. Puis, nous définirons une partition de cet ensemble qui servira de fil conducteur au prochain chapitre.

3.2 Notation

Nous utiliserons la notation log pour désigner le logarithme naturel vérifiant la propriété $log(e) = 1$.
Nous noterons α un nombre réel ≥ 1. Ainsi, si λ est un réel diffèrent de 0, nous définirons les deux suites suivantes :

$$u_n = E(\lambda\alpha^n) \quad et \quad \epsilon_n = \epsilon(\lambda\alpha^n) \quad \forall n \in \mathbb{N}$$

On peut écrire tout nombre réel x comme somme de deux termes (et la décomposition est unique) : $x = E(x) + \epsilon(x)$ où $E(x) \in \mathbb{Z}$ et $\epsilon(x) \in]-\frac{1}{2}, \frac{1}{2}]$ avec $|\epsilon(x)|$ qui représente la distance de x à $\mathbb{Z}$. On aura donc :

$$u_n + \epsilon_n = \lambda\alpha^n$$

On observe alors que $E(x)$ sera égale soit au plus petit entier inférieur à x soit au plus petit entier inférieur à x. Exemple : $1,1 = 1 + 0,1$, $1,6 = 2 + (-0,4)$ et $1,5 = 1 + 0.5$ (l'intervalle de définition de ϵ nous permet donc bien d'assurer l'unicité de la décomposition.)
Nous noterons en plus : $\|\lambda\alpha^n\| = |\epsilon_n|$.

Nous étudierons aussi les deux séries entières suivantes : $\sum_{n=0}^{+\infty} u_n z^n$ et $\sum_{n=0}^{+\infty} \epsilon_n z^n$.
Elles correspondent aux séries associées aux fonctions respectivement notées f et g. Elles seront, en outre, analytique respectivement sur $D(0, \frac{1}{\alpha})$ et $D(0,1)$.
Les fonctions seront rationnelle quand $\sum_{n\in\mathbb{N}} u_n X^n$ le sera.
Enfin, si α est un nombre algébrique, nous noterons $P_{\mathbb{K},\alpha}$ son polynôme minimale sur le corps considéré (qui existe par algébricité de α). Les autres racines de ce polynôme seront les conjugués de α et on les notera : $\alpha^{(j)} \quad (j = 2, \ldots s)$. On rappelle que le polynôme minimal de α sur le corps considéré est le polynôme unitaire de plus bas degré à coefficients dans $\mathbb{K}$ admettant α pour racine.
Nous rappelons aussi cette définition :

Définition : Un entier algébrique est un nombre complexe annulé par un polynôme unitaire à coefficients dans $\mathbb{Z}$.

Dans la suite, nous travaillerons avec des entiers algébriques réels et quelques fois, nous omettrons de le rappeler.

Enfin, $\mathbb{Q}(\alpha)$ est par définition le plus petit corps contenant $\mathbb{Q}$ et α. C'est un $\mathbb{Q}$-espace vectoriel de dimension $s-1$ (où s représente le degré de α), une base étant : $(1, \alpha, \ldots, \alpha^{s-1})$. Nous admettrons que $\frac{1}{\alpha} \in \mathbb{Q}(\alpha)$ et que tout élément différent de 0 est inversible (propriété déjà inclue dans le fait que $\mathbb{Q}(\alpha)$ est un corps), et plus particulièrement : $\frac{1}{M(\alpha)} \in \mathbb{Q}(\alpha)$ où M est un polynôme quelconque dans $Q[X]$. Nous n'aurons pas besoin d'aller plus loin dans les propriétés des extensions algébriques.

3.3 Théorème et démonstration

Théorème 2 *Soit α un réel ≥ 1. Supposons qu'il existe un réel $\lambda \geq 1$ tel que :*

$$\|\lambda \alpha^n\| \quad \leq \quad \frac{1}{2e\alpha(\alpha+1)(1+\log\lambda)} \qquad \forall n \in \mathbb{N} \tag{3.1}$$

Alors α est un entier algébrique réel, ses conjugués sont de modules au plus égaux à 1 et λ appartient au corps $\mathbb{Q}(\alpha)$.

