Nombres de Pisot-Vijayaraghavan et de Salem, et application aux systèmes de numération

Adrien VINÇOTTE

2016

Table des matières

Introduction

Les nombres de Pisot-Vijayaraghavan ont été découverts par les mathématiciens Alex Thue et Godfrey Hardy au début du XX$^{\text{ème}}$ siècle, dans le cadre de résolution d'un problème traitant de l'approximation diophantienne, l'approximation de nombres irrationnels par des rationnels. Les mathématiciens Tirukkannapuram Vijayaraghavan et Charles Pisot, grâce à leurs travaux respectifs, le premier ayant collaboré avec Godfrey Hardy dans le cadre de l'approximation diophantienne, le second ayant démontré de nombreuses propriétés algébriques et topologiques en relation avec ces nombres, leur donneront leurs noms. Les nombres de Salem seront découverts plus tard, par le mathématicien Raphaël Salem, et ont permis de compléter le travail de Godfrey Hardy sur l'approximation diophantienne, et de démontrer certains résultats en analyse harmonique.

Nous allons donc partiellement étudier ces nombres particuliers en donnant quelques propriétés, avant d'en faire une autre application, très différente de celles ci-dessus, aux systèmes de numération.

Avant de définir ces nombres, la première partie traitera des notions d'algèbre indispensables pour une bonne compréhension de la suite.
Deuxièmement, on définira les nombres de Pisot-Vijayaraghavan et de Salem, et donnera les propriétés fondamentales.
En troisième partie, on démontrera certaines propriétés topologiques de ces nombres.
Enfin, la dernière partie sera consacrée aux systèmes de numération et au rôle de ces nombres.

La majorité des résultats énoncés seront démontrés. Toutefois, la preuve certains d'entre eux, notamment dans la deuxième partie, nécessite des résultats de théorie de Galois. L'explication seule des fondamentaux de cette branche des mathématiques aurait nécessité de longs prérequis, ces résultats seront donc admis.

Pour terminer, je remercie Julien Bernat pour m'avoir bénévolement encadré tout au long de ce stage et avoir pris le temps de m'aider à surmonter certaines difficultés, ainsi que l'institut Elie Cartan de Nancy pour avoir accepté de m'accueillir pour ce stage.

1 Prérequis d'algèbre

On va dans cette partie commencer par des rappels sur les polynômes. On établira ensuite la structure des éléments entiers, puis on parlera des extensions de corps, qui sont l'un des outils fondamentaux dans la théorie algébrique des nombres.

1.1 Polynômes

Définition 1.1.1
Soit $P(X) = \sum_{i=0}^{n} a_i X^i$ un polynôme de $\mathbb{Z}[X]$, avec $a_n \neq 0$.
Son polynôme réciproque est $P^*(X) = \sum_{i=0}^{n} a_{n-i} X^i = X^n P(\frac{1}{X})$.
Si un polynôme est égal à son polynôme réciproque, on le dira palindromique. S'il est égal à l'opposé de son polynôme réciproque, on le dira antipalindromique.

Propriété 1.1.2
Soit P un polynôme palindromique ou antipalindromique. Si $z \in \mathbb{C}$ est racine de P, alors z^{-1} est racine de P également, et de même multiplicité.
Réciproquement, s'il existe $z \in \mathbb{C}$ tel que z et z^{-1} sont racine de même multiplicité d'un polynôme P, alors P est palindromique ou antipalindromique.

Propriété 1.1.3
Un polynôme différent de X est irréductible si et seulement si son polynôme réciproque est irréductible.

Démonstration. On prouve facilement avec la forme $X^n P(\frac{1}{X})$ le résultat équivalant : un polynôme n'est pas irréductible si et seulement si son polynôme réciproque n'est pas irréductible. □

Définition 1.1.4 Soit $P = \sum_{i=0}^{n-1} c_i X^i + X^n$ un polynôme unitaire.
La matrice compagnon associée à P est la matrice carrée : $\begin{pmatrix} 0 & 0 & \cdots & 0 & -c_0 \\ 1 & 0 & \cdots & 0 & -c_1 \\ 0 & 1 & \cdots & 0 & -c_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -c_{n-1} \end{pmatrix}$

Propriété 1.1.5
Un polynôme unitaire est égal au polynôme caractéristique de sa matrice compagnon associée.

Démonstration. On raisonne par récurrence sur le degré du polynôme. Développer la dernière ligne de la matrice pour parvenir au résultat voulu. □

1.2 Eléments entiers

Définition 1.2.1
Soit $\alpha \in \mathbb{C}$. On dit que α est un nombre algébrique s'il est racine d'un polynôme à coefficients entiers.
S'il est racine d'un polynôme à coefficients entiers qui de plus est unitaire, on dira que α est un entier algébrique.
En notant P son polynôme minimal, le degré de l'entier algébrique α est égal au degré de P.
Si P est de degré 2, on dira que α est un entier quadratique.

Exemple
L'ensemble $\mathbb{Z}[i]$ des entiers de Gauss est inclus dans l'ensemble des entiers algébriques : posons

$\alpha = a + ib$, avec $a, b \in \mathbb{Z}$. On constate que α est racine du polynôme $X^2 - 2aX + (a^2 + b^2)$, qui est bien un polynôme unitaire de $\mathbb{Z}[X]$.

Au cours des démonstrations futures, on se servira plusieurs fois du fait que l'ensemble des entiers algébriques possède une structure d'anneaux. On se servira de la théorie des groupes pour montrer qu'il s'agit d'un sous-anneau de $\mathbb{C}$, et on aura besoin du résultat suivant :

Lemme 1.2.2
Soit $\alpha \in \mathbb{C}$. Alors α est un entier algébrique si et seulement si le sous-groupe abélien de $\mathbb{C}$: $B = \langle 1, \alpha, \alpha^2, ... \rangle$ a un nombre fini de générateurs.

Démonstration. Soit α un entier algébrique. Il existe alors une famille finie $a_0, ..., a_{n-1}$ d'éléments de $\mathbb{Z}$ telle que $\alpha^n + a_{n-1}\alpha^{n-1} + ... + a_0 = 0$.
Considérons alors le groupe $C = \langle 1, \alpha, ..., \alpha^{n-1} \rangle$.
On a : $\alpha^n = -a_{n-1}\alpha^{n-1} - ... - a_0 \in C$.
De même, par récurrence immédiate, $\forall m \geq n : \alpha^m \in C$.
Donc $B = C$, d'où B a un nombre fini de générateurs.

Réciproquement, supposons que $B = \langle 1, \alpha, \alpha^2, ... \rangle$ ait un nombre fini de générateurs.
On constate d'autre part que B est un groupe sans torsion, c'est à dire qu'il n'admet aucun élément d'ordre fini. Il est donc isomorphe à un groupe de la forme $\mathbb{Z}^r$. On dit que B est de rang r, et tout sous-groupe de B est isomorphe à $\mathbb{Z}^s$, avec $s \leq r$.
Supposons que le rang de B vaut r. On considère $b_1, ..., b_r$ une base de B. Donc tout élément de B est de la forme $b = z_1 b_1 + ... + z_r b_r$, avec $\forall i, z_i \in \mathbb{Z}$.
Tout b_i peut s'écrire comme combinaison linéaire finie de puissances de α. Donc les termes $b_1, ..., b_r$ sont des combinaisons linéaires des éléments d'une famille finie de la forme $\{1, \alpha, ..., \alpha^{n-1}\}$.
Donc $\alpha^n \in \langle b_1, ..., b_r \rangle \subset \langle 1, \alpha, ..., \alpha^{n-1} \rangle$.
Ainsi, α^n est combinaison linéaire des $\{1, \alpha, ..., \alpha^{n-1}\}$. Donc α est un entier algébrique. □

Théorème 1.2.3
L'ensemble des entiers algébriques est un anneau.

Démonstration. Soit α et β des entiers algébriques. On pose $B = \langle 1, \alpha, \alpha^2, ... \rangle$ et $C = \langle 1, \beta, \beta^2, ... \rangle$.
Par le lemme 1.2.2, B et C ont un nombre fini de générateurs, que l'on notera $b_1, ..., b_m$ et $c_1, ..., c_n$.
Posons $BC = \langle bc : b \in B, c \in C \rangle$. BC est un groupe abélien, et engendré par les mn éléments $m_i c_j$.
En outre, $(\alpha + \beta)BC \subset BC$ et $\alpha\beta BC \subset BC$.
Par le lemme, $\alpha + \beta$ et $\alpha\beta$ sont des entiers algébriques. □

Définition 1.2.4
Soit $\alpha \in \mathbb{C}$. α est une unité algébrique si α est un entier algébrique dont le terme constant du polynôme minimal vaut ± 1.

Définition 1.2.5
Soit α un entier algébrique de polynôme minimal P. Les conjugués de α sont les racines de P.
Par abus de langage, on définit dans le cas quadratique "le" conjugué pour l'autre conjugué que α.

Exemple
Reprenons l'exemple précédent des entiers de Gauss. Le conjugué de $\alpha = a + ib$, dont le polynôme minimal est $X^2 - 2aX + (a^2 + b^2)$, est $\alpha' = a - ib$, car α' a le même polynôme minimal que α.

Théorème 1.2.6
Soit P le polynôme minimal d'un entier algébrique quelconque. Alors toutes les racines de P dans $\mathbb{C}$ sont de multiplicité 1.
Ce résultat vient du fait que le polynôme minimal d'un entier algébrique est irréductible. [1]

1.3 Extensions de corps

Définition 1.3.1
Soit K un corps. Une extension de K est un corps L qui contient K .

On remarque que L est un espace vectoriel sur K. En effet, L est stable par addition, et la multiplication d'un élément de L par un scalaire de K aura pour image un élément de L.
On peut donc définir le degré d'une extension de corps : il correspond à la dimension de cette extension considérée comme K-espace vectoriel.
Une extension de corps de degré fini est appelée extension finie.

Définition 1.3.2
Un corps de nombres est une extension finie de $\mathbb{Q}$.

Définition 1.3.3
Une extension algébrique L sur un corps K est une extension de corps de K tel que tout élément de L soit algébrique sur K, c'est à dire racine d'un polynôme à coefficients dans K.
Etant donné que K est un corps, une définition équivalente est que tout élément de L est entier sur K, c'est à dire est racine d'un polynôme unitaire à coefficients dans K.

Exemple
On veut construire L la plus petite extension de corps de $\mathbb{Q}$ contenant $\sqrt{d}$, tel que $d \in \mathbb{N}$ et ne soit pas un carré ("plus petit" signifie que tout sous-corps de $\mathbb{R}$ contenant $\sqrt{d}$ devra contenir L). On notera ce corps $\mathbb{Q}(\sqrt{d})$.
Ce corps doit nécessairement contenir l'ensemble L' nombres de la forme $a + b\sqrt{d}$, avec a et b entiers. On montre très facilement que L' est un corps (stable par addition et par produit, L' contient l'opposé et l'inverse de tous ses éléments.
On en déduit que $L{=}L'$.
Déterminons maintenant le degré de l'extension : une $\mathbb{Q}$-base de L est $(1, \sqrt{d})$. On en déduit que cette extension de corps est de degré 2, et donc que c'est une extension finie. L est donc un corps de nombres.

