Développements périodiques de familles paramétrées de nombres algébriquues : application à la recherche d'unité

Brigitte Adam

UNIVERSITÉ DE METZ

THÈSE

présentée par

Brigitte ADAM

en vue d'obtenir le titre de

DOCTEUR DE L'UNIVERSITÉ DE METZ

Spécialité : Mathématiques

Sujet : Développements périodiques de familles paramétrées de nombres algébriques.
Application à la recherche d'unités.

Soutenue le 30 novembre 1995

Devant le jury composé de :

P. LIARDET	Université d'Aix-Marseille 1	Président
E. DUBOIS	ISMRA et Université de Caen	Rapporteur
C. LEVESQUE	Université de Laval	Rapporteur
O. LEC		Examinateur
M. OLI		Examinateur
G. RHI		Directeur de thèse

UNIVERSITÉ DE METZ

THÈSE

présentée par

Brigitte ADAM

en vue d'obtenir le titre de

DOCTEUR DE L'UNIVERSITÉ DE METZ

Spécialité : Mathématiques

Sujet : Développements périodiques de familles paramétrées de nombres algébriques.
Application à la recherche d'unités.

Soutenue le 30 novembre 1995

Devant le jury composé de :

P. LIARDET	Université d'Aix-Marseille 1	Président
E. DUBOIS	ISMRA et Université de Caen	Rapporteur
C. LEVESQUE	Université de Laval	Rapporteur
O. LECACHEUX	Université Pierre et Marie Curie	Examinateur
M. OLIVIER	Université de Bordeaux 1	Examinateur
G. RHIN	Université de Metz	Directeur de thèse

Quand, faute de fil conducteur dans le labyrinthe des montagnes. nul ne peut progresser par déduction, car ton chemin tu connais qu'il échoue à l'instant seulement où se montre l'abîme, et qu'ainsi le versant opposé est encore ignoré, ..., alors parfois se propose ce guide qui, ..., te trace la route. Mais une fois parcourue, cette route demeure tracée et t'apparaît comme évidente.

Antoine de Saint-Exupéry

A Marie,

Remerciements :

Je remercie particulièrement Georges Rhin de m'avoir accueillie en thèse et proposé ce travail. Merci pour sa patience et sa disponibilité presque sans limites. Il a supporté mes nombreux doutes et par son optimisme a toujours su me donner la force de persévérer.

Je remercie sincèrement Eugène Dubois qui s'est toujours intéressé à mon travail. Sa gentillesse, ses encouragements lors de chacune de nos rencontres et son soutien moral m'ont été une aide précieuse. Merci d'avoir accepté d'être rapporteur de cette thèse.

Je remercie également Claude Levesque d'avoir accepté d'être rapporteur. Ses visites à Metz et nos discussions ont été très fructueuses et essentielles dans l'accomplissement de ce travail.

Je remercie Odile Lecacheux, Pierre Liardet et Michel Olivier d'avoir accepté d'être membres du jury de cette thèse.

Je tiens à remercier Josef Kühner pour l'intérêt qu'il a porté à mon travail. Les échanges que nous avons eus m'ont beaucoup aidée.

Un grand Merci à Odile pour son aide en informatique et à Valérie pour ses nombreux conseils. Mais c'est surtout par leur écoute qu'elles m'ont aidée toutes les deux, au quotidien, à garder une certaine sérénité et à surmonter les moments les plus difficiles.

Table des matières

INTRODUCTION

L'algorithme des **fractions continues** a les propriétés suivantes :

- Le développement en fraction continue d'un nombre réel α est périodique si et seulement si α est quadratique. De plus, dans ce cas si α est un nombre réel racine d'un polynôme $f(X) = X^2 - aX - b$ à coefficients dans $\mathbb{Z}$ avec $a \geq b \geq 1$ alors le développement en fraction continue de α est symétrique.
- L'algorithme des fractions continues fournit l'unité fondamentale de tout corps de nombres quadratique réel.

De nombreuses tentatives ont été faites dans le but de généraliser l'algorithme des fractions continues.
L'une des généralisations les plus classiques est l'algorithme de **Jacobi-Perron (AJP)** introduit par Jacobi en dimension 2 et généralisé par Perron à des dimensions supérieures.

- Pour cet algorithme on ne connaît aucune condition nécessaire et suffisante pour qu'un développement soit périodique. E. Dubois a montré l'existence dans tout corps de nombres réels d'une base dont le développement est périodique.
- Lorsque le développement par l'AJP d'une base d'un corps de nombres réels est périodique, il fournit une unité de ce corps mais cette unité n'appartient pas nécessairement à un système fondamental d'unités.

Une autre généralisation bien connue de l'algorithme des fractions continues est l'algorithme de **Voronoï** pour les corps cubiques.
Le développement par l'algorithme de Voronoï est purement périodique et fournit un système fondamental d'unités de tout corps de nombres algébriques de degré 3. Par contre dans la pratique son calcul peut être complexe.
J. Buchmann a généralisé cet algorithme à des corps de nombres algébriques de degré supérieur à 3 et ainsi obtenu un algorithme (GVA) purement périodique permettant de calculer un système fondamental d'unités de corps dont le rang du groupe des unités est 1 ou 2.

Un problème classique de la théorie des nombres est la recherche de familles paramétrées infinies de corps de nombres algébriques dont un système fondamental d'unités s'écrit simplement en fonction des paramètres.
En degré 2, F. Halter-Koch, H.C. Williams et beaucoup d'autres ont donné des familles paramétrées infinies de nombres entiers positifs N tels que le développement en fraction continue de $\sqrt{N}$ fournisse une unité de $\mathbb{Q}(\sqrt{N})$ qui s'écrit simplement en fonction des paramètres.
En degré 3, L. Bernstein et plus tard C. Levesque et G. Rhin ont étudié le développement par l'AJP de familles paramétrées infinies de nombres algébriques. Ces développements

étant périodiques, ils ont ainsi obtenu une unité de corps de nombres algébriques de degré 3. E. Dubois et H.C. Williams ont étudié le développement par l'algorithme de Voronoï de certaines familles et obtenu ainsi une unité fondamentale de corps de nombres algébriques cubiques non totalement réels. Pour toutes ces familles la longueur du développement par l'algorithme de Voronoï est au plus égale à 6. On peut encore citer, parmi d'autres, les travaux de H.J. Stender sur des familles de systèmes fondamentaux d'unités dépendant de paramètres.

L'étude de telles familles met en évidence plusieurs problèmes :

- Détermination effective d'un système fondamental d'unités de corps de nombres algébriques. Pour ce calcul, l'algorithme de Voronoï et plus tard ceux de E. Dubois et H.C. Williams conviennent pour les corps de degré 3 et l'algorithme GVA de J. Buchmann convient pour les corps de degré supérieur à 3 dont le rang du groupe des unités est 1 ou 2. Plus récemment, J. Buchmann a donné un algorithme théorique pour calculer le nombre de classes, la structure du groupe des classes, le régulateur et un système fondamental d'unités de tout corps de nombres algébriques de degré quelconque. Cet algorithme a été implanté par H. Cohen, F. Diaz y Diaz et M. Olivier dans le système PARI : cette technique permet de traiter des corps de degré allant jusqu'à 15, par contre la validité des résultats dépend de l'Hypothèse de Riemann Généralisée.
- Calcul du développement en fraction continue d'un nombre algébrique réel et plus généralement celui par l'AJP de n nombres algébriques réels ($n > 1$). Pour le calcul en fraction continue, nous disposons d'algorithmes tels que celui donné par S. Lang et A. Trotter qui utilise les polynômes réduits. E. Bombieri et A.J. van der Poorten ont donné un algorithme simple qui fournit le développement en fraction continue de $\sqrt[3]{2}$, par contre la méthode ne se généralise pas de façon évidente. Pour le développement par l'AJP, G. Rhin a étudié le développement par l'algorithme de Jacobi-Perron de $(\sqrt[3]{4}, \sqrt[3]{16})$ jusqu'à l'ordre 1954 sans faire apparaître de période.

Dans ce travail, nous commençons par rappeler dans le **chapitre 1** les définitions et propriétés principales de l'algorithme de Jacobi-Perron et de celui de Voronoï et nous introduisons une notion de développement par l'AJP symétrique généralisant celle du développement en fraction continue symétrique.

Nous examinons ensuite dans le **chapitre 2** les deux familles infinies de polynômes dépendant chacune de deux paramètres introduites par C. Levesque et G. Rhin :

(1) $f(X) = X^3 - c^m X^2 - (c-1)X - c^m$ (pour la première famille)

(2) $f(X) = X^3 - (c^m + c - 1)X^2 - (c^m - 1)X - c^m$ (pour la deuxième famille)

où $c \geq 2$ et $m \geq 1$ sont deux entiers.
Pour chacune de ces familles C. Levesque et G. Rhin ont donné le développement par l'AJP d'un vecteur à composantes dans $\mathbb{Q}(\alpha)$, avec α l'unique racine réelle du polynôme $f(X)$. Ces développements étant périodiques, ils ont ainsi obtenu une unité de ces corps et ont conjecturé que cette unité était fondamentale dans l'ordre $\mathbf{Z}[\alpha]$. De plus, pour ces

développements, la longueur de la période tend vers l'infini.
Ces familles fournissent des exemples de développement par l'AJP symétriques.
Dans ce même chapitre, nous déterminons le développement par l'algorithme de Voronoï de ces deux familles et obtenons les résultats suivants :

- la longueur de la période de ces développements tend vers l'infini.
- le développement par l'algorithme de Voronoï et celui par l'AJP sont étroitement liés pour ces deux familles.
- l'unité donné par l'AJP est fondamentale dans l'ordre $\mathbf{Z}[\alpha]$: ce qui résout une conjecture de C. Levesque et G. Rhin.

Ces résultats sont à l'origine d'un article accepté pour publication dans Mathematics of Computation.
Nous généralisons ces familles à des familles infinies de corps de degré quelconque pour lesquelles nous étudions un développement par l'AJP. Ces développements étant périodiques (nous remarquons de plus qu'ils sont symétriques), nous obtenons ainsi pour des familles paramétrées infinies de corps de nombres de degré quelconque une unité qui s'écrit simplement en fonction des paramètres. Nous sommes alors amenés à poser le problème suivant : peut-on pour ces familles infinies de polynômes de degré quelconque, donner le développement par l'algorithme de Voronoï et un système fondamental d'unités dépendant des paramètres ?

Dans ce but, nous proposons dans le **chapitre 3** une nouvelle méthode de calcul du développement par l'algorithme GVA introduit par J. Buchmann. Nous donnons une définition plus générale de points extrémaux et décrivons une méthode de recherche de ces points. Cette méthode nous permet de calculer des unités de tout corps de nombres algébriques et un système fondamental d'unités lorsque le rang du groupe des unités est 1 ou 2. Nous l'appliquons ensuite à une des familles précédentes de degré 4 pour laquelle le rang du groupe des unités est 2. De plus, nous proposons un algorithme (utile pour le calcul de points extrémaux) qui permet entre autre de trianguláriser une matrice sous forme normale d'Hermite (HNF). Nous l'appliquons à une matrice 20×20 donnée par J.L. Hafner et K.S. McCurley et montrons que la taille des entiers intervenant dans l'algorithme est nettement plus petite que dans l'algorithme de réduction standard d'Hermite.

Nous donnons dans le **chapitre 4** un algorithme dont le calcul n'utilise que des nombres entiers qui permet de déterminer le développement par l'AJP de n nombres réels algébriques (en particulier, si $n = 1$, celui en fraction continue d'un nombre réel algébrique). Nous présentons quelques exemples numériques dont le développement en fraction continue de $\sqrt[3]{2}$ (on constate alors que les calculs sont plus rapides et la taille des entiers nécessaires au calcul plus petite qu'en utilisant les formules données par E. Bombieri et A.J. Van der Poorten) et le développement par l'algorithme de Jacobi-Perron de $(\sqrt[3]{4}, \sqrt[3]{16})$ jusqu'à l'ordre 2000. Ce chapitre est à l'origine d'un article accepté pour publication dans le Bulletin of the Australian Mathematical Society.

Nous donnons en **annexe** :

- En complément du chapitre 3, la description de l'algorithme qui permet de trianguláriser une matrice sous forme HNF, sa programmation en PARI et détaillons

l'application à la matrice 20×20 citée dans ce même chapitre.

- Le programme en PARI de l'algorithme permettant de déterminer le développement par l'algorithme de Jacobi-Perron de nombres réels algébriques.
- Des exemples de calculs de points extrémaux pour des familles de degré 4.

CHAPITRE 1

Définitions de l'algorithme de Jacobi-Perron et de l'algorithme de Voronoï

Dans ce chapitre, nous rappelons les définitions classiques du développement par l'algorithme de Jacobi-Perron d'un vecteur de $\mathbb{R}^n$.
Lorsque celui-ci est périodique nous définissons un développement symétrique pour $n \geq 1$, qui généralise la notion de développement en fraction continue symétrique.
Enfin, nous rappelons les définitions et propriétés essentielles de l'algorithme de Voronoï dans un corps de nombres cubique à conjugués complexes.

1.1 Rappels sur l'algorithme de Jacobi-Perron.

1.1.1 Premières définitions et notations

Définition 1.1.1 *Soit $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ un vecteur de $\mathbb{R}^n$ $(n \geq 1)$. Le développement par* **l'algorithme de Jacobi-Perron** *[24] (noté* **AJP***) de α est la donnée :*

- *d'une suite de vecteurs $(a^\nu)_{\nu \geq 0}$ de $\mathbb{Z}^n$ appelés* **quotients incomplets**, *notés $a^\nu = (a_1^\nu, a_2^\nu, \ldots, a_n^\nu)$*
- *d'une suite de vecteurs $(\alpha^\nu)_{\nu \geq 0}$ de $\mathbb{R}^n$ appelés* **quotients complets**, *notés $\alpha^\nu = (\alpha_1^\nu, \alpha_2^\nu, \ldots, \alpha_n^\nu)$*

définis par :

$$\begin{cases} \alpha^0 = \alpha \\ \text{et pour } \nu \geq 0 \quad a_i^\nu = [\alpha_i^\nu] \quad \text{pour } 1 \leq i \leq n \\ \text{et si } \alpha_1^\nu \neq a_1^\nu \quad \alpha_n^{\nu+1} = \dfrac{1}{\alpha_1^\nu - a_1^\nu} \ ; \ \alpha_i^{\nu+1} = \dfrac{\alpha_{i+1}^\nu - a_{i+1}^\nu}{\alpha_1^\nu - a_1^\nu} \text{ pour } 1 \leq i < n. \end{cases}$$

où $[x]$ désigne la partie entière du réel x.

Remarque 1: L'algorithme de Jacobi-Perron est une généralisation de l'algorithme des fractions continues qui correspond à $n = 1$ dans la définition précédente.

Remarque 2: Si pour tout $\nu \geq 0$ on a $\alpha_1^\nu \neq a_1^\nu$ (ce qui est vrai si $1, \alpha_1, \ldots, \alpha_n$ sont $\mathbb{Q}$ linéairement indépendants) alors le développement est infini et sera noté

$$\begin{pmatrix} & & & & a_n^0 & a_n^1 & \ldots & \ldots & a_n^\nu & \ldots \\ & & & a_4^0 & \cdot & \cdot & & & \cdot & \\ & & a_3^0 & \cdot & \cdot & & & & & \\ & a_2^0 & & a_2^1 & \cdot & & & & & \\ a_1^0 & & a_1^1 & \ldots & \ldots & & a_1^\nu & \ldots & & \end{pmatrix}$$

Définition 1.1.2 *A un tel développement on peut associer une suite de vecteurs* $(A^\nu)_{\nu \geq 0}$ *de* $\mathbb{Z}^n$ *appelés* **réduites**, *notés* $A^\nu = (A_0^\nu, A_1^\nu, A_2^\nu, \ldots, A_n^\nu)$ *définis par:*

$$\begin{cases} \text{pour } 0 \leq i \leq n \text{ et } 0 \leq j \leq n, \quad A_i^j = \begin{cases} 1 \text{ si } i = j \\ 0 \text{ sinon} \end{cases} \\ \\ \text{pour } \nu \geq 0 \text{ et } 0 \leq i \leq n, \quad A_i^{\nu+n+1} = A_i^\nu + a_i^\nu A_i^{\nu+1} + \ldots + a_n^\nu A_i^{\nu+n} \end{cases}$$

On a alors les formules suivantes :

(1) $\alpha_i = \dfrac{\sum_{j=0}^{n} A_i^{\nu+j} \alpha_j^\nu}{\sum_{j=0}^{n} A_0^{\nu+j} \alpha_j^\nu}$, pour tout $\nu \geq 0$ et en notant $\alpha_0^\nu = 1$,

(2) $\lim\limits_{\nu \to \infty} \dfrac{A_i^\nu}{A_0^\nu} = \alpha_i$,

(3) En notant $\mathcal{A}_\nu$ les matrices définies par

$$\mathcal{A}_\nu = \begin{pmatrix} a_n^\nu & 1 & 0 & \ldots & 0 \\ a_{n-1}^\nu & 0 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ a_1^\nu & 0 & \ldots & 0 & 1 \\ 1 & 0 & \ldots & \ldots & 0 \end{pmatrix}$$

on a

$$\mathcal{A}_0 \mathcal{A}_1 \ldots \mathcal{A}_{\nu-1} = \begin{pmatrix} A_n^{\nu+n} & . & . & . & A_n^\nu \\ . & . & . & . & . \\ . & . & . & . & . \\ . & . & . & . & . \\ A_0^{\nu+n} & . & . & . & A_0^\nu \end{pmatrix}.$$

1.1.2 Développements périodiques

Définition 1.1.3 *Le développement par l'AJP est dit* **périodique** *s'il existe deux nombres entiers k positif et l strictement positif tels que* $a_i^{k+\nu} = a_i^{k+\nu+l}$ *pour* $\nu \geq 0$ *et* $0 \leq i \leq n$.

Si k et l sont les plus petits entiers vérifiant cette égalité, alors k est la longueur de la prépériode et l la longueur de la période du développement. Le développement est dit **purement périodique** *si $k = 0$.*

Remarque: Lorsque le développement par l'AJP de $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ est purement périodique de longueur l, il fournit une unité du corps $K = \mathbb{Q}[\alpha_1, \ldots, \alpha_n]$, à savoir:

$$\epsilon = A_0^l + \alpha_1 A_0^{l+1} + \ldots + \alpha_n A_0^{l+n} = \prod_{\nu=0}^{l-1} \alpha_n^{\nu}.$$

Dans ce cas, la matrice $\mathcal{A}_0\mathcal{A}_1 \ldots \mathcal{A}_{l-1}$ est la transposée de la matrice de la multiplication par ϵ exprimée dans la base $\{\alpha_n, \ldots, \alpha_1, 1\}$.
On a une formule analogue dans le cas plus général d'un développement périodique, de longueur de prépériode k, que l'on obtient en remplaçant α_i par α_i^k ($1 \leq i \leq n$).

1.1.3 Développements symétriques

Dans le cas des fractions continues, on a la proposition suivante:

Proposition 1.1.4 *Soit α un nombre réel non rationnel, quadratique tel que $\alpha > 1$ soit racine du polynôme $f(X) = X^2 - aX - b$ avec $a \geq b \geq 1$, alors le développement par l'algorithme des fractions continues de α est purement périodique et symétrique, c'est-à-dire:*
si l désigne la longueur de la période, $a_{l-i} = a_i$ pour tout i tel que $0 \leq i \leq l$ ou encore si on note $\alpha = [\overline{a_0, a_1, \ldots, a_{l-1}}]$, le "mot" $[a_0, a_1, \ldots, a_{l-1}, a_l]$ est un palindrome.

On montre facilement cette proposition en considérant le développement en fraction continue de $-\frac{1}{\overline{\alpha}}$, où $\overline{\alpha}$ désigne le conjugué de α.

On va dans ce paragraphe généraliser cette notion de développement symétrique aux développements par l'AJP de n nombres algébriques réels avec $n \geq 2$.

a) Définitions

Définition 1.1.5 *Soient $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ n nombres algébriques réels dont le développement par l'AJP est purement périodique de longueur l. Soit k le plus petit entier tel que $kl \geq n - 1$. On dit que ce développement est* **symétrique** *si et seulement si pour tout i tel que $0 \leq i \leq n-1$ et tout ν tel que $0 \leq \nu \leq l - i$ on a*

$$\begin{cases} a_{i+1}^{kl-\nu-i} = a_{i+1}^{\nu} & (1) \\ a_{i+1}^{2kl-\nu-i} = a_{i+1}^{\nu} & (2) \end{cases}$$

La condition (1) entraîne que le "mot"

$$\begin{pmatrix} & & & a_n^0 & \ldots & \ldots & \ldots & a_n^{kl-n+1} & & & \\ & & \iddots & \ldots & \ldots & \ldots & \ldots & \ldots & \ddots & & \\ & a_2^0 & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & a_2^{kl-1} & \\ a_1^0 & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & a_1^{kl} \end{pmatrix}$$

est symétrique,
et la condition (2) entraîne que le "mot"

$$\begin{pmatrix} a_n^{kl-n+2} & \dots & \dots & \dots & a_n^{kl-1} \\ & \ddots & \dots & \iddots & \\ & & a_3^{kl-1} & & \end{pmatrix}$$

est symétrique.

b) Exemples

E. Dubois et R. Paysant-Le Roux [10] ont démontré le théorème suivant :

Théorème 1.1.6 *Soit* $g(x) = x^{n+1} - a_n x^n - \ldots - a_1 x - a_0$ *où les nombres* a_i $(0 \leq i \leq n)$ *sont des entiers positifs tels que* a_0 *divise* a_i $(1 \leq i \leq n)$, $a_0 > 1$ *et* $a_n > a_i$ $(0 \leq i \leq n-1)$. *Soit* α *la racine positive de* g. *On pose*

$$\begin{cases} \alpha_n = \alpha \\ \alpha_i = \alpha(\alpha_{i+1} - a_{i+1}) \end{cases}$$

alors $(\alpha_n, \alpha_{n-1}, \ldots, \alpha_1)$ *admet un développement par l'AJP purement périodique de longueur* $(n+1)$, *la période étant donnée par :*

$$\begin{cases} a_i^0 = a_i & 1 \leq i \leq n \\ a_i^\nu = \dfrac{a_i}{a_0} & 1 \leq \nu \leq n, 1 \leq i \leq n - \nu + 1 \\ a_i^\nu = a_i & n - \nu + 1 < i \leq n \end{cases} .$$

Ces développements sont symétriques.

Explicitons un exemple pour $n = 4$. Considérons le polynôme

$$g(X) = X^5 - 8X^4 - 6X^3 - 2X^2 - 4X - 2.$$

Le développement par l'AJP de $(\alpha_4, \alpha_3, \alpha_2, \alpha_1)$ est purement périodique de longueur 5 et s'écrit

$$\begin{pmatrix} & & 8 & & 4 & & 8 & & 8 & & 8 & & 8 & \\ & 6 & & 3 & & 3 & & 6 & & 6 & & 6 & & \\ 2 & & 1 & & 1 & & 1 & & 2 & & 2 & & \dots & \\ 4 & & 2 & & 2 & & 2 & & 2 & & 4 & & & \end{pmatrix}.$$

Les mots

$$\begin{pmatrix} & & 8 & & 4 & & 8 & & \\ & 6 & & 3 & & 3 & & 6 & \\ 2 & & 1 & & 1 & & 1 & & 2 \\ 4 & & 2 & & 2 & & 2 & & 2 & & 4 \end{pmatrix}$$

et

$$\begin{pmatrix} 8 & & 8 \\ & 6 & \end{pmatrix}$$

sont symétriques.

c) Notation matricielle

On considère les matrices $\mathcal{A}_\nu$ définies précédemment, associées à un développement par l'AJP.

Dans le cas des fractions continues :

(1) ces matrices sont de la forme $\begin{pmatrix} a_1^\nu & 1 \\ 1 & 0 \end{pmatrix}$ et sont donc symétriques.

(2) de plus, si le développement est purement périodique symétrique de longueur l, le produit de matrices $\mathcal{A}_0\mathcal{A}_1 \dots \mathcal{A}_l$ est symétrique c'est-à-dire $\mathcal{A}_{l-i} = \mathcal{A}_i$ pour tout i tel que $0 \leq i \leq l$.

On généralise ces deux résultats au cas $n > 1$.

Définition 1.1.7 *Soit n un entier strictement positif. Pour tout entier a et tout entier i tel que $1 \leq i \leq n$, on définit la matrice $A_i(a)$, appelée* **matrice élémentaire** *par*

$$A_i(a) = \begin{pmatrix} \overbrace{\begin{vmatrix} 1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & 1 \end{vmatrix}}^{(n-i)} & 0 & 0 \\ 0 & \begin{vmatrix} a & 1 \\ 1 & 0 \end{vmatrix} & 0 \\ 0 & 0 & \underbrace{\begin{vmatrix} 1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & 1 \end{vmatrix}}_{(i-1)} \end{pmatrix}.$$

Notation : Soient A_i $(1 \leq i \leq n)$ n matrices carrées. On note $(\prod_{i=1}^{n})^* A_i = A_1 A_2 \dots A_n$ le produit de ces matrices selon les indices i croissants.
On obtient alors la proposition suivante :

Proposition 1.1.8 *Soient $(\alpha_1, \alpha_2, \dots, \alpha_n)$ n nombres réels $(n > 1)$.*

(1) Les matrices $\mathcal{A}_\nu$, définies précédemment, associées au développement par l'AJP de $(\alpha_1, \alpha_2, \dots, \alpha_n)$ se décomposent en un produit de matrices symétriques élémentaires, noté :
$\mathcal{A}_\nu = (\prod_{i=1}^{n})^* \mathcal{A}_i^\nu = \mathcal{A}_1^\nu \mathcal{A}_2^\nu \dots \mathcal{A}_n^\nu$.

(2) Lorsque le développement par l'AJP de $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ *est purement périodique symétrique de longueur* l *alors le produit de matrices* $(\prod_{\nu=0}^{kl})^*(\prod_{i=1}^{min(kl-\nu+1,n)})^*\mathcal{A}_i^\nu$ *s'écrit sous forme d'un produit symétrique de matrices symétriques, toutes élémentaires sauf éventuellement une, où* k *est le plus petit entier tel que* $kl \geq n-1$.