Démonstration :
Nous allons tenter de démontrer ce théorème en montrant que la série $\sum_{n\in\mathbb{N}} u_n X^n$ est rationnelle en appliquant la proposition vue précédemment. Le but est donc

de démontrer qu'il existe un entier $s \geq 1$ et un élément $a = (a_i)_{0\leq i\leq s} \in \mathbb{Z}^{s+1} \setminus \{0\}$ tel que, si on note V_n la forme linéaire définie sur $\mathbb{R}^{s+1}$ par :

$$V_n(x) = \sum_{i=0}^{s} u_{n+i} x_i$$

Alors $V_n(a) = 0 \quad \forall n \in \mathbb{N}$
Pour démontrer cela, supposons qu'il existe des nombres $A \in \mathbb{N}^*$ et $\epsilon \in \mathbb{R}^*$ tel que $|\epsilon_n| \quad \leq \quad \epsilon$ et $|a_i| \quad \leq \quad A \quad , i \in \{0,..,s\} \quad \forall n \in \mathbb{N}$.
Le but sera de poser des conditions sur ϵ et A afin de déterminer que (3.1) nous permet d'obtenir la nullité de la forme linéaire V_n sous certaines conditions. Le reste en découlera.

a) $V_n(a) = 0$ et

$$|\epsilon_n| \quad < \quad \frac{1}{(s+1)(\alpha+1)A} \tag{3.2}$$

implique que $V_{n+1}(a) = 0$.

En effet, nous avons :

$$\begin{aligned} |V_{n+1}(a) - \alpha V_n(a)| &= |\sum_{i=0}^{s} a_i(u_{n+1+i} - \alpha u_{n+i})| \\ &= |\sum_{i=0}^{s} a_i((\lambda\alpha^{n+1+i} - \epsilon_{n+1+i}) - \alpha(\lambda\alpha^{n+i} - \epsilon_{n+i}))| \end{aligned}$$

On obtient donc : $|V_{n+1}(a) - \alpha V_n(a)| \quad \leq \quad \sum_{i=0}^{s} |a_i(\epsilon_{n+1+i} - \alpha\epsilon_{n+i})|$
Or, en remarquant que

$$|\epsilon_{n+1+i} - \alpha\epsilon_{n+i}| \quad \leq \quad |\epsilon_{n+1+i}| + |\alpha\epsilon_{n++i}| \quad \leq \quad |(\alpha+1)\epsilon|$$

On obtient : $|V_{n+1}(a) - \alpha V_n(a)| \quad \leq \quad (s+1)(\alpha+1)A\epsilon$.
Avec (3.2), si $V_n(a) = 0$ alors $|V_{n+1}(a)| < 1$ or c'est un entier, on a donc $V_{n+1}(a) = 0$. Ce qui est bien ce qu'on cherchait à démontrer.

b) (3.2) et

$$A \geq 2\lambda^{\frac{1}{s}}\alpha - 1 \tag{3.3}$$

implique qu'il existe $a \in \mathbb{Z}^{s+1} \setminus \{0\}$ tel que $V_0(a) = 0$.

Soit W_0 la forme linéaire définie par $W_0(x) = \sum_{i=0}^{s} |u_i| x_i$. Considérons l'ensemble de points de $\mathbb{Z}^{s+1}$: $D(A,s) = \{x = (x_0,...,x_s) \in \mathbb{Z}^{s+1}, 0 \leq x_i \leq A\}$.

On a $\text{Card}(D(A,s)) = (A+1)^{s+1}$ et :

$$0 \leq |V_0(x)| \leq W_0(x) = \sum_{i=0}^{s} |(\lambda\alpha^i + \epsilon_i)x_i| \leq \sum_{i=0}^{s} (\lambda\alpha^s + \epsilon)x_i \leq (s+1)A(\lambda\alpha^s + \epsilon)$$

En utilisant la condition (3.2), on obtient alors :

$$0 \quad \leq \quad W_0(x) \quad < \quad (s+1)(A+1)\lambda\alpha^s - 1$$

En effet, cela reviens à prouver que :

$$(s+1)A(\lambda\alpha^s + \epsilon) < (s+1)(A+1)\lambda\alpha^s - 1$$

En développant les deux parties, et en soustrayant les termes communs, on observe que cela revient à démontrer que : $(s+1)A\epsilon < (s+1)\lambda\alpha^s - 1$. Or d'après (3.2), $(s+1)A\epsilon < \dfrac{1}{\alpha+1}$ et par hypothèse $\alpha \geq 1$, on obtient donc que :

$$(s+1)A\epsilon < \frac{1}{2}$$

Par hypothèse, nous avons aussi : $s \geq 2$, $\alpha \geq 1$, $\lambda \geq 1$ donc : $(s+1)\lambda\alpha^s \geq 2$ et donc en soustrayant 1, on obtient bien que :

$$(s+1)\lambda\alpha^s \geq 1 > (s+1)A\epsilon$$

Et c'est ce que nous voulions démontrer.
Et avec (3.3), on a finalement :

$$(A+1)^{s+1} \quad \geq \quad 2^s(A+1)\lambda\alpha^s \quad \geq \quad (s+1)(A+1)\lambda\alpha^s$$