Théorème - Définition 1.3.4
Soit L une extension algébrique de $\mathbb{Q}$. Alors il existe un polynôme irréductible P à coefficients dans $\mathbb{Q}$, tel que L soit isomorphe à $\mathbb{Q}[X]/P(X)$.
P est appelé polynôme minimal de l'extension L sur $\mathbb{Q}$. Celui-ci est égal au polynôme minimal des entiers algébriques de L

Exemple
Comme dans l'exemple précédent, considérons un entier naturel d qui est sans facteur carré. Alors le polynôme $X^2 - d$, qui a $\sqrt{d}$ pour racine, est irréductible dans $\mathbb{Q}[X]$. On en déduit que L est isomorphe à $\mathbb{Q}[X]/(X^2 - d)$.
Le polynôme $X^2 - d$ est le polynôme minimal de l'extension L sur $\mathbb{Q}$.

Propriété 1.3.5
Soit α un nombre algébrique sur K de degré n. Alors une base de $K(\alpha)$ est $(1, \alpha, \alpha^2, ..., \alpha^{n-1})$. On a un résultat similaire pour les entiers algébriques.

Démonstration. On note f la famille $(1, \alpha, \alpha^2, ..., \alpha^{n-1})$, et P le polynôme minimal de α.
f est bien génératrice de $K(\alpha)$, car si $m \geq n$, alors α^m est combinaison linéaire des éléments de f.
f est bien une famille libre, car P, de degré n, est le polynôme non nul de degré minimal à coefficients dans $\mathbb{Q}$ qui annule α. □

Remarque
On en déduit de cette propriété que le degré d'une extension coïncide avec le degré de son polynôme minimal.

Définition 1.3.6
Une extension totalement réelle est une extension de $\mathbb{Q}$ dont le polynôme minimal a toutes ses racines réelles.

Exemple
Si n est toujours un entier naturel sans facteur carré, le corps $\mathbb{Q}(\sqrt{n})$ est une extension totalement réelle de $\mathbb{Q}$, car son polynôme minimal a pour racines $\sqrt{n}$ et $-\sqrt{n}$, qui sont réelles.
Par contre, l'extension de corps de polynôme minimal X^3-2 n'est pas une extension totalement réelle.

1.4 Morphismes de conjugaison

Définition 1.4.1
Soit K un corps de nombre de degré d.
On appelle morphisme de conjugaison tout morphisme de corps σ de K dans $\mathbb{C}$ laissant $\mathbb{Q}$ invariant, c'est à dire :

$$\begin{cases} \sigma : K \longrightarrow \mathbb{C} \\ \forall x, y \in K \;\; \sigma(x+y) = \sigma(x) + \sigma(y) \\ \forall x, y \in K \;\; \sigma(xy) = \sigma(x)\sigma(y) \\ \forall a \in \mathbb{Q} \;\; \sigma(a) = a \end{cases}$$

Exemple
Soit $K = \mathbb{Q}(\sqrt{2})$, et $a + b\sqrt{2} \in K$, avec donc $a, b \in \mathbb{Q}$.
Considérons le morphisme σ tel que $\sigma(a + b\sqrt{2}) = a - b\sqrt{2}$.
σ est bien un morphisme de conjugaison : soit $a, b, c, d \in \mathbb{Q}$
$\sigma(a + b\sqrt{2} + c + d\sqrt{2}) = a + c - (b + d)\sqrt{2} = \sigma(a + b\sqrt{2}) + \sigma(c + d\sqrt{2})$
$\sigma((a+b\sqrt{2})(c+d\sqrt{2})) = \sigma(ac+bd+(ad+bc)\sqrt{2}) = ac+bd-(ad+bc)\sqrt{2} = \sigma(a+b\sqrt{2})\sigma(c+d\sqrt{2})$
$\sigma(a) = \sigma(a + 0\sqrt{2}) = a$

σ peut être caractérisé de la façon suivante : σ est le morphisme qui envoie $\sqrt{2}$ sur $-\sqrt{2}$.
On va en effet montrer qu'il est l'unique morphisme de conjugaison qui envoie $\sqrt{2}$ sur $-\sqrt{2}$.

Théorème 1.4.2
Soit $K = \mathbb{Q}(\theta)$ un corps de nombres de degré d. On note alors $\theta^{(j)}$avec$j = 1, ..., d$ les conjugués de θ, avec $\theta^{(1)} = \theta$.
Il existe exactement d morphismes de conjugaison $\sigma_1, ..., \sigma_d$.
Chacun de ces morphismes est défini par $\sigma_i(\theta) = \theta^{(i)}$.

Démonstration. Soit $P(X) = \sum_{i=0}^{d} a_i X^i$ le polynôme minimal de θ.
On a par définition du polynôme minimal $P(\theta) = \sum_{i=0}^{d} a_i \theta^i = 0$
Donc

$$\sum_{i=0}^{d} a_i \sigma(\theta)^i = \sigma(\sum_{i=0}^{d} a_i \theta^i) = \sigma(0) = 0$$

On en déduit que pour tout morphisme de conjugaison σ, $\sigma(\theta)$ est une racine de P. Comme $\sigma(\theta)$ détermine σ (l'unicité est simple à montrer, en supposant que σ et σ' sont tous deux déterminés par θ, on trouve $\sigma = \sigma'$), alors il existe au plus d morphismes de conjugaison.

Pour montrer qu'il y a exactement d morphismes de conjugaison, déterminons les tous.
On les définit ainsi :

$$\sigma_k \left(\sum_{i=0}^{d-1} a_i \theta^i \right) = \sum_{i=0}^{d-1} a_i \sigma_k(\theta)^i = \sum_{i=0}^{d-1} a_i \theta^{(k)^i}$$

□

A partir de la notion de morphisme de conjugaison, on définit la notion de discriminant associé à une base d'un corps de nombres.

Définition 1.4.3
Soit $K = \mathbb{Q}(\theta)$ un corps de nombres de degré d. On assimilera K à un $\mathbb{Q}$-espace vectoriel. On considère $(\lambda_1, ..., \lambda_d)$ une base de K.
On définit le discriminant associé à cette base par $\Delta(\lambda_1, ..., \lambda_d) = D(\lambda_1, ..., \lambda_d)^2$,
avec $D(\lambda_1, ..., \lambda_d) = \det \begin{pmatrix} \sigma_1(\lambda_1) & \sigma_1(\lambda_2) & \cdots & \sigma_1(\lambda_d) \\ \sigma_2(\lambda_1) & \sigma_2(\lambda_2) & \cdots & \sigma_2(\lambda_d) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_d(\lambda_1) & \sigma_d(\lambda_2) & \cdots & \sigma_d(\lambda_d) \end{pmatrix}$

2 Premières définitions et propriétés

Introduisons les notations suivantes :
Soit α un réel strictement supérieur à 1. Alors α admet une unique décomposition de la forme $E(\alpha) + \varepsilon(\alpha)$, avec $E(\alpha) \in \mathbb{N}^*$ et $\varepsilon(\alpha) \in]-\frac{1}{2}, \frac{1}{2}]$.
Soit β un entier algébrique de degré n. On notera $\beta^{(j)}$ avec $j \in [[2, n]]$ l'ensemble des conjugués de β, et $\beta^{(1)} = \beta$.
Le cercle unité sera noté $\mathbb{S}$.

2.1 Nombres de Pisot-Vijayaraghavan

Définition 2.1.1
Un nombre de Pisot-Vijayaraghavan (ou de Pisot par abus) est un entier algébrique réel strictement supérieur à 1, dont tous les conjugués sont de module strictement inférieur à 1.
On notera S l'ensemble des nombres de Pisot.

Définition 2.1.2
Un nombre de Pisot est totalement réel si tous les conjugués sont réels.

Exemples
Considérons le polynôme $X^2 - 2X - 1$. Il s'agit bien d'un polynôme unitaire de $\mathbb{Z}[X]$. Ses racines

sont $1-\sqrt{2}$ et $1+\sqrt{2}$. Etant donné que $|1-\sqrt{2}|<1$ et que $1+\sqrt{2}>1$, alors $1+\sqrt{2}$ est un nombre de Pisot réel.
Tous les entiers positifs supérieurs ou égaux à 2 sont des nombres de Pisot (car ceux-ci n'ont pas de conjugué), et ce sont les seuls rationnels qui le soient (p/q a pour polynôme minimal $qX-p$ qui n'est pas unitaire).

Propriété 2.1.3
Soit $\theta \in S$ de degré s. Alors $\forall j \in [[2,s]] : |\theta^{(j)}| \geq \frac{1}{\theta}$

Démonstration. Soit $P = X^s + q_{s-1} + ... + q_0$ le polynôme minimal de θ. On supposera premièrement que θ n'est pas quadratique. Nécessairement, $q_0 \neq 0$, P ne serait sinon pas irréductible. On a alors $\prod_{i=1}^{s} |\theta^{(i)}| \geq 1$, et donc pour $j \in [[2,s]] : |\theta^{(j)}| \geq \prod_{i\neq 1,j} \frac{1}{|\theta^{(i)}|\theta}$.
On conclut en rappelant que $\forall j \in [[2,s]] : |\theta^{(j)}| < 1$.
Si θ est quadratique, le résultat découle immédiatement de l'inégalité $\theta\theta^{(2)} \geq 1$. □

Si θ est un entier quadratique de S, alors il est racine d'un polynôme de la forme $X^2 + q_1X + q_0$ avec $q_1 + |1 + q_0| < 0$.

De façon plus générale, les polynômes $X^s + q_{s-1}X^{s-1+}... + q_0$ dont les coefficients vérifient la relation $|q_{s-1}| > 1 + \sum_{i=0}^{s-2} |q_i|$ ont par le théorème de Rouché une racine dans S :
Considérons les polynômes $f(X) = X^s + q_{s-1}X^{s-1+}... + q_0$ et $g(X) = q_{s-1}X^{s-1}$ sur $\mathbb{S}$.
Grâce à la relation sur les coefficients du polynôme, on trouve bien $|f-g| < |g|$ sur $\mathbb{S}$.
g ayant $s-1$ zéros comptés avec multiplicité dans $D(0,1)$, f en a également $s-1$. Etant donné que f ne peut pas avoir de racine sur $\mathbb{S}$, f a une racine de module strictement supérieur à 1.

On peut également montrer, mais cette preuve est beaucoup plus complexe et fait appel à la théorie de Gallois, que le polynôme minimal de tout nombre de nombre de Pisot vérifie : $1 + \sum_{i=0}^{s-1} q_i < 0$. [2]

Propriété 2.1.4
Soit $\theta \in S$, de polynôme minimal P. Tous les conjugués de θ sont des racines simples de P.
Ce résultat est un cas particulier du théorème 1.2.6.