Avant de démontrer cette proposition on considère l'exemple donné précédemment.
On a :

$$\mathcal{A}_0 = \begin{pmatrix} 8 & 1 & 0 & \ldots & 0 \\ 6 & 0 & \ddots & \ddots & \vdots \\ 2 & \vdots & \ddots & \ddots & 0 \\ 4 & 0 & \ldots & 0 & 1 \\ 1 & 0 & \ldots & \ldots & 0 \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & 0 & 0 & & \\ 0 & 1 & 0 & 0 & \\ 0 & 0 & 1 & & \\ & 0 & & 4 & 1 \\ & & & 1 & 0 \end{pmatrix}}_{\mathcal{A}_1^0} \underbrace{\begin{pmatrix} 1 & 0 & & 0 & 0 \\ 0 & 1 & & & \\ & & 2 & 1 & 0 \\ 0 & & 1 & 0 & \\ & & 0 & & 1 \end{pmatrix}}_{\mathcal{A}_2^0}$$

$$\underbrace{\begin{pmatrix} 1 & & 0 & 0 & \\ & 6 & 1 & 0 & \\ 0 & 1 & 0 & & 0 \\ & 0 & & 1 & 0 \\ & & 0 & 0 & 1 \end{pmatrix}}_{\mathcal{A}_3^0} \underbrace{\begin{pmatrix} 8 & 1 & & 0 & \\ 1 & 0 & & & \\ & & 1 & 0 & 0 \\ 0 & & 0 & 1 & 0 \\ & & 0 & 0 & 1 \end{pmatrix}}_{\mathcal{A}_4^0}$$

On définit de même les matrices $\mathcal{A}_\nu$ pour $1 \leq \nu \leq 5$.
On a alors

$$(\prod_{\nu=0}^{5})^*(\prod_{i=1}^{min(6-\nu,4)})^*\mathcal{A}_i^\nu = \mathcal{A}_1^0 \ldots \mathcal{A}_4^0 \mathcal{A}_1^1 \ldots \mathcal{A}_4^1 \mathcal{A}_1^2 \ldots \mathcal{A}_4^2 \mathcal{A}_1^3 \ldots \mathcal{A}_3^3 \mathcal{A}_1^4 \mathcal{A}_2^4 \mathcal{A}_1^5.$$

En permutant certaines matrices (en effet, pour tout ν et tout μ tels que $0 \leq \nu \leq 5$ et $0 \leq \mu \leq 5$ on a $\mathcal{A}_1^\nu \mathcal{A}_4^\mu = \mathcal{A}_4^\mu \mathcal{A}_1^\nu$, $\mathcal{A}_1^\nu \mathcal{A}_3^\mu = \mathcal{A}_3^\mu \mathcal{A}_1^\nu$ *et* $\mathcal{A}_2^\nu \mathcal{A}_4^\mu = \mathcal{A}_4^\mu \mathcal{A}_2^\nu$) on a successivement:

$$(\prod_{\nu=0}^{5})^*(\prod_{i=1}^{min(6-\nu,4)})^*\mathcal{A}_i^\nu = \mathcal{A}_1^0\mathcal{A}_2^0\mathcal{A}_3^0\mathcal{A}_4^0\mathcal{A}_1^1\mathcal{A}_2^1\mathcal{A}_3^1\mathcal{A}_4^1\mathcal{A}_1^2\mathcal{A}_2^2\mathcal{A}_3^2\mathcal{A}_4^2\mathcal{A}_1^3\mathcal{A}_2^3\mathcal{A}_3^3\mathcal{A}_1^4\mathcal{A}_2^4\mathcal{A}_1^5$$

$$= \mathcal{A}_1^0\mathcal{A}_2^0\mathcal{A}_3^0\mathcal{A}_4^0\mathcal{A}_1^1\mathcal{A}_2^1\mathcal{A}_3^1\mathcal{A}_4^1\mathcal{A}_1^2\mathcal{A}_2^2\mathcal{A}_3^2\mathcal{A}_4^2\mathcal{A}_1^3\mathcal{A}_2^3(\mathcal{A}_1^4\mathcal{A}_3^3)\mathcal{A}_2^4\mathcal{A}_1^5$$

$$= \mathcal{A}_1^0\mathcal{A}_2^0\mathcal{A}_3^0\mathcal{A}_4^0\mathcal{A}_1^1\mathcal{A}_2^1\mathcal{A}_3^1\mathcal{A}_4^1\mathcal{A}_1^2\mathcal{A}_2^2\mathcal{A}_3^2(\mathcal{A}_1^3\mathcal{A}_4^2)\mathcal{A}_2^3\mathcal{A}_1^4\mathcal{A}_3^3\mathcal{A}_2^4\mathcal{A}_1^5$$

$$= \mathcal{A}_1^0\mathcal{A}_2^0\mathcal{A}_3^0\mathcal{A}_4^0\mathcal{A}_1^1\mathcal{A}_2^1\mathcal{A}_3^1\mathcal{A}_4^1\mathcal{A}_1^2\mathcal{A}_2^2\mathcal{A}_3^2\mathcal{A}_1^3(\mathcal{A}_2^3\mathcal{A}_4^2)\mathcal{A}_1^4\mathcal{A}_3^3\mathcal{A}_2^4\mathcal{A}_1^5$$

$$= \mathcal{A}_1^0\mathcal{A}_2^0\mathcal{A}_3^0\mathcal{A}_4^0\mathcal{A}_1^1\mathcal{A}_2^1\mathcal{A}_3^1\mathcal{A}_4^1\mathcal{A}_1^2\mathcal{A}_2^2\mathcal{A}_3^2\mathcal{A}_1^3\mathcal{A}_2^3(\mathcal{A}_1^4\mathcal{A}_4^2)\mathcal{A}_3^3\mathcal{A}_2^4\mathcal{A}_1^5$$

$$= \mathcal{A}_1^0\mathcal{A}_2^0\mathcal{A}_3^0\mathcal{A}_4^0\mathcal{A}_1^1\mathcal{A}_2^1\mathcal{A}_3^1(\mathcal{A}_1^2\mathcal{A}_4^1)\mathcal{A}_2^2(\mathcal{A}_1^3\mathcal{A}_3^2)\mathcal{A}_2^3\mathcal{A}_1^4\mathcal{A}_4^2\mathcal{A}_3^3\mathcal{A}_2^4\mathcal{A}_1^5.$$

En utilisant les égalités $\mathcal{A}_{i+1}^{5-\nu-i} = \mathcal{A}_{i+1}^{\nu}$ $(0 \leq i \leq 4,\ 0 \leq \nu \leq 5-i)$ ce produit s'écrit de la façon symétrique suivante:

$$(\prod_{\nu=0}^{5})^*(\prod_{i=1}^{min(6-\nu,4)})^*\mathcal{A}_i^{\nu} = \mathcal{A}_1^0 \ldots \mathcal{A}_4^0\mathcal{A}_1^1 \ldots \mathcal{A}_3^1\mathcal{A}_1^2 \underbrace{(\mathcal{A}_4^1\mathcal{A}_2^2)}_{\text{matrice symétrique}} \mathcal{A}_1^2\mathcal{A}_3^1 \ldots \mathcal{A}_1^1\mathcal{A}_4^0 \ldots \mathcal{A}_1^0.$$

Preuve de la proposition 1.1.8

(1) Soit n un entier tel que $n \geq 2$. Montrons par récurrence la propriété, notée (H_n), suivante :

Quels que soient les entiers $a_1, \ldots, a_n$, la matrice $\begin{pmatrix} a_n & 1 & 0 & \ldots & 0 \\ a_{n-1} & 0 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ a_1 & 0 & \ldots & 0 & 1 \\ 1 & 0 & \ldots & \ldots & 0 \end{pmatrix}$ s'écrit sous la forme d'un produit $A_1A_2 \ldots A_n$, où les matrices A_i $(1 \leq i \leq n)$ sont les matrices élémentaires telles que $A_i = A_i(a_i)$.

Si $n = 2$, $\begin{pmatrix} a_2 & 1 & 0 \\ a_1 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & a_1 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} a_2 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

Ainsi (H_2) est démontrée.

Supposons donc (H_n) et montrons (H_{n+1}).

On a

$$\begin{pmatrix} a_{n+1} & 1 & 0 & \ldots & 0 \\ a_n & 0 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ a_1 & 0 & \ldots & 0 & 1 \\ 1 & 0 & \ldots & \ldots & 0 \end{pmatrix} = \underbrace{\left(\begin{array}{cccc|cc} 1 & 0 & \ldots & 0 & & \\ 0 & \ddots & \ddots & \vdots & & \\ \vdots & \ddots & \ddots & 0 & & 0 \\ 0 & \ldots & 0 & 1 & & \\ \hline & & 0 & & a_1 & 1 \\ & & & & 1 & 0 \end{array}\right)}_{(n+2)} \begin{pmatrix} a_{n+1} & 1 & 0 & \ldots & 0 & 0 \\ a_n & 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 & \vdots \\ a_2 & 0 & \ldots & 0 & 1 & \vdots \\ 1 & 0 & \ldots & \ldots & 0 & 0 \\ 0 & \ldots & \ldots & \ldots & 0 & 1 \end{pmatrix}$$

et l'hypothèse de récurrence implique que

$$\begin{pmatrix} a_{n+1} & 1 & 0 & \dots & 0 \\ a_n & 0 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ a_2 & 0 & \dots & 0 & 1 \\ 1 & 0 & \dots & \dots & 0 \end{pmatrix} = \underbrace{\begin{pmatrix} \begin{vmatrix} 1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & 1 \end{vmatrix} & 0 \\ 0 & \begin{vmatrix} a_2 & 1 \\ 1 & 0 \end{vmatrix} \end{pmatrix}}_{(n+1)} \dots \begin{pmatrix} \begin{vmatrix} a_{n+1} & 1 \\ 1 & 0 \end{vmatrix} & 0 \\ 0 & \begin{vmatrix} 1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & 1 \end{vmatrix} \end{pmatrix}.$$

D'où

$$\begin{pmatrix} a_{n+1} & 1 & 0 & \dots & 0 \\ a_n & 0 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ a_1 & 0 & \dots & 0 & 1 \\ 1 & 0 & \dots & \dots & 0 \end{pmatrix} = \begin{pmatrix} \begin{vmatrix} 1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & 1 \end{vmatrix} & 0 \\ 0 & \begin{vmatrix} a_1 & 1 \\ 1 & 0 \end{vmatrix} \end{pmatrix}$$

$$\begin{pmatrix} \begin{vmatrix} 1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & 1 \end{vmatrix} & 0 & 0 \\ 0 & \begin{vmatrix} a_2 & 1 \\ 1 & 0 \end{vmatrix} & 0 \\ 0 & 0 & 1 \end{pmatrix} \dots \begin{pmatrix} \begin{vmatrix} a_{n+1} & 1 \\ 1 & 0 \end{vmatrix} & 0 \\ 0 & \begin{vmatrix} 1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & 1 \end{vmatrix} \end{pmatrix}.$$

Ce qui démontre (H_{n+1}).

Ainsi $\mathcal{A}_\nu = (\prod_{i=1}^{n})^* \mathcal{A}_i^\nu = \mathcal{A}_1^\nu \mathcal{A}_2^\nu \dots \mathcal{A}_n^\nu$, où

$$\mathcal{A}_i^\nu = \begin{pmatrix} \begin{vmatrix} 1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & 1 \end{vmatrix} & 0 & 0 \\ 0 & \begin{vmatrix} a_i^\nu & 1 \\ 1 & 0 \end{vmatrix} & 0 \\ 0 & 0 & \underbrace{\begin{vmatrix} 1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & 1 \end{vmatrix}}_{(i-1)} \end{pmatrix}.$$

(2) Montrons que le produit de matrices $(\prod_{\nu=0}^{kl})^* (\prod_{i=1}^{min(kl-\nu+1,n)})^* \mathcal{A}_i^\nu$ s'écrit sous forme d'un produit symétrique de matrices symétriques.

On note $\mathcal{B}_0 = (\prod_{\nu=0}^{kl})^* (\prod_{i=1}^{min(kl-\nu+1,n)})^* \mathcal{A}_i^\nu$.

On a :

$$\mathcal{B}_0 = (\mathcal{A}_1^0 \dots \mathcal{A}_n^0) \dots (\mathcal{A}_1^{kl-n+1} \dots \underline{\mathcal{A}_n^{kl-n+1}})(\mathcal{A}_1^{kl-n+2} \dots \underline{\mathcal{A}_{n-1}^{kl-n+2}}) \dots (\mathcal{A}_1^{kl-1} \underline{\mathcal{A}_2^{kl-1}})\underline{\mathcal{A}_1^{kl}}.$$

En utilisant les égalités $\mathcal{A}_i^\nu \mathcal{A}_j^\mu = \mathcal{A}_j^\mu \mathcal{A}_i^\nu$ pour tout i et j tels que $|i-j| \geq 2$ $(0 \leq \nu \leq kl,\ 0 \leq \mu \leq kl)$,
on a

$$(\mathcal{A}_1^{kl-n+1} \dots \underline{\mathcal{A}_n^{kl-n+1}})(\mathcal{A}_1^{kl-n+2} \dots \mathcal{A}_n^{kl-n+2}) =$$

$$(\mathcal{A}_1^{kl-n+1} \dots \mathcal{A}_{n-1}^{kl-n+1})(\mathcal{A}_1^{kl-n+2} \dots \mathcal{A}_{n-2}^{kl-n+2})\mathcal{A}_n^{kl-n+1}\mathcal{A}_{n-1}^{kl-n+2}$$

et en poursuivant

$$(\mathcal{A}_1^{kl-n+1} \dots \underline{\mathcal{A}_n^{kl-n+1}})(\mathcal{A}_1^{kl-n+2} \dots \underline{\mathcal{A}_{n-1}^{kl-n+2}}) \dots (\mathcal{A}_1^{kl-1} \underline{\mathcal{A}_2^{kl-1}})\underline{\mathcal{A}_1^{kl}} =$$

$$(\mathcal{A}_1^{kl-n+1} \dots \mathcal{A}_{n-1}^{kl-n+1})(\mathcal{A}_1^{kl-n+2} \dots \mathcal{A}_{n-2}^{kl-n+2}) \dots \mathcal{A}_1^{kl-1}(\mathcal{A}_n^{kl-n+1}\mathcal{A}_{n-1}^{kl-n+2} \dots \mathcal{A}_2^{kl-1}\mathcal{A}_1^{kl}).$$

En utilisant les égalités $\mathcal{A}_{i+1}^0 = \mathcal{A}_{i+1}^{kl-i}$ $(0 \leq i \leq n-1)$, on obtient

$$\mathcal{B}_0 = (\mathcal{A}_1^0 \dots \mathcal{A}_n^0)\mathcal{B}_1(\mathcal{A}_n^0 \dots \mathcal{A}_1^0)$$

avec

$$\mathcal{B}_1 = (\mathcal{A}_1^1 \dots \mathcal{A}_n^1) \dots (\mathcal{A}_1^{kl-n} \dots \mathcal{A}_n^{kl-n})(\mathcal{A}_1^{kl-n+1} \dots \mathcal{A}_{n-1}^{kl-n+1}) \dots (\mathcal{A}_1^{kl-2}\mathcal{A}_2^{kl-2})\mathcal{A}_1^{kl-1}.$$

On poursuit ce processus et on obtient ainsi, pour tout j tel que $0 \leq j \leq \frac{kl-n+1}{2}$,

$$\mathcal{B}_j = (\mathcal{A}_1^j \dots \mathcal{A}_n^j) \dots (\mathcal{A}_1^{kl-n-j+1} \dots \mathcal{A}_n^{kl-n-j+1}) \dots (\mathcal{A}_1^{kl-j-1}\mathcal{A}_2^{kl-j-1})\mathcal{A}_1^{kl-j},$$

et

$$\mathcal{B}_0 = (\mathcal{A}_1^0 \dots \mathcal{A}_n^0) \dots (\mathcal{A}_1^{j-1} \dots \mathcal{A}_n^{j-1})\mathcal{B}_j(\mathcal{A}_n^{j-1} \dots \mathcal{A}_1^{j-1}) \dots (\mathcal{A}_n^0 \dots \mathcal{A}_1^0).$$

Cas 1 : $(kl-n)$ impair : on pose $kl-n+1 = 2p$.
Ainsi

$$\mathcal{B}_p = (\mathcal{A}_1^p \dots \mathcal{A}_n^p)(\mathcal{A}_1^{kl-n-p+2} \dots \underline{\mathcal{A}_{n-1}^{kl-n-p+2}}) \dots (\mathcal{A}_1^{kl-p-1}\underline{\mathcal{A}_2^{kl-p-1}})\underline{\mathcal{A}_1^{kl-p}}.$$

Soit

$$\mathcal{B}_p = (\mathcal{A}_1^p \dots \mathcal{A}_{n-1}^p)\mathcal{A}_n^p(\mathcal{A}_1^{kl-n-p+2} \dots \mathcal{A}_{n-2}^{kl-n-p+2}) \dots \mathcal{A}_1^{kl-p-1}(\mathcal{A}_{n-1}^{kl-n-p+2} \dots \mathcal{A}_1^{kl-p}).$$

En utilisant les égalités $\mathcal{A}_{i+1}^p = \mathcal{A}_{i+1}^{kl-p-i}$ $(0 \leq i \leq n-1)$, on obtient

$$\mathcal{B}_p = (\mathcal{A}_1^p \dots \mathcal{A}_{n-1}^p)\mathcal{B}_{p+1}(\mathcal{A}_{n-1}^p \dots \mathcal{A}_1^p)$$

avec

$$\mathcal{B}_{p+1} = \mathcal{A}_n^p(\mathcal{A}_1^{kl-n-p+2} \dots \mathcal{A}_{n-2}^{kl-n-p+2}) \dots (\mathcal{A}_1^{kl-p-2}\mathcal{A}_2^{kl-p-2})\mathcal{A}_1^{kl-p-1}$$

et de même

$$\mathcal{B}_{p+1} = (\mathcal{A}_1^{p+1} \dots \mathcal{A}_{n-3}^{p+1})\mathcal{B}_{p+2}(\mathcal{A}_{n-3}^{p+1} \dots \mathcal{A}_1^{p+1})$$

avec

$$\mathcal{B}_{p+3} = \mathcal{A}_n^p \mathcal{A}_{n-2}^{p+1} (\mathcal{A}_1^{kl-n-p+3} \dots \mathcal{A}_{n-4}^{kl-n-p+3}) \dots \mathcal{A}_1^{kl-p-2}.$$

En poursuivant ce processus, on obtient, en notant :

$$\mathcal{B} = \begin{cases} \mathcal{A}_n^p \mathcal{A}_{n-2}^{p+1} \dots \mathcal{A}_2^{p+\frac{n-2}{2}} & si\ n\ pair \\ \\ \mathcal{A}_n^p \mathcal{A}_{n-2}^{p+1} \dots \mathcal{A}_1^{p+\frac{n-1}{2}} & si\ n\ impair \end{cases}$$

$$\mathcal{B}_0 = (\mathcal{A}_1^0 \dots \mathcal{A}_n^0) \dots (\mathcal{A}_1^{p-1} \dots \mathcal{A}_n^{p-1})(\mathcal{A}_1^p \dots \mathcal{A}_{n-1}^p) \dots \mathcal{B} \dots (\mathcal{A}_{n-1}^p \dots \mathcal{A}_1^p) \dots (\mathcal{A}_n^0 \dots \mathcal{A}_1^0)$$

où $\mathcal{B}$ est une matrice symétrique.

Cas 2 : $(kl-n)$ pair : on pose $kl - n = 2p$.
Une démonstration analogue nous donne :

$$\mathcal{B}_0 = (\mathcal{A}_1^0 \dots \mathcal{A}_n^0) \dots \mathcal{B} \dots (\mathcal{A}_n^0 \dots \mathcal{A}_1^0)$$

où $\mathcal{B}$ est une matrice symétrique, à savoir :

$$\mathcal{B} = \begin{cases} \mathcal{A}_{n-1}^{p+1} \mathcal{A}_{n-3}^{p+2} \dots \mathcal{A}_1^{p+\frac{n}{2}} & si\ (n-1)\ impair \\ \\ \mathcal{A}_{n-1}^{p+1} \mathcal{A}_{n-3}^{p+2} \dots \mathcal{A}_1^{p+\frac{n+1}{2}} & si\ (n-1)\ pair \end{cases},$$

ce qui termine la démonstration de la proposition 1.1.8.

1.2 Rappels sur l'algorithme de Voronoï

1.2.1 Unités d'un corps de nombres

On note :
k un corps de nombres algébriques de degré $n = r_1 + 2r_2$ où r_1 (respectivement $2r_2$) désigne le nombre de plongements réels (respectivement complexes) de k dans $\mathbb{C}$,
$\mathcal{O}$ un ordre de k,
$\mathcal{U}$ le groupe des unités de $\mathcal{O}$.

On rappelle le théorème de Dirichlet suivant :

Théorème 1.2.1 *On a*

$$\mathcal{U} \simeq G \times \mathbb{Z}^r$$

où G est l'ensemble des racines de l'unité qui sont dans $\mathcal{O}$ et $r = r_1 + r_2 - 1$.

Définition 1.2.2 *Une base $\{\epsilon_1, \dots \epsilon_r\}$ de la partie libre de $\mathcal{U}$ est appelée un* **système fondamental d'unités** *de $\mathcal{O}$.*

Ainsi, tout élément ϵ de $\mathcal{U}$ s'écrit de façon unique sous la forme :

$$\epsilon = \zeta \epsilon_1^{n_1} \dots \epsilon_r^{n_r}$$

où ζ est une racine de l'unité dans $\mathcal{O}$ et $n_1, \ldots n_r$ sont des éléments de $\mathbb{Z}$.

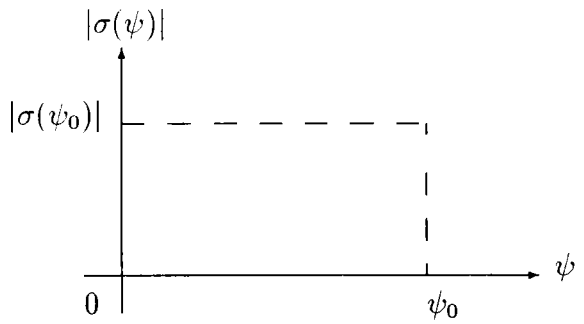
L'algorithme de Voronoï [9] permet de déterminer un système fondamental d'unités dans le cas $n = 3$. On se limitera ici au cas $r_1 = 1$ (le cas $r_1 = 3$ sera traité dans le troisième chapitre).

1.2.2 Notations et Définitions

Soit $K \subseteq \mathbb{R}$ un corps de nombres cubique à conjugués complexes. Soit L un $\mathbb{Z}$-module libre de rang 3 de K de base $\{1, \alpha_1, \alpha_2\}$. On dira que L est un réseau de K et on notera $L =< 1, \alpha_1, \alpha_2 >$. Tout point ψ de L s'écrit $\psi = u + v\alpha_1 + w\alpha_2$ avec (u, v, w) un élément de $\mathbb{Z}^3$.
On note σ et $\overline{\sigma}$ les plongements complexes de K dans $\mathbb{C}$.

Définition 1.2.3 *On dit que $\psi_0 \in L$ est un* **point extrémal** *de L si et seulement si pour tout ϕ de L tel que $0 < \phi < \psi_0$ on a $|\sigma(\phi)| > |\sigma(\psi_0)|$.*

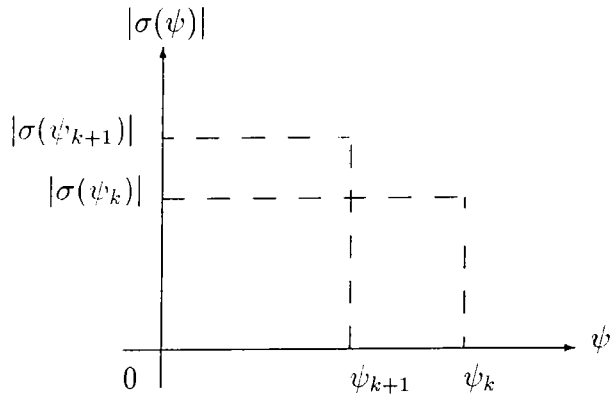
C'est-à-dire que le rectangle ci-dessous (fig.1) ne contient aucun point de L.



(fig.1)

Définition 1.2.4 *Soit k un entier positif, on dit que ψ_{k+1} est le* **point extrémal adjacent** *à ψ_k de* **première espèce** *dans L (fig.2) si et seulement si ψ_{k+1} est tel que*

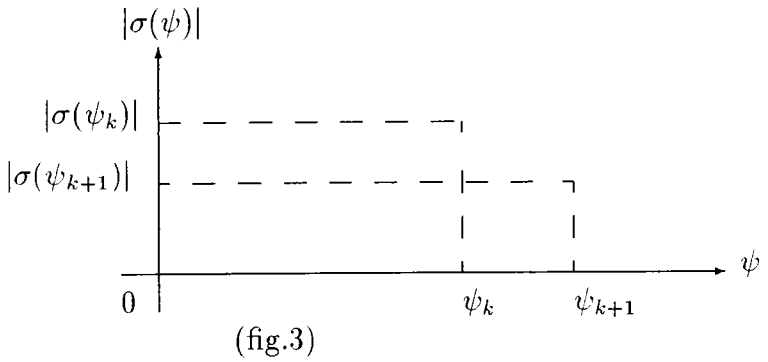
$$\begin{cases} 0 < \psi_{k+1} < \psi_k \\ |\sigma(\psi_{k+1})| = min\{|\sigma(\psi)| \text{ tel que } 0 < \psi < \psi_k,\ \psi \in L \text{ et } \psi \neq 0\} \end{cases}$$



(fig.2)

Définition 1.2.5 *Soit k un entier positif, on dit que ψ_{k+1} est le* **point extrémal adjacent** *à ψ_k de* **deuxième espèce** *dans L (fig.3) si et seulement si*

$$\psi_{k+1} = \min\{\psi \text{ tel que } \psi > \psi_k \text{ et } |\sigma(\psi)| < |\sigma(\psi_k)|\}.$$



(fig.3)

Définition 1.2.6 *Un réseau L est* **réduit** *si et seulement si 1 est un point extrémal de L.*

1.2.3 Périodicité et unité fondamentale

Si L est un réseau réduit, on peut construire la suite décroissante (respectivement croissante) de points extrémaux adjacents de première (respectivement deuxième) espèce par :

$$\begin{cases} \psi_0 = 1 \\ \\ \psi_{k+1} \text{ est le point extrémal adjacent à } \psi_k \text{ de première} \\ \qquad \text{(respectivement deuxième) espèce si } k \geq 0. \end{cases}$$

Par Voronoï [9] on sait que cette suite est purement périodique de la forme:

$$\ldots, \overbrace{\epsilon^2\psi_{l-1}, \ldots, \epsilon^2}, \overbrace{\epsilon\psi_{l-1}, \ldots, \epsilon\psi_1, \epsilon = \psi_l}, \overbrace{\psi_{l-1}, \ldots, \psi_0 = 1} \quad (1^e \text{ espèce})$$

$$\overbrace{1=\psi_0,\ldots,\psi_{l-1}},\overbrace{\psi_l=\epsilon^{-1},\epsilon^{-1}\psi_1,\ldots,\epsilon^{-1}\psi_{l-1}},\overbrace{\epsilon^{-2},\ldots,\epsilon^{-2}\psi_{l-1}},\ldots \quad (2^e \text{ espèce})$$

où ϵ est l'unité fondamentale de L inférieure à 1 et l désigne la longueur de la période.

1.2.4 Méthode de construction de points extrémaux

Pour construire une suite de points extrémaux, il suffit de savoir construire le point extrémal adjacent à 1 dans un réseau réduit. On décrit ici la méthode due à Voronoï [9] [28] qui permet de construire la suite de points extrémaux adjacents de première espèce. Soit L_0 un réseau réduit de K. Dans L_0 on détermine $\theta_g^0 = \psi_1$ le point extrémal adjacent à 1 (de première espèce) et un point θ_h^0 tel que $|\sigma(\theta_h^0)|$ soit petit et tel que $\{\theta_g^0, \theta_h^0, 1\}$ soit une base de L_0.

Dire que ψ_2 est le point extrémal adjacent à ψ_1 dans L_0 équivaut à dire que $\frac{\psi_2}{\psi_1}$ est le point extrémal adjacent à 1 dans $\frac{L_0}{\psi_1}$. Ainsi, pour déterminer ψ_2, on définit $L_1 = \frac{L_0}{\psi_1} =< 1, \frac{\theta_h^0}{\theta_g^0}, \frac{1}{\theta_g^0} >$, on cherche θ_g^1 le point extrémal adjacent à 1 dans L_1 et on aura $\frac{\psi_2}{\psi_1} = \theta_g^1$ c'est-à-dire $\psi_2 = \theta_g^1 \psi_1$.

On itère ce processus. On suppose que l'on connaît la suite des points extrémaux jusqu'à ψ_k. Pour déterminer ψ_{k+1} on considère le réseau réduit $L_k =< 1, \frac{\theta_h^{k-1}}{\theta_g^{k-1}}, \frac{1}{\theta_g^{k-1}} >$.

(1) Dans ce réseau on détermine θ_g^k le point extrémal adjacent à 1 de première espèce, c'est-à-dire que θ_g^k est le point de L_k tel que

$$\begin{cases} 0 < \theta_g^k < 1 \\ |\sigma(\theta_g^k)| = \min\{|\sigma(\psi)| \text{ tel que } 0 < \psi < 1,\ \psi \in L_k \text{ et } \psi \neq 0\} \end{cases}.$$

On aura alors $\frac{\psi_{k+1}}{\psi_k} = \theta_g^k$ c'est-à-dire $\psi_{k+1} = \theta_g^k \psi_k$.

(2) On choisit alors un élément θ_h^k de L_k tel que $|\sigma(\theta_h^k)|$ soit petit et tel que $\{\theta_g^k, \theta_h^k, 1\}$ soit une base de L_k.

On pose $L_{k+1} =< 1, \frac{\theta_h^k}{\theta_g^k}, \frac{1}{\theta_g^k} >$.

On obtient ainsi une suite décroissante de points extrémaux adjacents à 1 de première espèce. Cette suite est périodique et si l désigne la longueur de la période, c'est-à-dire le plus petit entier strictement positif tel que $\theta_g^l = \theta_g^0$, alors une unité fondamentale de $\mathcal{O} = L_0$ est $\epsilon = \prod_{k=0}^{l-1} \theta_g^k$.

Pour cette construction le problème essentiel est la détermination de θ_g^k. Pour cela, Voronoï réduit la base de L_k de manière à n'avoir plus que trois points à considérer dans la base réduite: parmi ces trois points, on choisit θ_g^k comme étant celui qui rend $|\sigma(\psi)|$ minimum.

Dans [29], Williams décrit une méthode analogue pour construire une suite de points extrémaux adjacents de deuxième espèce.
Ainsi, à chaque étape, il s'agit dans un réseau réduit L_k de déterminer θ_g^k le point extrémal adjacent à 1 de deuxième espèce, c'est-à-dire que θ_g^k est le point de L_k tel que
$$\begin{cases} |\sigma(\theta_g^k)| < 1 \\ \\ \theta_g^k \quad \text{minimum} \end{cases}.$$
Pour cela, on réduit la base de L_k de manière à n'avoir plus que dix points à considérer parmi lesquels on choisit le minimum.

CHAPITRE 2

Familles infinies de développements

C. Levesque et G. Rhin [20] ont étudié deux familles infinies de corps $\mathbb{Q}(\alpha)$ dépendant chacune de deux paramètres et ont donné, pour chacune d'elles, le développement par l'AJP d'un vecteur à composantes dans $\mathbb{Q}(\alpha)$. Ces développements étant périodiques (la longueur de la période tendant vers l'infini) ils ont ainsi obtenu une unité de ces corps et ont conjecturé que cette unité était fondamentale dans l'ordre $\mathbf{Z}[\alpha]$.
Ces familles ont également été étudiées par A. Fahrane [12] qui, le premier, a montré la fondamentalité de cette unité pour l'une des familles lorsque l'un des paramètres est suffisamment grand (ce résultat n'est pas effectif), par S. Louboutin [22] qui a montré que cette unité était une puissance bornée (la borne étant indépendante des paramètres) de l'unité fondamentale de l'ordre $\mathbf{Z}[\alpha]$, ainsi que par J. Kühner [16] qui donne également le développement par l'algorithme de Voronoï pour une de ces familles.
Après avoir rappelé les résultats obtenus par C. Levesque et G. Rhin nous allons, dans ce chapitre :

- étudier le lien entre le développement par l'AJP et par l'algorithme de Voronoï de ces deux familles : ce qui nous permettra de prouver la fondamentalité de l'unité obtenue par l'AJP pour toutes les valeurs positives des paramètres.
- généraliser ces deux familles à des familles infinies de corps $\mathbb{Q}(\alpha)$ de degré quelconque pour lesquelles nous donnerons le développement par l'AJP d'un vecteur à composantes dans $\mathbb{Q}(\alpha)$.