On a donc, plus particulièrement : $W_0(x) < (A+1)^{s+1} - 1$. Ceci étant une inégalité mettant en jeu des entiers, nous avons donc encore plus précisément :

$$W_0(x) \leq (A+1)^{s+1} - 2$$

Ainsi, on a la donnée d'une forme linéaire allant d'un ensemble $D(A,s)$ possédant $(A+1)^{s+1}$ élément dans un ensemble de valeurs $\{0, \ldots, (A+1)^{s+1} - 2\}$ comportant $(A+1)^{s+1} - 1$ éléments. D'après le principe des tiroirs ("pigeonhole principle" en anglais), il existe deux points différents b et b' dans $D(A,s)$ tel que $W_0(b) = W_0(b')$. Ainsi, en posant $a = b - b'$, on obtient : $a \in \mathbb{Z}^{s+1} \setminus \{0\}$ avec $|a_i| \leq A$ et $V_0(a) = 0$.

c) Avec la condition (3.1), on peut déterminer s et A tel qu'il existe $a \in \mathbb{Z}^{s+1} \setminus \{0\}$ satisfaisant $V_n(a) = 0 \quad \forall n \in \mathbb{N}$.

Définissons s en posant : $s-1 \leq \log\lambda < s$ et A en posant : $A < 2\lambda^{\frac{1}{s}}\alpha \leq A+1$.
Définissons aussi la fonction continue et dérivable sur $[s-1; s]$:

$$\phi(x) = 1 - \frac{x}{s} + \log\frac{1+x}{1+s}$$

On a $\phi(s-1) = \frac{1}{s} - \log(1+\frac{1}{s}) > 0$.
On a $\phi(s) = 0$.
De plus : $\phi'(x) = -\frac{1}{s} + \frac{1}{1+x}$ est tel que :

$$\phi'(x) \leq 0 \quad \text{pour} \quad x \geq s-1$$

ϕ est strictement décroissante pour $x > s-1$, on a donc :

$$\phi(s-1) \geq \phi(\log\lambda) > \phi(s)$$

Nous avons donc : $\phi(\log\lambda) > 0$, d'où :

$$\frac{\log\lambda}{s} + \log(1+s) \quad < \quad 1 + \log(1+\log\lambda)$$

et en passant à l'exponentielle :

$$(s+1)\lambda^{\frac{1}{s}} < e(1+\log\lambda)$$

Vérifions maintenant que la condition (3.1) et la définition de A implique que les conditions(3.2) et (3.3) sont vérifiées.
Tout d'abord, on a bien que la définition de A implique (3.3). On a :

$$A(s+1) \quad < \quad 2\alpha\lambda^{\frac{1}{s}}(s+1) \quad < \quad 2e\alpha(1+\log\lambda)$$

(en utilisant la définition de A et la dernière inégalité après passage à l'exponentielle.)
En utilisant (3.1), on a que :

$$2e\alpha(1+\log\lambda) < \frac{1}{(\alpha+1)|\epsilon_n|}$$

et donc :

$$A(s+1) < \frac{1}{(\alpha+1)|\epsilon_n|}$$

d'où :

$$|\epsilon_n| < \frac{1}{(s+1)(\alpha+1)A}$$

Ce qui est bien (3.2)
Ainsi, on peut trouver un a avec les conditions voulues tel que $V_n(a) = 0$ pour tout entier n.