Propriété 2.1.5
Soit $\theta \in S$. Alors $\forall n \in \mathbb{N}\ \theta^n \in S$

Démonstration. Soit $n \in \mathbb{N}$, et soit M dans $\mathcal{M}_s(\mathbb{Z})$ la matrice compagnon du polynôme minimal P de θ, de degré s. Par la propriété 2.1.4, P est un polynôme ayant s racines distinctes. Étant donné que le polynôme caractéristique est égal à P (cf propriété 1.1.5), M est diagonalisable, et est semblable à la matrice $diag(\theta, \theta^{(2)}, ..., \theta^{(s)})$.
On en déduit que M^n est semblable à $diag(\theta^n, \theta^{(2)^n}, ..., \theta^{(s)^n})$, et on a toujours M^n dans $\mathcal{M}_d(\mathbb{Z})$.
D'autre part, on aura toujours $\theta > 1$ et $\mid \theta^{(j)} \mid < 1$ pour $j \in [[2,s]]$
Le polynôme caractéristique de M^n est donc le polynôme minimal d'un nombre de Pisot. □

Remarque
On en déduit également de la preuve que les conjugués de θ^n valent $\theta^{(j)}$. Ce résultat reste valable pour tous les entiers algébriques.

2.2 Nombres de Pisot-Vijayaraghavan et extensions de $\mathbb{Q}$

Montrons maintenant que toute extension finie de $\mathbb{Q}$ est engendrée par un nombre de Pisot. On utilisera pour cela le théorème de Minkowski que nous allons tout de suite rappeler et admettre (une démonstration de ce théorème est proposée ici :[3]).

Théorème 2.2.1 (de Minkowski)
Soit $(L_i)_{1\leq i\leq n}$ une famille de n formes linéaires à coefficients réels de déterminant D non nul.
Soit $(\gamma_i)_{1\leq i\leq n}$ n réels positifs tels que $\prod_{i=1}^{n}\gamma_i \geq |D|$
Alors il existe $u \in \mathbb{Z}^n \setminus 0$ tel que $|L_i(u)| \leq \gamma_i, i = 1, ..., n$.

Théorème 2.2.2
Toute extension finie réelle de $\mathbb{Q}$ contient une infinité de nombres de Pisot dont le degré est celui de l'extension. De plus, certains de ces nombres sont des unités.

Démonstration. Soit K une extension algébrique de $\mathbb{Q}$, de degré s.
Soit $(\omega_i)_{1\leq i\leq s}$ une base réelle de K. On pose $(\omega_i^{(j)})_{1\leq i\leq s} = (\sigma_j(\omega_i))_{1\leq i\leq s}$.
On pose Δ le discriminant de associé à la base $(\omega_i)_{1\leq i\leq s}$.

$$\text{On a donc : } \sqrt{|\Delta|} = \det\begin{pmatrix} \sigma_1(\omega_1) & \sigma_1(\omega_2) & \cdots & \sigma_1(\omega_d) \\ \sigma_2(\omega_1) & \sigma_2(\omega_2) & \cdots & \sigma_2(\omega_d) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_d(\omega_1) & \sigma_d(\omega_2) & \cdots & \sigma_d(\omega_d) \end{pmatrix} = \det\begin{pmatrix} \omega_1 & \omega_2 & \cdots & \omega_d \\ \omega_1^{(2)} & \omega_2^{(2)} & \cdots & \omega_d^{(2)} \\ \vdots & \vdots & \ddots & \vdots \\ \omega_1^{(d)} & \omega_2^{(d)} & \cdots & \omega_d^{(d)} \end{pmatrix}$$

On choisit M et δ convenables pour qu'en appliquant le théorème de Minkowski, en prenant une famille de s formes linéaires ayant pour matrice $m_{ji} = (\omega_i^{(j)})_{1\leq i,j\leq s} : u = (u_i)_{1\leq i\leq s} \in \mathbb{Z}^s \setminus 0$ tel qu'il existe $|\sum_{i=1}^{s} u_i\omega_i| \leq M$ et $|\sum_{i=1}^{s} u_i\omega_i^{(j)}| \leq \delta < 1$ vérifiant $M\delta^{s-1} \geq D = \sqrt{|\Delta|}$.
Soit $\theta = \sum_{i=1}^{s} u_i\omega_i$
θ est un entier algébrique. En lui appliquant les morphismes de conjugaison σ_j, et étant donné que pour tout i, u_i est entier donc invariant par σ_j, on en déduit que θ a comme conjugués $\theta^{(j)} = \sum_{i=1}^{s} u_i\omega_i^{(j)}$.
Ainsi : $|\theta^{(j)}| \leq \delta < 1$.
On a : $1 \leq |\prod_{j=1}^{s}\theta^{(j)}| \leq |\theta|\delta^{(s-1)}$ car $|\prod_{j=1}^{s}\theta^{(j)}| = q_0 \geq 1$.
Donc $|\theta| > \delta^{(1-s)}$ et $|\theta^{(j)}| < 1$ pour $j = 2, ..., s$.
On en déduit que $\theta \in S$ (ou $-\theta \in S$), et que θ est de degré s, étant racine d'un polynôme irréductible.

Montrons maintenant que certains de ces nombres sont des unités.
D'après ce que l'on vient de faire, il existe une suite (δ_n) de réels et une suite (θ_n) de nombres de $K \cap S$ de degré s tous distincts,

$$\text{tels que : } \begin{cases} 1 \leq \theta_1 \leq \sqrt{|D|}\delta_1^{1-s} \\ 0 < \delta_n < \inf\limits_{j\in[[2,s]]} |\theta_{n-1}^{(j)}| \\ \forall j = 2, ..., s, n \geq 2 : |\theta_n^{(j)}| \leq \delta_n \qquad \text{où } \delta_1 \in]0, 1[\text{ arbitraire} \end{cases}$$

On pose $N(\theta_s) = \prod_{j=1}^{s}\theta^{(j)}$.
La suite $|N(\theta_s)|$ est bornée par $\sqrt{|D|}$. On peut alors trouver un entier m tel que $N(\theta_s) = m$ pour une infinité de valeurs de n.
Dans la suite (θ_s), il existe alors deux termes notés θ' et θ'' de la forme $\theta' = \sum_{i=1}^{s} u_i'\omega_i$ et $\theta'' = \sum_{i=1}^{s} u_i''\omega_i$, avec $\delta' > \delta''$ tels que $N(\theta') = N(\theta'') = m$ et $u_i' = u_i'' \pmod m$, puisqu'il y a un nombre fini de valeurs entières dans l'intervalle $[0, m]$.

On a alors $\theta'' - \theta' = m\alpha$, où α est un entier algébrique dans K.
Soit $\xi = \dfrac{\theta''}{\theta'}$. ξ est un réel et $\xi = 1 + \alpha \prod_{j=2}^{s} \theta^{(j)}$. C'est un entier algébrique satisfaisant l'égalité $N(\xi) = 1$, c'est donc une unité de K.
L'inégalité $\delta' > \delta''$ implique que $|\xi^{(j)}| = |\dfrac{\theta''^{(j)}}{\theta'^{(j)}}| < 1$, pour $j = 2, ..., s$, alors que $|\xi| > 1$.
Ainsi, ξ (ou $-\xi$) est un nombre de Pisot. □

Exemple
$K = \mathbb{Q}(\sqrt{5})$ est un corps quadratique, engendré par une infinité de nombres de Pisot de degré 2. Par exemple, $\dfrac{1+\sqrt{5}}{2}$, de polynôme minimal $X^2 - X - 1$, et $2 + \sqrt{5}$, de polynôme minimal $X^2 - 4X - 1$, engendrent K, car $K = \mathbb{Q}(\dfrac{1+\sqrt{5}}{2}) = \mathbb{Q}(2 + \sqrt{5})$.
Les nombres de Pisot $\dfrac{3+\sqrt{5}}{2}$ et $\dfrac{7+3\sqrt{5}}{2}$, de polynômes minimaux respectifs $X^2 - 3X + 1$ et $X^2 - 7X + 1$, sont des unités algébriques dans K.

2.3 Nombres de Salem

Définition 2.3.1
Soit τ un entier algébrique réel strictement supérieur à 1.
τ est un nombre de Salem si : $\sup\limits_{j \in [[2,n]]} | \tau^{(j)} | = 1$.
Les nombres de Salem correspondent au "cas limite" des nombres de Pisot. On notera T l'ensemble des nombres de Salem.

On note U l'ensemble des entiers algébriques réels strictement supérieurs à 1 dont les conjugués sont tous de module inférieur ou égal à 1. On constate que les ensembles S et T forment une partition de U.

Soit $\tau \in T$ d'ordre n, de polynôme minimal P. Alors l'un de ses conjugués $\tau^{(j)}$ est de module 1. De plus, $1/\tau^{(j)} = \overline{\tau^{(j)}}$ est également conjugué de τ, et donc racine de P. On en déduit que P est (anti)palindromique.
D'autre part, 1 et -1 ne peuvent pas être racine de P, il ne serait sinon pas irréductible dans $\mathbb{Z}[X]$. On en déduit que P est un polynôme de degré pair palindromique. Son degré ne peut de plus pas être égal à 2 : soit il n'aurait que des racines de module 1, soit aucune d'elle ne le serait.
On en déduit ainsi que les conjugués de τ sont $1/\tau$ et des éléments du cercle unité 2 à 2 conjugués (au sens des nombres complexes).

On en conclut, en opérant par la transformation $x \longrightarrow x + \frac{1}{x}$, que τ est un nombre de Salem si et seulement si l'entier algébrique totalement réel $\tau + \frac{1}{\tau}$ est supérieur à 2, et tous ses conjugués sont dans l'intervalle]-2,2[.

Propriété 2.3.2
Soit τ un nombre de Salem de degré s. Alors $\forall n \in \mathbb{N}, \tau^n$ est un nombre de Salem de degré s.
La preuve de ce résultat est identique à celle de la propriété 2.1.5, le raisonnement nécessite juste quelques ajustements pour les nombres de Salem.

2.4 Nombres de Salem et extensions de $\mathbb{Q}$

Propriété 2.4.1
Soit K un corps de nombres de degré d sur $\mathbb{Q}$. Alors K contient un nombre de Salem τ de degré d si et seulement si K est l'extension quadratique d'un corps totalement réel K', et $K = K'(\gamma)$ avec $\gamma = \tau + \frac{1}{\tau}$, où $\gamma > 2$ est un entier quadratique sur K', dont tous les conjugués sont dans]-2,2[.

Démonstration. Posons $\gamma = \tau + \frac{1}{\tau}$, dont tous les conjugués sont dans]-2,2[.
Si K contient un nombre de Salem τ de degré d, alors $K = \mathbb{Q}(\tau)$, et alors le sous-corps $K' = \mathbb{Q}(\gamma)$ est totalement réel.
Puisque $\tau^2 - \gamma\tau + 1 = 0$, alors K est une extension quadratique de K'.