2.1 Rappels des résultats obtenus par C. Levesque et G. Rhin

2.1.1 Première famille

Soit $c \geq 2$ et $m \geq 1$ deux entiers, on considère le polynôme :

$$f(X) = X^3 - c^m X^2 - (c-1)X - c^m.$$

$f(X)$ est irréductible, admet une racine réelle, notée α, unique et on a le théorème suivant :

Théorème 2.1.1 *Le développement par l'AJP de* $(\alpha_1, \alpha_2) = (\alpha^2 - c^m\alpha, \alpha)$ *est purement périodique de longueur* $l = 3m + 1$ *et* $\epsilon = \alpha\left(\frac{\alpha}{\alpha - c^m}\right)^m$ *est l'unité de* $\mathbb{Q}(\alpha)$ *fournie par ce développement.*

2.1.2 Deuxième famille

Soit $c \geq 2$ et $m \geq 1$ deux entiers, on considère le polynôme :

$$f(X) = X^3 - (c^m + c - 1)X^2 - (c^m - 1)X - c^m.$$

$f(X)$ est irréductible, admet une racine réelle, notée α, unique et on a le théorème suivant:

Théorème 2.1.2 *Le développement par l'AJP de* $(\alpha_1, \alpha_2) = (\alpha^2 - (c^m + c - 1)\alpha, \alpha)$ *est purement périodique de longueur* $l = 4m + 1$ *et* $\epsilon = \alpha\left(\frac{\alpha^2}{\alpha - c^m}\right)^m$ *est l'unité de* $\mathbb{Q}(\alpha)$ *fournie par ce développement.*

Remarque : Pour chacune de ces familles, ces développements sont symétriques.

2.2 Algorithme de Voronoï et comparaison avec l'AJP

2.2.1 Méthode de recherche de points extrémaux

On décrit ici une méthode qui permet dans certains cas de déterminer une suite croissante de points extrémaux. On sait que pour déterminer une telle suite il suffit de savoir construire le point extrémal adjacent à 1 de deuxième espèce dans un réseau réduit $L =< 1, \alpha_1, \alpha_2 >$.
Ainsi on cherche un élément $\psi = u + v\alpha_1 + w\alpha_2$ de L tel que

$$\begin{cases} \psi > 1 \\ |\sigma(\psi)| < 1 \\ \psi \text{ minimum} \end{cases}$$

Notons $F(u, v, w) = |\sigma(\psi)|^2$. F définit une forme quadratique à trois variables u, v, w à coefficients réels, positive de rang 2. On va dans ce paragraphe énoncer une proposition qui, utilisant un vecteur isotrope de cette forme quadratique, nous permet de restreindre à 5 au maximum le nombre de choix pour un point extrémal adjacent à 1.
Un avantage de cette méthode est qu'une réduction de la base n'est plus nécessaire à chaque étape.

On supposera dans la suite du paragraphe que $(\gamma_2, 1, \gamma_1)$ est un vecteur isotrope de F

et on pose

$$\begin{array}{ll}
\phi_1 = [\gamma_2] + \alpha_1 & Q_1 = ([\gamma_2], 1, 0) \\
\phi_2 = [\gamma_2] + \alpha_1 + \alpha_2 & Q_2 = ([\gamma_2], 1, 1) \\
\phi_3 = [\gamma_2] + \alpha_1 - \alpha_2 & Q_3 = ([\gamma_2], 1, -1) \\
\phi_4 = [\gamma_2] - 1 + \alpha_1 & Q_4 = ([\gamma_2] - 1, 1, 0) \\
\phi_5 = [\gamma_2] - 1 + \alpha_1 + \alpha_2 & Q_5 = ([\gamma_2] - 1, 1, 1) \\
\phi_6 = [\gamma_2] + 1 + 2\alpha_1 - \alpha_2 & Q_6 = ([\gamma_2] + 1, 2, -1) \\
\phi_7 = [\gamma_2] + 2\alpha_1 & Q_7 = ([\gamma_2], 2, 0) \\
\phi_8 = [\gamma_2] + 1 + \alpha_1 - \alpha_2 & Q_8 = ([\gamma_2] + 1, 1, -1)
\end{array}$$

où $[x]$ désigne la partie entière du réel x.

Lemme 2.2.1 *Si $0 < \alpha_1 < 1$ et $0 < \alpha_2 < 1$ on remarque que l'on a*

$$\begin{cases}
\phi_4 < \phi_3 < \phi_1 < \phi_2 \\
\phi_4 < \phi_5 < \phi_1 < \phi_2 \\
\phi_1 < \phi_7 < \phi_6 \\
\phi_1 < \phi_8 < \phi_6
\end{cases}$$

et

$$\begin{cases}
\text{si } \alpha_2 < \alpha_1 \text{ alors } \phi_2 < \phi_7 \\
\text{si } 2\alpha_2 - 1 < \alpha_1 < \alpha_2 \text{ alors } \phi_7 < \phi_2 < \phi_6 \\
\text{si } \alpha_1 < 2\alpha_2 - 1 \text{ alors } \phi_7 < \phi_6 < \phi_2 \\
\text{si } 2\alpha_2 - 1 < 0 \text{ alors } \phi_2 < \phi_8.
\end{cases}$$

Lemme 2.2.2 *Soit F une forme quadratique à trois variables u, v, w, à coefficients réels, positive de rang 2 telle que*

$$F(1,0,0) = 1 \text{ et } F(0,0,1) > 1.$$

Si F admet un vecteur isotrope $(\gamma_2, 1, \gamma_1)$ alors F s'écrit :

$$F(u,v,w) = a(w - \gamma_1 v)^2 + 2b(w - \gamma_1 v)(u - \gamma_2 v) + (u - \gamma_2 v)^2 \qquad (2.1)$$

et

$$F(u,v,w) = \frac{a}{2}[w - (\gamma_1 + 2\frac{b}{a}\gamma_2)v + 2\frac{b}{a}u]^2 + \frac{a}{2}(w - \gamma_1 v)^2 + (1 - 2\frac{b^2}{a})(u - \gamma_2 v)^2 \qquad (2.2)$$

avec $a > 1$ et $b^2 < a$.

Preuve

Soit M la matrice de la forme polaire associée à F. M s'écrit :

$$M = \begin{pmatrix} 1 & a_{12} & a_{13} \\ a_{12} & a_{22} & a_{23} \\ a_{13} & a_{23} & a_{33} \end{pmatrix}$$

avec $a_{33} > 1$.

On a

$$\begin{cases}
a_{12} = -\gamma_2 - \gamma_1 a_{13} \\
a_{22} = (\gamma_2)^2 + 2\gamma_1\gamma_2 a_{13} + a_{33}(\gamma_1)^2 \\
a_{23} = -a_{13}\gamma_2 - a_{33}\gamma_1
\end{cases}$$

car $(\gamma_2, 1, \gamma_1)$ est un vecteur isotrope de F.
En posant : $a = a_{33}$ et $b = a_{13}$ on obtient les formules (2.1) et (2.2).
F étant une forme positive de rang 2, on a $b^2 < a$.

Proposition 2.2.3 *Si* $0 < \gamma_1 < 1$, $\gamma_2 > 1$, $0 < \alpha_1 < 1$, $0 < \alpha_2 < 1$ *et* $4b^2 < a$ *on a*

1. *Si* $F(Q_1) < 1$
   a. *si* $b < 0$ *alors le point extrémal adjacent à 1 est* ϕ_1,φ_3 *ou* ϕ_4
   b. *si* $b \geq 0$ *alors le point extrémal adjacent à 1 est* ϕ_1 *ou* ϕ_5
2. *Si* $F(Q_1) > 1$ *et* $F(Q_2) < 1$
   a. *si* $b < 0$ *alors le point extrémal adjacent à 1 est :*
      i. ϕ_2,ϕ_3 *ou* ϕ_4 *si* $\alpha_2 < \alpha_1$
      ii. ϕ_2,ϕ_3,ϕ_4 *ou* ϕ_7 *si* $2\alpha_2 - 1 < \alpha_1 < \alpha_2$
      iii. ϕ_2,ϕ_3,ϕ_4,ϕ_6 *ou* ϕ_7 *si* $\alpha_1 < 2\alpha_2 - 1$
   b. *si* $b \geq 0$ *alors le point extrémal adjacent à 1 est :*
      i. ϕ_2 *ou* ϕ_5 *si* $2\alpha_2 - 1 < 0$
      ii. ϕ_2,ϕ_5 *ou* ϕ_8 *si* $2\alpha_2 - 1 > 0$.

Remarque 2.2.4 *Une condition suffisante pour avoir* $4b^2 < a$ *est* $|2b| < 1$ *(car* $a > 1$*).*

Preuve de la proposition 2.2.3 On note $\psi = u + v\alpha_1 + w\alpha_2$ le point extrémal adjacent à 1 et $P = (u, v, w)$ l'élément de $\mathbb{Z}^3$ correspondant.

1. On suppose d'abord que $F(Q_1) < 1$.

   a. Montrons que v est non nul. Si $v = 0$ on a :
   si $u = 0$ alors $F(P) = aw^2 > 1$, si $w = 0$ alors $F(P) = u^2 \geq 1$, et
   si $u \neq 0$ et $w \neq 0$ alors $F(P) > \frac{a}{2} + (1 - 2\frac{b^2}{a}) > 1$
   ce qui est impossible.

   b. Montrons que si $\psi \neq \phi_3$ alors u, v, w sont tous positifs ou nuls.
   On a $(u - \gamma_2 v)^2 < 2$ car $F(P) < 1$ et $4b^2 < a$, or $\gamma_2 > 1$ donc $uv \geq 0$. On a $(w - \gamma_1 v)^2 < 2$ donc $wv \geq 0$ ou $|w| \leq 1$.
   Si $wv \geq 0$, $v < 0$ entraîne $u \leq 0$ et $w \leq 0$ ce qui est impossible car $\psi > 0$, donc on a $v > 0$, $u \geq 0$ et $w \geq 0$.
   Si $wv < 0$ alors $|w| = 1$. Si $w = 1$ alors $v < 0$ et $u \leq 0$. Si $u = 0$ on a $F(P) > \frac{a}{2} + (1 - 2\frac{b^2}{a}) > 1$ et si $u < 0$ on a $\psi < 0$ ce qui est impossible.
   Si $w = -1$, $v > 0$, $u \geq 0$ et $(w - \gamma_1 v)^2 > 1$ et si $u < [\gamma_2 v]$ alors $(u - \gamma_2 v)^2 \geq 1$ et $F(P) > 1$, si $u = [\gamma_2 v]$ alors $\psi = \phi_3$ ou $\psi > \phi_1$, et si $u \geq [\gamma_2 v] + 1$ alors $\psi > \phi_1$.
   Ainsi $wv < 0$ entraîne $\psi = \phi_3$.
   On a donc démontré que si $\psi \neq \phi_3$ alors $v > 0$ et u et w sont positifs ou nuls.

c. Montrons que $v = 1$.
Si $v \geq 2$ on a $(u - \gamma_2 v)^2 < 2$ donc $u > 2[\gamma_2] - \sqrt{2}$ et $u \geq [\gamma_2]$, donc $\psi > \phi_1$.

d. Etude de u et w.
On a $(u - \gamma_2 v)^2 < 2$ donc $u \geq [\gamma_2] - 1$.
Montrons que $w < 2$.
Si $w \geq 2$ et $u \geq [\gamma_2]$ alors $\psi > \phi_2 > \phi_1$ et si $u = [\gamma_2] - 1$ alors $(u - \gamma_2 v)^2 > 1$ et $(w - \gamma_1 v)^2 > 1$ donc $F(P) > 1$.
Si $u \geq [\gamma_2] + 1$ alors $\psi > \phi_2 > \phi_1$.
Dans le cas où $w = 1$, si $u = [\gamma_2 v]$ alors $\psi > \phi_1$ donc $u = [\gamma_2] - 1$ et $v = \phi_5$.
Dans le cas où $w = 0$, si $u = [\gamma_2 v]$ alors $\psi = \phi_1$ et si $u = [\gamma_2] - 1$ alors $\psi = \phi_4$.

De plus si $b < 0$ on a $F(Q_5) > 1$ et si $b \geq 0$ on a $F(Q_3) > 1$ et $F(Q_4) > 1$ ce qui démontre la première partie de la proposition.

2. Supposons maintenant que $F(Q_1) > 1$ et $F(Q_2) < 1$.
De même que précédemment on a $u \geq 0$, $v > 0$ et $w \geq 1$.

a. Montrons que $v \leq 2$.
Si $v \geq 3$ on a $u \geq [\gamma_2] + 1$ et si $w \geq 0$ alors $\psi > \phi_2$. Si $w = -1$ et $u > [\gamma_2] + 1$ alors $\psi > \phi_2$ et si $u = [\gamma_2] + 1$ on a $(u - \gamma_2 v)^2 > 1$ et $(w - \gamma_1 v)^2 > 1$ donc $F(P) > 1$. Ainsi $v = 1$ ou $v = 2$.

b. Le cas $v = 1$. De même que dans la démonstration de la première partie on a $u \geq [\gamma_2] - 1$ et $w < 2$.
Si $w = 1$, si $u > [\gamma_2]$ alors $\psi > \phi_2$, si $u = [\gamma_2]$ alors $\psi = \phi_2$ et si $u = [\gamma_2] - 1$ alors $\psi = \phi_5$.
Si $w = 0$, si $u > [\gamma_2]$ alors $\psi > \phi_2$, si $u = [\gamma_2]$ alors $\psi = \phi_1$ et si $u = [\gamma_2] - 1$ alors $\psi = \phi_4$.
Si $w = -1$, si $u > [\gamma_2] + 1$ alors $\psi > \phi_2$, si $u = [\gamma_2] + 1$ alors $\psi = \phi_8$, si $u = [\gamma_2]$ alors $\psi = \phi_3$ et si $u = [\gamma_2] - 1$ on a $(w - \gamma_1 v)^2 > 1$ et $(u - \gamma_2 v)^2 > 1$ donc $F(P) > 1$.

c. Le cas $v = 2$. On a alors $u \geq [\gamma_2]$.
Si $w \geq 1$ alors $\psi > \phi_2$.
Si $w = 0$, si $u > [\gamma_2]$ alors $\psi > \phi_2$ et si $u = [\gamma_2]$ alors $\psi = \phi_7$.
Si $w = -1$, si $u > [\gamma_2] + 1$ alors $\psi > \phi_2$, si $u = [\gamma_2] + 1$ alors $\psi = \phi_6$ et si $u = [\gamma_2]$ alors $(w - \gamma_1 v)^2 > 1$ et $(u - \gamma_2 v)^2 > 1$ donc $F(P) > 1$.

De plus si $b < 0$ on a $F(Q_5) > 1$ et $F(Q_8) > 1$ et si $b \geq 0$ on a $F(Q_3) > 1$, $F(Q_4) > 1$, $F(Q_7) > 1$ et $F(Q_6) > 1$ ce qui démontre la deuxième partie de la proposition.

Cette proposition va nous permettre de donner explicitement la suite croissante des points extrémaux du développement par l'algorithme de Voronoï pour les deux familles précédentes.

2.2.2 Application à la première famille

Soit $c \geq 2$ et $m \geq 1$ deux entiers, on considère le polynôme:

$$f(X) = X^3 - c^m X^2 - (c-1)X - c^m.$$

Théorème 2.2.5 *Soit α la racine réelle du polynôme $f(X)$, $K = \mathbb{Q}(\alpha)$ et $\mathcal{O} = \mathbb{Z}[\alpha]$.*

i) La suite des points extrémaux de $\mathcal{O}$ est: pour $0 \leq s \leq m-1$

$$\psi_0 = 1 \ , \psi_{3s+1} = \alpha \left(\frac{\alpha}{\alpha - c^m}\right)^s \ , \psi_{3s+2} = \alpha^2 \left(\frac{\alpha}{\alpha - c^m}\right)^s \ , \psi_{3s+3} = \left(\frac{c\alpha}{\alpha - c^m}\right)^{s+1}$$

$$\text{et } \psi_{3m+1} = \alpha \left(\frac{\alpha}{\alpha - c^m}\right)^m.$$

ii) L'unité fondamentale de $\mathcal{O}$ est $\epsilon = \alpha \left(\frac{\alpha}{\alpha - c^m}\right)^m$ et la longueur de la période du développement par l'algorithme de Voronoï est $l = 3m+1$.

Preuve du théorème

Pour cette démonstration on sera amené à utiliser les formules suivantes:

$$c^m < \alpha < c^m + \frac{c}{\alpha}$$

et

$$1 + \frac{1}{\alpha^2} = \frac{c}{\alpha(\alpha - c^m)}.$$

Soit $L =< 1, \alpha_1, \alpha_2 >$ un réseau de K et ψ le point extrémal adjacent à 1 dans L. En notant $\psi = u + v\alpha_1 + w\alpha_2$ on a les lemmes suivants:

Lemme 2.2.6 *Pour un entier s, $0 \leq s \leq m$*

$$\text{si } L =< 1, \alpha - c^m, \frac{c^s}{\alpha} > \text{ alors } (u,v,w) = (c^m, 1, 0).$$

Preuve
On vérifie dans ce cas que F est une forme quadratique positive de rang 2 qui s'écrit à l'aide des formules (2.1) et (2.2) avec:

$$a = \frac{\alpha}{c^{m-2s}} \ , b = -\frac{\alpha(\alpha - c^m)}{2c^{m-s}} \ , \gamma_2 = \alpha \ , \gamma_1 = \frac{c^{m-s}}{\alpha}.$$

On a $0 < \gamma_1 < 1$, $\gamma_2 > 1$, $0 < \alpha_1 < 1$, $0 < \alpha_2 < 1$ et $4b^2 < a$ car

$$\frac{4b^2}{a} = \frac{\alpha(\alpha - c^m)^2}{c^m} < 1.$$

En reprenant les notations du paragraphe 3.2.1, on a $\phi_1 = \alpha$ donc

$$F(Q_1) = \frac{N(\alpha)}{\alpha} = \frac{c^m}{\alpha} < 1 \text{ et } b < 0.$$

D'après la proposition 2.2.3 le point extrémal adjacent à 1 est ϕ_1, ϕ_3 ou ϕ_4.
Or $Q_3 = (c^m, 1, -1)$ et l'on a, d'après (2.2)

$$F(Q_3) > \frac{\alpha}{2c^{m-2s}}(1 + \frac{c^{m-s}}{\alpha})^2 > \frac{\alpha}{2c^{m-2s}} + c^s + \frac{c^m}{2\alpha} > c^s \geq 1.$$

Enfin $\phi_4 = \alpha - 1$ et

$$F(Q_4) = \frac{N(\alpha - 1)}{\alpha - 1} = \frac{2c^m + c - 2}{\alpha - 1} > \frac{2c^m + c - 2}{c^m} > 1.$$

Donc $\psi = \phi_1$ c'est-à-dire $(u, v, w) = (c^m, 1, 0)$.

Lemme 2.2.7 *Pour un entier* s, $0 \leq s \leq m - 1$

$$\text{si } L =< 1, \frac{c^s}{\alpha^2}, \frac{1}{\alpha} > \text{ alors } (u, v, w) = (c^s, 1, 0).$$

Preuve
En procédant de la même façon que pour le lemme 2.2.6 on a :

$$a = \frac{\alpha}{c^m}, b = -\frac{\alpha(\alpha - c^m)}{2c^m}, \gamma_2 = \frac{c^s\alpha}{c^m}, \gamma_1 = \frac{c^s\alpha}{c^m}(\alpha - c^m)$$

et $0 < \gamma_1 < 1$, $\gamma_2 > 1$, $0 < \alpha_1 < 1$, $0 < \alpha_2 < 1$.
De plus

$$|2b| = \frac{\alpha(\alpha - c^m)}{c^m} < 1.$$

On peut donc utiliser la proposition 2.2.3.
On a $\phi_1 = \dfrac{c^{s+1}}{\alpha(\alpha - c^m)}$ et $N(\alpha - c^m) = c^{m+1}$ donc

$$F(Q_1) = \frac{\alpha(\alpha - c^m)}{c^{2m-2s-1}} < 1 \text{ et } b < 0.$$

On a $Q_3 = (c^s, 1, -1)$ et d'après (2.2)

$$F(Q_3) > \frac{\alpha}{2c^m}\left((1 + c^s(\alpha - c^m))^2 + (1 + \frac{c^s\alpha}{c^m}(\alpha - c^m))^2\right) > 1.$$

On a $Q_4 = (c^s - 1, 1, 0)$ et d'après (2.1)

$$F(Q_4) = \frac{\alpha}{c^m}(\gamma_1)^2 + \frac{\alpha(\alpha - c^m)}{c^m}\gamma_1\left(c^s - 1 - \frac{c^s\alpha}{c^m}\right) + \left(1 + \frac{c^s(\alpha - c^m)}{c^m}\right)^2.$$

En développant les deux derniers termes, on obtient

$$F(Q_4) = 1 + \frac{\alpha^2(\alpha - c^m)^2}{c^{2m-s}}(c^s - 1) + \frac{2c^s(\alpha - c^m)}{c^m} + \frac{c^{2s}}{c^{2m}}(\alpha - c^m)^2 > 1.$$

Donc $\psi = \phi_1$ c'est-à-dire $(u, v, w) = (c^s, 1, 0)$.

Lemme 2.2.8 *Pour un entier s, $0 \leq s \leq m-1$*

$$si\ L =< 1, \frac{\alpha - c^m}{c^{s+1}}, \frac{\alpha(\alpha - c^m)}{c^{s+1}} >\ alors\ (u,v,w) = (c^{m-1-s}, 1, 0).$$

Preuve
En procédant de la même façon que précédemment on a :

$$a = \frac{c^{2m-2s-1}}{\alpha(\alpha - c^m)}\ .\ b = \frac{c^{m-s-1}}{2}(\frac{c-1}{c^m} - \frac{1}{\alpha})\ .\ \gamma_2 = \frac{c^{m-s}}{\alpha(\alpha - c^m)}\ ,\ \gamma_1 = \frac{1}{\alpha}$$

et $0 < \gamma_1 < 1$, $\gamma_2 > 1$, $0 < \alpha_1 < 1$, $0 < \alpha_2 < 1$.
De plus

$$|2b| = c^{m-s-1}(\frac{c-1}{c^m} - \frac{1}{\alpha}) < c^{-s} \leq 1.$$

On peut donc utiliser la proposition 2.2.3.
On a

$$\phi_1 = \frac{\alpha}{c^{s+1}} \text{ et } F(Q_1) = \frac{c^{m-2s-2}}{\alpha} < 1 \text{ et } b > 0$$

donc $\psi = \phi_1$ ou $\psi = \phi_5$.
En utilisant la formule (2.1) pour $F(Q_5)$ et $F(Q_1)$ on a

$$F(Q_5) = F(Q_1) + 1 + (a - 2a\gamma_1 - 2b) + (2\{\gamma_2\} - 2b\{\gamma_2\}) + 2b\gamma_1$$

où $\{\gamma_2\} = \gamma_2 - [\gamma_2]$.
Montrons que $a - 2a\gamma_1 - 2b > 0$. On a

$$\frac{b}{c^{m-s-1}} < \frac{1}{2c^{m-1}} \text{ donc } \frac{a - 2a\gamma_1 - 2b}{c^{m-s-1}} > \frac{c^{m-s}}{\alpha(\alpha - c^m)}(1 - \frac{2}{\alpha}) - \frac{1}{c^{m-1}}.$$

Puisque $\frac{c}{\alpha(\alpha - c^m)} = 1 + \frac{1}{\alpha^2}$ on a

$$\frac{a - 2a\gamma_1 - 2b}{c^{m-s-1}} > c^{m-s-1} - 2\frac{c^{m-s-1}}{\alpha} + \frac{c^{m-s-1}}{\alpha^2}(1 - \frac{2}{\alpha}) - \frac{1}{c^{m-1}}.$$

Si $s < m-1$, $c^{m-1-s} \geq 2$, $2\frac{c^{m-s-1}}{\alpha} < 1$ et $\frac{1}{c^{m-1}} \leq 1$ donc $a - 2a\gamma_1 - 2b > 0$.
Si $s = m-1$, $a - 2a\gamma_1 - 2b = (1 + \frac{1}{c^{m-1}}) + (\frac{1}{\alpha^2} - \frac{2}{\alpha^3}) + (\frac{1}{c^m} - \frac{1}{\alpha}) > 0$.
De plus $2\{\gamma_2\} - 2b\{\gamma_2\} > 0$ donc $F(Q_5) > 1$.
On en conclut que $\psi = \phi_1$ c'est-à-dire $(u,v,w) = (c^{m-1-s}, 1, 0)$.

A l'aide de ces lemmes, on démontre par récurrence le théorème de la façon suivante:
Soit $L_0 =< 1, \alpha - c^m, \frac{c^m}{\alpha} >$. Par le lemme 2.2.6 on a $\psi_1 = \alpha$.
On choisit un point auxiliaire ϕ_1 tel que $\{\psi_1, \phi_1, \psi_0\}$ soit une base de L_0, à savoir, $\phi_1 = \alpha(\alpha - c^m)$.
Pour déterminer ψ_2 on cherche le point extrémal adjacent à 1 dans le réseau
$L_1 =< 1, \frac{\phi_1}{\psi_1}, \frac{\psi_0}{\psi_1} >=< 1, \alpha - c^m, \frac{1}{\alpha} >$ et par le même lemme 2.2.6 on a : $\frac{\psi_2}{\psi_1} = \alpha$ c'est-à

-dire: $\psi_2 = \alpha^2$.
En poursuivant ce processus, on obtient pour $0 \leq s \leq m-1$ les résultats donnés dans le tableau qui suit :

k	$L_k =< 1, \frac{\phi_k}{\psi_k}, \frac{\psi_{k-1}}{\psi_k} >$	$\frac{\psi_{k+1}}{\psi_k}$	$\frac{\phi_{k+1}}{\psi_k}$
0	$< 1, \alpha - c^m, \frac{c^m}{\alpha} >$	$(c^m, 1, 0)$	$(c-1, 0, 1)$
$3s+1$	$< 1, \alpha - c^m, \frac{c^s}{\alpha} >$	$(c^m, 1, 0)$	$(0, 0, 1)$
$3s+2$	$< 1, \frac{c^s}{\alpha^2}, \frac{1}{\alpha} >$	$(c^s, 1, 0)$	$(0, 0, 1)$
$3s+3$	$< 1, \frac{\alpha - c^m}{c^{s+1}}, \frac{\alpha(\alpha - c^m)}{c^{s+1}} >$	$(c^{m-1-s}, 1, 0)$	$(0, 0, 1)$

On a noté

$$\phi_0 = \alpha - c^m \ , \ \psi_{-1} = \frac{c^m}{\alpha}$$

et les troisième et quatrième colonnes donnent les coordonnées de $\frac{\psi_{k+1}}{\psi_k}$ et de $\frac{\phi_{k+1}}{\psi_k}$ dans le réseau L_k.
A l'aide des quotients successifs $\frac{\psi_{k+1}}{\psi_k}$ on peut facilement déterminer la suite des points extrémaux ψ_k de $\mathbb{Z}[\alpha]$.

On en déduit que

$$\psi_{3m+1} = \alpha \left(\frac{\alpha}{\alpha - c^m} \right)^m .$$

On a

$$N(\psi_{3m+1}) = 1 \text{ et } N(\psi_i) \neq 1 \text{ si } 0 < i \leq 3m.$$

Donc ψ_{3m+1} est l'unité fondamentale ϵ de $\mathcal{O}$ et la longueur de la période du développement de l'algorithme de Voronoï est $l = 3m + 1$.

2.2.3 Application à la deuxième famille

Soit $c \geq 2$ et $m \geq 1$ deux entiers, on considère le polynôme :

$$f(X) = X^3 - (c^m + c - 1)X^2 - (c^m - 1)X - c^m$$

Théorème 2.2.9 *Soit α la racine réelle du polynôme $f(X)$, $K = \mathbb{Q}(\alpha)$ et $\mathcal{O} = \mathbf{Z}[\alpha]$.*

i) La suite des points extrémaux de $\mathcal{O}$ est :

$$\psi_0 = 1 \ , \psi_1 = \alpha \ , \psi_2 = \alpha^2 \ , \psi_3 = \frac{c\alpha^2}{\alpha - c^m}$$

$$\psi_{4t} = \alpha \left(\frac{\alpha^2}{\alpha - c^m}\right)^t \ , \psi_{4t+1} = \alpha^2 \left(\frac{\alpha^2}{\alpha - c^m}\right)^t \quad \text{pour } 1 \leq t \leq m-1$$

$$\psi_{4t+2} = \frac{\alpha(c^{t+1} - 1) + c^m}{\alpha - c^m} \alpha \left(\frac{\alpha^2}{\alpha - c^m}\right)^t \ , \psi_{4t+3} = \left(\frac{c\alpha^2}{\alpha - c^m}\right)^{t+1} \quad \text{pour } 1 \leq t \leq m-2$$

$$\text{et } \psi_{4m-2} = \left(\frac{c\alpha^2}{\alpha - c^m}\right)^m \ , \psi_{4m-1} = \alpha \left(\frac{\alpha^2}{\alpha - c^m}\right)^m .$$

ii) L'unité fondamentale de $\mathcal{O}$ est $\epsilon = \alpha \left(\frac{\alpha^2}{\alpha - c^m}\right)^m$ et la longueur de la période du développement de l'algorithme de Voronoï est $l = 4m - 1$.