d) Dans ce dernier paragraphe, nous allons démontrer que α est un nombre algébrique et que ses conjugués sont de modules au plus égaux à 1.
Avec les trois points précédents, nous avons démontré que la série $\sum_{n\in\mathbb{N}} u_n X^n$ est rationnelle. Et donc, on peut trouver deux polynômes B et Q à coefficients entiers et premier entre eux et donc par le lemme de Fatou, on a $Q(0) = 1$.
La fonction g (tel que $g(z) = \sum \epsilon_n z^n$, voir Notation) est analytique sur le disque $D(0,1)$ (et donc holomorphe). L'égalité :

$$f(z) = \frac{B(z)}{Q(z)} = \sum_n u_n z^n = \sum_n (\lambda\alpha^n - \epsilon_n) z^n = \frac{\lambda}{1-\alpha z} - \sum_n \epsilon_n z^n$$

implique que f a unique pôle sur $D(0,1)$ qui est le pôle de $\dfrac{\lambda}{1-\alpha z}$ et ce pôle se situe en $z = \frac{1}{\alpha}$. f est donc méromorphe sur $D(0,1)$.
Donc Q possède un unique zéro sur $D(0,1)$ en $z = \frac{1}{\alpha}$.
Ainsi, $\frac{1}{\alpha}$ est un entier algébrique, α l'est donc aussi.
De plus, si Q possède d'autres racines, elles appartiennent au plan complexe privé du disque unité. Leurs modules seront donc supérieurs ou égaux à 1. Or les autres racines sont les conjugués de $\frac{1}{\alpha}$, par définition. Ainsi, les conjugués de α seront bien de modules au plus égaux à 1.
Si on calcule le résidu de la fonction f en $\frac{1}{\alpha}$, on trouve : $Res(f, \frac{1}{\alpha}) = \frac{-\lambda}{\alpha}$. Nous avons donc : $\lambda = -\alpha \dfrac{B(\frac{1}{\alpha})}{Q'(\frac{1}{\alpha})}$ et donc λ appartient bien à $\mathbb{Q}(\alpha)$.
Le théorème est ainsi démontré.

3.4 L'ensemble $\mathbb{U}$

Le théorème démontré dans la partie précédente nous invite à nous intéresser à un ensemble de nombre qu'on aimerait pouvoir caractériser totalement par le résultat précédent. Nous pouvons alors définir :

Définition : Soit $\mathbb{U}$ l'ensemble des nombres réels algébriques $\alpha \geq 1$ tel que ses conjugués soient de modules au plus 1.

Comme nous pouvons le voir, le théorème 2 nous donne une condition suffisante d'appartenance à $\mathbb{U}$. Il en existe d'autres, utilisant des critères de rationalités différents à chaque fois.

Pour finir cette partie, donnons maintenant la réciproque du théorème 2, nous permettant ainsi d'avoir une condition nécessaire et suffisante d'appartenance à $\mathbb{U}$.

Théorème 3 *(Réciproque du théorème 2 :) Un réel* $\alpha > 1$ *appartient à* $\mathbb{U}$ *si et seulement si, il existe* $\lambda \in \mathbb{R}$, $\lambda \geq 1$ *tel que :*

$$\|\lambda \alpha^n\| \quad \leq \quad \frac{1}{2e\alpha(\alpha+1)(1+\log \lambda)} \qquad \forall n \in \mathbb{N} \tag{3.4}$$

Pour la preuve, on pourra consulter avec profit [5].

Chapitre 4

Les nombres de Pisot

4.1 L'ensemble S

Nous avons défini précédemment l'ensemble $\mathbb{U}$. Il est intéressant de noter que nous pouvons partitionner $\mathbb{U}$ en plusieurs sous-ensembles suivant les valeurs possibles prises par le module des nombres appartenant à $\mathbb{U}$. Nous définissons donc maintenant l'ensemble des nombres de Pisot :

Définition : L'ensemble S des nombres de Pisot est l'ensemble des entiers algébriques réels plus grand que 1 et tel que ses conjugués sont de module strictement inférieur à 1.

Remarque : Tout entier relatif plus grand que 1 appartient à S.
Nous allons maintenant énoncer plusieurs propriétés liées aux nombres de Pisot.

4.2 Propriétés des nombres de Pisot

4.2.1 Convergence

Théorème 4 *Soit $\theta \in S$. La suite $(\|\theta^n\|)$ converge vers* 0.

Peuve : Notons : $P = X^n + c_{n-1}X^{n-1} + ... + c_0$ le polynôme tel que $P(\theta) = 0$.