Réciproquement, soit K l'extension quadratique d'un corps totalement réel K'. On pose $K = K'(\gamma)$, où γ est un entier algébrique sur K' supérieur à 2, dont tous les conjugués sont dans]-2,2[.
Soit τ une racine de $X^2 - \gamma X + 1$. On a $K = \mathbb{Q}(\tau)$, où τ est un nombre de Salem, car $\gamma = \tau + \frac{1}{\tau}$. □

Lemme 2.4.2
Soient τ et τ' deux nombres de Salem de degré d sur $\mathbb{Q}$ dans un corps K, tels que $\tau < \tau'$.
Alors $\dfrac{\tau}{\tau'}$ est un nombre de Salem de degré d.

Démonstration. Puisque τ est de degré d, alors $K = \mathbb{Q}$. On en conclut que τ' est polynomial en τ. On notera $\tau' = \sum_{i=0}^{n} a_i \tau^i$.
Considérons l'automorphisme σ qui envoie τ sur $\frac{1}{\tau}$.
σ envoie τ' sur lui même ou son conjugué réel, car $\sigma(\tau') = \sum_{i=0}^{n} a_i \sigma(\tau)^i = \sum_{i=0}^{n} a_i (\frac{1}{\tau})^i$ (on reconnaît en effet ici le polynôme réciproque).
Or τ' ne peut pas être envoyé sur lui même, car τ est également un polynôme en τ'. On en déduit que τ' est envoyé sur $\frac{1}{\tau'}$.
On sait que $\frac{\tau'}{\tau}$ est un entier algébrique. Or, $\sigma\left(\frac{\tau'}{\tau}\right) = \frac{\tau}{\tau'}$. On en déduit que $\frac{\tau}{\tau'}$ est un conjugué de $\frac{\tau'}{\tau}$. Ainsi, son polynôme minimal est palindromique, et donc que les conjugués de $\frac{\tau'}{\tau}$ sont un ensemble de paires de la forme $x, \frac{1}{x}$.
Comme τ' est polynomial en τ, alors tout automorphisme fixant τ fixera τ', et fixera également $\frac{\tau'}{\tau}$. Réciproquement, tout endomorphisme fixant τ' fixera τ.
Déterminons maintenant l'ensemble des conjugués de $\frac{\tau'}{\tau}$ dans $\overline{D(0,1)}^C$.
Ceux-ci sont de la forme $\frac{\tau_1'}{\tau_1}$ où τ_1' est un conjugué de τ' et τ_1 un conjugué de τ. On rappelle que les conjugués de τ et τ' sont tous sur le cercle unité sauf 2, et que le conjugué réel dans $D(0,1)$ de τ est supérieur à celui de τ', puisque $\tau < \tau'$. Ainsi, pour qu'ils soient dans $\overline{D(0,1)}^C$, il faut nécessairement soit $|\tau_1'| > 1$, soit $|\tau_1| < 1$, c'est à dire $\tau_1' = \tau'$ ou $\tau_1 = \frac{1}{\tau}$.
Dans le premier cas, on aurait $\tau_1 = \tau$ et donc $\frac{\tau_1'}{\tau_1} = \frac{\tau}{\tau'}$, car $\tau_1 > \tau_1'$. Dans le second cas, on aurait $\tau_1' = \frac{1}{\tau'}$, d'où $\frac{\tau_1'}{\tau_1} = \frac{\tau}{\tau'} \in D(0,1)$.
On en déduit que $\frac{\tau'}{\tau}$ n'a pas d'autre conjugué que lui même dans $\overline{D(0,1)}^C$. De plus, $\frac{\tau'}{\tau}$ a au moins un conjugué sur $\mathbb{S}$, ce qui fait de lui un nombre de Salem.

Montrons maintenant qu'il est bien de degré d.
Considérons tous les automorphismes qui envoient τ sur ses d conjugués. Comme on l'a vu, seul l'automorphisme qui envoie τ sur lui même envoie $\frac{\tau'}{\tau}$ sur lui même.
Si $\frac{\tau'}{\tau}$ est de degré d/k, alors il existe k automorphismes l'envoyant sur lui-même. Donc $k = 1$, $\frac{\tau'}{\tau}$ est ainsi un nombre de Salem de degré d. □

Propriété 2.4.3
Si $K = \mathbb{Q}(\tau)$, avec τ un nombre de Salem de degré d, alors il existe un nombre de Salem τ_1 tel que l'ensemble des nombres de Salem de degré d dans K est égal aux puissances de τ_1.

Démonstration. Constatons pour commencer que l'ensemble des nombres de Salem inférieurs à τ de degré d est fini. En effet, le polynôme minimal d'un entier algébrique a ses coefficients de la forme $\sum\prod \alpha_{i_1}...\alpha_{i_n}$, avec α_i les conjugués de ce nombre. Etant donné qu'il s'agit ici d'un nombre de Salem τ' inférieur à τ, les coefficients sont majorés au moins par $\tau^d d!$ (il s'agit d'une majoration très grossière, mais suffisante).
Les coefficients des polynômes minimaux étant entiers, il existe un nombre fini de polynômes minimaux de nombres de Salem inférieurs à τ de degré d.
On en déduit qu'il existe un plus petit nombre de Salem de degré d, noté τ_1.
Soit $\tau' \in K$. On peut choisir un entier r tel que $\tau_1^r \leq \tau' < \tau_1^{r+1}$. Or si $\tau_1^r < \tau'$, alors $\frac{\tau'}{\tau_1^r}$ est un nombre de Salem de K plus petit que τ_1.
On en conclut que $\tau' = \tau_1^r$. □

2.5 Distribution modulo 1 des séquences (α^n), avec $\alpha \in U$

Théorème 2.5.1
Soit $\theta \in S$. La suite $(\theta^n)_n$ converge vers 0 modulo 1.

Démonstration. Soit $\theta \in S$, et $\delta = \sup_{j\in[[2,n]]} | \theta^{(j)} |$.
Le nombre $\theta^n + \sum_{j=2}^{s} \theta^{(j)^n}$ est un nombre entier, car θ^n est un nombre de Pisot par la propriété 2.1.5, donc ce nombre est égal au coefficient q_{s-1} de son polynôme minimal.
L'inégalité $|\sum_{j=2}^{s} \theta^{(j)^n}| \leq (s-1)\delta^n$ implique que pour un n suffisamment grand, on aura $\varepsilon(\theta^n) = |\sum_{j=2}^{s} \theta^{(j)^n}|$. En effet, le terme $|\sum_{j=2}^{s} \theta^{(j)^n}|$ tend vers 0, et donc sera plus petit que $1/2$ à partir d'un certain rang.
On en déduit que la suite $(\varepsilon(\theta^n))_n$ tend vers 0 géométriquement. □

Remarque
C'est de ce résultat que découle le rôle des nombres de Pisot dans l'approximation diophantienne.
Prenons par exemple $2 + \sqrt{5}$ (on a vu en section 2.2 qu'il s'agit d'un nombre de Pisot). Si on l'élève à une puissance élevée, il sera "proche" d'un entier, permettant une approximation rationnelle de $\sqrt{5}$.
En effet : $(2 + \sqrt{5})^n = a + b\sqrt{5}$, avec $a, b \in \mathbb{N}$.
Comme $(2 + \sqrt{5})^n \approx C$, avec $C \in \mathbb{N}$, alors $\sqrt{5} \approx \dfrac{C - a}{b}$.

Théorème 2.5.2
Soit$\tau \in T$. La suite $(\tau^n)_n$ est dense modulo 1.

Pour prouver ce théorème, on utilisera le lemme suivant que l'on admettra : [2]
Lemme 2.5.3
Soit $\alpha = (\alpha_k)_{1\leq k\leq p} \in \mathbb{R}^p$ tel que $\alpha_1, ..., \alpha_p$ soient $\mathbb{Q}$-linéairement indépendants. Soit $\mu \in \mathbb{R}^p$, $N \in \mathbb{N}$, $\delta > 0$.
Alors $\exists n > N$ tel que $|\varepsilon_k(n\alpha - \mu)| < \delta$, avec $\varepsilon_k(\psi) = \varepsilon(\psi_k)$.

Démonstration. Soit$\tau \in T$.
Le nombre $\tau^n + \tau^{-n} + \sum_{j=2}^{s}(\tau^{(j)^n} + \tau^{(j)^{-n}})$ est entier, donc $\varepsilon(\tau^n) = \tau^{-n} + \sum_{j=2}^{s}(\tau^{(j)^n} + \tau^{(j)^{-n}})$.
Etant donné que $\lim_{n\to\infty} \tau^n = 0$, on ne tiendra compte dans la preuve que de la distribution de la

suite $(\sum_{j=2}^{s}(\tau^{(j)^n}+\tau^{(j)^{-n}}))_n = (2\sum_{j=2}^{s}\cos(2n\pi\omega^{(j)})_n$.

Montrons que $1,\omega^{(1)},...,\omega^{(s)}$ sont $\mathbb{Q}$-linéairement indépendants.
Soit $l_1,...,l_s \in \mathbb{Z}$ tels que $l_1+\sum_{j=2}^{s} l_j\omega^{(j)}=0$
Donc $\exp(2\pi i\sum_{j=2}^{s} l_j\omega^{(j)})=1$, d'où $\prod_{j=2}^{s}\tau^{(j)^{l_j}}=1 \qquad (1)$
Dans l'extension $\mathbb{Q}(\tau,\tau^{-1},\tau^{(2)},\tau^{(2)^{-1}},...,\tau^{(s)},\tau^{(s)^{-1}})$, il existe un morphisme de conjugaison σ laissant $\mathbb{Q}$ invariant tel que $\sigma(\tau^{(2)})=\tau$.
Ainsi, $(1)\Leftrightarrow \tau^{l_2}\prod_{j=3}^{s}(\sigma(\tau^{(j)}))^{l_j}=1$, est insoluble si $l_2\neq 0$, car $|\tau|>1$. En réitérant ce raisonnement, on conclut que $l_3=l_4=...=l_s=0$.
Donc $1,\omega^{(1)},...,\omega^{(s)}$ sont $\mathbb{Q}$-linéairement indépendants.

Montrons que la suite $(2\sum_{j=2}^{s}\cos(2n\pi\omega^{(j)}))_n$ est dense modulo 1.
Soit $\rho\in[-\frac{1}{2},\frac{1}{2}]$. Alors $\rho=2\cos(2\pi\beta)$ avec $\beta\in[-1,1]$.
Par le lemme précédemment énoncé, en considérant $(\omega^{(j)})_{2\leq j\leq s}\in\mathbb{R}^{s-1}$ et $\mu=(\beta,1/4,...,1/4)$, on peut conclure que : $\forall\delta>0$, il existe m assez grand tel que $\varepsilon(m\omega^{(2)}-\beta)<\delta$, et tel que $\forall 3\leq j\leq s\ \varepsilon(m\omega^{(j)}-1/4)<\delta$.
On peut donc trouver un réel $2\sum_{j=2}^{s}\cos(2m\pi\omega^{(j)})$ arbitrairement proche de ρ. □

3 Propriétés topologiques

Introduisons ces nouvelles notations :
Soit $\delta>0$. On note $\mathcal{F}(\delta)$ l'ensemble des fonctions $f=\dfrac{A}{Q}$ avec $A,Q\in\mathbb{Z}[X]$, tels que :
$Q(0)=1$, $A(0)\neq 0$, $|A(z)|\leq|Q(z)|$ sur $\mathbb{S}$, et Q possède au plus une racine dans $D(0,1)$ et soit non nul sur $D(0,\delta)\cup\mathbb{S}$.
Dans toute la suite du rapport, on admettra que $\mathcal{F}(\delta)$ est compact pour la norme de la convergence uniforme.
Soit $P=X^s+q_{s-1}+...+q_0\in\mathbb{Z}[X]$. On note $P^+=\varepsilon P$, avec $\varepsilon=\pm1$, tel que $P^+(0)>0$.
De plus, on notera P^* le polynôme réciproque de P.