Preuve du théorème

Pour cette démonstration on sera amené à utiliser les formules suivantes :

$$c_2 < \alpha < c_2 + \frac{c^m}{\alpha}$$

et

$$1 + \frac{1}{\alpha} + \frac{1}{\alpha^2} = \frac{c}{\alpha - c^m}$$

en notant $c_2 = c^m + c - 1$.
Avec les mêmes notations que celles définies précédemment on a les lemmes suivants :

Lemme 2.2.10 *Pour un entier t, $0 \leq t \leq m$*

$$\text{si } L =< 1, \alpha - c_2, \frac{c^t}{\alpha} > \text{ alors } (u, v, w) = (c_2, 1, 0).$$

Preuve
La démonstration de ce lemme est analogue à celle du lemme 2.2.6 du paragraphe précédent.

Lemme 2.2.11 *Si*

$$L =< 1, \frac{c^t - 1}{\alpha} + \frac{c^t}{\alpha^2}, \frac{1}{\alpha} >,$$

(i) si $0 < t < m - 1$ alors $(u, v, w) = (c^t, 1, 0)$
(ii) si $t = 0$ ou $t = m - 1$ alors $(u, v, w) = (c^t, 1, 1)$.

Preuve
Les coefficients a et b de la forme quadratique F associée à L et le vecteur isotrope sont donnés par:

$$a = \frac{\alpha}{c^m}\ , b = -\frac{\alpha(\alpha - c_2)}{2c^m}\ , \gamma_2 = \frac{\alpha}{c^{m-t}}\ , \gamma_1 = \frac{\alpha(c^{m-t}-1)+c^m}{c^{m-t}\alpha}$$

et $0 < \gamma_1 < 1$, $\gamma_2 > 1$, $0 < \alpha_1 < 1$, $0 < \alpha_2 < 1$.
De plus

$$|2b| = \frac{\alpha(\alpha - c_2)}{c^m} < 1.$$

D'après (2.1) on a

$$F(Q_1) = \frac{\alpha}{c^m}\left(1 - \frac{c^t}{c^m\alpha}(\alpha - c^m)\right)^2 + c^{2t}(\frac{\alpha}{c^m} - 1)^2 - \frac{\alpha(\alpha - c_2)}{c^m}\left(1 - \frac{c^t}{c^m\alpha}(\alpha - c^m)\right)\frac{c^t}{c^m}(\alpha - c^m)$$

c'est-à-dire en développant:

$$F(Q_1) = \frac{\alpha}{c^m} + \frac{c^{2t}}{c^{2m}}(\alpha - c^m)^2(\frac{1}{c^m\alpha} + 1 + \frac{\alpha - c_2}{c^m}) - 2\frac{c^t}{c^{2m}}(\alpha - c^m) - \frac{c^t}{c^{2m}}(\alpha - c^m)\alpha(\alpha - c_2).$$

En remarquant que

$$\frac{1}{c^m\alpha} + 1 + \frac{\alpha - c_2}{c^m} = \frac{c}{\alpha - c^m}, \tag{2.3}$$

on obtient $F(Q_1) = \frac{\alpha}{c^m} - \frac{c^t}{c^{2m}}(\alpha - c^m)\left(2 + \alpha(\alpha - c_2) - c^{t+1}\right)$.

On a $F(Q_3) = F(Q_1) + a + 2a\gamma_1 + 2b\{\gamma_2\}$
donc

$$F(Q_3) = F(Q_1) + \frac{\alpha}{c^m} + 2\frac{\alpha}{c^m}\frac{\alpha(c^{m-t}-1)+c^m}{c^{m-t}\alpha} - \frac{\alpha(\alpha - c_2)}{c^m}.\frac{(\alpha - c^m)}{c^{m-t}}.$$

On remarque que $\alpha - c_2 < 2$ et que
$\alpha - c^m < \frac{\alpha(c^{m-t}-1)+c^m}{\alpha}$ équivaut à $c - 1 + \frac{c^m - 1}{\alpha} + \frac{c^m}{\alpha^2} < c^{m-t} - 1 + \frac{c^m}{\alpha}$
soit $0 < (c^{m-t} - c) + \frac{1}{\alpha}(1 - \frac{c^m}{\alpha})$ ce qui est vérifié.
Donc $F(Q_3) > \frac{\alpha}{c^m} > 1$.
On a

$$F(Q_4) = F(Q_1) + 2b\gamma_1 + 1 + 2\{\gamma_2\} \tag{2.4}$$

donc $F(Q_4) > F(Q_1) + 2\{\gamma_2\}$ car $-1 < 2b\gamma_1 < 0$,
c'est-à-dire $F(Q_4) > \frac{\alpha}{c^m} - \frac{c^t}{c^{2m}}(\alpha - c^m)\left(2 + \alpha(\alpha - c_2) - c^{t+1}\right) + 2\frac{\alpha - c^m}{c^{m-t}}$.
Le terme de droite est supérieur à 1 si et seulement si
$\frac{\alpha - c^m}{c^m}\left(1 - \frac{c^t}{c^m}(2 + \alpha(\alpha - c_2) - c^{t+1}) + 2c^t\right) > 0$
ce qui équivaut (en remplaçant $\alpha(\alpha - c_2)$ par $c^m - 1 + \frac{c^m}{\alpha}$) à

$1 + c^t + c^{2t+1-m} - c^{t-m} - \dfrac{c^t}{\alpha} > 0$ ce qui est vrai pour $0 \leq t \leq m-1$ donc $F(Q_4) > 1$.

On applique la proposition 2.2.3 en remarquant que $b < 0$.
$F(Q_1) < 1$ équivaut à $1 - \dfrac{\alpha}{c^m} + \dfrac{c^t}{c^{2m}}(\alpha - c^m)\left(2 + \alpha(\alpha - c_2) - c^{t+1}\right) > 0$.
En multipliant par $\dfrac{c^m}{\alpha - c^m}$ et en remplaçant $\alpha(\alpha - c_2)$ par $c^m - 1 + \dfrac{c^m}{\alpha}$ on voit que cette condition est équivalente à $1 + c^m + \dfrac{c^m}{\alpha} - c^{t+1} - c^{m-t} > 0$. D'où
(i) si $0 < t < m-1$ alors $F(Q_1) < 1$,
(ii) si $t = 0$ ou $t = m-1$ alors $F(Q_1) > 1$ mais dans ce cas $\phi_2 = \dfrac{c^{t+1}}{\alpha - c^m}$ et $N(\phi_2) = c^{2m+1}$ donc $F(Q_2) = \dfrac{\alpha - c^m}{c^{2m-2t-1}} < 1$.

Ainsi :
(i) si $0 < t < m-1$ alors $\psi = \phi_1$ c'est-à-dire $(u, v, w) = (c^t, 1, 0)$;

(ii) si $t = 0$ alors $2\alpha_2 - 1 < \alpha_1 < \alpha_2$ donc $\psi = \phi_2$ ou ϕ_7.
$F(Q_7) = 4a\gamma_1^2 + 8b\gamma_1\gamma_2 - 4b\gamma_1[\gamma_2] + (2\gamma_2 - [\gamma_2])^2$ et $4a\gamma_1^2 + 8b\gamma_1\gamma_2 = 0$ si $t = 0$
donc $F(Q_7) > 1$ et $\psi = \phi_2$ c'est-à-dire $(u, v, w) = (c^t, 1, 1)$.

Si $t = m-1$ et $m \geq 2$ alors $\alpha_1 > \alpha_2$ donc $\psi = \phi_2$ c'est-à-dire $(u, v, w) = (c^t, 1, 1)$.

Lemme 2.2.12 *Pour un entier t, $1 \leq t \leq m-2$*

$$\text{si } L =< 1, \frac{\alpha - c^m}{\alpha(c^{t+1} - 1) + c^m}, \frac{\alpha(\alpha - c^m)}{\alpha(c^{t+1} - 1) + c^m} > \text{ alors } (u, v, w) = (1, 1, 0).$$

Preuve
On a :

$$a = \frac{c^{2m+1}}{(\alpha - c^m)\left((c^{t+1} - 1)^2 - \alpha(\alpha - c_2)(c^{t+1} - 1) + c^m\alpha\right)},$$

$$b = \frac{(c^{t+1} - 1)(c_2 - \alpha - 2c^m) + \alpha(\alpha - c_2)^2 - 2c^m + c^m\alpha(\alpha - c_2)}{2\left((c^{t+1} - 1)^2 - \alpha(\alpha - c_2)(c^{t+1} - 1) + c^m\alpha\right)},$$

$$\gamma_2 = \frac{c^{m-t}\alpha}{\alpha(c^{m-t} - 1) + c^m}, \gamma_1 = \frac{\alpha(\alpha - c^m)}{\alpha(c^{m-t} - 1) + c^m},$$

et $0 < \gamma_1 < 1$, $\gamma_2 > 1$, $0 < \alpha_1 < 1$, $0 < \alpha_2 < 1$.
Etude de b.
En posant $2b = \dfrac{N}{D}$ on a

$$N = \alpha(\alpha - c_2)^2 + c^m\alpha(\alpha - c_2) - 2c^{m+t+1} - (\alpha - c_2)(c^{t+1} - 1),$$

d'où $N \geq \alpha(\alpha - c_2)^2 + c^m\alpha(\alpha - c_2) - c^{2m} - (\alpha - c_2)(c^{m-1} - 1) = n$.
On a $n = (\alpha - c_2)\left(\alpha(\alpha - c_2) + c^m\alpha - (c^{m-1} - 1)\right) - c^{2m}$ donc
$n = c^{m-1}(\alpha - c_2)\left(c - 1 + c\alpha + \dfrac{c}{\alpha}\right) - c^{2m}$ en remplaçant $\alpha(\alpha - c_2)$ par $c^m - 1 + \dfrac{c^m}{\alpha}$.

Et de même $c^{1-m}n = (\alpha - c_2)(c-1) - \dfrac{c^2-c}{\alpha} = (c-1)(\alpha - c_2\dfrac{c}{\alpha}) > 0.$
On a $D > 0$ donc $b > 0$.

Montrons que $|2b| < 1$, ce qui équivaut à $N - D < 0$.
On a $N - D = (\alpha(\alpha - c_2)^2 - c^{m+t+1}) + (c^m\alpha(\alpha - c_2) - c^{m}\alpha)$

$$+ (\alpha(\alpha - c_2)(c^{t+1} - 1) - c^{m+t+1}) - (c^{t+1} - 1)^2 - (\alpha - c_2)(c^{t+1} - 1).$$

Donc $N - D < 0$ et $|2b| < 1$.

On a

$$F(Q_1) = \frac{N(\phi_1)}{\phi_1} = \frac{c^{2t+2}}{(c^{t+1}-1)^2 - \alpha(\alpha - c_2)(c^{t+1}-1) + c^m\alpha} < 1$$

donc le point extrémal adjacent à 1 est ϕ_1 ou ϕ_5,
or $\phi_5 < 1$ donc $\psi = \phi_1$ c'est-à-dire $(u, v, w) = (1, 1, 0)$.

Lemme 2.2.13 *Pour un entier t, $1 \leq t \leq m-1$*

$$\text{si } L =< 1, \frac{\alpha - c^m}{c^{t+1}}, \frac{\alpha(c^{t+1}-1) + c^m}{c^{t+1}\alpha} > \text{ alors } (u, v, w) = (c^{m-1-t}, 1, 0).$$

Preuve
On a

$$a = \frac{(c^{t+1}-1)^2 - \alpha(\alpha - c_2)(c^{t+1}-1) + c^m\alpha}{c^{2t+2}}, b = \frac{2(c^{t+1}-1) - \alpha(\alpha - c_2)}{2c^{t+1}},$$

$$\gamma_2 = \frac{\alpha(c^{m-t}-1) + c^m}{\alpha(\alpha - c^m)}, \gamma_1 = \frac{1}{\alpha}$$

et $0 < \gamma_1 < 1$, $\gamma_2 > 1$, $0 < \alpha_1 < 1$, $0 < \alpha_2 < 1$.
De plus $4b^2 < a$, en effet

$$a - 4b^2 = \frac{1}{c^{2t+2}}\left(c^m\alpha - \alpha^2(\alpha - c_2)^2 + 3(c^{t+1}-1)\left(\alpha(\alpha - c_2) - (c^{t+1}-1)\right)\right) > 0.$$

On a

$$F(Q_1) = \frac{c^m}{c^{2t+2}\alpha} < 1.$$

(i)Si $t \leq m-2$ alors $b < 0$ et $\psi = \phi_1$, ϕ_3 ou ϕ_4. Or

$$F(Q_3) > \frac{a}{2}(1 + \frac{1}{\alpha})^2 > \frac{a}{2}$$

et en utilisant les inégalités $(c^{t+1}-1)^2 > 0$, $\alpha(\alpha - c_2) < c^m$,
$(c^{t+1}-1) \leq (c^{m-1}-1)$ et $\alpha > c_2$ on obtient $a > 2$ donc $F(Q_3) > 1$.

D'après (2.4) on a $F(Q_4) = F(Q_1) + 2b\gamma_1 + 1 + 2\{\gamma_2\} > F(Q_1) + 2\{\gamma_2\}$.
Pour montrer que $F(Q_4) > 1$ il suffit de prouver que $2b\gamma_1 + 1 + 2\{\gamma_2\} \geq 0$.
On a

$$2b\gamma_1 + 1 + 2\{\gamma_2\} = \frac{2(c^{t+1}-1) - \alpha(\alpha - c_2)}{c^{t+1}\alpha} + 2\left(\frac{\alpha(c^{m-t}-1) + c^m}{\alpha(\alpha - c^m)} - c^{m-t-1}\right)$$

$$= \frac{2}{c^{t+1}}\left(-\frac{1}{\alpha} + \frac{c^{m+1}}{\alpha - c^m} - c^m - (\alpha - c_2)\right) + \frac{\alpha - c_2}{c^{t+1}} + 2\left(\frac{1}{\alpha} - \frac{1}{\alpha - c^m} + \frac{c^m}{\alpha(\alpha - c^m)}\right)$$

et d'après (2.3) le premier terme est nul et donc $F(Q_4) > 1 + \frac{\alpha - c_2}{c^{t+1}} > 1$.
Ainsi $\psi = \phi_1$ c'est-à-dire $(u, v, w) = (c^{m-1-t}, 1, 0)$.

(ii)Si $t = m - 1$ alors $b > 0$ et $\psi = \phi_1$ ou ϕ_5. On a $F(Q_5) = \frac{\alpha(\alpha - 1) + c^m}{c^m \alpha}$ et en faisant le produit des conjugués on obtient

$$F(Q_5) = \frac{\alpha(\alpha - c_2) + \alpha^2(\alpha - c_2)^2 + c^m(\alpha^2 - \alpha) + 2c^m}{c^{2m}\alpha} > \frac{\alpha^2 - \alpha}{c^m \alpha} > 1$$

donc $F(Q_5) > 1$ et $\psi = \phi_1$ c'est-à-dire $(u, v, w) = (c^{m-1-t}, 1, 0)$.

Ainsi, à l'aide de ces lemmes et en procédant de même que pour la première famille on obtient pour $1 \leq t \leq m - 2$ les résultats donnés dans le tableau qui suit :

k	$L_k =< 1, \frac{\phi_k}{\psi_k}, \frac{\psi_{k-1}}{\psi_k} >$	$\frac{\psi_{k+1}}{\psi_k}$	$\frac{\phi_{k+1}}{\psi_k}$
0	$< 1, \alpha - c_2, \frac{c^m}{\alpha} >$	$(c_2, 1, 0)$	$(c^m - 1, 0, 1)$
1	$< 1, \alpha - c_2, \frac{1}{\alpha} >$	$(c_2, 1, 0)$	$(0, 0, 1)$
2	$< 1, \frac{1}{\alpha^2}, \frac{1}{\alpha} >$	$(1, 1, 1)$	$(1, 1, 0)$
3	$< 1, \frac{\alpha(c-1)+c^m}{c\alpha}, \frac{\alpha - c^m}{c} >$	$(c^{m-1}, 0, 1)$	$(c^{m-1}, 1, 0)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$4t$	$< 1, \alpha - c_2, \frac{c^t}{\alpha} >$	$(c_2, 1, 0)$	$(c^t - 1, 0, 1)$
$4t+1$	$< 1, \frac{c^t - 1}{\alpha} + \frac{c^t}{\alpha^2}, \frac{1}{\alpha} >$	$(c^t, 1, 0)$	$(0, 0, 1)$
$4t+2$	$< 1, \frac{\alpha - c^m}{\alpha(c^{t+1}-1)+c^m}, \frac{\alpha(\alpha - c^m)}{\alpha(c^{t+1}-1)+c^m} >$	$(1, 1, 0)$	$(0, 0, 1)$
$4t+3$	$< 1, \frac{\alpha - c^m}{c^{t+1}}, \frac{\alpha(c^{t+1}-1)+c^m}{c^{t+1}\alpha} >$	$(c^{m-1-t}, 1, 0)$	$(c^{m-1-t} - 1, 0, 1)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$4m-4$	$< 1, \alpha - c_2, \frac{c^{m-1}}{\alpha} >$	$(c_2, 1, 0)$	$(c^{m-1} - 1, 0, 1)$
$4m-3$	$< 1, \frac{c^{m-1} - 1}{\alpha} + \frac{c^{m-1}}{\alpha^2}, \frac{1}{\alpha} >$	$(c^{m-1}, 1, 1)$	$(c^{m-1}, 1, 0)$
$4m-2$	$< 1, \frac{\alpha(c^m - 1)+c^m}{c^m\alpha}, \frac{\alpha - c^m}{c^m} >$	$(1, 0, 1)$	$(0, 1, 0)$

On a noté

$$\phi_0 = \alpha - c_2 \text{ et } \psi_{-1} = \frac{c^m}{\alpha}.$$

De même que précédemment on en déduit que

$$\psi_{4m-1} = \alpha \left(\frac{\alpha^2}{\alpha - c^m} \right)^m.$$

On a

$$N(\psi_{4m-1}) = 1 \text{ et } N(\psi_i) \neq 1 \text{ si } 0 < i \leq 4m-2.$$

Donc ψ_{4m-1} est l'unité fondamentale ϵ de $\mathcal{O}$ et la longueur de la période du développement de l'algorithme de Voronoï est $l = 4m - 1$.

2.2.4 Comparaison de ces résultats avec ceux obtenus par l'AJP

Pour la méthode utilisée précédemment, il faut déterminer à chaque étape un point auxiliaire ϕ_k tel que $\{\psi_k, \phi_k, \psi_{k-1}\}$ soit une base du réseau L_k. La comparaison de ces résultats avec ceux obtenus par l'AJP est facilitée par le choix de ce point auxiliaire que nous avons fait.

Remarque 2.2.14 *Les points auxiliaires peuvent être choisis, pour ces deux familles, par le développement par l'AJP de (α_1, α_2) de la façon suivante : (où α_1 et α_2 sont définis par les théorèmes 2.1.1 et 2.1.2)*
Si on définit les matrices de passage de L_k à L_{k+1} par

$$M_k \begin{pmatrix} \psi_k \\ \phi_k \\ \psi_{k-1} \end{pmatrix} = \begin{pmatrix} \psi_{k+1} \\ \phi_{k+1} \\ \psi_k \end{pmatrix},$$

on a :

- *pour la première famille ($l = 3m + 1$)*

$$M_k = \mathcal{A}_{l-k} \quad \text{pour} \quad 0 \leq k \leq 3m,$$

- *pour la deuxième famille ($l = 4m + 1$)*

$$M_k = \mathcal{A}_{l-k} \quad \text{pour} \quad k = 0 \text{ ou } k = 1$$

$$M_k = \mathcal{A}_{l-k-1} \quad \text{pour} \quad 4 \leq k \leq 4m-4$$

$$M_3 M_2 = \mathcal{A}_{l-4}\mathcal{A}_{l-3}\mathcal{A}_{l-2}$$

$$M_{4m-3} M_{4m-2} = \mathcal{A}_1 \mathcal{A}_2 \mathcal{A}_3$$

où l désigne la longueur du développement par l'AJP de (α_1, α_2) et les $\mathcal{A}_i$ sont les matrices définies dans le premier chapitre associées au même développement.

On en déduit que le développement par l'AJP de (α_1, α_2) et celui par l'algorithme de Voronoï donnent la même unité qui est donc l'unité fondamentale de $\mathbb{Z}[\alpha]$.

Remarque 2.2.15 *Un vecteur isotrope Γ_k de la forme quadratique F exprimée dans un réseau L_k est donné par les quotients complets du développement par l'AJP de (α_1, α_2) de la façon suivante :*

- *pour la première famille :*

$$\Gamma_k = (\alpha_2^{k-1}, 1, \alpha_1^{k-1} - [\alpha_1^{k-1}]) \quad \text{pour} \quad 1 \leq k \leq 3m,$$

- *pour la deuxième famille :*

$$\Gamma_k = (\alpha_2^{k-1}, 1, \alpha_1^{k-1} - [\alpha_1^{k-1}]) \quad \text{pour} \quad k = 1 \text{ ou } k = 2$$
$$\Gamma_3 = (\alpha_2^3, \alpha_1^3 - [\alpha_1^3], 1)$$
$$\Gamma_k = (\alpha_2^k, 1, \alpha_1^k - [\alpha_1^k]) \quad \text{pour} \quad 4 \leq k \leq 4m-3$$
$$\Gamma_{4m-2} = (\alpha_2^{4m-1}, \alpha_1^{4m-1} - [\alpha_1^{4m-1}], 1).$$

2.3 Généralisation de ces familles

Dans ce paragraphe on donne le développement par l'AJP de familles infinies obtenues en généralisant les polynômes précédents à des polynômes de degré quelconque et on obtient les résultats suivants :

2.3.1 Première famille

Soit $c \geq 2$, $m \geq 1$ et $n \geq 1$ des entiers, on considère le polynôme

$$f(X) = X^{n+1} - c^m X^n - (c-1)X^{n-1} - \sum_{i=1}^{n-2}(c^m - 1)X^i - c^m.$$

$f(X)$ admet une unique racine réelle notée α telle que $c^m < \alpha < c^m + 1$.

En notant $f(X) = X^{n+1} - \sum_{i=0}^{n} b_i X^i$ et en posant

$$\begin{cases} \alpha_n = \alpha \\ \alpha_i = \alpha(\alpha_{i+1} - b_{i+1}) \end{cases}$$

on a le théorème suivant:

Théorème 2.3.1 *Le développement par l'AJP de $(\alpha_1, \ldots, \alpha_n)$ est purement périodique de longueur $l = (2n-1)m + 1$ et, en supposant que le degré de α soit n, $\epsilon = \alpha \left(\dfrac{\alpha^{n-1}}{\alpha - c^m} \right)^m$ est une unité de $\mathbb{Q}(\alpha)$. De plus, ce développement est symétrique.*

2.3.2 Deuxième famille

Soit $c \geq 2$, $m \geq 1$ et $n \geq 1$ des entiers, on considère le polynôme

$$f(X) = X^{n+1} - (c^m + c - 1)X^n - \sum_{i=1}^{n-1}(c^m - 1)X^i - c^m.$$

$f(X)$ admet une unique racine réelle notée α telle que $c^m + c - 1 < \alpha < c^m + c$.
Avec les mêmes notations que pour la première famille on a le théorème suivant:

Théorème 2.3.2 *Le développement par l'AJP de* $(\alpha_1, \ldots, \alpha_n)$ *est purement périodique de longueur* $l = (2n)m + 1$ *et, en supposant que le degré de* α *soit* n, $\epsilon = \alpha\left(\frac{\alpha^n}{\alpha - c^m}\right)^m$ *est une unité de* $\mathbb{Q}(\alpha)$. *De plus, ce développement est symétrique.*

2.3.3 Généralisation

C. Levesque a encore généralisé ces deux familles de la façon suivante :
Soit $c \geq 2$, $m \geq 1$ et $n \geq 1$ des entiers, on considère les polynômes

$$f_t(X) = X^{n+1} - c^m X^n - (c-1)X^t - \sum_{i=1}^{t-1}(c^m - 1)X^i - c^m \quad \text{pour} \quad 1 \leq t \leq n.$$

Lemme 2.3.3 $f_t(X)$ *admet une unique racine réelle notée* α *telle que*

$$\begin{cases} c^m + c - 1 < \alpha < c^m + c & \text{pour} \quad t = n \\ c^m < \alpha < c^m + 1 & \text{pour} \quad 1 \leq t \leq n-1 \end{cases}.$$

Preuve
Pour cette démonstration on utilise la règle de Descartes [23], à savoir :
Soit $f = a_n X^n + a_{n-1}X^{n-1} + \ldots + a_0$ un polynôme à coefficients réels, avec $a_0 a_n \neq 0$. Soit v le nombre de changements de signe dans la suite $(a_0, \ldots, a_n)$ de ses coefficients et soit r le nombre de ces racines réelles positives, comptées avec leur ordre de multiplicité, alors il existe un entier naturel m tel que $r = v - 2m$.
On en déduit que $f_t(X)$ admet une unique racine réelle positive et on a :

$$\begin{cases} f_t(c^m + c - 1) < 0 \text{ et } f_t(c^m + c) > 0 & \text{si} \quad t = n \\ f_t(c^m) < 0 \text{ et } f_t(c^m + 1) > 0 & \text{si} \quad 1 \leq t \leq n-1 \end{cases}$$

d'où le résultat.

En notant $f_t(X) = X^{n+1} - \sum_{i=0}^{n} b_t^{(i)} X^i$ et en posant

$$\begin{cases} \alpha_n = \alpha \\ \alpha_i = \alpha(\alpha_{i+1} - b_t^{(i+1)}) \end{cases}$$

on a le théorème suivant:

Théorème 2.3.4 *[19] Le développement par l'AJP de* $(\alpha_1, \ldots, \alpha_n)$ *est purement périodique de longueur* $l = (n+t)m + 1$ *et, en supposant que le degré de* α *soit* n, $\epsilon = \alpha\left(\frac{\alpha^t}{\alpha - c^m}\right)^m$ *est une unité de* $\mathbb{Q}(\alpha)$. *De plus, ce développement est symétrique.*

Remarque : Si $n = 1$, la seule valeur possible pour t est 1 et on obtient la famille de polynômes :

$$f_1(X) = X^2 - (c^m + c - 1)X - c^m.$$

Si $n = 2$, les valeurs possibles pour t sont 1 ou 2 et on obtient les deux familles de polynômes étudiées par C. Levesque et G. Rhin.

2.3.4 Preuve du théorème 2.3.4

(i) Cas n=t=1 (fraction continue)

α étant la racine réelle de $f_1(X)$ telle que $c^m + c - 1 < \alpha < c^m + c$, il faut montrer que le développement en fraction continue de α est purement périodique de longueur $l = 2m + 1$ et que $\epsilon = \alpha \left(\frac{\alpha}{\alpha - c^m}\right)^m$ est une unité de $\mathbb{Q}(\alpha)$.

On a

$$\alpha_1^0 = \alpha; \quad a_1^0 = c^m + c + 1$$

et les formules de récurrence suivantes (pour $0 \leq s \leq m - 1$) qui sont immédiates

$$\begin{cases} \alpha_1^{2s+1} = \dfrac{\alpha}{c^{m-s}}; & a_1^{2s+1} = c^s \\ \alpha_1^{2s+2} = c^{m-s-1} + \dfrac{c^{m-s-1}}{\alpha}; & a_1^{2s+2} = c^{m-s-1} \end{cases}$$

Ce qui nous donne au rang $2m$

$$\alpha_1^{2m} = 1 + \frac{1}{\alpha}; \quad a_1^{2m} = 1.$$

Ainsi, on obtient

$$\alpha_1^{2m+1} = \alpha = \alpha_1^0,$$

ce qui démontre que le développement est purement périodique de longueur $l = 2m + 1$.