Considérons sa matrice compagnon :

$$A = \begin{vmatrix} 0 & 0 & \dots & 0 & -c_0 \\ 1 & 0 & \dots & 0 & -c_1 \\ 0 & 1 & \dots & 0 & -c_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -c_{n-1} \end{vmatrix}$$

C'est une matrice à coefficients entiers. Son polynôme caractéristique est P (par construction), on peut donc la diagonaliser et obtenir la matrice suivante :

$$D = \begin{vmatrix} \theta & 0 & \dots & 0 \\ 0 & \theta^{(2)} & \dots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \dots & \theta^{(s)} \end{vmatrix}$$

Où $\theta^{(j)}, \quad j = \{2, .., s\}$ sont les valeurs propres de la matrice et par construction les conjugués de θ.
On a alors que $Tr(A) = Tr(D)$ et même plus : $Tr(A^n) = Tr(D^n)$. On en déduit alors que $Tr(D^n) \in \mathbb{Z}$. Or $Tr(D^n) = \theta^n + \sum_{j=2}^{s} \theta^{(j)^n}$. Notons $d = \sup_{j=2,..s} |\theta^{(j)}| < 1$ (par définition de θ). On a donc :

$$|Tr(D^n) - \theta^n| \leq \sum_{j=2}^{s} |\theta^{(j)^n}| \leq (s-1)d^n$$

Or $(s-1)d^n$ va tendre vers 0 quand $n \to +\infty$ donc θ^n tend vers un nombre entier, ce qui signifie, par définition de ϵ_n, que $\|\theta^n\|$ va tendre vers en $+\infty$. Ce qui achève la démonstration.

Ce théorème conduit à la question suivante : Peut-on trouver une condition nécessaire et suffisante d'appartenance à S par une convergence du même type que le théorème ?

Démontrons tout d'abord un lemme venant de l'analyse complexe :

Propriété : Soit ϕ une fonction méromorphe sur U un ouvert contenant $\overline{D}(0,1)$. Supposons que ϕ ne possède aucun pôle en 0 et que ses coefficients a_n de son développement en série de Taylor satisfassent $\lim_{n\to+\infty} a_n = 0$. Alors ϕ, qui est analytique sur le disque $D(0,1)$, ne possède pas de pôle sur le cercle $C(0,1)$.

Preuve : Par hypothèse, le rayon de convergence de $\sum_{n=0}^{+\infty} a_n z^n$ est au moins égal à 1. La fonction ϕ est donc analytique sur $D(0,1)$. Supposons maintenant que $R=1$ (où R est le rayon de convergence de la série), on a alors que ϕ possède au moins un point singulier sur le cercle $C(0,1)$ (sinon, $R>1$ et par hypothèse, ce n'est pas le cas.) On peut supposer, sans aucune perte de généralité, que cette singularité se trouve en $z=1$. Soit alors $\epsilon>0$, il existe n_0 tel que pour $n \geq n_0$, on ait $|a_n|<\epsilon$. Ainsi pour $0<r<1$, on a :

$$|\phi(r)| \leq |\sum_{n=0}^{n_0-1} a_n r^n| + |\sum_{n=n_0}^{+\infty} a_n r^n| \leq M + \epsilon \frac{r^{n_0}}{1-r}$$

avec M une constante. Nous avons donc :

$$(1-r)|\phi(r)| \leq M(1-r)+\epsilon$$

D'où $\lim_{r\to 1, r<1}(1-r)\phi(r)=0$. Ce qui est en contradiction avec le fait que 1 est pôle de ϕ. En effet, si 1 est un pôle de la fonction, on a sur un voisinage de 1 : $\phi(r) = \frac{g(r)}{(r-1)}$ avec $g(1)\neq 0$ et la limite nous donne justement que $g(1)=0$. C'est donc bien absurde. On a donc $R>1$.
Nous pouvons donc maintenant énoncer le résultat suivant, réciproque du théorème 4 :

Théorème 5 *(Réciproque du théorème 4 :) Un réel algébrique $\theta>1$ appartient à S si et seulement si il existe un réel λ différent de 0 tel que :*