3.1 Fermeture de l'ensemble des nombres de Pisot

On montrera dans cette partie que l'ensemble des nombres de Pisot est un fermé de $\mathbb{R}_+$. On tire de ce résultat des conséquences diverses, entre autres qu'il existe donc un plus petit nombre de Pisot.
La preuve de cette propriété nécessite quelques résultats intermédiaires.

Lemme 3.1.1
Soit f et g des fonctions analytiques sur $D(0,r)$, avec $r>1$, telles que :
$i : |f(z)|\leq|g(z)|$ si $z\in\mathbb{S}$
$ii : f(z)-g(z)=\sum_{i=n}^{\infty}\gamma_i X^i$, avec $\gamma_n\neq 0$
Alors g a au moins n zéros dans $D(0,1)$.

Démonstration. Soit k le nombre de zéros de g dans $D(0,1)$.
Supposons que g est non nulle sur $\mathbb{S}$, et considérons la fonction $h_\lambda=f-\lambda g$, avec $\lambda>1$. Par le théorème de Rouché, h_λ possède k zéros dans $D(0,1)$. On fait tendre λ vers 1 pour conclure que $f-g$ possède au plus k zéros dans $D(0,1)$.
Soit $\alpha_1,\alpha_2,...,\alpha_s$ les zéros de g de module 1, et $P(z)=\prod_{i=1}^{s}(z-\alpha_i)$.
On déduit de l'inégalité (i) que $f_1=f/P$ et $g_1=g/P$ sont analytiques dans $D(0,1)$. En outre,

$f_1(z) - g_1(z) = \frac{\gamma_n}{P(0)} z^n + ...$ dans $D(0,1)$, et g possède k zéros dans $D(0,1)$.
Donc $n \leq k$. □

Lemme 3.1.2
Soit $\theta \in S$, de polynôme minimal P. On pose $Q = P^*$.
Alors $\exists! A \in \mathbb{Z}[X]$ vérifiant : $\begin{cases} A \neq Q \\ A(0) \geq 1 \\ |A| \neq |Q| \text{ sur } \mathbb{S} \end{cases}$

Démonstration. Soit θ de degré s. Si P n'est pas palindromique, $A = P^+$ convient.
Sinon, θ est nécessairement quadratique : en effet, P a $s-1$ racines dans $D(0,1)$, et une racine de module supérieur à 1, et donc P^* aura $s-1$ racines de module supérieur à 1, et une racine dans $D(0,1)$. On en déduit que $s = 2$.
On a alors $P^+ = Q = X^2 - q_1 X + 1$, avec $q_1 \geq 3$ (voir partie 2.1).
On choisit alors les polynômes $A_1 = 1$ et $A_2 = (1-X)^2$. □

On remarque que $A \neq Q$ si et seulement si A et Q sont premiers entre eux. Q étant irréductible (car P l'est), alors si A n'est pas premier avec Q, il est un multiple de Q. L'égalité $A = BQ$ dans $\mathbb{Z}[X]$ avec $|B(z)| \leq 1$ sur $\mathbb{S}$ et $B(0) \geq 1$ implique $B = 1$

Selon le lemme précédent, on peut associer à chaque nombre de Pisot θ au moins une fonction de $\mathcal{F}(\delta)$. Pour $f(z) = A(z)/Q(z)$, $f \in \mathcal{F}(\delta)$ avec $0 < \delta < 1/\theta$, et vérifiant $f(0) \geq 1$ (car $f(0) = A(0)/Q(0)$, avec $A(0) \geq 1$ et $Q(0) = 1$).

Théorème 3.1.3
L'ensemble des nombres de Pisot est un fermé de $\mathbb{R}$.

Démonstration. Soit ω un élément de la frontière de S. On veut montrer qu'il appartient bien à S.
Il y a deux cas possibles : soit c'est un point isolé, et dans ce cas il s'agit bien d'un nombre de Pisot, soit il s'agit d'un point d'accumulation de S. On note alors $(\theta_\nu)_\nu$ une suite d'éléments de S qui converge vers ω quand ν tend vers l'infini.
D'après le lemme précédent, on peut associer à chaque θ_ν une fonction f_ν de $\mathcal{F}(\delta)$, avec $\delta < \inf 1/\theta_\nu$, de la forme A_ν/Q_ν, et telle que $f_\nu(0) \geq 1$.
Etant donné que l'ensemble $\mathcal{F}(\delta)$ est compact, on peut extraire de la suite $(\theta_\nu)_\nu$ une sous-suite, que l'on notera toujours (θ_ν), telle que la suite (f_ν) associée à cette sous-suite converge vers $f \in \mathcal{F}(\delta)$. Montrons que f a un pôle dans $D(0,1)$.

Ecrivons le développement de Taylor des fonctions f_ν et f :

$$f_\nu(z) = \sum_{n=0}^{\infty} u_{\nu,n} z^n \qquad f(z) = \sum_{n=0}^{\infty} u_n z^n$$

Tous les coefficients $u_{\nu,n}$ et u_n sont des entiers : en effet, $f^{(n)}(0) \in \mathbb{Z}$, car $\forall n \in \mathbb{N} \quad Q(0)^n = 1$.
Etant donné que $\lim_{\nu \to \infty} u_{\nu,n} = u_n$, alors $\forall n \in \mathbb{N} \quad \exists \nu_0(n)$ tel que $\forall \nu(n) \geq \nu_0(n) \quad u_{\nu(n)} = u_n$.
Pour tout $\nu \in \mathbb{N}$, la fonction $_\nu$ admet un pôle dans $D(0,1)$ (plus précisément en $1/\theta_\nu$), et telle que $u_{\nu,0} \geq 1$ (car $u_{\nu,0} = |q_{\nu,0}| \neq 0$).

Considérons la fonction $g_\nu(z) = (f_\nu(z) - u_{\nu,0}) Q_\nu(z)$. Par le lemme : $u_{\nu,1} \neq 0$.
En effet, si $u_{\nu,1} = 0$: $g_\nu(z) = A_\nu(z) - u_{\nu,0} Q(z)$
Alors $|A_\nu(z)| \leq |u_{\nu,0} Q_\nu(z)|$ et $g_\nu(z) = \gamma_2 z^2 + ...$

Cela signifie que Q a au moins 2 zéros dans $D(0,1)$, ce qui est contradictoire avec la définition d'un nombre de Pisot, puisque celui associé au polynôme Q aurait un conjugué de module supérieur à 1. Donc $u_{\nu,1} \neq 0$.

On a alors $u_0 \geq 1$, et $u_1 \neq 0$.
f a nécessairement un pôle dans $D(0,1)$, sinon elle y serait holomorphe, et Q diviserait le polynôme A. D'après une remarque précédant le théorème, on en déduit que f serait égale à la fonction constante égale à 1. Cela signifierait que $u_n = 0$ pour tout entier $n \geq 1$, et donc en particulier $u_1 = 0$.
On en déduit que f admet un pôle dans $D(0,1)$, en $\lim_{\nu\to\infty} 1/\theta_\nu = 1/\omega$.

On écrit alors $f(z) = A(z)/Q(z)$, où A et Q sont des polynômes premiers entre eux et à coefficients entiers. Ils satisfont bien la condition $|A| \leq |Q|$ sur $\mathbb{S}$. D'autre part, Q ne peut pas avoir de racines sur $\mathbb{S}$ car A n'a pas de racine sur $\mathbb{S}$.
On déduit de l'égalité $Q(0) = 1$ que $\omega \in S$. □

Remarques

- La fonction limite f appartient à l'ensemble $\mathcal{F}'(\delta)$, la frontière de $\mathcal{F}(\delta)$.

- Du fait que S est fermé et minoré par 1, on peut affirmer qu'il existe un plus petit nombre de Pisot. Carl Siegel a montré que celui ci correspond à la racine supérieure à 1 du polynôme $X^3 - X - 1$. Il appelé "nombre plastique", et vaut environ 1,3247. [4]

3.2 Frontière de l'ensemble des nombres de Pisot

On notera désormais S' la frontière de S.
On énoncera dans cette sous partie quelques propriétés remarquables sur la frontière de l'ensemble des nombres de Pisot. Les démonstrations étant généralement très fastidieuses, ces résultats seront admis. Le lecteur intéressé pourra consulter [2] pour les preuves.

Propriété 3.2.1
Si $f = A/Q$ appartient à $\mathcal{F}'(\delta)$, alors A est différent de $\pm Q^*$.

Théorème 3.2.2
Un nombre de Pisot θ appartient à S' si et seulement s'il existe un polynôme A à coefficients entiers différent des polynômes P^+ et Q satisfaisant les propriétés suivantes :
(i) $A(0) \geq 1$
(ii) $|A(z)| \leq |Q(z)|$

Cela signifie qu'un nombre de Pisot appartient à la frontière si et seulement si on peut lui associer plusieurs fonctions de $\mathcal{F}(\delta)$ comme précédemment.

Théorème 3.2.3
Soit $\theta \in S$. Alors $\forall m \geq 2, \theta^m \in S'$.

Ce résultat vient du fait qu'on peut associer m polynômes distincts à θ^m, d'où θ^m appartient à S'.

Théorème 3.2.4
Tout nombre de Pisot totalement réel appartient à S'.

3.3 Adhérence de l'ensemble des nombres de Salem

Lemme 3.3.1
Soit θ un nombre de Pisot de polynôme minimal P.
Alors $\forall n \in \mathbb{N}$, le polynôme $R_n = X^n P + P^*$ a une unique racine dans $D(0,1)$.

La preuve de ce résultat, très fastidieuse, utilise le théorème de Rouché. [2]

Théorème 3.3.2
S est inclus dans l'adhérence $\overline{T}$ de T.

Démonstration. Soit $\theta \in S$, de polynôme minimal P, et $Q = P^*$. La preuve générale ne s'appliquant pas lorsque les polynômes P et Q sont égaux, le cas où P est palindromique sera traité séparément.

Premier cas : P n'est pas palindromique

Soit (R_n) la suite de polynômes définis par $R_n(X) = X^n P(X) + Q(X)$.
Par le lemme précédent, on sait que R_n a au plus une racine dans $D(0,1)$.
Il s'agit d'un polynôme palindromique vérifiant $R_n(1) = 2P(1) < 0$, par la caractérisation des nombres de Pisot vue dans la section 2.1. Il a alors une unique racine réelle supérieure à 1, que l'on notera τ_n, et a donc également pour racine $1/\tau_n$. Les $n-2$ autres racines se situent donc sur le cercle unité $\mathbb{S}$.
On veut montrer que la suite (τ_n) converge quand n tend vers l'infini vers le nombre de Pisot θ, et qu'à partir d'un certain rang n_0, les nombres de la suite (τ_n) sont de Salem.
Remarque : Etant donné que $R_n(1) = 2P(1) \neq 0$, alors la suite (τ_n) ne peut pas converger vers 1.