L'unité fondamentale de $\mathbb{Q}(\alpha)$ est donnée par la formule de Hasse-Bernstein [2]. à savoir :

$$\epsilon = \prod_{r=0}^{2m} \alpha_1^r = \alpha \left(\frac{\alpha}{\alpha - c^m}\right)^m.$$

(ii) Cas n≠1

Pour cette démonstration on utilisera la formule suivante (pour $1 \leq t \leq n$) :

$$1 + \alpha + \alpha^2 + \ldots + \alpha^{t-1} + \alpha^n = \frac{c\alpha^t}{\alpha - c^m}.$$

Au rang 0 on montre facilement que

$$\begin{cases} a_n^0 = [\alpha_n^0] = \begin{cases} c^m + c - 1 & \text{si } t = n \\ c^m & \text{si } t < n \end{cases} \\ a_i^0 = [\alpha_i^0] = 0 \quad \text{pour } t < i < n \quad (\text{si } t < n - 1) \\ a_t^0 = [\alpha_t^0] = c - 1 \quad \text{si } t \neq n \\ a_i^0 = [\alpha_i^0] = c^m - 1 \quad \text{pour } 1 \leq i < t \quad (\text{si } t > 1) \end{cases}$$

Supposons t≠1 et que pour $0 \leq s \leq m - 1$ on ait les formules suivantes, que l'on

démontrera par récurrence : (en notant $k = n + t$)

$$\begin{cases} \alpha_i^{ks} = \alpha_i^0; & a_i^{ks} = a_i^0 \text{ pour } 2 \leq i \leq n \\ \alpha_1^{ks} = (c^{m-s} - 1) + \dfrac{c^{m-s}}{\alpha}; & a_1^{ks} = c^{m-s} - 1 \end{cases}$$

On a alors

$$\begin{cases} \alpha_n^{ks+1} = \dfrac{\alpha}{c^{m-s}}; & a_n^{ks+1} = c^s \\ \text{si } t < n, \text{ pour } t \leq i \leq n-1, & \\ \alpha_i^{ks+1} = \dfrac{\alpha^{n-i}(\alpha - c^m)}{c^{m-s}}; & a_i^{ks+1} = 0 \\ \text{pour } 1 \leq i \leq t-1, & \\ \alpha_i^{ks+1} = \dfrac{c^m + \sum_{r=1}^{i} \alpha^r (c^m - 1)}{\alpha^i c^{m-s}}; & a_i^{ks+1} = c^s - 1 \end{cases}$$

et

$$\begin{cases} \alpha_n^{ks+2} = \dfrac{c^{m-s}\alpha}{\alpha(c^{m-s} - 1) + c^m}; & a_n^{ks+2} = 1 \\ \text{pour } t-1 \leq i \leq n-1, & \\ \alpha_i^{ks+2} = \dfrac{\alpha^{n-i}(\alpha - c^m)}{\alpha(c^{m-s} - 1) + c^m}; & a_i^{ks+2} = 0 \\ \text{pour } 1 \leq i < t-1, & \\ \alpha_i^{ks+2} = \dfrac{\alpha^{i+1}(c^{m-s} - 1) + c^m + \sum_{r=1}^{i} \alpha^r (c^m - 1)}{\alpha^i [\alpha(c^{m-s} - 1) + c^m]}; & a_i^{ks+2} = 0 \end{cases}$$

Puis, pour $3 \leq \nu \leq t$ on a

$$\begin{cases} \alpha_n^{ks+\nu} = \dfrac{\alpha^{\nu-1}(c^{m-s}-1) + c^m\alpha + \sum_{r=2}^{\nu-2} \alpha^r(c^m-1)}{\alpha^{\nu-1}(c^{m-s}-1) + c^m + \sum_{r=1}^{\nu-2} \alpha^r(c^m-1)}; & a_n^{ks+\nu} = 1 \\ \text{pour } t+1-\nu \leq i \leq n-1, \\ \alpha_i^{ks+\nu} = \dfrac{\alpha^{n-i}(\alpha - c^m)}{\alpha^{\nu-1}(c^{m-s}-1) + c^m + \sum_{r=1}^{\nu-2} \alpha^r(c^m-1)}: & a_i^{ks+\nu} = 0 \\ \text{pour } 1 \leq i \leq t-\nu \text{ et } \nu < t, \\ \alpha_i^{ks+\nu} = \dfrac{\alpha^{i+\nu-1}(c^{m-s}-1) + c^m + \sum_{r=1}^{i+\nu-2} \alpha^r(c^m-1)}{\alpha^i[\alpha^{\nu-1}(c^{m-s}-1) + c^m + \sum_{r=1}^{\nu-2} \alpha^r(c^m-1)]}; & a_i^{ks+\nu} = 0 \end{cases}$$

Au rang $(ks+t+1)$ on a

$$\begin{cases} \alpha_n^{ks+t+1} = \dfrac{\alpha^{t-1}(c^{m-s}-1) + c^m + \sum_{r=1}^{t-2} \alpha^r(c^m-1)}{\alpha^{n-1}(\alpha - c^m)}; & a_n^{ks+t+1} = c^{m-s-1} \\ \text{pour } 1 \leq i \leq n-1, \\ \alpha_i^{ks+t+1} = \dfrac{1}{\alpha^i}; & a_i^{ks+t+1} = 0 \end{cases}$$

En effet,

$$\alpha_n^{ks+t+1} = \frac{c^{m-s-1}}{\alpha^n}\left(\frac{c\alpha^t}{\alpha - c^m}\right) - \sum_{r=1}^{t-1} \frac{1}{\alpha^{n-r}}$$

i.e.

$$\alpha_n^{ks+t+1} = \frac{c^{m-s-1}}{\alpha^n}(1 + \alpha + \ldots + \alpha^{t-1} + \alpha^n) - \sum_{r=1}^{t-1} \frac{1}{\alpha^{n-r}},$$

$$\alpha_n^{ks+t+1} = c^{m-s-1} + (c^{m-s-1}-1)\left(\sum_{r=1}^{t-1} \frac{1}{\alpha^{n-r}}\right) + \frac{c^{m-s-1}}{\alpha^n},$$

d'où le résultat.

Pour $2 \leq \nu < n-t+2$, $t < \nu$ on a

$$\begin{cases} \text{pour } n-\nu+1 < i \leq n, \\ \alpha_i^{ks+t+\nu} = \alpha_i^0; & a_i^{ks+t+\nu} = a_i^0 \\ \alpha_{n-\nu+1}^{ks+t+\nu} = (c^{m-s-1}-1)\left(1+\sum_{r=\nu}^{\nu+t-2}\frac{1}{\alpha^{n-r}}\right)+\frac{c^{m-s-1}}{\alpha^{n-\nu+1}}; & a_{n-\nu+1}^{ks+t+\nu} = 0 \\ \text{pour } 1 \leq i < n-\nu+1, \\ \alpha_i^{ks+t+\nu} = \frac{1}{\alpha^i}; & a_i^{ks+t+\nu} = 0 \end{cases}$$

Au rang $ks+n+2$ on a

$$\begin{cases} \text{pour } t-1 < i \leq n, \\ \alpha_i^{ks+n+2} = \alpha_i^0; & a_i^{ks+n+2} = a_i^0 \\ \alpha_{t-1}^{ks+n+2} = (c^{m-s-1}-1)\left(1+\sum_{r=0}^{t-2}\frac{1}{\alpha^r}\right)+\frac{c^{m-s-1}}{\alpha^{t-1}}; & a_{t-1}^{ks+n+2} = c^{m-s-1}-1 \\ \text{pour } 1 \leq i < t-1, \\ \alpha_i^{ks+n+2} = \frac{1}{\alpha^i}; & a_i^{ks+n+2} = 0 \end{cases}$$

Pour $3 \leq \nu < t$ on a

$$\begin{cases} \text{pour } t-\nu+1 < i \leq n, \\ \alpha_i^{ks+n+\nu} = \alpha_i^0; & a_i^{ks+n+\nu} = a_i^0 \\ \alpha_{t-\nu+1}^{ks+n+\nu} = (c^{m-s-1}-1)\left(1+\sum_{r=0}^{t-\nu}\frac{1}{\alpha^r}\right)+\frac{c^{m-s-1}}{\alpha^{t-\nu+1}}; & a_{t-\nu+1}^{ks+n+\nu} = c^{m-s-1}-1 \\ \text{pour } 1 \leq i < t-\nu+1, \\ \alpha_i^{ks+n+\nu} = \frac{1}{\alpha^i}; & a_i^{ks+n+\nu} = 0 \end{cases}$$

ce qui nous donne au rang $ks+k$

$$\begin{cases} \alpha_i^{ks+k} = \alpha_i^0; & a_i^{ks+k} = a_i^0 \text{ pour } 2 \leq i \leq n \\ \alpha_1^{ks+k} = (c^{m-s-1}-1)+\frac{c^{m-s-1}}{\alpha}; & a_1^{ks+k} = c^{m-s-1}-1 \end{cases}$$

Ainsi on a montré que toutes les formules précédentes sont valables pour tout entier s tel que $0 \leq s \leq m$.

Pour t=1, on peut montrer facilement que l'on a les formules de récurrence suiv-

antes: (en notant $k = n + 1$)

$$\begin{cases} \alpha_i^{ks} = \alpha_i^0 \ \text{ pour } 2 \leq i \leq n \\ \\ \alpha_1^{ks} = \begin{cases} \dfrac{c^{m-s}}{\alpha} \ \text{ pour } 1 \leq s \leq m \\ \\ (c-1) + \dfrac{c^m}{\alpha} \ \text{ pour } s = 0 \end{cases} \end{cases}.$$

Ainsi, pour tout t tel que $1 \leq t \leq n$ au rang km on a

$$\begin{cases} \alpha_i^{km} = \alpha_i^0; \quad a_i^{km} = a_i^0 \ \text{ pour } 2 \leq i \leq n \\ \\ \alpha_1^{km} = \dfrac{1}{\alpha}; \quad a_1^{km} = 0 \end{cases}.$$

Finalement, on obtient

$$\alpha_i^{km+1} = \alpha_i^0; \quad a_i^{km+1} = a_i^0 \ \text{ pour } 0 \leq i \leq n,$$

ce qui démontre que le développement est purement périodique de longueur $l = km + 1$, i.e. $l = (n + t)m + 1$.
Une unité de $\mathbb{Q}(\alpha)$ est donnée par la formule de Hasse-Bernstein [2], à savoir :

$$\epsilon = \prod_{r=0}^{km} \alpha_n^r = \alpha \left(\frac{\alpha^t}{\alpha - c^m} \right)^m.$$

Ceci termine la démonstration du théorème.

CHAPITRE 3

Généralisation de l'algorithme de Voronoï

Dans [4] J. Buchmann a généralisé l'algorithme de Voronoï à des corps de degré supérieur à 3 en définissant des points extrémaux adjacents dans différentes directions. L'algorithme ainsi obtenu (GVA) permet de calculer un système fondamental d'unités de corps dont le rang des unités est 1 ou 2.
Nous donnons dans ce chapitre une définition plus générale de points extrémaux adjacents dans une direction donnée et une méthode de recherche de ces points extrémaux. Pour cette méthode nous utilisons entre autre :

- Un algorithme que nous décrivons dans le premier paragraphe qui permet dans certains cas de compléter un sous-ensemble $\{x_1, \ldots, x_r\}$ de $\mathbb{Z}^n$ en une base de $\mathbb{Z}^n$. Nous montrons de plus comment utiliser cet algorithme pour trianguläriser une matrice sous forme normale d'Hermite (HNF) et l'appliquons à une matrice 20×20 donnée par J.L. Hafner et K.S. McCurley.
- L'algorithme LLL [18] dont nous rappelons dans le deuxième paragraphe les définitions et propriétés essentielles.

Après avoir appliqué cette recherche à celle de points extrémaux au sens de J. Buchmann, nous étudions une famille infinie de polynômes de degré 4 obtenue en généralisant une des familles de degré 3 vue dans le chapitre précédent. Comme pour le degré 3 nous étudions le lien entre le développement par l'AJP et le développement par la généralisation de l'algorithme de Voronoï.

3.1 Méthode de construction d'une base dans un module

Définition 3.1.1[27] *Soient n et r deux entiers strictement positifs tels que $r \leq n$. Soient $x_1, \ldots, x_r$, r éléments de $\mathbb{Z}^n$. On dit que le système $\{x_1, \ldots, x_r\}$ est* **primitif** *si et seulement si on peut le compléter en une base de $\mathbb{Z}^n$. Si $r = 1$, on dit que x_1 est* **admissible.**

On peut remarquer qu'un élément $x = (x^1, \ldots, x^n)^t$ de $\mathbb{Z}^n$ est admissible si et seulement si $pgcd(x^1, \ldots, x^n) = 1$ (en notant x^t la transposée de x).

On va dans ce paragraphe donner un algorithme, noté (A1) permettant, si $x = x_1$ est un élément admissible de $\mathbb{Z}^n$, de construire $(n-1)$ éléments de $\mathbb{Z}^n$, notés $x_2, \ldots, x_n$ tels que $\{x_1, \ldots, x_n\}$ soit une base de $\mathbb{Z}^n$. En d'autres termes : si x est admissible l'algorithme (A1) nous permettra de construire une matrice carrée d'ordre n à coefficients entiers de déterminant ± 1 dont la première colonne est x. Cet algorithme se généralise en un algorithme, noté (Ar) qui permet, si $\{x_1, \ldots, x_r\}$ est un système primitif de $\mathbb{Z}^n$, de construire $(n-r)$ éléments de $\mathbb{Z}^n$ notés $x_{r+1}, \ldots, x_n$ tels que $\{x_1, \ldots, x_r, x_{r+1}, \ldots, x_n\}$ soit une base de $\mathbb{Z}^n$.

3.1.1 Description de l'algorithme (A1)

(1) $k = 1$, $x_k = x$.

(2) Tant que $x_k \neq (1, 0, \ldots, 0)^t$:

Soit j le plus petit entier positif tel que $x_k^{n-j} \neq 0$.

Pour $1 \leq i \leq n-j-1$ on pose $a_k^i = \left[\frac{x_k^i}{x_k^{n-j}}\right]$,

$$u_k = \begin{pmatrix} \left|\begin{array}{ccccc} a_k^1 & 1 & 0 & \ldots & 0 \\ a_k^2 & 0 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ a_k^{n-j-1} & 0 & \ldots & 0 & 1 \\ 1 & 0 & \ldots & \ldots & 0 \end{array}\right| & \begin{matrix} 0 \\ \end{matrix} \\ \begin{matrix} \\ 0 \\ \\ \end{matrix} & \underbrace{\left|\begin{array}{cccc} 1 & 0 & \ldots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \ldots & 0 & 1 \end{array}\right|}_{j} \end{pmatrix},$$

$x_{k+1} = u_k^{-1} x_k$, $k = k+1$.

(3) On note $k_0 = k$, $U = \prod_{k=1}^{k_0} u_k$, $x_i = (U_{1i}, \ldots, U_{ni})^t$ pour $2 \leq i \leq n$.
$(x_1, x_2, \ldots, x_n)$ est alors une base de $\mathbb{Z}^n$.

3.1.2 Validité de l'algorithme (A1)

On peut remarquer que si $j = 0$ les matrices u_k sont du type de celles définies dans le premier chapitre par l'AJP. Ainsi, on montre facilement le résultat suivant, issu des travaux de Perron [24] :

Résultat : Soit $x = (x^1, \ldots, x^n)$ un élément non nul de $\mathbb{Z}^n$. Soit d le pgcd des nombres $x^1, \ldots, x^n$. Il existe un entier strictement positif k_0 tel que $x_{k_0} = (d, 0, \ldots, 0)^t$, où x_{k_0} est construit à l'aide de l'algorithme (A1).

Démontrons ce résultat :

soit k un entier strictement positif et j le plus petit entier positif tel que $x_k^{n-j} \neq 0$. Pour $1 \leq i \leq n-j-1$ on note a_k^i le quotient de la division euclidienne de x_k^i par x_k^{n-j}. La relation $x_{k+1} = u_k^{-1} x_k$ entraîne le système suivant :

$$\begin{cases} x_k^i = a_k^i x_k^{n-j} + x_{k+1}^{i+1} \quad pour \quad 1 \leq i \leq n-j-1 \quad (*) \\ \\ x_k^{n-j} = x_{k+1}^1 \end{cases}$$

et on a : $pgcd(x_k^1, \ldots, x_k^{n-j}) = pgcd(x_{k+1}^1, \ldots, x_{k+1}^{n-j}) = d$.
Par $(*)$ on a $0 \leq x_{k+1}^{n-j} < x_k^{n-j}$. La suite $(x_k^{n-j})_{k \in \mathbb{N}^*}$ étant une suite de nombres entiers positifs strictement décroissante, il existe un entier strictement positif l tel que $x_l^{n-j} = 0$. On a alors $d = pgcd(x_l^1, \ldots, x_l^{n-j-1})$.
On reprend alors le même processus avec $(n-j-1)$ entiers et ceci jusqu'à n'avoir plus que 2 entiers à considérer : dans ce cas il s'agit de l'algorithme d'Euclide qui fournit donc le pgcd de $(x^1, \ldots, x^n)$.

x étant admissible, on a $d = 1$ ce qui montre que l'algorithme se termine.
Dans ce cas, la matrice $U = \prod_{k=1}^{k_0} u_k$ est telle que :

(i) $U^{-1}x = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$,

(ii) dét U $= \pm 1$.

U est donc une matrice de déterminant ± 1 dont le premier vecteur colonne est $x = x_1$ et en notant $x_2, \ldots, x_n$ les autres vecteurs colonnes de U, $\{x_1, \ldots, x_n\}$ est une base de $\mathbb{Z}^n$. Ceci montre la validité de l'algorithme (A1) dans ce cas.

3.1.3 Forme normale d'Hermite

Définition 3.1.2 *Soient n et r deux entiers strictement positifs tels que $r \leq n$. Soit $A = (a_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq r}}$ une matrice $n \times r$ dont les termes sont des éléments de $\mathbb{Z}$. On dit que A est sous* **forme normale d'Hermite** *(on notera* **HNF** *) si et seulement si A s'écrit :*

$$A = \left(\begin{array}{c|ccc} d_1 & \star & \ldots & \star \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \star \\ 0 & \ldots & 0 & d_r \\ \hline & & \mathbf{0} & \end{array} \right)$$

où $H = \begin{pmatrix} d_1 & \star & \ldots & \star \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \star \\ 0 & \ldots & 0 & d_r \end{pmatrix}$ *est telle que :*

(i) $h_{ij} = 0$ *pour tout* (i,j) *tel que* $i > j$,

(ii) $h_{ii} > 0$ *pour tout* i *tel que* $1 \leq i \leq r$,

(iii) $0 \leq h_{ij} < h_{jj}$ *pour tout* (i,j) *tel que* $i < j$.

Remarque : Dans la définition donnée par H. Cohen [7], la matrice A est une matrice à r lignes et n colonnes. Nous utilisons la notation contraire.

Théorème 3.1.3 *Soient* n *et* r *deux entiers strictement positifs tels que* $r \leq n$. *Soit* $\mathcal{M}$ *une matrice* $n \times r$, *de rang* r *dont les termes sont des éléments de* $\mathbb{Z}$. *Il existe* U *une matrice* $n \times n$ *unimodulaire telle que* $U\mathcal{M}$ *soit une matrice HNF.*

Les algorithmes classiques permettant de trianguliariser une matrice sous forme normale d'Hermite utilisent une méthode semblable à l'algorithme d'Euclide qui fait intervenir un certain nombre de calculs de PGCD. Dans la pratique ces méthodes sont presque inutilisables lorsque n et r sont "grands". En effet, les entiers utiles au calcul "explosent" rapidement. Ainsi, J.L. Hafner et K.S. McCurley [13] ont donné un exemple de matrice 20×20 dont les coefficients sont tous inférieurs ou égaux à 10 et telle que certains entiers intervenant dans le calcul soient de l'ordre de 10^{5000}. Ils donnent un algorithme modulaire qui permet de transformer cette même matrice en une matrice HNF en utilisant des entiers dont le plus grand est environ 10^{33} (de l'ordre de la borne d'Hadamard pour le déterminant de cette matrice).

Remarque: L'algorithme (Ar) fournit une méthode pour transformer une matrice en une matrice HNF.

En effet,

on a montré précédemment que, pour tout $x = (x^1, \ldots, x^n)$ élément non nul de $\mathbb{Z}^n$. l'algorithme (A1) fournit une matrice U, $n \times n$, unimodulaire telle que $U^{-1}x = \begin{pmatrix} d \\ 0 \\ \vdots \\ 0 \end{pmatrix}$

où $d = pgcd(x^1, \ldots, x^n)$.

Soit $\mathcal{M} = (x_1, \ldots, x_r)$ une matrice $n \times r$. Appliquer l'algorithme (Ar) à $\mathcal{M}$ consiste à appliquer l'algorithme (A1) successivement aux colonnes de $\mathcal{M}$. Ainsi l'algorithme (Ar) fournit une matrice U, $n \times n$, unimodulaire telle que

$$U^{-1}\mathcal{M} = \left(\begin{array}{|cccc|} d_1 & \star & \ldots & \star \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \star \\ 0 & \ldots & 0 & d_r \\ \hline \multicolumn{4}{|c|}{0} \\ \hline \end{array} \right)$$

où $U^{-1}\mathcal{M}$ est une matrice HNF.

En appliquant cet algorithme à la matrice 20×20 citée précédemment on obtient rapidement la matrice HNF correspondante et le plus grand entier nécessaire au calcul est de l'ordre de 10^{68}.

3.2 Définition et méthode de recherche de points extrémaux

Soit n un entier strictement positif et $\mathcal{L}_1, \ldots, \mathcal{L}_n$, n formes linéaires indépendantes sur $\mathbb{R}^n$. On notera $\mathcal{L} = (\mathcal{L}_1, \ldots, \mathcal{L}_n)$.

Définition 3.2.1 *Soit j_c un entier strictement positif tel que $j_c \leq n$. Soit $x = (x_1, \ldots, x_n)$ un élément non nul de $\mathbb{Z}^n$. On dit que x est le* **point extrémal adjacent** *à 1 dans la* **direction** *j_c relativement à $\mathcal{L}$ si et seulement si*

$$(S_1) \quad \begin{cases} \max\limits_{i \neq j_c} |\mathcal{L}_i(x)| < 1 \quad (S) \\ \\ |\mathcal{L}_{j_c}(x)| = min\{|\mathcal{L}_{j_c}(y)| \text{ tel que } y \text{ vérifie } (S), y \in \mathbb{Z}^n \text{ et } y \neq 0\} \end{cases}.$$

3.2.1 Méthode de recherche

Pour déterminer le point extrémal adjacent à 1 dans la direction j_c relativement à $\mathcal{L}$:

(1) on recherche un point particulier x_0 non nul tel que:

$$\max_{i \neq j_c} |\mathcal{L}_i(x_0)| < 1,$$

(2) on pose $B = |\mathcal{L}_{j_c}(x_0)|$. Le système $\begin{cases} \max\limits_{i \neq j_c} |\mathcal{L}_i(x)| < 1 \\ \\ |\mathcal{L}_{j_c}(x)| \leq B \end{cases}$ admet un nombre fini de solutions, dont $x_0 \neq 0$, dans $\mathbb{Z}^n$. Parmi ces solutions, on choisit celle qui rend $|\mathcal{L}_{j_c}(x)|$ minimum.

Le problème essentiel ici est la recherche d'un point particulier.

3.2.2 Recherche d'un point particulier

On veut donc trouver une solution particulière x_0 dans $\mathbb{Z}^n$ du système, noté (S) suivant:

$$|\mathcal{L}_i(x)| < 1 \quad \text{pour tout i tel que } i \neq j_c$$

telle que

$$|\mathcal{L}_{j_c}(x_0)| \quad \text{"petit"}$$

où $\mathcal{L}_i$ $(1 \leq i \leq n)$ sont n formes linéaires indépendantes sur $\mathbb{R}^n$.

Pour cela, on utilise un algorithme de réduction de réseaux, à savoir l'algorithme LLL de A.K. Lenstra, H.W. Lenstra et L. Lovasz [18].

a) Description de l'algorithme LLL

Soient $b_1, \ldots, b_n$ n vecteurs linéairement indépendants de $\mathbb{Z}^n$ et L le réseau engendré par ces n vecteurs, c'est-à-dire $L = \bigoplus_{i=1}^{n} \mathbb{Z}b_i$.

Réduire un réseau c'est trouver une "bonne" base de ce réseau c'est-à-dire une base dont les vecteurs sont "assez petits" et "presque orthogonaux". Cette notion fait donc intervenir la structure euclidienne de l'espace dans lequel on se place.

Définition d'une base réduite au sens de Lovasz

Soient $b = (b_1, \ldots, b_n)$ une base de $\mathbb{R}^n$, $L = \bigoplus_{i=1}^{n} \mathbb{Z}b_i$ et $b^* = (b_1^*, \ldots, b_n^*)$ la base orthogonale obtenue à partir de b par le procédé d'**orthogonalisation de Gram-Schmidt** c'est-à-dire définie par

$$b_i^* = b_i - \sum_{1 \leq j < i} \mu_{ij} b_j^* \quad (\text{pour } \ 1 \leq i \leq n)$$

avec

$$\mu_{ij} = \frac{b_i . b_j^*}{b_j^* . b_j^*}.$$

Définition 3.2.2 *b est une base* **LLL-réduite** *si et seulement si*

(1) $|\mu_{ij}| \leq \dfrac{1}{2}$ *pour tout* (i,j) *tel que* $1 \leq j < i \leq n$,

(2) $|b_i^*|^2 \leq \left(\dfrac{3}{4} - \mu_{i,i-1}^2\right) |b_{i-1}^*|^2$.

Théorème 3.2.3 *Soit $b = (b_1, \ldots, b_n)$ une base LLL-réduite. Pour tout x non nul de L on a :*

$$|b_1| \leq 2^{\frac{n-1}{2}} |x|.$$

L'algorithme LLL transforme, en temps polynomial, une base b d'un réseau L en une base LLL-réduite. Le théorème précédent montre que l'algorithme LLL fournit "presque" le plus petit vecteur d'un réseau c'est-à-dire un vecteur de petite norme.

b) Application à la recherche d'un point particulier

On note :

$\mathcal{L}_i(x) = \sum_{j=1}^{n} x_j a_{ij}$ pour tout i tel que $1 \leq i \leq n$,

$m = (a_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}}$ la matrice associée,

b_j les vecteurs colonnes de m $(1 \leq j \leq n)$,

A_j le vecteur colonne obtenu en supprimant dans b_j la composante j_c $(1 \leq j \leq n)$,

$a_j = a_{j_c, j}$ $(1 \leq j \leq n)$,

L le réseau engendré par $(b_1, \ldots, b_n)$.

On va appliquer l'algorithme LLL à ce réseau. Si on utilise le produit scalaire usuel, le "petit" vecteur obtenu alors n'est pas forcément satisfaisant. C'est pourquoi on définit un nouveau produit scalaire dépendant d'une constante c, ce qui va nous permettre, en faisant varier c, d'obtenir un vecteur aussi "petit" que l'on veut.
Soit c une constante réelle positive quelconque. On définit sur $\mathbb{R}^n$ le produit scalaire noté $(.|_c.)$ par:

$$(b_j|_c b_k) = (A_j.A_k) + ca_j a_k$$

où $(.)$ désigne le produit scalaire usuel.
La norme notée $\|\ldots\|_c$ associée à ce produit scalaire est définie par:

$$\|x\|_c^2 = \|\sum_{j=1}^{n} x_j A_j\|^2 + c|\sum_{j=1}^{n} x_j a_j|^2$$

où $\|\ldots\|$ désigne le norme euclidienne.
On pose $c = 1$. Le produit scalaire $(.|_1.)$ correspond au produit scalaire usuel. Si le vecteur obtenu ne vérifie pas le système (S) on fait décroître c jusqu'à ce qu'il en soit ainsi.

3.2.3 Recherche du minimum

Le système $\begin{cases} \max\limits_{i \neq j_c} |\mathcal{L}_i(x)| < 1 \\ \\ |\mathcal{L}_{j_c}(x)| \leq B \end{cases}$, noté (Σ), équivaut à:

$$\begin{cases} |\sum_{j=1}^{n} x_j a_{ij}| < 1 \ \textit{pour tout } i \textit{ tel que } i \neq j_c \\ \\ |\sum_{j=1}^{n} x_j a_{j_c,j}| \leq B \end{cases}$$

Après avoir triangularisé la matrice $m = (a_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}}$ par la méthode du Pivot de Gauss, on peut facilement exhiber toutes les solutions dans $\mathbb{Z}^n$ de (Σ) et le point extrémal adjacent à 1 dans la direction j_c relativement à $\mathcal{L}$ est la solution qui rend $|\mathcal{L}_{j_c}(x)|$ minimum.

3.2.4 Généralisation

On peut généraliser cette notion de point extrémal de la façon suivante: soient n et k deux entiers strictement positifs tels que $k \leq n$ et $J = \{j_1, j_2, \ldots, j_k\}$ un sous-ensemble de $\{1, 2, \ldots, n\}$. Si $\mathcal{L}_1, \ldots, \mathcal{L}_n$ sont n formes linéaires indépendantes sur $\mathbb{R}^n$, on note $\mathcal{L} = (\mathcal{L}_1, \ldots, \mathcal{L}_n)$ et $\mathcal{L}_J = (\mathcal{L}_{j_1}, \ldots, \mathcal{L}_{j_k})$. Soit $|\ldots|_k$ une norme définie sur $\mathbb{R}^k$.

Définition 3.2.4 *Soit $x = (x_1, \ldots, x_n)$ un élément non nul de $\mathbb{Z}^n$. On dit que x est le* **point extrémal adjacent** *à 1 dans la* **direction J** *relativement à $\mathcal{L}$ et à $|\ldots|_k$ si et seulement si*

$$(S_2) \quad \begin{cases} \max\limits_{i \notin J} |\mathcal{L}_i(x)| < 1 \quad (S) \\ \\ |\mathcal{L}_J(x)|_k = min\{|\mathcal{L}_J(y)|_k \ tel \ que \ y \ vérifie \ (S), y \in \mathbb{Z}^n \ et \ y \neq 0\} \end{cases}$$

La méthode de recherche de points extrémaux définie ainsi est semblable à celle décrite précédemment.