$$\lim_{n\to+\infty} \|\lambda\theta^n\| = 0$$

Preuve : θ étant algébrique, nous pouvons trouver un polynôme à coefficients entiers qui s'annule en θ. Soit $\sum_{i=0}^{s} q_i X^i$ ce polynôme. On a alors : $\sum_{i=0}^{s} q_i\theta^i = 0$ et donc $\lambda\sum_{i=0}^{s} q_i\theta^{n+i}=0$ et ceci pour tout entier n. Par décomposition de $\|\lambda\theta^n\|$ en somme de $u_n = E(\lambda\theta^n)$ et $\epsilon_n = \epsilon(\lambda\theta^n)$, on peut écrire : $\sum_{i=0}^{s} q_i u_{n+i} = -\sum_{i=0}^{s} q_i\epsilon_{n+i}$. On a, par hypothèse, $\lim_{n\to+\infty}\epsilon_n = 0$. Ainsi, à partir d'un certains n_0 et pour tout $n\geq n_0$, on a : $|\sum_{i=0}^{s} q_i\epsilon_{n+i}|<1$. Et donc, par conséquent : $\sum_{i=0}^{s} q_i u_{n+i}=0$. On a donc que la série $\sum_{n\in\mathbb{N}} u_n X^n = 0$ est rationnelle. Comme dans la démonstration du théorème 2, la série est égale $\frac{B}{Q}$ avec B et Q des polynômes à coefficients entiers, premier entre eux et tel que $Q(0) = 1$. On aura alors :

$$f(z) = \frac{B(z)}{Q(z)} = \frac{\lambda}{1-\theta z} - g(z),\ \forall z \in D(0, 1/\theta)$$

Ce sont des fonctions rationnelles. En utilisant la propriété précédente, de la condition : $\lim_{n\to+\infty} \epsilon_n = 0$, il s'ensuit que g n'a pas de pôle sur $\overline{D}(0,1)$. Q a un unique zéro sur $\overline{D}(0,1)$ et $\theta \in S$. L'autre partie de la démonstration est donné par le théorème 4.

Nous allons maintenant énoncer un dernier résultat, bien qu'il en existe encore beaucoup d'autres.

Théorème 6 *Un réel $\theta > 1$ appartient à S si et seulement si il existe un réel λ différent de* 0 *tel que la série $\sum_{n\in\mathbb{N}} \|\lambda\theta^n\|^2$ converge.*

Pour la preuve, on pourra consulter [5] ou [6] sans aucune préférence.

4.2.2 Autre propriété

Nous ne ferons qu'énoncer ici une propriété importante de S que nous ne démontrerons pas.

Théorème 7 *L'ensemble S des nombres de Pisot est fermé.*

Le lecteur intéressé pourra consulter [6] pour trouver la preuve du théorème 7, ainsi qu'une démonstration différente du théorème 5.

4.3 Ouverture

Nous avons vu à travers les théorèmes 5 et 6 plusieurs façons de caractériser les nombres de Pisot. En effet dans le théorème 6, nous prenons un θ réel et dans le théorème 5 un réel algébrique. La question qui se pose est : Peut-on enlever la condition d'algébricité de θ dans le théorème 5 ?

Conjecture (Pisot) : Un réel (non supposé algébrique) $\theta > 1$ appartient à S si et seulement si il existe un réel λ diffèrent de 0 tel que :

$$\lim_{n\to+\infty} \|\lambda\theta^n\| = 0$$

Il est évident que si la conjecture est vraie, le théorème 6 devient un simple corollaire inutile car les nombres de Pisot ne seraient caractérisés que par la convergence de $\|\lambda\theta^n\|$ vers 0. Cependant, même si certaines avancées ont été faites, le problème n'est pas encore résolu.

Dans un autre registre, nous aurions pu parler de l'ensemble des nombres de Salem T :

Définition : L'ensemble T des nombres de Salem est l'ensemble des entiers algébriques réels plus grand que 1 tel que ses conjugués soient de modules au plus 1, l'un au moins ayant un module égal à 1.

Cet ensemble est bien sûr lié à l'ensemble S, et on peut trouver des propriétés assez similaire à celles sur les nombres de Pisot. Mais nous avons fait le choix de nous concentrer sur un seul ensemble.

Bibliographie

[1] Henri Cartan, Hermann, Théorie élémentaire des fonctions analytiques d'une ou plusieurs variables complexes.

[2] Eric Amar, Etienne Matheron, Cassini, Analyse Complexe.

[3] Patrice Tauvel, Dunod, Analyse complexe pour la Licence 3 : Cours et exercices corrigés.

[4] Pierre Fatou, Acta Mathematica 30, Séries Trigonométriques et séries de Taylor, 1906.

[5] Marie Jose Bertin, A. Descomps-Guilloux, M. Pathiaux-Delefosse, M. Grandet-Hugot, J.P. Schreiber, Birkhäuser, Pisot and Salem numbers.

[6] J.W.S. Cassels,Cambridge Tracts in Mathematics and Mathematical Physics. 45.,An introduction to Diophantine approximation.pp. 133-144,1957.