On a d'une part $P(\tau_n) = (\tau_n - \theta)\prod_{j=2}^{s}(\tau_n - \theta^{(j)})$, et $\tau_n^n P(\tau_n) = -Q(\tau_n) = -\tau_n^s P(1/\tau_n)$ d'autre part, car τ_n est une racine de R_n. On en déduit que :

$$\begin{aligned}
|\tau_n - \theta| \prod_{j=2}^{s} |\tau_n - \theta^{(j)}| &= |P(\tau_n)| \\
&= \tau_n^{s-n} |P(\frac{1}{\tau_n})| \\
&= \tau_n^{s-n} |\frac{1}{\tau_n} - \theta| \prod_{j=2}^{s} |\frac{1}{\tau_n} - \theta^{(j)}| \\
&= \tau_n^{-n} |1 - \theta\tau_n| \prod_{j=2}^{s} |1 - \tau_n \theta^{(j)}|
\end{aligned}$$

D'où :

$$|\tau_n - \theta| \leq \frac{2\theta\tau_n^{1-n}(1+\tau_n)^{s-1}}{\prod_{j=2}^{s}(1-|\theta^{(j)}|)} \leq c\tau_n^{s-n} \leq \delta^{s-n}$$

avec c une constante, et $\delta = \sup \tau_n > 1$.
On en conclut que $\lim_{n\to\infty} \tau_n = \theta^n$

Si R_n est un polynôme irréductible, alors R_n est le polynôme minimal de τ_n, et alors $\tau_n \in T$

pour $n+s \geq 4$, car deg $R_n = n+s$.

Sinon, R_n est le produit d'un polynôme cyclotomique et du polynôme minimal P_n de τ_n.
Si P_n a pour racine au moins un élément de $\mathbb{S}$, alors τ_n est bien un nombre de Salem.
Le problème se pose si pour tout n, toutes les racines de R_n sur $\mathbb{S}$ sont celles du polynôme cyclotomique. Dans ce cas, P_n serait le polynôme minimal d'un nombre de Pisot.
Considérons alors V un voisinage borné de θ. On constate que le coefficient constant de R_n vaut 1 pour tout n. Donc on aurait un polynôme P_n de la forme $X^2 + a_n X + 1$, c'est à dire que τ_n serait une unité quadratique. Or l'ensemble des unités quadratiques n'admet aucun point d'accumulation dans $]1, +\infty[$ [5], il y en a donc un nombre fini dans V. La suite τ_n ne peut donc pas être une suite d'unités quadratiques, et sera donc à partir d'un certain rang une suite de nombres de Salem.

Second cas : P est palindromique

Soit $\theta \in S$ tel que θ soit racine d'un polynôme palindromique P. Nécessairement, deg $P = 2$, sinon il serait le polynôme minimal d'un nombre de Salem.
Le polynôme minimal de θ est donc de la forme $X^2 - q_1 X + 1$. On a, par le résultat $q_1 + |1 + q_0| < 0$ énoncé en section 2.1, $q_1 \geq 3$, et $\theta \in S'$.
Alors θ est limite de la suite $(\theta_\nu)_{\nu \geq 1}$, où θ_ν est racine du polynôme $X^{\nu+2} - q_1 X^{\nu+1} + X^\nu + 1$, et qui est donc un nombre de Pisot pour tout $\nu \geq 1$ par la propriété énoncée en 2.1.
Par la démonstration faite pour le premier cas, on peut trouver pour tout $\nu \in \mathbb{N}^*$, une suite $(\tau_{\nu,n})_{n \geq 1}$ de limite θ_ν, où $\tau_{\nu,n}$ est la racine du polynôme $X^n(X^{\nu+2} - q_1 X^{\nu+1} + X^\nu + 1) + X^{\nu+2} + X^2 - q_1 X + 1$. Les nombres $\tau_{\nu,n}$ sont de Salem à partir d'un rang n assez grand.
Etudions la suite de polynômes obtenue pour $\nu = n$: $X^{2n+2} - q_1 X^{2n+1} + X^{2n} + X^n + X^2 - q_1 X + 1$.
On définit alors une suite (τ_n) de nombres qui sont dans T à partir d'un certain rang, et ainsi que $\lim_{n \to \infty} ({\tau^2}_n - q_1 \tau_n + 1) = 0$.
On en déduit que (τ_n) converge vers θ. □

4 Fondamentaux sur les systèmes de numération

On étudiera dans cette partie les numérations de base β, où β est un réel supérieur à 1. On remarquera des propriétés intéressantes lorsque β est un nombre de Pisot. Par ailleurs, on déduira de cette théorie un résultat intéressant sur les nombres de Pisot.
Dans cette partie, on notera $\lfloor x \rfloor$ la partie entière du réel x, et $\{x\}$ sa partie décimale. On remarque que ces valeurs sont différentes de $E(x)$ et $\varepsilon(x)$ définies précédemment.

4.1 Représentation standard des nombres

Définition 4.1.1
Soit β un entier supérieur ou égal à 2, que l'on appellera "base" du système de numération. La β-représentation d'un entier naturel N est un mot $d_k ... d_0$ fini, tel que $N = \sum_{i=0}^{k} d_i \beta^i$, avec $d_i \in A = \{0, ..., \beta - 1\}$.

Avec la condition $d_k \neq 0$, une telle représentation est unique. L'existence de cette représentation est donnée par un algorithme glouton qui sera explicité dans la sous-partie 4.2. Cette représentation de N est notée :

$$\langle N \rangle_\beta = d_k ... d_0$$

L'ensemble des représentations des entiers naturels est noté A^*.

Etudions maintenant la représentation des nombres réels (on ne s'intéressera ici qu'à la numération des nombres positifs), avec le même alphabet $A = \{0, ..., \beta - 1\}$. Une β-représentation d'un nombre réel est une suite infinie $(x_i)_{i \leq k}$ de $A^{\mathbb{N}}$ telle que :

$$x = \sum_{i \leq k} x_i \beta^i$$

Une représentation est dite normale si elle ne finit pas par $(\beta - 1)^\infty$, et si $x_k \neq 0$ quand $x \geq 1$. Tout nombre a une unique représentation normale. On la note :

$$\langle x \rangle_\beta = x_k ... x_0, x_{-1} x_{-2} ...$$

Par exemple, en base $\beta = 10$, le nombre 1 possède plusieurs représentations, dont $0,(9)^\infty = 0,9999...$ ou $0...01$; mais $\langle 1 \rangle_{10} = 1,(0)^\infty$.

Le mot $x_k ... x_0$ est appelé partie entière de x, et le mot (possiblement infini) $x_{-1} x_{-2} ...$ est appelé partie décimale de x. Ceux-ci dépendent clairement de la valeur de β. On note que les entiers ont une partie décimale nulle.
On constate que si $\langle x \rangle_\beta = x_k ... x_0, x_{-1} x_{-2} ...$, alors $\dfrac{x}{\beta^{k+1}} < 1$, et on en déduit simplement que $\langle \dfrac{x}{\beta^{k+1}} \rangle_\beta = 0, x_k ... x_0 x_{-1} x_{-2} ....$
On peut donc se restreindre à l'étude des nombres réels de l'intervalle [0,1], le résultat pouvant simplement se généraliser aux réels avec un décalage de la virgule. Désormais, si $x \in [0,1]$, on notera $\langle x \rangle_\beta = (x_i)_{i \geq 1}$.

4.2 β-développements

On considère maintenant les systèmes de numération ayant pour base β, où β est un nombre réel strictement supérieur à 1. La représentation d'un nombre x par ce système est appelée β-développement de x.

Définition 4.2.1
Soit $\beta \in]1, \infty[, x \in [0,1]$. Une β-représentation de x est un mot infini $(x_i)_{i \geq 1}$ tel que :

$$x = \sum_{i \geq 1} x_i \beta^{-i}$$

Une β-représentation particulière de x, appelée β-développement de x, est celle donnée par l'algorithme glouton suivant :
On pose $r_0 = x$. Pour $i \geq 1$, $x_i = \lfloor \beta r_{i-1} \rfloor$, $r_i = \{\beta r_{i-1}\}$.
On a alors $x = \sum_{i \geq 1} x_i \beta^{-i}$.
Le β-développement de x est noté $d_\beta(x)$. Il s'agit bien d'une représentation normale de x, et l'alphabet utilisé est $\{0, ..., \lfloor \beta \rfloor\}$

Soit l'application de $\mathbb{R}$ dans [0,1] : $T_\beta : x \longrightarrow \beta x \bmod 1$.
On a $d_\beta(x) = (x_i)_{i \geq 1}$ si et seulement si $x_i = \lfloor \beta T_\beta^{i-1}(x) \rfloor$.

Pour les mêmes raisons que précédemment, on peut se restreindre à l'étude des réels de l'intervalle [0,1], car si $x > 1$, alors $\exists k \in \mathbb{N}$ tel que $0 \leq \dfrac{x}{\beta^{k+1}} \leq 1$.

Si $\beta \notin \mathbb{N}$, les x_i obtenus sont des éléments de l'alphabet $\{0, ..., \lfloor\beta\rfloor\}$, appelé alphabet canonique.
Si $\beta \in \mathbb{N}$, alors $d_\beta(x) = \langle x\rangle_\beta$, avec x_i dans $\{0, ..., \beta - 1\}$, à l'exception de $x = 1$, où on aura $d_\beta(1) = \beta$, mais $\langle 1\rangle_\beta = 1$.

Exemple
Soit $\beta = \dfrac{1+\sqrt{5}}{2}, x = 3 - \sqrt{5}$.
On a $d_\beta(x) = 1001(0)^\infty$, et on trouve bien $3 - \sqrt{5} = \dfrac{2}{1+\sqrt{5}} + \left(\dfrac{2}{1+\sqrt{5}}\right)^4$

Définitions 4.2.2
Lorsque le β-développement d'un nombre se termine par une infinité de zéros, la représentation sera dite finie. Par abus de notation, les derniers zéros seront parfois omis.
Le β-développement d'un nombre x est dit périodique si $\exists a_1, ..., a_n$ non tous nuls tels que $d_\beta(x) = (a_1...a_n)^\infty$.
Le β-développement d'un nombre x est dit ultimement périodique si $\exists a_1, ..., a_n, a_{n+1}, ..., a_p$ tels que $d_\beta(x) = a_1...a_n(a_{n+1}...a_p)^\infty$. Etant donné que l'on n'a aucune hypothèse à propos des valeurs de a_i, si le β-développement d'un nombre est fini, alors il est également ultimement périodique.