3.3 Généralisation de l'algorithme de Voronoï

3.3.1 Travaux de J. Buchmann

On a décrit dans le premier chapitre l'algorithme de Voronoï dans un corps cubique à conjugués complexes. On décrit ici une généralisation de cet algorithme due à J. Buchmann [4] [5] (la généralisation aux corps cubiques totalement réels avait été faite par Voronoï lui-même).

a) Notations et Définitions

On note :
K un corps de nombres algébriques de degré $n = r_1 + 2r_2$ où r_1 (respectivement $2r_2$) désigne le nombre de plongements réels (respectivement complexes) de K dans $\mathbb{C}$,
$r = r_1 + r_2 - 1$,
$\mathcal{O}$ un ordre de K,
$\sigma_1, \ldots, \sigma_{r_1}$ les plongements réels de K dans $\mathbb{C}$,
$\sigma_{r_1+1}, \overline{\sigma_{r_1+1}}, \ldots, \sigma_{r_1+r_2}, \overline{\sigma_{r_1+r_2}}$ les plongements complexes de K dans $\mathbb{C}$.
Pour tout ψ de K on note :

$\underline{\psi} = (|\sigma_1(\psi)|, \ldots, |\sigma_{r_1}(\psi)|, |\sigma_{r_1+1}(\psi)|^2, \ldots, |\sigma_{r_1+r_2}(\psi)|^2)$,
$Q(\underline{\psi}) = \{y \in \mathbb{R}^{r+1}$ tel que $0 \leq y_i \leq \underline{\psi_i}$, $\forall i$, $1 \leq i \leq r+1\}$ où y_i (respectivement $\underline{\psi_i}$) désigne la i-ième composante du vecteur y (respectivement $\underline{\psi}$) pour tout i tel que $1 \leq i \leq r+1$.

Définition 3.3.1 *On dit que ψ est un* **point extrémal** *de $\mathcal{O}$ si et seulement si $Q(\underline{\psi}) \cap \mathcal{O} = \{\underline{0}, \underline{\psi}\}$.*

Définition 3.3.2 *Soit k un entier positif et j_c un entier tel que $1 \leq j_c \leq r+1$, on dit que ψ_{k+1} est* **un point extrémal adjacent** *à ψ_k dans la* **direction** *j_c dans $\mathcal{O}$ si et seulement si ψ_{k+1} est tel que*

$$\begin{cases} 0 < |\sigma_i(\psi_{k+1})| < |\sigma_i(\psi_k)| \quad \text{pour } i \neq j_c \quad (S') \\ \\ |\sigma_{j_c}(\psi_{k+1})| = min\{|\sigma_{j_c}(\psi)| \text{ tel que } \psi \text{ vérifie } (S'),\ \psi \in \mathcal{O} \text{ et } \psi \neq 0\} \end{cases}$$

On peut remarquer que si ψ_{k+1} est un point extrémal adjacent à ψ_k alors $-\psi_{k+1}$ et $\overline{\psi_{k+1}}$ sont également des points extrémaux adjacents à ψ_k (où $\overline{\psi_{k+1}}$ désigne le conjugué complexe de ψ_{k+1}). Ainsi, pour éviter toute ambiguïté on dira que :

Définition 3.3.3 *ψ_{k+1} est* **le point extrémal adjacent** *à ψ_k dans la* **direction** *j_c dans $\mathcal{O}$ si et seulement si ψ_{k+1} vérifie le système précédent et est tel que :*
$Re(\psi_{k+1}) \geq 0$ et $Im(\psi_{k+1}) \geq 0$ où Re (respectivement Im) désigne la partie réelle (respectivement imaginaire).

Remarque : Si $n = 3$ et $r_1 = 1$, les valeurs possibles pour j_c sont 2 et 1 et la définition précédente est équivalente aux définitions de points extrémaux adjacents respectivement de première et de deuxième espèce.

b) Périodicité et système fondamental d'unités

Si L est un réseau réduit, on peut ainsi construire une suite de points extrémaux adjacents dans $r_1 + r_2$ directions par

$$\begin{cases} \psi_0 = 1 \\ \psi_{k+1} \text{ est le point extrémal adjacent à } \psi_k \\ \qquad \text{dans la direction } j_c \text{ si } k \geq 0 \end{cases}$$

J. Buchmann a démontré que, de même que pour le cas $n = 3$, $r_1 = 1$, chacune de ces suites est purement périodique et fournit une unité de $\mathcal{O}$ ainsi que les résultats suivants :

Résultat 1 : Si $r = 1$, les valeurs possibles pour j_c sont 1 et 2 et les deux unités que l'on obtient sont inverses l'une par rapport à l'autre et chacune d'elles est une unité fondamentale de $\mathcal{O}$.

Résultat 2 : Si $r = 2$, les valeurs possibles pour j_c sont 1, 2 et 3. Pour déterminer un système fondamental d'unités de $\mathcal{O}$:

- on détermine la suite des points extrémaux adjacents à 1 dans une première direction. On note $(\psi_k)_{k \leq l}$ cette suite avec $\psi_0 = 1$ et l le plus petit entier strictement positif tel qu'il existe un entier l_1 vérifiant $0 \leq l_1 < l$ et tel que $\dfrac{\psi_l}{\psi_{l_1}}$ soit une unité.
- On détermine la suite des points extrémaux adjacents à ψ_{l_1} dans une deuxième direction. On note $(\phi_k)_{k \leq i}$ cette suite avec $\phi_0 = \psi_{l_1}$ et i le plus petit entier strictement positif tel qu'il existe un entier l_2 vérifiant $l_1 \leq l_2 \leq l$ et tel que $\dfrac{\phi_i}{\psi_{l_2}}$ soit une unité.

En notant $\epsilon_1 = \dfrac{\psi_l}{\psi_{l_1}}$ et $\epsilon_2 = \dfrac{\phi_i}{\psi_{l_2}}$, $\{\epsilon_1, \epsilon_2\}$ est un système fondamental d'unités de $\mathcal{O}$.

3.3.2 Méthode proposée pour la recherche de points extrémaux

Pour construire une suite de points extrémaux, on procède comme dans le cas d'un corps cubique à conjugués complexes. Il suffit de savoir construire le point extrémal adjacent à 1 dans un réseau réduit. Pour déterminer ψ_{k+1} (on suppose que l'on connaît la suite des points extrémaux jusqu'à ψ_k) on considère un réseau réduit L_k.

(1) Dans ce réseau on détermine θ_1^k le point extrémal adjacent à 1 dans la direction j_c, c'est-à-dire que θ_1^k est le point de L_k tel que

$$\begin{cases} 0 < |\sigma_i(\theta_1^k)| < 1 \quad i \neq j_c \quad (S') \\ |\sigma_{j_c}(\theta_1^k)| = min\{|\sigma_{j_c}(\psi)| \; tel \; que \; \psi \; vérifie \; (S'), \; \psi \in L_k \; et \; \psi \neq 0\} \end{cases}$$

On aura alors $\psi_{k+1} = \theta_1^k \psi_k$.

(2) On choisit alors, à l'aide de l'algorithme (A1) décrit dans le premier paragraphe, $(n-1)$ éléments $\theta_2^k, \ldots \theta_n^k$ de L_k tels que $\theta_1^k, \ldots \theta_n^k$ soit une base de $\mathbb{Z}^n$.
On pose $L_{k+1} =< 1, \frac{\theta_2^k}{\theta_1^k}, \ldots, \frac{\theta_n^k}{\theta_1^k} >$

et on poursuit ce processus.

Pour cette construction le problème est encore la détermination de θ_1^k. Pour cela, on utilise la méthode décrite dans le paragraphe précédent .
En effet, on remarque que pour tout $i > r_1$, on a

$$|\sigma_i(\psi)| < 1 \ \ entraîne \ \begin{cases} |\mathrm{Re}\,(\sigma_i(\psi))\,| < 1 \\ \\ |\mathrm{Im}\,(\sigma_i(\psi))\,| < 1 \end{cases}$$

où Re(x) (respectivement Im(x)) désigne la partie réelle (respectivement imaginaire) de x et en considérant les n applications linéaires de $\mathbb{Z}^n$ dans $\mathbb{R}$ définies par :

$$\mathcal{L}_i(x) = \begin{cases} \sigma_i(\psi) & \text{si } i \leq r_1 \\ \\ \mathrm{Re}\left(\sigma_{\frac{i+r_1+1}{2}}(\psi)\right) & \text{si } i > r_1 \text{ et } (i-r_1) \text{ impair} \\ \\ \mathrm{Im}\left(\sigma_{\frac{i+r_1}{2}}(\psi)\right) & \text{si } i > r_1 \text{ et } (i-r_1) \text{ pair} \end{cases}$$

où l'on note $x = (x_1, \ldots, x_n)$ si $\psi = x_1 + x_2\alpha_1 + \ldots + x_n\alpha_{n-1}$.
Alors, rechercher θ_1^k revient "presque" à résoudre un système du type (S_1) (si $j_c \leq r_1$) ou (S_2) (si $j_c > r_1$ avec $k = 2$ et $|\ldots|_k$ est la norme euclidienne).
En effet, il suffit de rajouter un contrôle supplémentaire à la première étape (recherche d'un point particulier) : le point particulier x_0 que l'on obtient est tel que

$$\begin{cases} |\mathrm{Re}\ \sigma_i(\psi_0)| < 1 \\ \\ |\mathrm{Im}\ \sigma_i(\psi_0)| < 1 \end{cases}.$$

Il faut vérifier que $|\sigma_i(\psi_0)| < 1$, sinon on change la valeur de c et l'on recommence.

3.3.3 Cas cubique à conjugués complexes

On a décrit dans le deuxième chapitre une méthode qui, dans un corps cubique à conjugués complexes permet dans certains cas de déterminer la suite des points extrémaux dans la direction $j_c = 1$. En effet, ψ est le point extrémal adjacent à 1 dans la direction $j_c = 1$ signifie que :

$$\begin{cases} 0 < |\sigma(\psi)| < 1 \\ \\ \psi = min\{\phi \ tel \ que \ \phi > 1 \ et \ |\sigma(\phi)| < 1\} \end{cases}.$$

Cette méthode n'est qu'un cas particulier de celle décrite plus haut. Effectivement,

(1) dans la proposition 2.2.3 on suppose que l'on connaît un point particulier ψ_0 qui correspond à Q_1 ou Q_2 (avec les notations utilisées dans le deuxième chapitre).

(2) Le système $\begin{cases} 0 < |\sigma(\psi)| < 1 \\ \\ \psi \leq \psi_0 \end{cases}$ admet un nombre fini de solutions parmi lesquelles on choisit le minimum.

En fait, dans cette même proposition on impose des hypothèses supplémentaires qui nous permettent de restreindre le nombre de solutions du système $\begin{cases} 0 < |\sigma(\psi)| < 1 \\ \\ \psi \leq \psi_0 \end{cases}$.

3.4 Applications

Soit $c \geq 2$, $m \geq 1$ et $n \geq 1$ des entiers. Dans le deuxième chapitre on a étudié la famille de polynômes :

$$f_t(X) = X^{n+1} - c^m X^n - (c-1)X^t - \sum_{i=1}^{t-1}(c^m - 1)X^i - c^m \quad \text{pour} \quad 1 \leq t \leq n.$$

On considère ici le cas où $n = 3$ et $t = 2$ c'est-à-dire le polynôme :

$$f(X) = X^4 - c^m X^3 - (c-1)X^2 - (c^m - 1)X - c^m.$$

Lemme 3.4.1 *$f(X)$ est irréductible dans $\mathbb{Z}[X]$, possède deux racines réelles et deux racines complexes.*

Preuve du lemme 3.4.1

On a $f(c^m) < 0$, $f(c^m + 1) > 0$, $f(-1) > 0$ et $f(-\frac{1}{2}) < 0$

donc f admet deux racines réelles, notées α et β telles que

$$\begin{cases} c^m < \alpha < c^m + 1 \\ \\ -1 < \beta < -\frac{1}{2}. \end{cases} \qquad (I)$$

Ainsi, on a $f(X) = (X^2 - (\alpha + \beta)X + \alpha\beta)\,Q(X)$ où $Q(X)$ est un polynôme de $\mathbb{R}[X]$ de degré 2.

Or les inégalités (I) entraînent que $(X^2 - (\alpha + \beta)X + \alpha\beta) \notin \mathbb{Z}[X]$, en effet :

si $\alpha + \beta$ est entier alors $\alpha + \beta = c^m$ et dans ce cas $\alpha\beta$ n'est pas entier.

Donc $f(X)$ est irréductible dans $\mathbb{Z}[X]$.

De plus, on a $Q(X) = X^2 + (\alpha + \beta - c^m)X - \dfrac{c^m}{\alpha\beta}$. Le discriminant de $Q(X)$ est

$$\Delta = (\alpha - c^m)^2 + 2\beta(\alpha - c^m) + \beta^2 + \frac{4c^m}{\alpha\beta} = (\alpha - c^m)\left((\alpha - c^m) + 2\beta\right) + \left(\beta^2 + \frac{4c^m}{\alpha\beta}\right).$$

On a $\alpha - c^m = \dfrac{c\alpha^2}{\alpha^3 + \alpha + 1} < \dfrac{c}{\alpha} < \dfrac{1}{c^{m-1}}$

et les inégalités $\begin{cases} c^m < \alpha < c^m + \dfrac{1}{c^{m-1}} \\ \\ -1 < \beta < -\dfrac{1}{2} \end{cases}$ entraînent $\Delta < 0$. Ainsi $Q(X)$ admet deux

racines complexes non réelles.
Ceci termine la démonstration du lemme.

On en déduit que $r_1 = r_2 = r = 2$ (où r_1, r_2 et r sont définis comme dans le paragraphe précédent) et qu'un système fondamental d'unités de $\mathcal{O}$ contient 2 éléments.
On peut se poser le problème de la détermination d'un tel système. Pour cela on a utilisé la méthode de recherche de points extrémaux dans différentes directions décrite précédemment et essayé de paramétrer les résultats obtenus: on a établi une conjecture dans la direction $j_c = 1$. Par contre on a obtenu un système fondamental d'unités de $\mathcal{O}$ de façon paramétré dans le seul cas où $m = 1$. On détaille ici les résultats obtenus.

3.4.1 Cas m $\geq$ 2

Les différents exemples traités nous ont permis de conjecturer le résultat suivant:

Conjecture 3.4.2 *Soit α la racine réelle du polynôme $f(X)$ telle que $c^m < \alpha < c^m + 1$, $K = \mathbb{Q}(\alpha)$ et $\mathcal{O} = \mathbb{Z}[\alpha]$.*

(i) La suite des points extrémaux de $\mathcal{O}$ dans la direction $j_c = 1$ est:

$$\psi_0 = 1$$

$$\psi_{2s+1} = \left(\frac{c\alpha^2}{\alpha - c^m}\right)^{s+1}, \quad \psi_{2s+2} = \alpha\left(\frac{\alpha^2}{\alpha - c^m}\right)^{s+1} \quad \text{pour} \quad 0 \leq s \leq m-2$$

$$\text{et } \psi_{2m-1} = \alpha\left(\frac{\alpha^2}{\alpha - c^m}\right)^m.$$

(ii) Une unité fondamentale de $\mathcal{O}$ est $\epsilon = \alpha\left(\frac{\alpha^2}{\alpha - c^m}\right)^m$ et la longueur de la période du développement dans la direction $j_c = 1$ est $l = 2m - 1$.

Remarque : Comme dans le cas $n = 2$, ces points sont donnés par le développement par l'AJP de $(\alpha_1, \alpha_2, \alpha_3)$ où:

$$\begin{cases} \alpha_3 = \alpha \\ \alpha_2 = \alpha(\alpha - c^m) \\ \alpha_1 = \alpha^3 - c^m\alpha^2 - (c-1)\alpha \end{cases}$$

de la façon suivante:
on se place à chaque étape dans des réseaux L_k de la forme $L_k = < \phi_k^{(1)}, \phi_k^{(2)}, \phi_k^{(3)}, \psi_k >$ où $\phi_k^{(1)}$, $\phi_k^{(2)}$ et $\phi_k^{(3)}$ sont trois points auxiliaires, avec $L_0 = < \alpha_3, \alpha_2, \alpha_1, 1 >$. Si on définit les matrices de passage de L_k à L_{k+1} (pour $0 \leq k \leq 2m-2$) par

$$M_{k+1}\begin{pmatrix} \phi_k^{(1)} \\ \phi_k^{(2)} \\ \phi_k^{(3)} \\ \psi_k \end{pmatrix} = \begin{pmatrix} \phi_{k+1}^{(1)} \\ \phi_{k+1}^{(2)} \\ \phi_{k+1}^{(3)} \\ \psi_{k+1} \end{pmatrix},$$

on a

$$M_1 = \mathcal{A}_{l-5} \dots \mathcal{A}_{l-1}$$
$$M_2 = \mathcal{A}_{l-6}$$
$$\text{pour } 1 \leq s \leq m-2 \quad \begin{cases} M_{2s+1} = \mathcal{A}_{l-(5s+5)} \mathcal{A}_{l-(5s+4)} \cdots \mathcal{A}_{l-(5s+2)} \\ M_{2s+2} = \mathcal{A}_{l-(5s+6)} \end{cases},$$
$$M_{2m-1} = \mathcal{A}_0 \dots \mathcal{A}_4$$

où $l = 5m+1$ est la longueur du développement par l'AJP de $(\alpha_1, \alpha_2, \alpha_3)$ et les $\mathcal{A}_i$ sont les matrices définies dans le premier chapitre associées au même développement.

Dans les directions $j_c = 2$ et $j_c = 3$ on pourrait déterminer la suite des points extrémaux pour toute valeur de c ($c \geq 2$) et de m ($m \geq 2$) et en déduire un système fondamental d'unités de $\mathcal{O}$ contenant $\epsilon = \alpha \left(\frac{\alpha^2}{\alpha - c^m} \right)^m$. Par contre on ne sait pas paramétrer les résultats obtenus.

3.4.2 Cas m=1

Les différents exemples traités nous ont permis de conjecturer le résultat suivant:

Conjecture 3.4.3 *Soit α la racine réelle du polynôme $f(X)$, où $f(X) = X^4 - cX^3 - (c-1)X^2 - (c-1)X - c$ telle que $c < \alpha < c+1$, $K = \mathbb{Q}(\alpha)$ et $\mathcal{O} = \mathbb{Z}[\alpha]$.*

(i) Dans la **direction** *$j_c = 1$ la longueur de la période du développement est $l = 4$ et la suite des points extrémaux de $\mathcal{O}$ et leur norme sont donnés par le tableau suivant:*

k	coordonnées de $\psi_k^{(1)}$	$\psi_k^{(1)}$	$N(\psi_k^{(1)})$
0	$(0,0,0,1)$	1	1
1	$(1,0,0,0)$	α	$-c$
2	$(c,1,0,0)$	α^2	c^2
3	$(c^2+c-1,c,1,0)$	α^3	$-c^3$
4	$(c^2+2c,c+1,1,1)$	$1+\alpha+\alpha^2+\alpha^3$	1

où la deuxième colonne désigne les coordonnées de $\psi_k^{(1)}$ *dans la base* $(\alpha_3, \alpha_2, \alpha_1, 1)$

avec $\begin{cases} \alpha_3 = \alpha \\ \alpha_2 = \alpha(\alpha - c) \\ \alpha_1 = \alpha^3 - c\alpha^2 - (c-1)\alpha \end{cases}$ *et* $N(\psi_k^{(1)})$ *désigne la norme de* $\psi_k^{(1)}$.

(ii) Dans la **direction** $j_c = 3$ *la longueur de la période du développement est* $l = 2$ *et la suite des points extrémaux de* $\mathcal{O}$ *et leur norme sont donnés par le tableau suivant:*

k	coordonnées de $\psi_k^{(3)}$	$N(\psi_k^{(3)})$
0	$(0,0,0,1)$	1
1	$(1,0,-1,0)$	c^2
3	$(-1,-1,1,c+1)$	1

Sous cette conjecture, on obtient le corollaire suivant :

Corollaire 3.4.4 *Un système fondamental d'unités de* $\mathcal{O}$ *est* $\{\epsilon_1, \epsilon_2\}$ *où* $\epsilon_1 = \dfrac{\alpha^3}{\alpha - c}$ *et* $\epsilon_2 = \alpha^2 + 1$.

Preuve

On a $r = 2$ donc pour obtenir un système fondamental d'unités de $\mathcal{O}$ on considère le développement dans deux directions (J. Buchmann [4]): on considère ici les directions $j_c = 1$ et $j_c = 3$.

On a

$$\psi_4^{(1)} \text{ est une première unité}$$

et

$$N(\psi_1^{(3)}) = N(\psi_2^{(1)})$$

donc

$$\{\psi_4^{(1)}; \frac{\psi_2^{(1)}}{\psi_1^{(3)}}\} \text{ est un système fondamental d'unités de } \mathcal{O}.$$

Or $\psi_4^{(1)} = \alpha^3 + \alpha^2 + \alpha + 1 = \dfrac{\alpha^3}{\alpha - c}$ et $\dfrac{\psi_2^{(1)}}{\psi_1^{(3)}} = \alpha^2 + 1$, ainsi en posant $\epsilon_1 = \psi_4^{(1)}$ et $\epsilon_2 = \dfrac{\psi_2^{(1)}}{\psi_1^{(3)}}$ on obtient le résultat énoncé.

Remarque : De même que précédemment, la suite des points extrémaux dans la direction $j_c = 1$ est donnée par le développement par l'AJP de $(\alpha_1, \alpha_2, \alpha_3)$ de la façon suivante :
en utilisant les mêmes notations que précédemment on a

$$M_1 = \mathcal{A}_{l-1},\ M_2 = \mathcal{A}_{l-2},\ M_3 = \mathcal{A}_{l-3},\ M_4 = \mathcal{A}_{l-6}\mathcal{A}_{l-5}\mathcal{A}_{l-4}$$

où $l = 6$ est la longueur du développement par l'AJP de $(\alpha_1, \alpha_2, \alpha_3)$.

CHAPITRE 4

Calculs des développements par Jacobi-Perron et en fraction continue de nombres algébriques

Dans ce chapitre nous décrivons un algorithme permettant de déterminer le développement par l'algorithme de Jacobi-Perron de n nombres algébriques réels et plus particulièrement celui en fraction continue si $n = 1$.
S. Lang, A. Trotter [17] et G. Cantor, P. Galyean, G. Zimmer [6] ont donné un algorithme, utilisant les polynômes réduits, qui fournit le développement en fraction continue d'un nombre algébrique.
E. Bombieri et A.J. van der Poorten [3] ont donné un algorithme simple qui fournit le développement en fraction continue de $\sqrt[3]{2}$. Pour cela ils donnent une formule explicite pour le calcul des quotients partiels notés c_h, à savoir

$$c_h = [\frac{(-1)^{h-1}}{q_{h-1}} \frac{3p_{h-1}^2}{p_{h-1}^3 - 2q_{h-1}^3} - \frac{q_{h-2}}{p_{h-1}}]$$

où p_h et q_h sont définis par

$$\begin{pmatrix} c_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} c_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} c_h & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} p_h & p_{h-1} \\ q_h & q_{h-1} \end{pmatrix} \quad \textit{pour tout } h \in \mathbb{N}.$$

Mais cette méthode ne se généralise pas de façon évidente. En effet, une formule analogue dans le cas général fait intervenir un terme d'erreur qu'on ne peut négliger qu'en utilisant le théorème de Roth qui n'est pas effectif.
P. Liardet et P. Stambul [21] donnent également un algorithme fournissant le développement en fraction continue de $\sqrt[3]{2}$ mais cette méthode utilise une mesure d'irrationalité de $\sqrt[3]{2}$ due à A. Baker, à savoir

$$|\sqrt[3]{2} - \frac{p}{q}| > \frac{10^{-6}}{q^{2,955}} \quad \textit{pour tout rationnel } \frac{p}{q} \textit{ (p et q premiers entre eux).}$$

Par contre, pour l'algorithme décrit ici le calcul ne fait intervenir que des nombres entiers, sans aucune condition du type précédent.
Après avoir démontré la validité de cet algorithme nous l'appliquons à certains nombres algébriques réels.
Enfin, nous donnons quelques exemples numériques dont le développement en fraction continue de $\sqrt[3]{2}$ et le développement par l'algorithme de Jacobi-Perron de $(\sqrt[3]{4}, \sqrt[3]{16})$.

4.1 Description de l'algorithme

4.1.1 Définitions et notations

Définition 4.1.1 *On dira qu'une matrice M à coefficients réels est* **positive** *si elle est à termes tous strictement positifs et* **positivement régulière** *s'il existe un entier $k > 0$ tel que M^k soit positive.*

Soit n un entier ($n \geq 1$) et $\alpha_1, \ldots, \alpha_n$, n entiers algébriques réels (strictement positifs) tels que $1, \alpha_1, \ldots, \alpha_n$ soient $\mathbb{Q}$-linéairement indépendants. On note $K = \mathbb{Q}[\alpha_1, \ldots, \alpha_n]$, d le degré de K sur $\mathbb{Q}$ et $m = d - 1$. On complète $\alpha_1, \ldots, \alpha_n$ par $\alpha_{n+1}, \ldots, \alpha_m$ tels que $\{1, \alpha_1, \ldots, \alpha_m\}$ soit une base de K sur $\mathbb{Q}$. On choisit un élément non nul ω de K tel que :

(1) $\omega > \max\limits_{2 \leq j \leq d} |\omega_j|$ où les ω_j sont les conjugués de ω dans $\mathbb{C}$;

(2) la transposée de la matrice de la multiplication par ω exprimée dans la base $\{\alpha_m, \ldots, \alpha_1, 1\}$, notée M, soit une matrice à coefficients entiers positivement régulière.

Notation : Contrairement à l'usage, les matrices seront, par la suite, notées de la façon suivante :

$$M = (a_{ij})_{\substack{0 \leq i \leq m \\ 0 \leq j \leq m}} = \begin{pmatrix} a_{m,m} & \cdot & \cdot & \cdot & a_{m,0} \\ \cdot & & & & \cdot \\ \cdot & & & & \cdot \\ \cdot & & & & \cdot \\ a_{0,m} & \cdot & \cdot & \cdot & a_{0,0} \end{pmatrix}$$

$M(n)$ désignera la matrice extraite de M en supprimant les lignes de numéro m à $(n+1)$. c'est-à-dire :

$$M(n) = (a_{ij})_{\substack{n+1 \leq i \leq m \\ 0 \leq j \leq m}} = \begin{pmatrix} a_{n+1,m} & \cdot & \cdot & \cdot & a_{n+1,0} \\ \cdot & & & & \cdot \\ \cdot & & & & \cdot \\ \cdot & & & & \cdot \\ a_{0,m} & \cdot & \cdot & \cdot & a_{0,0} \end{pmatrix}$$

4.1.2 Algorithme

On donne un algorithme qui fournit le développement par l'AJP de $(\alpha_1, \ldots, \alpha_n)$ jusqu'à l'ordre p donné.
Soit k_0 un entier tel que M^{k_0} soit à termes tous strictement positifs.

(1) $k = 0$, $\quad M_k = M^{k_0}(n)$. On note $M_k = (a_{ij})_{\substack{0 \leq i \leq n \\ 0 \leq j \leq m}}$.

(2) Si M_k vérifie la condition (C1) suivante :

(C1) Pour $0 \leq i \leq n$, les quotients de la division de a_{ij} par a_{0j} dans $\mathbb{Z}$ sont tous égaux pour $0 \leq j \leq m$.

alors on pose $b_i = [\frac{a_{ij}}{a_{0j}}]$ et

$$A = \begin{pmatrix} b_n & 1 & 0 & \dots & 0 \\ b_{n-1} & 0 & 1 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ b_1 & 0 & \dots & 0 & 1 \\ 1 & 0 & \dots & \dots & 0 \end{pmatrix}.$$

Si M_k ne vérifie pas la condition (C1) on passe à l'étape (4).

(3) On pose $H = A^{-1}M_k = (h_{ij})_{\substack{0\leq i\leq n \\ 0\leq j\leq m}}$. On peut remarquer que H est à coefficients positifs ou nuls.
Si H vérifie la condition (C2) suivante:

(C2) Pour $0 \leq j \leq m$, $h_{0j} > 0$,

alors on a $A = \mathcal{A}_k$ (où $\mathcal{A}_k$ désigne la k-ième matrice de l'algorithme de Jacobi-Perron définie dans le premier chapitre) et on pose $M_{k+1} = H$, $k = k+1$. Si $k < p$ on passe à l'étape (2), sinon on s'arrête.
Si H ne vérifie pas la condition (C2) on passe à l'étape (4).

(4) $M_k = M_k M$. On réitère cette opération jusqu'à ce que M_k soit à termes tous strictement positifs. On passe à l'étape (2).

4.2 Preuve de l'algorithme

On montre que l'algorithme précédent fournit le développement par l'AJP de $(\alpha_1, \dots, \alpha_n)$, i.e. à chaque étape on a $A = \mathcal{A}_k$. Pour cette démonstration on utilise le théorème de Frobenius [15] suivant:

Théorème 4.2.1 *Soit A une matrice carrée à coefficients réels d'ordre n positivement régulière alors:*

(a) A admet un vecteur propre x^0 à termes tous strictement positifs tel que $Ax^0 = \lambda_0 x^0$.

(b) Si $\lambda \neq \lambda_0$ est une autre valeur propre de A alors $|\lambda| < \lambda_0$.

(c) Il existe un n-uple f^0 à termes tous strictement positifs tel que ${}^t f^0 A = \lambda_0 \, {}^t f^0$ et tel que

$$\sum_{i=1}^{n} x_i^0 f_i^0 = 1.$$

(d) En posant $P = (x_i^0 f_j^0)_{\substack{0\leq i\leq n \\ 0\leq j\leq n}}$, on a $\lim_{k\to\infty} \frac{1}{\lambda_0^k} A^k = P$.