Théorème - définition 4.2.3
On définit la relation d'ordre suivante sur les suites, appelée ordre lexicographique :
Soit (x_n) et (y_n) des suites de $\mathbb{N}^\mathbb{N}$. $(x_n) \leq (y_n)$ si et seulement si $\exists n \in \mathbb{N}$ tel que $\forall i < n : x_i = y_i$ et $x_n \leq y_n$.

Proposition 4.2.4
Soit x et y deux réels de l'intervalle [0,1].
Alors $x < y$ si et seulement si $d_\beta(x) \leq d_\beta(y)$ et $d_\beta(x) \neq d_\beta(y)$.

Démonstration. On pose $d_\beta(x) = (x_i)_i$ et $d_\beta(y) = (y_i)_i$
Supposons que $d_\beta(x) \leq d_\beta(y)$. Alors il existe k tel que $x_k \leq y_k$ et $x_1...x_{k-1} = y_1...y_{k-1}$. Du fait que $\sum_{i=\geq 1} x_{k+i}\beta^{-k-i} < \beta^{-k}$, alors $x \leq y_1\beta^{-1} + ... + y_{k-1}\beta^{-k+1} + (y_k - 1)\beta^{-k} + x_{k+1}\beta^{-k-1} + ... < y$
La réciproque est immédiate. □

Corollaire 4.2.5
$\forall \beta \in]1, \infty[$, le β-développement de 1 n'est jamais périodique.

Démonstration. Supposons par l'absurde que $d_\beta(1)$ est périodique, c'est à dire $d_\beta(1) = (a_1, ..., a_n)^\infty$, avec n minimal. Alors :

$$\begin{aligned} 1 &= \sum_{i=1}^{n} a_i\beta^{-i}\left(1 + \beta^{-n} + \beta^{-2n} + ...\right) \\ &= \sum_{i=1}^{n} a_i\beta^{-i} + \beta^{-n}\left(\sum_{i=1}^{n} a_i\beta^{-i}\left(1 + \beta^{-n} + \beta^{-2n} + ...\right)\right) \\ &= \sum_{i=1}^{n} a_i\beta^{-i} + \beta^{-n} \end{aligned}$$

Cela signifie que $d'_\beta(1) = a_1...a_{n-1}(a_n + 1)$ est également une représentation de 1. Or $d_\beta(1) \leq d'_\beta(1)$ et $d_\beta(1) \neq d'_\beta(1)$, ce qui est impossible en vertu de la proposition 4.2.4. □

Remarque
$\forall \beta \in]1, \infty[$, le β-développement de 1 ne commence jamais par un 0 : en effet, $x_i = \lfloor \beta \rfloor \geq 1$.
Cela semble logique, puisque le β-développement est régi par un algorithme glouton, et on peut retirer à 1 au moins une fois $\frac{1}{\beta}$.

On considérera désormais des développements de nombres dans une base β avec l'alphabet $\{-\lfloor \beta \rfloor, ..., 0, ..., \lfloor \beta \rfloor\}$. On notera $\overline{a} = -a$.
On établira dans la suite une propriété sur les β-développements lorsque β est de Pisot, afin de démontrer un théorème sur les polynômes dont certaines racines sont des nombres de Pisot.

4.3 Nombres de Pisot et périodicité des β-développements

Théorème 4.3.1
Si β est un nombre de Pisot, alors tout nombre de $\mathbb{Q}(\beta) \cap [0, 1]$ a un β-développement ultimement périodique.

Démonstration. Soit β un nombre de Pisot de degré d, de polynôme minimal $X^d - a_1 X^{d-1} - ... - a_d$
Soit $x \in \mathbb{Q}(\beta) \cap [0, 1]$. Alors $x = \frac{1}{q} \sum_{i=0}^{d-1} p_i \beta^i$, avec les p_i dans $\mathbb{Z}$, et q dans $\mathbb{N}$ le plus petit possible afin d'avoir l'unicité.
Soit $(x_k)_{k \geq 1}$ le β-développement de x, et on pose :

$$r_n^{(1)} = \sum_{i \geq 1} \frac{x_{n+i}}{\beta^i} = \beta^n \left(x - \sum_{k=1}^{n} x_k \beta^{-k} \right)$$

On montre par récurrence que $r_n^{(1)} = T_\beta^n(x)$. Montrons l'hérédité :

$$\begin{aligned} T_\beta^{n+1}(x) &= \{\beta T_\beta^n(x)\} \\ &= \beta T_\beta^n(x) - \lfloor \beta T_\beta^n(x) \rfloor \\ &= \beta^{n+1} \left(x - \sum_{k=1}^{n} x_k \beta^{-k} \right) - x_{n+1} \\ &= \beta^{n+1} \left(x - \sum_{k=1}^{n+1} x_k \beta^{-k} \right) \end{aligned}$$

Donc $r_n^{(1)} = T_\beta^n(x) < 1$

Pour $2 \leq j \leq d$, on pose :

$$r_n^{(j)} = {\beta^{(j)}}^n \left(\frac{1}{q} \sum_{i=0}^{d-1} p_i {\beta^{(j)}}^i - \sum_{k=0}^{n} x_k {\beta^{(j)}}^{-k} \right)$$

Posons $\delta = \max_{2 \leq j \leq d} |\beta^{(j)}| < 1$. Puisque $x_k \leq \lfloor \beta \rfloor$, on a :

$$|r_n^{(j)}| \leq \frac{1}{q} \sum_{i=0}^{d-1} |p_i| \delta^{n+i} + \lfloor \beta \rfloor \sum_{k=0}^{n-1} \delta^k$$

Puisque $\delta < 1$, on a $\max_{2 \leq j \leq d} \sup_n |r_n^{(j)}| < \infty$
Posons maintenant $R_n = (r_n^{(1)}, ..., r_n^{(d)})$, et la matrice $B = \left({\beta^{(j)}}^{-i} \right)_{1 \leq i,j \leq d}$

Pour poursuivre la preuve, on aura besoin du résultat suivant :

Lemme 4.3.2
Soit $x = \frac{1}{q}\sum_{i=0}^{d-1} p_i\beta^i$.
$\forall n \in \mathbb{N}$, il existe un unique $Z_n = (z_n^{(1)}, ..., z_n^{(d)}) \in \mathbb{Z}^d$ tel que $R_n = \frac{1}{q}Z_nB$.

L'unicité ne pose aucun problème.
Prouvons l'existence dans $\mathbb{Z}^d$ par récurrence sur n :
Initialisation : preuve pour $n = 1$:

$$\begin{aligned} r_1^{(1)} &= \beta x - x_1 \\ &= \frac{1}{q}\left(\sum_{i=0}^{d-1} p_i\beta^{i+1} - qx_1\right) \\ &= \frac{1}{q}\left(\frac{z_1^{(1)}}{\beta} + ... + \frac{z_1^{(d)}}{\beta^d}\right) \quad \text{avec } z_1^{(i)} \in \mathbb{Z} \ \text{ car } \beta^d = a_1\beta^{d-1} + ... + a_d \end{aligned}$$

Hérédité : supposons la preuve vraie pour n :

$$\begin{aligned} r_{n+1}^{(1)} &= \beta r_n - x_{n+1} \\ &= \frac{1}{q}\left(z_n^{(1)} + \frac{z_n^{(2)}}{\beta} + ... + \frac{z_n^{(d)}}{\beta^{d+1}} - qx_{n+1}\right) \\ &= \frac{1}{q}\left(\frac{z_{n+1}^{(1)}}{\beta} + ... + \frac{z_{n+1}^{d}}{\beta^{(d)}}\right) \quad \text{car } \ z_n^{(1)} - qx_{n+1} \in \mathbb{Z} \quad \text{donc :} \\ r_n^{(1)} &= \beta^n\left(\frac{1}{q}\sum_{i=0}^{d-1} p_i\beta^i - \sum_{k=1}^{n} x_k\beta^{-k}\right) \\ &= \frac{1}{q}\sum_{k=1}^{d} z_n^{(k)}\beta^{-k} \end{aligned}$$

En procédant de la même façon, on déduit que pour que pour $2 \leq j \leq d$:

$$r_n^{(j)} = \frac{1}{q}\sum_{k=1}^{d} z_n^{(k)}\beta^{(j)-k}$$

On en déduit l'existence d'un vecteur Z_n de $\mathbb{Z}^d$ tel que $R_n = \frac{1}{q}Z_nB$. On a en fait montré que B est inversible.

Reprenons la preuve du théorème :
On pose $V_n = qR_n$. $(V_n)_n$ a une borne supérieure finie puisque $\max\limits_{1\leq j\leq d} \sup\limits_n |r_n^{(j)}| < \infty$. Etant donné que B est inversible, et que $Z_n = qR_nB^{-1}$, on a :

$$\sup_n ||Z_n|| = \sup_n \max_{1\leq j\leq d} |z_n^{(j)}| < \infty$$

Puisque les Z_i sont dans $\mathbb{Z}$, alors le nombre de valeurs que peuvent prendre les Z_i est fini. On en déduit que $\exists p, m \geq 1$ tels que $Z_{m+p} = Z_m$, d'où $r_{m+p} = r_m$.
Etant donné que les r_i sont établis par une relation de récurrence, alors la suite $(r_i)_i$ sera périodique, et donc le β-développement de x le sera également. □

Il est toutefois impossible de montrer un tel résultat si β est un nombre de Salem. Toutefois, on montrera dans la sous-partie suivante que la réciproque est vraie, et que ce résultat sera également valable si β est un nombre de Salem.

Exemple
Déterminons le β-développement de 1, avec β racine de $X^3 - X - 1$, de deux façons différentes.

La méthode la plus directe est d'appliquer l'algorithme glouton défini en partie 4.2. On a ainsi $r_0 = 1$.
$x_1 = \lfloor \beta r_0 \rfloor = \lfloor \beta \rfloor = 1$, car $\beta^3 - \beta - 1 = 0$ implique $(\beta + 1)\beta(\beta - 1) = 1$. On a ainsi $r_1 = \{\beta\} = \beta - 1 = \dfrac{1}{\beta(\beta+1)}$
$x_2 = \lfloor \dfrac{1}{\beta+1} \rfloor = 0$, et $r_2 = \{\dfrac{1}{\beta+1}\} = \dfrac{1}{\beta+1}$.
$x_3 = \lfloor \dfrac{\beta}{\beta+1} \rfloor = 0$, et $r_3 = \{\dfrac{\beta}{\beta+1}\} = \dfrac{\beta}{\beta+1}$.
$x_4 = \lfloor \dfrac{\beta^2}{\beta+1} \rfloor = \lfloor \dfrac{1}{\beta} \rfloor = 0$, et $r_4 = \dfrac{1}{\beta}$
$x_5 = \lfloor 1 \rfloor = 1$, et $r_5 = r_6 = ... = 0$
Ainsi, $d_\beta(1) = 10001$.