1) Premièrement on montre qu'il est toujours possible de construire une matrice M_k, à partir d'une matrice M positivement régulière, vérifiant la condition (C1) et telle que $H = A^{-1}M_k$ vérifie la condition (C2).

M étant positivement régulière, on peut utiliser le théorème de Frobenius par lequel on a :

(i) ω est la seule valeur propre de M de plus grand module dont le vecteur propre associé est :

$$\Omega = \begin{pmatrix} \alpha_m \\ \vdots \\ \alpha_1 \\ 1 \end{pmatrix}$$

(ii) $\lim_{l\to\infty} \frac{1}{\omega^l} M^l = P$ avec $P = (\alpha_i \lambda_j)_{\substack{0\le i\le m \\ 0\le j\le m}}$ (en notant $\alpha_0 = 1$) où $\Lambda = \begin{pmatrix} \lambda_m \\ \vdots \\ \lambda_1 \\ \lambda_0 \end{pmatrix}$

est à termes tous strictement positifs.

On en déduit que pour tout $\epsilon > 0$, il existe $l_0 > 0$ tel que si $l > l_0$, alors, en notant $M^l = (a_{ij})_{\substack{0\le i\le m \\ 0\le j\le m}}$, on a $|\frac{a_{ij}}{a_{0j}} - \frac{\alpha_i \lambda_j}{\alpha_0 \lambda_j}| < \epsilon$.

Or $\alpha_i \neq [\alpha_i]$, donc pour tout l assez grand on aura $[\frac{a_{ij}}{a_{0j}}] = [\alpha_i]$.

C'est-à-dire que pour tout i, $0 \le i \le n$, les quotients de a_{ij} par a_{0j}, notés b_i, sont tous égaux pour $0 \le j \le m$.

On a de plus

$$\lim_{l\to\infty} \frac{1}{\omega^l} A^{-1} M^l(n) = A^{-1} P(n) = \begin{pmatrix} \lambda_m & \cdots & \lambda_0 \\ (\alpha_n - b_n)\lambda_m & \cdots & (\alpha_n - b_n)\lambda_0 \\ \cdot & \cdots & \cdot \\ \cdot & \cdots & \cdot \\ (\alpha_1 - b_1)\lambda_m & \cdots & (\alpha_1 - b_1)\lambda_0 \end{pmatrix}.$$

Donc pour tout l assez grand la matrice H définie dans (3) par $H = A^{-1} M^l(n)$ vérifie la condition (C2), à savoir $h_{0j} > 0$, pour $0 \le j \le m$.

2) On montre à présent que si les b_i sont définis par (2) alors $b_i = [\alpha_i]$ $(1 \le i \le n)$.

On a

$$H = \begin{pmatrix} a_{0,m} & \cdots & a_{0,0} \\ a_{n,m} - a_{0,m} b_n & \cdots & a_{n,0} - a_{0,0} b_n \\ \cdot & \cdots & \cdot \\ \cdot & \cdots & \cdot \\ a_{1,m} - a_{0,m} b_1 & \cdots & a_{1,0} - a_{0,0} b_1 \end{pmatrix}$$

ω étant la valeur propre de M associée au vecteur propre Ω, il existe un entier $l > 0$ tel que $M_k \Omega = \omega^l \Omega(n)$, c'est-à-dire :

$$\begin{pmatrix} a_{n,m} & \cdots & a_{n,0} \\ \cdot & \cdots & \cdot \\ \cdot & \cdots & \cdot \\ \cdot & \cdots & \cdot \\ a_{0,m} & \cdots & a_{0,0} \end{pmatrix} \begin{pmatrix} \alpha_m \\ \vdots \\ \alpha_1 \\ 1 \end{pmatrix} = \omega^l \begin{pmatrix} \alpha_n \\ \vdots \\ \alpha_1 \\ 1 \end{pmatrix};$$

d'où (pour $0 \leq i \leq n$)

$$\alpha_i = \frac{\sum_{j=0}^{m} a_{ij}\alpha_j}{\sum_{j=0}^{m} a_{0j}\alpha_j},$$

i.e.

$$\alpha_i = b_i + \frac{\sum_{j=0}^{m}(a_{ij} - a_{0j}b_i)\alpha_j}{\sum_{j=0}^{m} a_{0j}\alpha_j};$$

$b_i = [\frac{a_{ij}}{a_{0j}}]$ entraîne que $0 < \frac{\sum_{j=0}^{m}(a_{ij} - a_{0j}b_i)\alpha_j}{\sum_{j=0}^{m} a_{0j}\alpha_j} < 1,$

i.e. $b_i = [\alpha_i]$ (pour $0 \leq i \leq n$).
Ainsi on a montré que $A = \mathcal{A}_0$.

3) Montrons par récurrence que l'algorithme fournit le développement par l'AJP de $(\alpha_1, \ldots, \alpha_n)$ jusqu'au rang p.

Soit (H_k) l'hypothèse : jusqu'au rang k on a $A = \mathcal{A}_k$.
Précédemment on a montré (H_0), supposons donc (H_k) et montrons (H_{k+1}).
On a $\lim_{l\to\infty} \frac{1}{\omega^l}\mathcal{A}_k^{-1}\ldots\mathcal{A}_0^{-1}M^l(n) = \mathcal{A}_k^{-1}\ldots\mathcal{A}_0^{-1}P(n)$
et $\mathcal{A}_k^{-1}\ldots\mathcal{A}_0^{-1}P(n) = \frac{1}{\alpha_n^{k+1}}\ldots\frac{1}{\alpha_n^1}(\alpha_i^{k+1}\lambda_j)_{\substack{0\leq i\leq n\\ 0\leq j\leq m}}$ (E)
où α_i^{k+1} sont les réels définis par le développement par l'AJP de $(\alpha_1, \ldots, \alpha_n)$.
En effet,

$$\mathcal{A}_0^{-1}P(n) = \begin{pmatrix} 0 & \ldots & \ldots & 0 & 1 \\ 1 & 0 & \ldots & 0 & -a_n^0 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \ldots & 0 & 1 & -a_1^0 \end{pmatrix} \begin{pmatrix} \alpha_n\lambda_m & . & . & . & \alpha_n\lambda_0 \\ . & & & & . \\ . & & & & . \\ . & & & & . \\ \lambda_m & . & . & . & \lambda_0 \end{pmatrix};$$

d'où

$$\mathcal{A}_0^{-1}P(n) = \begin{pmatrix} \lambda_m & . & . & . & \lambda_0 \\ (\alpha_n - a_n^0)\lambda_m & . & . & . & (\alpha_n - a_n^0)\lambda_0 \\ . & & & & . \\ . & & & & . \\ (\alpha_1 - a_1^0)\lambda_m & . & . & . & (\alpha_1 - a_1^0)\lambda_0 \end{pmatrix} = \frac{1}{\alpha_n^1}(\alpha_i^1\lambda_j)_{\substack{0\leq i\leq n\\ 0\leq j\leq m}}$$

et par récurrence on obtient la formule (E).
En remplaçant dans les démonstrations précédentes $(\alpha_1, \ldots, \alpha_n)$ par $(\alpha_1^{k+1}, \ldots, \alpha_n^{k+1})$ on obtient $b_i = [\alpha_i^{k+1}]$ soit $A = \mathcal{A}_{k+1}$ ce qui termine la démonstration.

4.3 Application à certains nombres algébriques

4.3.1 Développement des racines r-ièmes

Soit $(\alpha_1, \ldots, \alpha_n) = (\sqrt[r]{d}, \sqrt[r]{d^2}, \ldots, \sqrt[r]{d^n})$ où r et n sont des entiers tels que $r \geq 2$ et $1 \leq n \leq r-1$ et d est un entier différent d'une puissance r-ième.

L'algorithme décrit précédemment nous permet de donner le développement par l'AJP de $(\alpha_1, \ldots, \alpha_n)$.
En effet,
on pose $K = \mathbb{Q}(\sqrt[r]{d})$,
une base de K sur $\mathbb{Q}$ est $\mathcal{B} = \{\sqrt[r]{d}^{r-1}, \ldots, \sqrt[r]{d}, 1\}$.
On choisit $\omega = 1 + \sqrt[r]{d} + \ldots + \sqrt[r]{d}^{r-1}$,
et on peut vérifier que la transposée de la matrice de la multiplication par ω exprimée dans la base $\mathcal{B}$ est positive. Ainsi on peut appliquer l'algorithme précédent avec $k_0 = 1$.

4.3.2 Autres nombres algébriques

Définition 4.3.1 *Soit* $f(X) = a_r X^r - (a_{r-1}X^{r-1} + \ldots + a_0)$ *un polynôme irréductible de* $\mathbb{Z}[X]$. *On dit que* f *est* **positivement réduit** *si et seulement si* $a_r a_0 > 0$, $a_i \geq 0$ $(1 \leq i \leq r-1)$ *et il existe deux entiers* k_1 *et* k_2 *premiers entre eux tels que* $a_{k_1} a_{k_2} > 0$.

Soient α la seule racine réelle positive de f (l'unicité de cette racine est donnée par la règle de Descartes [23]) et $(\alpha_1, \ldots, \alpha_n) = (\alpha, \alpha^2, \ldots, \alpha^n)$ où $n \leq r-1$.

On peut utiliser l'algorithme précédent pour donner le développement par l'AJP de $(\alpha_1, \ldots, \alpha_n)$.
En effet,
on pose $K = \mathbb{Q}(\alpha)$,
une base de K sur $\mathbb{Q}$ est $\{\alpha^{r-1}, \ldots, \alpha, 1\}$.
On choisit $\omega = a_r \alpha$,
et la transposée de la matrice de la multiplication par ω exprimée dans la base $\{\alpha^{r-1}, \ldots, \alpha, 1\}$ est

$$M = \begin{pmatrix} a_{r-1} & \ldots & \ldots & \ldots & a_0 \\ a_r & 0 & \ldots & 0 & 0 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \ldots & 0 & a_r & 0 \end{pmatrix}.$$

Lemme 4.3.2 *f est positivement réduit implique que M est positivement régulière.*

Preuve
Pour montrer que M est positivement régulière, on utilise la proposition [8] suivante :

Proposition 4.3.3 *Soit* $A = (a_{ij})_{\substack{0 \leq i \leq n \\ 0 \leq j \leq n}}$ *une matrice carrée d'ordre n à termes réels positifs ou nuls. Soit $G(A)$ le graphe orienté associé à A de la façon suivante:*

- *les sommets de $G(A)$ sont $1, 2, \ldots, n$,*

- *$G(A)$ possède un arc de i vers j si $a_{ij} \neq 0$.*

Alors les deux propositions suivantes sont équivalentes :

(i) A est positivement régulière.

(ii) $G(A)$ est un graphe fortement connexe (i.e. pour tout couple (x,y) de sommets il existe un chemin de x à y et un chemin de y à x) tel que le PGCD des longueurs des circuits (chemin $(x_1,\ldots,x_q)$ tel que $x_1 = x_q$) de $G(A)$ soit égal à 1.

$a_r a_0 > 0$ entraîne que $G(M)$ est fortement connexe
et
f positivement réduit entraîne que le PGCD des longueurs des circuits est égal à 1 (en effet, il existe deux circuits de longueur respective k_1 et k_2).
M étant à termes tous positifs ou nuls, la proposition 4.3.3 implique donc que M est positivement régulière. Ceci termine la démonstration du lemme 4.3.2.

D'après le théorème de Frobenius, ω est la valeur propre de M de plus grand module ce qui nous permet d'utiliser l'algorithme précédent.

Remarque 4.3.4 *Si $f(X) = a_r X^r - (a_{r-1}X^{r-1} + \ldots + a_0)$ avec $a_r a_0 > 0$, $a_i \geq 0$ $(1 \leq i < r-1)$, $a_{r-1} < 0$ est tel qu'il existe deux entiers k_1 et k_2 premiers entre eux tels que $a_{k_1} a_{k_2} > 0$ (on dira que f est* **"presque positivement réduit"***) alors en remplaçant ω par $a_r \alpha + |a_{r-1}|$ on aura*

$$M = \begin{pmatrix} a_{r-1} + |a_{r-1}| & \ldots & \ldots & \ldots & a_0 \\ a_r & |a_{r-1}| & \ldots & 0 & 0 \\ 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & |a_{r-1}| & \vdots \\ 0 & \ldots & 0 & a_r & |a_{r-1}| \end{pmatrix}$$

qui est positivement régulière.

4.4 Le cas des fractions continues

On étudie dans ce paragraphe comment appliquer l'algorithme dans le cas des fractions continues à un nombre algébrique α.

Soit α une racine réelle d'un polynôme irréductible P de degré $r \geq 2$ de $\mathbb{Z}[X]$. Soit $[c_0, c_1, \ldots, c_h, \ldots]$ le développement en fraction continue de α. On peut construire une suite de polynômes P_h de $\mathbb{Z}[X]$ par :

$$\begin{cases} P_0 = P \\ P_{h+1}(X) = -X^r P_h(c_h + \dfrac{1}{X}) \end{cases}.$$

D'après H. Zassenhaus [30] les polynômes P_h admettent α_h, quotients complets de α, pour racine et pour h suffisamment grand, A.G. Akritas [1] a montré que ce résultat peut être rendu effectif, les autres racines, notées β_h, vérifient

$$|\beta_h| < 1 \quad \text{et} \quad -1 < \mathrm{Re}(\beta_h) < 0,$$

où $\mathrm{Re}(\beta_h)$ désigne la partie réelle de β_h. On dit que P_h (ou α_h) est réduit.

Pour développer α en fraction continue, on construit la suite des polynômes P_h (en utilisant, par exemple, l'algorithme de G. Cantor, P. Galyean et G. Zimmer[3]) et si P_h est positivement réduit ou presque positivement réduit on peut alors utiliser l'algorithme précédent pour développer α_h.
Nous donnons dans la proposition suivante une condition suffisante pour que P_h soit positivement réduit.

Proposition 4.4.1 *(i) Si $r = 2$, alors P_h réduit équivaut à P_h positivement réduit.*

(ii) Si $r \geq 3$, alors P_h réduit et $c_h \geq r-1$ impliquent que P_{h+1} est positivement réduit.

Preuve
(i) étant évident, montrons (ii). En notant

$$P_h(X) = a_r X^r - (a_{r-1}X^{r-1} + \ldots + a_0) = a_r(X - \alpha_h)\sum_{j=0}^{r-1} s_j X^{r-j-1},$$

on a, pour $0 \leq j \leq r-1$, $s_j > 0$ et $\dfrac{a_{r-j}}{a_r} = \alpha_h s_{j-1} - s_j$.
En posant

$$P_{h+1}(X) = A_r X^r - (A_{r-1}X^{r-1} + \ldots + A_0),$$

on a d'après la formule de Taylor,

$$P_{h+1}(X) = -X^r P_h(c_h) + \sum_{k=0}^{r-1} \frac{P^{(r-k)}(c_h)}{(r-k)!} X^k;$$

donc, pour $0 \leq k < r$

$$A_k = \binom{r}{k} a_r c_h^k - \sum_{l=1}^{k} \binom{r-l}{k-l} a_{r-l} c_h^{k-l}.$$

D'où (pour $0 \leq k < r$, $1 \leq l \leq k$)

$$\frac{A_k}{a_r} = \sum_{l=0}^{k-1} s_l \left(\binom{r-l}{k-l} c_h^{k-l} - \binom{r-l-1}{k-l-1} c_h^{k-l-1}\alpha \right) + s_k.$$

Posons

$$A = \binom{r-l}{k-l} c_h^{k-l} - \binom{r-l-1}{k-l-1} c_h^{k-l-1}\alpha;$$

$c_h \leq \alpha < c_h + 1$ implique que

$$A > c_h^{k-l-1} \left(c_h \binom{r-l-1}{k-l} - \binom{r-l-1}{k-l-1} \right),$$

i.e. $A > c_h^{k-l-1} \dfrac{(r-l-1)!}{(k-l)!(r-k-1)!} \left(c_h - \dfrac{k-l}{r-k} \right)$

et $c_h \geq r-1$ implique que $c_h - \dfrac{k-l}{r-k} \geq 0$, i.e. $A > 0$.
Or pour $0 \leq l \leq k$, on a $s_l > 0$, donc pour $0 \leq k < r$, on a $A_k > 0$.
Or $A_r = -P_h(c_h) > 0$, donc P_{h+1} est positivement réduit.

Remarque 4.4.2 *(a) Si $r = 3$, alors P_h réduit et $c_h \geq 1$ impliquent que P_h ou P_{h+1} ou P_{h+2} est positivement réduit.*
(b) Si $r > 3$, alors P_h réduit et $c_h \geq r-2$ impliquent que P_{h+1} est presque positivement réduit. Dans ce cas on ne peut pas remplacer la borne $(r-2)$ par 1. En effet, le polynôme $P_h(X) = 8X^4 + 2X^3 - 14X^2 - 13X - 3$ fournit un contre-exemple. On a P_h réduit et $c_h = [\alpha_h] = 1$, or P_{h+1} n'est pas positivement réduit.

4.5 Exemples numériques

4.5.1 Développement en fraction continue

On développe $\sqrt[3]{2}$ en fraction continue à l'ordre 1000.

Pour cela, on choisit $\omega = 1 + \sqrt[3]{2} + \sqrt[3]{4}$ et on utilise l'algorithme précédent avec

$$M = \begin{pmatrix} 1 & 2 & 2 \\ 1 & 1 & 2 \\ 1 & 1 & 1 \end{pmatrix}.$$

Les calculs ont été effectués sur une station Sun Sparc1 avec le langage Pari développé par C. Batut, D. Bernardi, H. Cohen et M. Olivier.
On constate alors que ces calculs sont nettement plus rapides (6 ms) et la taille des entiers nécessaires au calcul (environ 170 chiffres) plus petite qu'en utilisant les formules données par E. Bombieri et A.J. Van der Poorten (6mn et 507 chiffres).

4.5.2 Développement par l'algorithme de Jacobi-Perron

On développe $(\sqrt[3]{4}, \sqrt[3]{16})$ par l'algorithme de Jacobi-Perron à l'ordre 2000.

Pour cela, on choisit $\omega = 1 + \sqrt[3]{4} + \sqrt[3]{16}$ et on utilise l'algorithme précédent avec

$$M = \begin{pmatrix} 1 & 4 & 4 \\ 1 & 1 & 4 \\ 1 & 1 & 1 \end{pmatrix}.$$

On constate que les plus grands entiers intervenant dans la suite des quotients incomplets sont $(1920, 2002)$ à l'ordre 1799 ainsi qu'une erreur dans la table donnée par G. Rhin [25]. Les plus grands entiers nécessaires au calcul ont environ 990 chiffres.
On peut remarquer que, pour cet exemple, en remplaçant dans l'algorithme M par $\frac{1}{9}M^3$ (matrice de déterminant 1) on diminue considérablement la taille (81 chiffres) des entiers nécessaires au calcul (par contre le temps est environ le même).

4.5.3 Développement en fraction continue de α où α est une racine de $P(X) = X^7 - 7X + 3$

P admet 3 racines réelles. Notons α l'une d'entre elles. En construisant la suite des polynômes P_h définies dans le paragraphe précédent on constate que P_4 est positivement

réduit. On note $P_4 = \sum_{i=0}^{7} a_i X^i$ et α_4 la racine réelle de P_4. On considère $\omega = a_7\alpha_4$ et l'algorithme précédent nous fournit le développement en fraction continue de α_4 et donc de α (quel que soit α, racine réelle de P).

APPENDICE A

Algorithme (Ar). Application à la triangularisation d'une matrice sous forme HNF

Nous donnons ici, en complément du chapitre 3, la description de l'algorithme (Ar) et sa programmation en PARI. Nous l'appliquons ensuite à la matrice 20×20 [?] citée dans ce même chapitre.

A.1 Principe de l'algorithme (Ar)

Soient n et r deux entiers strictement positifs tels que $r \leq n$. Soit x une matrice $n \times r$, on note

$$x = (x_{ij})_{\substack{0 \leq i \leq n \\ 0 \leq j \leq r}} = \begin{pmatrix} x_{11} & \cdot & \cdot & \cdot & x_{1r} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ x_{n1} & \cdot & \cdot & \cdot & x_{nr} \end{pmatrix}.$$

Rappelons que l'algorithme (Ar) fournit une matrice U, $n \times n$, unimodulaire telle que

$$U^{-1}x = \left(\begin{array}{c|ccc} d_1 & \star & \dots & \star \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \star \\ 0 & \dots & 0 & d_r \\ \hline & 0 & & \end{array} \right)$$

où $U^{-1}x$ est une matrice HNF.
Appliquer l'algorithme (Ar) à x consiste à appliquer l'algorithme (A1) successivement aux colonnes de x.

On note s l'indice de la colonne sur laquelle on travaille :

(1) $s = 1$. On applique l'algorithme (A1) à $(x_{11}, \dots, x_{n1})^t$. Ainsi on obtient une matrice U_1, $n \times n$, unimodulaire telle que la première colonne de $U_1^{-1}x$ soit $(d_1, 0, \dots, 0)^t$ où $d_1 = pgcd(x_{11}, \dots, x_{n1})$.

(2) $s = 2$. De même, (A1) nous fournit une matrice U_2, $n \times n$, unimodulaire telle que les deux premières colonnes de $U_2^{-1}U_1^{-1}x$ soient de la forme $\begin{pmatrix} d_1 & x_{12} \\ 0 & d_2 \\ \vdots & 0 \\ \vdots & \vdots \\ 0 & 0 \end{pmatrix}$.

Si $d_2 < 0$, on multiplie $U_2^{-1}U_1^{-1}x$ par $\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & -1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & 1 \end{pmatrix}$.

En posant $H = \begin{pmatrix} \left|\begin{matrix} 1 & \left[\frac{x_{12}}{d_2}\right] \\ 0 & 1 \end{matrix}\right| & \mathbf{0} \\ \mathbf{0} & \underbrace{\left|\begin{matrix} 1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & 1 \end{matrix}\right|}_{r-2} \end{pmatrix}$,

les deux premières colonnes de $H^{-1}U_2^{-1}U_1^{-1}x$ sont $\begin{pmatrix} d_1 & r_2 \\ 0 & d_2 \\ \vdots & 0 \\ \vdots & \vdots \\ 0 & 0 \end{pmatrix}$, avec $0 \leq r_2 < d_2$.

(3) $s = 3$. On poursuit ce processus .....

A.2 Description de l'algorithme (Ar)

(1) $s = 1$, $x_s = x$.

(2) Tant que $s \leq r$:

(a) $k = 1$, $x^{(k)} = x_s$.

(b) Tant que $(x_1^{(k)}, \dots, x_s^{(k)}) \neq \begin{pmatrix} \left|\begin{matrix} d_1 & \star & \dots & \star \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \star \\ 0 & \dots & 0 & d_s \end{matrix}\right| \\ \mathbf{0} \end{pmatrix}$:

soit j le plus petit entier positif tel que $x_{n-j,s}^{(k)} \neq 0$,

pour $s \leq i \leq n-j-1$ on pose $a_k^i = \left[\frac{x_{i,s}^{(k)}}{x_{n-j,s}^{(k)}}\right]$,

$$h_k = \begin{pmatrix} \overbrace{\begin{vmatrix} 1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & 1 \end{vmatrix}}^{s-1} & 0 & 0 \\ 0 & \begin{vmatrix} a_k^1 & 1 & 0 & \dots & 0 \\ a_k^2 & 0 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ a_k^{n-j-1} & 0 & \dots & 0 & 1 \\ 1 & 0 & \dots & \dots & 0 \end{vmatrix} & 0 \\ 0 & 0 & \underbrace{\begin{vmatrix} 1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & 1 \end{vmatrix}}_{j} \end{pmatrix}.$$

$x^{(k+1)} = h_k^{-1} x^{(k)},\ k = k+1\ .$

(c) On note $k_0 = k,\ u_s = \prod_{k=1}^{k_0} h_k,\ x_s = x^{(k_0)},$

$$h_{s_1} = \begin{pmatrix} \overbrace{\begin{vmatrix} 1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & 1 \end{vmatrix}}^{s-1} & \begin{matrix} 0 \\ \vdots \\ 0 \end{matrix} & 0 \\ 0 & signe(x_{ss}^{(k)}) & 0 \\ 0 & 0 & \underbrace{\begin{vmatrix} 1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & 1 \end{vmatrix}}_{n-s} \end{pmatrix},$$

$x_s = h_{s_1}^{-1} x_s.$

Pour $1 \leq i \leq s-1$ on pose $b_k^i = \left[\frac{x_{i,s}^{(k)}}{x_{s,s}^{(k)}}\right]$,

$$h_{s_2} = \begin{pmatrix} \overbrace{\begin{vmatrix} 1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & 1 \end{vmatrix}}^{s-1} & \begin{matrix} b_k^1 \\ \vdots \\ b_k^{s-1} \\ 0 \end{matrix} & \begin{matrix} \\ 0 \\ \\ \end{matrix} \\ \begin{matrix} \\ 0 \\ \\ \end{matrix} & \begin{matrix} \\ signe(x_{ss}^{(k)}) \\ \\ \end{matrix} & \begin{matrix} \\ 0 \\ \\ \end{matrix} \\ \begin{matrix} \\ 0 \\ \\ \end{matrix} & \begin{matrix} \\ 0 \\ \\ \end{matrix} & \underbrace{\begin{vmatrix} 1 & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & 1 \end{vmatrix}}_{n-s} \end{pmatrix}.$$

$x_s = h_{s_2}^{-1} x_s.$

(3) On note $k_s = k$, $s = s+1$, $U = \prod_{s=1}^{r} u_s h_{s1} h_{s2}$.

A.3 Programme en PARI

A.3.1 Notations

Entrée : x désigne une matrice $n \times r$ où $r \leq n$.

Sortie : x est sous Forme Normale d'Hermite.

u =matricebase(x) est la matrice de passage ($n \times n$ et unimodulaire).

A.3.2 Programme

initialiser n et r;
x =matrix($n, r, j, k, 0$);

```
{matricebase(x)=u=matrix(n,n,j,k,if(j-k,0,1));
                maux=u;
                h=maux;
                for(s=1,r,
                    for(j=0,n-s-1,
                        while(x[n-j,s],
                            a=vector(n-j,k,x[k,s]/x[n-j,s]);
                            for(k=1,s-1,
                                h[k, ]=maux[k, ]);
                            for(k=1,n-j-s,
                                h[k+s-1, ]=maux[k+s, ];
                                h[k+s-1,s]=round(a[k+s-1]));
                            h[n-j, ]=maux[s, ];
                            for(k=0,j-1,
```

```
                    h[n-k, ]=maux[n-k, ]);
                u=u*h;
                x=h^-1*x));
        h=maux;
        h[s,s]=sign(x[s,s]);
        x=h^-1*x;
        u=u*h;
        for(k=1.s-1.
            h[k.k]=sign(x[k,k]);
            qr=floor(x[k,s]/x[s,s]);
            h[k,s]=qr*sign(x[s,s]));
        h[s,s]=sign(x[s,s]);
        u=u*h;
        x=h^-1*x);
print(x);
u;}
```

A.4 Application

On considère la matrice 20×20 suivante [13] :

$$x = \begin{pmatrix}
10 & 8 & 10 & 5 & 5 & 10 & 0 & 8 & 5 & 9 & 8 & 3 & 0 & 9 & 9 & 2 & 7 & 6 & 0 & 4 \\
4 & 10 & 8 & 5 & 2 & 6 & 5 & 1 & 2 & 6 & 9 & 1 & 4 & 6 & 2 & 7 & 7 & 1 & 4 & 10 \\
2 & 4 & 6 & 4 & 3 & 0 & 3 & 0 & 10 & 2 & 3 & 0 & 6 & 7 & 5 & 7 & 7 & 3 & 3 & 2 \\
1 & 5 & 0 & 4 & 8 & 0 & 10 & 10 & 2 & 0 & 5 & 3 & 6 & 10 & 2 & 10 & 2 & 10 & 10 & 2 \\
9 & 8 & 5 & 4 & 10 & 6 & 3 & 10 & 3 & 8 & 7 & 4 & 7 & 1 & 5 & 8 & 6 & 8 & 3 & 1 \\
10 & 3 & 1 & 0 & 0 & 9 & 8 & 2 & 1 & 6 & 0 & 10 & 7 & 4 & 9 & 2 & 3 & 10 & 2 & 9 \\
8 & 2 & 8 & 0 & 0 & 9 & 3 & 0 & 7 & 8 & 0 & 3 & 4 & 5 & 3 & 8 & 1 & 4 & 4 & 9 \\
0 & 4 & 8 & 6 & 0 & 1 & 5 & 0 & 0 & 3 & 4 & 6 & 9 & 5 & 10 & 10 & 3 & 5 & 9 & 9 \\
4 & 6 & 4 & 8 & 9 & 2 & 5 & 6 & 9 & 8 & 9 & 3 & 6 & 7 & 3 & 8 & 5 & 10 & 1 & 7 \\
2 & 0 & 7 & 10 & 8 & 4 & 7 & 5 & 3 & 7 & 1 & 10 & 6 & 2 & 2 & 9 & 9 & 9 & 1 & 10 \\
2 & 2 & 1 & 5 & 4 & 1 & 4 & 4 & 6 & 7 & 0 & 10 & 0 & 2 & 5 & 1 & 9 & 10 & 2 & 5 \\
4 & 1 & 10 & 2 & 4 & 0 & 9 & 7 & 8 & 9 & 9 & 3 & 3 & 9 & 10 & 1 & 7 & 1 & 3 & 1 \\
5 & 3 & 3 & 9 & 2 & 1 & 4 & 2 & 7 & 8 & 5 & 7 & 5 & 5 & 9 & 4 & 5 & 4 & 10 & 6 \\
4 & 8 & 10 & 1 & 0 & 8 & 10 & 4 & 4 & 10 & 3 & 10 & 7 & 4 & 5 & 7 & 3 & 2 & 1 & 2 \\
6 & 9 & 4 & 7 & 10 & 3 & 6 & 9 & 5 & 8 & 4 & 6 & 9 & 8 & 7 & 5 & 9 & 8 & 9 & 7 \\
5 & 10 & 5 & 6 & 10 & 0 & 9 & 5 & 1 & 4 & 0 & 9 & 8 & 9 & 3 & 5 & 2 & 2 & 0 & 8 \\
1 & 3 & 10 & 2 & 5 & 5 & 1 & 1 & 10 & 6 & 10 & 4 & 3 & 8 & 1 & 6 & 1 & 2 & 6 & 9 \\
6 & 4 & 1 & 5 & 8 & 2 & 3 & 1 & 3 & 7 & 4 & 10 & 2 & 9 & 10 & 3 & 3 & 6 & 5 & 8 \\
3 & 7 & 5 & 2 & 10 & 0 & 10 & 4 & 0 & 0 & 10 & 3 & 2 & 9 & 5 & 1 & 7 & 10 & 5 & 3 \\
10 & 2 & 10 & 6 & 2 & 9 & 3 & 2 & 0 & 2 & 5 & 3 & 3 & 1 & 5 & 5 & 10 & 0 & 7 & 3
\end{pmatrix}.$$

En appliquant le programme précédent à x on obtient la matrice HNF :

$$\begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2493458668016156498 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 7556416162606434903 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 4231394917846061254 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 6550643086271827800 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 5894433903726787389 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2888190720018309095 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2295323497751105773 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 8561026937410374622 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 887407506661256647 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3774323279430667234 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 8991458640024406418 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 8774977490966952608 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 3028895122851664353 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 311014351189915057 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1639942404139121094 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 7095458530815061658 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 3582422800395622835 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 5352248112149263337 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 1516991708448737959 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 9253708263869640819
\end{pmatrix}$$

Le plus grand entier intervenant dans le calcul a 68 chiffres et le temps nécessaire au calcul est environ 2mn40s (sur un Macintosh Quadra 650).

APPENDICE B

Programme permettant de déterminer le développement par l'AJP de nombres réels algébriques

Nous donnons ici, en complément du chapitre 4, la programmation en PARI de l'algorithme, décrit dans ce chapitre, permettant de déterminer le développement par l'AJP de n nombres réels algébriques. Nous l'appliquons ensuite aux racines r-ièmes de 2 (pour $3 \leq r \leq 10$).

B.1 Programme en PARI

B.1.1 Notations

On rappelle que pour déterminer le développement par l'AJP de n nombres réels algébriques $(\alpha_1, \ldots, \alpha_n)$, il suffit de considérer une matrice, notée m, régulièrement positive qui est une matrice de multiplication par un élément ω de $\mathbb{Q}[\alpha_1, \ldots, \alpha_n]$.
En entrant :

n : le nombre de réels à développer
m : la matrice de multiplication par ω
dim : le rang de m
lg : la longueur du développement,

le programme suivant nous fournit la suite des quotients incomplets du développement par l'AJP de $(\alpha_1, \ldots, \alpha_n)$.

B.1.2 Programme

```
entrer m, dim, n et lg;

mid=matrix(dim,dim,j,k,if(j-k,0,1));
h1=m;
a=vector(n,j,0);
{boucle(j)=t=divres(ht[dim-j,1],ht[dim-j+1,1]);
           u=t[1];
           k=2;
```

```
            while(test,
                  t=divres(ht[dim-j,k],ht[dim-j+1,k]);
                  v=t[1];
                  if(abs(u-v),
                  test=0
                  ,
                  if(dim-k,
                    test=1;
                    a[j]=v
                    ,
                    test=0);
                  k=k+1));
            if(dim+1-k,
              test=0
              ,
              test=1;
              h=mid;
              h[,dim-j]=mid[,dim-j+1];
              h[,dim-j+1]=mid[,dim-j];
              h[dim-j+1,dim-j+1]=-v;
              ht=h*ht;
              if(n-j,
                boucle(j+1)
                ,
                ));}
tour=0;
ht=m;
while(tour<lg,
      ht=m;
      test=1;
      boucle(1);
      if(test,
        print(tour," ",a);
        tour=tour+1;
        m=ht
        ,
        m=m*h1));
```

B.2 Application

Nous donnons dans le tableau suivant la liste des plus grands quotients incomplets apparaissant dans le développement en fraction continue des racines r-ièmes de 2 (pour $3 \leq r \leq 10$), avec $lg < 1000$.

r	*plus grand quotient incomplet*	*ordre*
3	7451	571
4	1018	870
5	678	587
6	26088	538
7	4532	342
8	1244	177
9	3132	291
10	327	688

APPENDICE C

Calculs de points extrémaux. Résultats justifiant les conjectures du chapitre 3

A partir de la méthode de recherche de points extrémaux décrite dans le chapitre 3 on a écrit un algorithme (et un programme en Pari) permettant de calculer cette suite de points.
On a essentiellement appliqué ce programme aux corps $K = \mathbb{Q}(\alpha)$ de degré 4 où α est la racine réelle du polynôme

$$f(X) = X^4 - c^m X^3 - (c-1)X^2 - (c^m - 1)X - c^m$$

telle que $c^m < \alpha < c^m + 1$.

On a conjecturé précédemment que ces points sont donnés par le développement par l'AJP de $(\alpha_1, \alpha_2, \alpha_3)$ avec $\begin{cases} \alpha_3 = \alpha \\ \alpha_2 = \alpha(\alpha - c^m) \\ \alpha_1 = \alpha^3 - c^m\alpha^2 - (c-1)\alpha \end{cases}$.
On note :

λ la longueur du développement par l'AJP de $(\alpha_1, \alpha_2, \alpha_3)$.

$A_i = \mathcal{A}_{\lambda-i} \dots \mathcal{A}_{\lambda-1}$ (pour $0 \leq i \leq \lambda$) où les matrices $\mathcal{A}_\nu$ $(\lambda - i \leq \nu \leq \lambda - 1)$ sont les matrices associées au développement par l'AJP définies dans le premier chapitre.

ϕ_i le vecteur de $\mathbb{Z}^4$ dont les composantes sont obtenues par la dernière ligne de A_i.

j_c la direction.

l la longueur du développement par la généralisation de l'algorithme de Voronoï.

$(\psi_k)_{0 \leq k \leq l}$ la suite de points extrémaux qui sont exprimés par leurs coordonnées dans la base $(\alpha_3, \alpha_2, \alpha_1, 1)$.

C.1 m $\geq$ 2, direction j_c=1

m=2 (l=3)

k	$c = 2$ *(coordonnées de ψ_k)*	$c = 3$ *(coordonnées de ψ_k)*	$c = 4$ *(coordonnées de ψ_k)*	*AJP*
1	(18, 4, 1, 1)	(84, 9, 1, 1)	(260, 16, 1, 1)	ϕ_5
2	(40, 9, 2, 2)	(261, 28, 3, 3)	(1056, 65, 4, 4)	ϕ_6
3	(1841, 416, 94, 85)	(71282, 7650, 821, 793)	(1136387, 69952, 4306, 4241)	ϕ_{11}

m=3 (l=5)

k	$c = 2$ *(coordonnées de ψ_k)*	$c = 3$ *(coordonnées de ψ_k)*	*AJP*
1	(66, 8, 1, 1)	(732, 27, 1, 1)	ϕ_5
2	(272, 33, 4, 4)	(6615, 244, 9, 9)	ϕ_6
3	(37536, 4556, 553, 537)	(14606244, 538767, 19873, 19792)	ϕ_{10}
4	(77313, 9384, 1139, 1106)	(43998068, 1622916, 59863, 59619)	ϕ_{11}
5	(21975151, 2667273, 323745, 314361)	(292642436033, 10794430604, 398164168, 396541252)	ϕ_{16}

Liste des matrices A_i

On donne ici quelques exemples pour les matrices A_i de manière à justifier la dernière colonne des tableaux précédents : on note en caractères gras les points correspondant aux points extrémaux. Pour plus de clarté, les matrices seront notées sur une seule ligne : ainsi la matrice $\begin{pmatrix} 4 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$ sera notée $[4, 1, 0, 0; 1, 0, 1, 0; 0, 0, 0, 1; 1, 0, 0, 0]$.

$c = 2;\ m = 2;$

$A_1 = [4,1,0,0;1,0,1,0;0,0,0,1;1,0,0,0]$
$A_2 = [17,4,1,0;0,0,0,1;1,0,0,0;4,1,0,0]$
$A_3 = [17,4,1,1;1,0,0,0;4,1,0,0;17,4,1,0]$
$A_4 = [18,4,1,1;4,1,0,0;17,4,1,0;17,4,1,1]$
$A_5 = [40,9,2,2;17,4,1,0;35,8,2,2;\mathbf{18,\ 4,\ 1,\ 1}]$
$A_6 = [177,40,9,8;75,17,4,4;58,13,3,3;\mathbf{40,\ 9,\ 2,\ 2}]$
$A_7 = [783,177,40,36;58,13,3,3;40,9,2,2;177,40,9,8]$
$A_8 = [1624,367,83,75;40,9,2,2;177,40,9,8;783,177,40,36]$
$A_9 = [1664,376,85,77;177,40,9,8;783,177,40,36;1624,367,83,75]$
$A_{10} = [1841,416,94,85;783,177,40,36;1624,367,83,75;1664,376,85,77]$
$A_{11} = [8147,1841,416,376;3465,783,177,160;7187,1624,367,332;\mathbf{1841,\ 416,\ 94,\ 85}]$

$c = 2;\ m = 3;$

$A_1 = [8,1,0,0;1,0,1,0;0,0,0,1;1,0,0,0]$
$A_2 = [65,8,1,0;0,0,0,1;1,0,0,0;8,1,0,0]$
$A_3 = [65,8,1,1;1,0,0,0;8,1,0,0;65,8,1,0]$
$A_4 = [66,8,1,1;8,1,0,0;65,8,1,0;65,8,1,1]$
$A_5 = [272,33,4,4;65,8,1,0;263,32,4,4;\mathbf{66,\ 8,\ 1,\ 1}]$
$A_6 = [2241,272,33,32;535,65,8,8;338,41,5,5;\mathbf{272,\ 33,\ 4,\ 4}]$
$A_7 = [18463,2241,272,264;338,41,5,5;272,33,4,4;2241,272,33,32]$
$A_8 = [37264,4523,549,533;272,33,4,4;2241,272,33,32;18463,2241,272,264]$
$A_9 = [37536,4556,553,537;2241,272,33,32;18463,2241,272,264;37264,4523,549,533]$
$A_{10} = [77313,9384,1139,1106;18463,2241,272,264;74800,9079,1102,1070;$
$\mathbf{37536,\ 4556,\ 553,\ 537}]$
$A_{11} = [636967,77313,9384,9112;152113,18463,2241,2176;269475,32708,3970,3855;$
$\mathbf{77313,\ 9384,\ 1139,\ 1106}]$
$A_{12} = [5247849,636967,77313,75072;269475,32708,3970,3855;77313,9384,1139,1106;$
$636967,77313,9384,9112]$
$A_{13} = [21260871,2580576,313222,304143;77313,9384,1139,1106;636967,77313,9384,9112;$
$5247849,636967,77313,75072]$
$A_{14} = [21338184,2589960,314361,305249;636967,77313,9384,9112;5247849,636967,77313,75072;$
$21260871,2580576,313222,304143]$
$A_{15} = [21975151,2667273,323745,314361;5247849,636967,77313,75072;$
$21260871,2580576,313222,304143;21338184,2589960,314361,305249]$
$A_{16} = [181049057,21975151,2667273,2589960;43236022,5247849,636967,618504;$
$175164241,21260871,2580576,2505776;\mathbf{21975151,\ 2667273,\ 323745,\ 314361}]$

Cas général : Conjecture

Le lien avec l'AJP nous permet de conjecturer l'expression générale de ces points. Ainsi :

$\phi_5 = (c^{2m} + c, c^m, 1, 1)$ c'est-à-dire $\psi_1 = (c^{2m} + c)\alpha_3 + c^m\alpha_2 + \alpha_1 + 1 = \dfrac{c\alpha^2}{\alpha - c^m}$.

$\phi_6 = (c^{3m-1} + 2c^m, c^{2m-1} + 1, c^{m-1}, c^{m-1})$ c'est-à-dire $\psi_2 = \dfrac{\alpha^3}{\alpha - c^m}$.

$\phi_{10} = (c^{5m} + 4c^{3m+1} + c^{3m} + c^{2m} + 3c^{m+2}, c^{4m} + 3c^{2m+1} + c^{2m} + c^m + c^2,$
$c^{3m} + 2c^{m+1} + c^m + 1, c^{3m} + c^{m+1} + c^m + 1)$

c'est-à-dire $\psi_3 = \dfrac{c^2\alpha^4}{(\alpha - c^m)^2}$ *si* $m = 3$.

$\phi_{11} = (c^{6m-2} + 5c^{4m-1} + c^{4m-2} + c^{3m-2} + 6c^{2m} + c - 1, c^{5m-2} + 4c^{3m-1} + c^{3m-2} + c^{2m-2} + 3c^m,$
$c^{4m-2} + 3c^{2m-1} + c^{2m-2} + c^{m-2} + 1, c^{4m-2} + 2c^{2m-1} + c^{2m-2} + c^{m-2})$

c'est-à-dire $\begin{cases} \psi_3 = \alpha\left(\dfrac{\alpha^2}{\alpha - c^m}\right)^2 & \text{si } m = 2 \\ \psi_4 = \alpha\left(\dfrac{\alpha^2}{\alpha - c^m}\right)^2 & \text{si } m = 3 \end{cases}$

$\phi_{16} = \alpha\left(\dfrac{\alpha^2}{\alpha - c^m}\right)^3$.

C.2 Résultats complémentaires

On donne ici d'autres résultats tels qu'ils sont obtenus par le programme. En entrant c et m, ce programme fournit pour chaque direction :
-la liste des points extrémaux par leurs coordonnées dans la base $(\alpha_3, \alpha_2, \alpha_1, 1)$ (au signe près),
-la norme de ces points,
-la longueur du développement.
On peut remarquer que l'on ne peut paramétrer de façon simple les résultats obtenus pour $j_c = 2$ ou $j_c = 3$.

c=2; m=2

direction : 2

coordonnees	*norme*
$(-3, 4, -5, 25)$	-11
$(14, -18, 23, -118)$	2
$(-213, 273, -350, 1795)$	-9
$(-755, 968, -1241, 6364)$	12
$(968, -1241, 1591, -8159)$	-3
$(3432, -4400, 5641, -28928)$	4
$(4400, -5641, 7232, -37087)$	1

longueur = 7

direction : 3

coordonnees	*norme*
$(-1, 0, 1, 1)$	-7
$(2, -1, -2, 1)$	-1

longueur = 2

c=2; m=3

direction : 2

coordonnees	*norme*
$(6,-8,11,-121)$	-56
$(8,-11,15,-164)$	4
$(-882,1206,-1649,18038)$	-14
$(-2401,3283,-4489,49104)$	16
$(-3283,4489,-6138,67142)$	-2
$(-360801,493339,-674564,7378887)$	7
$(-982189,1342990,-1836329,20087144)$	-8
$(-1342990,1836329,-2510893,27466031)$	1

longueur = 8

direction : 3

coordonnees	*norme*
$(-1,-2,0,12)$	4
$(21,13,-11,-111)$	97
$(-43,-28,22,234)$	-2
$(1013,70,-737,-2609)$	1

longueur = 4

c=3; m=2

direction : 2

coordonnees	*norme*
$(-9,12,-16,191)$	-189
$(-9,12,-16,192)$	3
$(-1050,1399,-1864,22352)$	-7
$(-3159,4209,-5608,67248)$	9
$([4209,-5608,7472,-89600)$	-1

longueur = 5

direction : 3

coordonnees	*norme*
$(-3,-1,2,13)$	-1

longueur = 1

c=3; m=3

direction : 2

coordonnees	*norme*
$(57,-81,115,-4408)$	1541
$(505,-717,1018,-39025)$	2081
$(1515,-2151,3054,-117074)$	-137
$(94573,-134275,190644,-7308275)$	1817
$(480633,-682404,968879,-37141658)$	929
$(5928836,-8417777,11951582,-458159967)$	-261
$(477439795,-677870281,962442014,-36894898212)$	2031
$(993357552,-1410371674,2002449425,-76763240419)$	1267
$(-12727016174,18069851153,-25655622357,983499848986)$	191
$(-33310541181,47294394282,-67148705821,2574123563077)$	-25
$(-79348098536,112658639717,-159953033999,6131746975140)$	27
$(-112658639717,159953033999,-227101739820,8705870538217)$	-1

longueur = 12

direction : 3

coordonnees	*norme*
$(-2,-1,1,30)$	483
$(9,8,-3,-187)$	961
$(-36,-13,20,475)$	29
$(-391,-56,253,3938)$	-301
$(-3119,-109,2160,26573)$	2215
$(4241,-4738,-4989,33901)$	2655
$(-5126,-16876,-3462,282985)$	-3805
$(44422,13436,-25773,-548788)$	841
$(167852,87719,-81868,-2603236)$	-8563
$(-62551,136014,101356,-1447877)$	1465
$(475158,-306035,-464555,576131)$	-1

longueur = 11

c=4; m=2

direction : 1

coordonnees	*norme*
$(260,16,1,1)$	-64
$(1056,65,4,4)$	4
$(1136387,69952,4306,4241)$	-1

longueur = 3

direction : 2

coordonnees	*norme*
$(-83,113,-154,3359)$	-2383
$(-91,124,-169,3685)$	-883
$(-182,248,-338,7371)$	-373
$(-471,642,-875,19081)$	671
$(-3750,5111,-6966,151908)$	-212
$(32074,-43715,59581,-1299287)$	151
$(-272253,371065,-505740,11028707)$	23
$(-11621618,15839589,-21588438,470780554)$	22
$(539145629,-734824116,1001522506,-21840270251)$	13
$(-1485487821,2024633450,-2759457566,60175681152)$	-16
$(-2024633450,2759457566,-3760980072,82015951403)$	1

longueur = 11

direction :3

coordonnees	*norme*
$(1,2,0,-24)$	-88
$(-5,-13,-1,149)$	35
$(55,-88,-73,624)$	368
$(295,-248,-310,1151)$	2545
$(350,-336,-383,1775)$	488
$(-672,-249,410,5355)$	-151
$(-3421,-485,2372,19591)$	-25
$(16732,23399,-3950,-301896)$	344
$(-66951,-15984,44059,447036)$	-1492
$(-25301,60769,40961,-485839)$	-545
$(-29660,-160436,-36285,1701019)$	-1472
$(222733,-13302,-170766,-835678)$	-274
$(-227092,-207903,93520,3022536)$	232
$(865631,7561,-642103,-3828551)$	239
$(-444230,1300480,804156,-10818813)$	145
$(2823985,230586,-2019829,-14508189)$	1

longueur = 16

c=2; m=4

direction : 1

coordonnees	*norme*
(258, 16, 1, 1)	−8
(2080, 129, 8, 8)	8
(1085888, 67348, 4177, 4145)	64
(4377089, 271472, 16837, 16708)	−4
(4570214664, 283449872, 17579881, 17445185)	−512
(9211003487, 571276833, 35431234, 35159762)	2
(19383335644081, 1202176355199, 74560334482, 73989057649)	−1

longueur = 7

c=3; m=4

direction : 1

coordonnees	*norme*
(6564, 81, 1, 1)	−27
(177309, 2188, 27, 27)	27
(3493701882, 43112421, 532009, 531766)	729
(−31457685530, −388189098, −4790269, −4788081)	−9
(1859529551032836, 22946669055846, 283162814200, 283033476937)	−19683
(−5581137890014235, −68871464853068, −849876631698, −849488442600)	3
(99019046133088302914 5, 12218989908385718414, 150782824327107459, 150713952862254391)	−1

longueur = 7

c=4; m=3

direction : 1

coordonnees	*norme*
(4100, 64, 1, 1)	−64
(65664, 1025, 16, 16)	16
(1078205440, 16830544, 262721, 262465)	4096
(4317028355, 67387840, 1051909, 1050884)	−4
(283819653993471, 4430360854595, 69156934785, 69089546945)	1

longueur = 5

C.3 m=1

c=2

direction : 1

coordonnees	*norme*
$(1,0,0,0)$	-2
$(-2,-1,0,0)$	4
$(5,2,1,0)$	-8
$(8,3,1,1)$	1

longueur = 4

direction :2

coordonnees	*norme*
$(-1,1,-1,2)$	-2
$(-5,6,-7,16)$	4
$(-18,21,-24,55)$	7
$(35,-40,46,-106)$	-8
$(-93,107,-123,283)$	1

longueur = 5

direction :3

coordonnees	*norme*
$(1,0,-1,0)$	4
$(-1,-1,1,3)$	1

longueur = 2

c=5

direction : 1

coordonnees	*norme*
$(-1,0,0,0)$	-5
$(-5,-1,0,0)$	25
$(29,5,1,0)$	-125
$(35,6,1,1)$	1

longueur = 4

direction :2

coordonnees	*norme*
$(-1,1,-1,5)$	-5
$(11,-12,13,-70)$	25
$(-36,39,-42,226)$	61
$(-143,154,-166,895)$	-125
$(-333,359,-387,2086)$	1

longueur = 5

direction :3

coordonnees	*norme*
$(1,0,-1,0)$	25
$(-1,-1,1,6)$	1

longueur = 2

c=15

direction : 1

coordonnees	*norme*
$(-1,0,0,0)$	-15
$(-15,-1,0,0)$	225
$(239,15,1,0)$	-3375
$(255,16,1,1)$	1

longueur = 4

direction :2

coordonnees	*norme*
$(-1,1,-1,15)$	-15
$(31,-32,33,-510)$	225
$(-96,99,-102,1576)$	631
$(-1023,1054,-1086,16785)$	-3375
$(-2173,2239,-2307,35656)$	1

longueur = 5

direction :3

coordonnees	*norme*
$(-1,0,1,0)$	225
$(-1,-1,1,16)$	1

longueur = 2

c=20

direction : 1

coordonnees	*norme*
$(-1,0,0,0)$	-20
$(-20,-1,0,0)$	400
$(419,20,1,0)$	-8000
$(440,21,1,1)$	1

longueur = 4

direction :2

coordonnees	*norme*
$(-1,1,-1,20)$	-20
$(41,-42,43,-880)$	400
$(-126,129,-132,2701)$	1141
$(1763,-1804,1846,-37780)$	-8000
$(-3693,3779,-3867,79141)$	1

longueur = 5

direction :3

coordonnees	*norme*
$(-1,0,1,0)$	400
$(-1,-1,1,21)$	1

longueur = 2

Cas général (conjecture) : lien avec l'AJP

k	*coordonnées de* $\psi_k^{(1)}$	*AJP*
1	$(1,0,0,0)$	ϕ_1
2	$(c,1,0,0)$	ϕ_2
3	$(c^2+c-1,c,1,0)$	ϕ_3
4	$(c^2+2c,c+1,1,1)$	ϕ_6

Liste des matrices A_i

$A_1 = [c,1,0,0;c-1,0,1,0;0,0,0,1;\mathbf{1,\ 0,\ 0,\ 0}]$

$A_2 = [c^2+c-1,c,1,0;0,0,0,1;1,0,0,0;\mathbf{c,\ 1,\ 0,\ 0}]$

$A_3 = [c^2+c-1,c,1,1;1,0,0,0;c,1,0,0;\mathbf{c^2 + c - 1,\ c,\ 1,0}]$

$A_4 = [c^2+c,c,1,1;c,1,0,0;c^2+c-1,c,1,0;c^2+c-1,c,1,1]$

$A_5 = [c^2+2c,c+1,1,1;c^2+c-1,c,1,0;c^2+c-1,c,1,1;c^2+c,c,1,1]$

$A_6 = [c^3+3c^2+c-1,c^2+2c,c+1,c;c^3+2c^2-c-1,c^2+c-1,c,c;$
$c^3+2c^2-c,c^2+c-1,c,c;\mathbf{c^2 + 2c,\ c + 1,\ 1,\ 1}]$

BIBLIOGRAPHIE

[1] A.G. AKRITAS : Elements of computer algebra with applications. Wiley Interscience publication.

[2] L. BERSTEIN : "The Jacobi-Perron Algorithm, Its Theory and Application", Lecture Notes in Mathematics, Vol. 207, Springer-Verlag, Berlin/New York, 1971.

[3] E. BOMBIERI et A.J. VAN DER POORTEN : Continued fractions of algebraic numbers. Computational Algebra and Number Theory, Sydney 1992, Wieb Bosma and Alf Van Der Poorten eds Kluwer 1995, 138-154.

[4] J. BUCHMANN : A generalization of Voronoï's unit algorithm.I.II, Jour. of Number Theory, 20, 1985, 177-209.

[5] J. BUCHMANN, M. POHST et J. VON SCHMETTOW : On unit groups and class groups of quartic fields of signature (2,1). Math. of computation, vol.62, number 205, 1994, 387-390.

[6] G. CANTOR, P. GALYEAN, G. ZIMMER : A Continued Fraction Algorithm for Real Algebraic Numbers. Math. of Computation. vol.26, nb 119, July 1972, p.785-791.

[7] H. COHEN : A course in Computational Algebraic Number Theory. Vol 138. Springer Verlag. 1993.

[8] Combinatorial Matrix Theory. Encyclopaedia of Mathematics. vol 39. Cambridge University Press.

[9] B.N. DELONE et D.K. FADDEEV : The Theory of Irrationalities of the Third Degree. Amer. Math. Soc., Providence, Rhode Island 1964 (Transl. of Math. Monographs 10).

[10] E. DUBOIS : Approximations diophantiennes simultanées de nombres algébriques. Calcul des meilleures approximations. Thèse de doctorat d'état. Univ. Pierre et Marie Curie Paris 1980.

[11] E. DUBOIS et A. FAHRANE : Unité fondamentale dans des familles d'ordres cubiques. Utilitas Mathematica 47 (1995), pp. 97-115.

[12] A. FAHRANE : Spécialisation de points extrémaux. Applications aux fractions continues et aux unités d'une famille de corps cubiques. Thèse, Univ. Caen 1992.

[13] J.L. HAFNER et K.S. MCCURLEY : Asymptotically fast triangularization of matrices over rings. Siam J.Comput. vol.20,No. 6, pp 1068-1083, Dec.1991.

[14] F. HALTER-KOCH : Einige periodische Kettenbruchentwicklungen und Grundeinheiten quadratischer Ordnungen. Abh. Math. Sem. Univ. Hamburg 59 (1989) 157-169.

[15] S. KARLIN : Initiation aux processus aléatoires. Dunod.

[16] J. KUHNER : On a family of generalized continued fraction expansions with period length going to infinity. Jour. of Number Theory. Vol.53. No.1. July 1995.

[17] S. LANG et A. TROTTER : Continued fractions for some algebraic numbers. J. für Math.255(1972)112-134.

[18] A.K. LENSTRA, H.W. LENSTRA et L. LOVASZ : Factoring polynomials with rational coefficients, Math. Ann. 261 (1982), 515-534.

[19] C. LEVESQUE et G. RHIN : Développements par l'AJP de familles infinies de degré quelconque. Communication personelle.

[20] C. LEVESQUE et G. RHIN : Two Families of Periodic Jacobi Algorithms with Period Lengths Going to Infinity. Jour. of Number Theory, Vol.37, No.2, 1991, 173-180.

[21] P. LIARDET et P. STAMBUL : Factorial algorithms and continued fractions. Preprint.

[22] S. LOUBOUTIN : Minorations d'unités fondamentales. Applications. Nagoya Math. J. Vol.130 (1993) 1-18.

[23] M. MIGNOTTE : Mathématiques pour le calcul formel. PUF. (p.208)

[24] O. PERRON : Grundlagen für eine Theorie des Jacobischen Kettenbruchalgorithmus Math.Ann.64 (1907) 1-76.

[25] G. RHIN : Développement par l'algorithme de Jacobi-Perron de $(\sqrt[3]{4}, \sqrt[3]{16})$ à l'ordre 1954. (Communication personnelle).

[26] H.J. STENDER : Eine Formel für Grundeinheiten in reinen algebraischen Zahlkörpern dritten, vierten und sechsten Grades. Jour. of Number Theory 7, 235-250 (1975) .

[27] B. VALLEE : Une approche géométrique de la réduction des réseaux en petite dimension. Thèse, Univ. Caen 1986.

[28] G.F. VORONOI : On a generalization of the Algorithm of Continued Fractions. Doctoral Dissertation. Warsaw 1896 (en Russe).

[29] H.C. WILLIAMS : The period length of Voronoï's algorithm for certain cubic orders. Publicationes Math. Debrecen., Tomus 37 (1990), 245-265.

[30] H. ZASSENHAUS : On the Continued Fraction Development of Real Irrational Algebraic Numbers, Ohio State University, Columbus, Ohio, 1968.(Unpublished.)