Procédons maintenant d'une autre façon, et définissons l'application f_β qui à une suite envoie le nombre correspondant en base β.
Etant donné que $1 = \frac{1}{\beta^2} + \frac{1}{\beta^3}$, alors un développement de 1 serait $\langle 1 \rangle =, 011$. Or, il ne s'agit pas de son β-développement : on peut en être certain puisqu'il commence par un 0, une remarque précédente affirmait que c'est impossible.
On va pour cela faire plusieurs développements impropres de 0, puisque l'on utilisera le chiffre $\overline{1}$ qui vaut 1, en base β : étant donné que $f_\beta(1, 000) = f_\beta(0, 011) = 1$, alors $f_\beta(1, 0\overline{1}\,\overline{1}) = 0$. De même, $f_\beta(0, 0...010\overline{1}\,\overline{1}) = 0$.
On va pouvoir sommer terme à terme le développement de 1 et deux développements différents de 0 :

0,	0	1	1		
	1	0	$\overline{1}$	$\overline{1}$	
0.	1	1	0	$\overline{1}$	
		$\overline{1}$	0	1	1
0,	1	0	0	0	1

On en déduit que $d_\beta(1) = 10001$.
On en déduit également que le polynôme $X^5 - X^4 - 1$ annule β, et que $X^3 - X - 1$ est un diviseur de $X^5 - X^4 - 1$.

4.4 Condition suffisante pour avoir $\beta \in U$

Pour démontrer que si le β-développement de tout élément de $\mathbb{Q} \cap [0, 1[$ est ultimement périodique alors $\beta \in U$, on aura besoin de plusieurs lemmes. Etant donné que les preuves de ceux-ci ressemblent au contenu de la sous-partie précédente, ils seront plus sommairement démontrés.
On considère dans cette sous partie que β est un entier algébrique, de polynôme minimal $P(X) = \sum_{i=0}^{d-1} a_i X^i + X^d$.

Lemme 4.4.1

Soit $x \in \mathbb{Q}(\beta) \cap [0,1[$ tel que $x = \frac{1}{q}\sum_{i=0}^{d-1} p_i\beta^i$.
Alors il existe un unique vecteur $Z_n = (z_n^{(1)}, ..., z_n^{(d)}) \in \mathbb{Z}^d$ tel que $T_\beta^n(x) = \frac{1}{q}\sum_{i=1}^{d} z_n^{(i)}\beta^i$.

La preuve se fait par récurrence, et ressemble à celle du lemme de la sous-partie précédente.

Lemme 4.4.2
Soit $n \in \mathbb{N}$, et γ une racine de P.
Alors :

$$\gamma^n\left(\frac{1}{q}\sum_{i=0}^{d-1} p_i\gamma^i - \sum_{k=1}^{n} x_k\gamma^{-k}\right) = \frac{1}{q} = \sum_{k=1}^{d} z_n^{(k)}\gamma^{-k} \qquad (1)$$

Démonstration. Par hypothèse, β est solution de l'équation polynômiale en X :

$$X^n\left(\frac{1}{q}\sum_{i=0}^{d-1} p_iX^i - \sum_{k=1}^{n} x_kX^{-k}\right) = \frac{1}{q} = \sum_{k=1}^{d} z_n^{(k)}X^{-k}$$

Etant donné que β et γ sont conjugués, alors γ est également solution de l'équation précédente. □

Lemme 4.4.3
En reprenant les notations du lemme précédent, si de plus γ est de module strictement supérieur à 1, et que le β-développement de x est ultimement périodique, alors :

$$\frac{1}{q}\sum_{i=0}^{d-1} p_i\gamma^i = \sum_{k=0}^{\infty} x_k\gamma^{-k}$$

Démonstration. Supposons que le β-développement de x est ultimement périodique. Alors il existe un nombre fini de Z_n vérifiant $T_\beta^n(x) = \frac{1}{q}\sum_{i=1}^{d} z_n^{(i)}\beta^i$, puisque $\left(T_\beta^n(x)\right)_n$ sera périodique à partir d'un certain rang.
On en déduit que $\sup_n ||Z_n|| = \sup_n \max_{1\leq j\leq d} |z_n^{(j)}| < \infty$.
On déduit de l'équation (1) :

$$\left|\frac{1}{q}\sum_{i=0}^{d-1} p_i\gamma^i = \sum_{k=0}^{n} x_k\gamma^{-k}\right| < cd|\gamma|^{-n}$$

On conclut en faisant tendre n vers l'infini. □

Théorème 4.4.4
Soit β un entier algébrique supérieur à 1. Si tout rationnel de l'intervalle [0,1] a un β-développement ultimement périodique, alors β est un nombre de Pisot ou de Salem.

Démonstration. Pour montrer ce résultat, on va raisonner par l'absurde en supposant l'existence de γ, un conjugué de β, de module strictement supérieur à 1. On a donc $P(\gamma) = 0$.
Posons $\eta = \max\left(\frac{1}{\beta}, \frac{1}{|\gamma|}\right)$, et $\delta = \left|\frac{1}{\beta} - \frac{1}{\gamma}\right|$.
Etant donné que $0 < \eta < 1$, alors on peut trouver un entier naturel m tel que $\frac{\lfloor\beta\rfloor\eta^m}{1-\eta} < \frac{\delta}{3}$.
On choisit un rationnel α dans l'intervalle [0,1] tel que son β-développement vérifie : $\alpha_1 = 1$ et pour $k = 2, ..., m-1$: $\alpha_k = 0$. Par hypothèse, α possède β-développement ultimement périodique. On déduit du lemme 4.4.3 :

$$\alpha = \beta^{-1} + \sum_{k=m}^{\infty} \alpha_k\beta^{-k} = \gamma^{-1} + \sum_{k=m}^{\infty} \alpha_k\gamma^{-k}$$

Donc :

$$\begin{aligned}
\delta &= \left|\frac{1}{\beta} - \frac{1}{\gamma}\right| \\
&\leq \sum_{k=m}^{\infty} \alpha_k \left|\gamma^{-k} - \beta^{-k}\right| && \text{or } \eta^k \geq \frac{1}{\beta^k} \text{ et } \eta^k \geq \frac{1}{|\gamma|^k} \\
&\leq \sum_{k=m}^{\infty} \alpha_k \eta^k && \text{or } \sup \alpha_k = \lfloor \beta \rfloor \text{ et } \eta < 1 \\
&\leq 2\frac{\eta^m \lfloor \beta \rfloor}{1-\eta} \\
&< \frac{2\delta}{3}
\end{aligned}$$

Cette contradiction interdit l'existence d'une racine de P différente de β ayant un module strictement supérieur à 1.
Donc β est un nombre de Pisot ou de Salem. □

4.5 Conséquence sur les polynômes

Théorème 4.5.1
Soit $\theta \in S$. Alors θ est racine d'un polynôme unitaire à coefficients entiers dont les valeurs absolues sont toutes inférieures ou égales à θ, à l'exception d'au plus un coefficient pouvant potentiellement être égal à $\lfloor \theta \rfloor + 1$.

Démonstration. Considérons le θ-développement de 1. Celui-ci est éventuellement périodique par le théorème précédent, car $1 \in \mathbb{Q}(\theta) \cap [0, 1]$. On traitera différemment le cas où $d_\theta(1)$ est fini, et le cas où il est infini.

Premier cas : $d_\theta(1)$ est fini

Il existe une suite finie $a_1...a_n$ de $\{0, ..., \lfloor \theta \rfloor\}$ telle que $d_\theta(1) = a_1, ..., a_n$.
On a alors $\sum_{i=1}^{n} a_i \theta^{-i} = 1$, soit $\sum_{i=1}^{n} a_i \theta^{n-i} = \theta^n$
Dans ce cas, le polynôme $X^n - \sum_{i=1}^{n} a_i X^{n-i}$ annule θ, et tous ses coefficients sont bien des entiers positifs inférieurs ou égaux à θ.

Second cas : $d_\theta(1)$ est infini

Ce développement étant donc périodique à partir d'un certain rang.
On écrit, avec $\forall i : 0 \leq a_i \leq \theta$, le θ-développement de 1, ainsi qu'une représentation de 0, dont on notera b_i les valeurs de ce développement noté $d(0)$:

$$\begin{aligned}
d_\theta(1) &= a_1...a_k(a_{k+1}...a_{k+p})^\infty \\
d(0) &= \underbrace{0\,0...0}_{p-1 \text{ zéros}}\,1\,\overline{a_1}...\overline{a_k}\,(\overline{a_{k+1}}...\overline{a_{k+p}})^\infty
\end{aligned}$$

En effet, on a :

$$1 - \sum_{i \geq 1} a_i \theta^{-i} = 0$$

On en a déduit l'écriture $d(0)$ en factorisant par θ^p le terme de gauche.

On pose alors la série formelle : $S_1(X) = \sum_{i\geq 1} a_i X^i$. On a $S_1(\theta^{-1}) = 1$, et le coefficient constant vaut 0.
On pose maintenant $S_2(X) = \sum_{i\geq p} b_i X^i$. On a $S_2(\theta^{-1}) = 0$, et le coefficient constant vaut aussi 0.
On en déduit que $P(\theta^{-1}) = (S_1 + S_2)(\theta^{-1}) - 1 = 0$.
Or P est de degré fini : puisque la suite des a_i est p-cyclique à partir d'un certain rang, les coefficients vont s'annuler à partir du rang $k+p+1$ lorsque l'on fera la somme des deux séries.
D'autre part, puisque $\forall i : 0 \leq a_i, -b_i \leq \theta$, alors les coefficients de P seront dans $[[-\theta, \theta]]$, à l'exception peut-être du p-ième, à cause du 1 dans le développement de 0.
On choisit alors $-P^*$ pour conclure : θ^{-1} étant racine de P, θ sera racine de P^*. De plus, il est unitaire car le coefficient constant de P vaut -1 □

Exemple
Soit θ un nombre de Pisot tel que $d_\theta(1) =, a(b)^\infty$.
D'autre part, on a $\langle 0\rangle_\theta =, 1\overline{a}\left(\overline{b}\right)^\infty$.
En reprenant les mêmes séries formelles que celles de la preuve du résultat précédent, on trouve : $S_1(X) = aX + \sum_{i\geq 2} bX^i$, et $S_2(X) = X - aX^2 - \sum_{i\geq 3} bX^i$.
On a ainsi $P(X) = (b-a)X^2 + (a+1)X - 1$
On trouve que θ est racine du polynôme $X^2-(a+1)X+(a-b)$. C'est donc un entier quadratique.

Références

[1] G.H. Hardy and E.M.Wright. *Introduction to the theory of numbers.* Vuibert-Springer, 2007.

[2] M.J. Bertin, A. Descomps-Guilloux, M. Grandet-Hugot, M. Patiaux-Delefosse, and J.P. Schreiber. *Pisot and Salem numbers.* Springer Baselag, 1992.

[3] Michiel Hazewinkel. Geometry of numbers, juin 2012. https ://www.encyclopediaofmath.org/index.php/Geometry-of-numbers.

[4] Jacques Ravatin and Anne-Marie Branca. *Théorie des formes et des champs de cohérences.* Éditions du Cosmogone, 1998.

[5] H.L. Montgomery I. Ninen, H.S. Zacherman. *An introduction to the theory of numbers.* 1991.