ANNALES MATHÉMATIQUES

BLAISE PASCAL

Rachid Mechik

Sur la constante d'Eisenstein

Volume 15, n° 1 (2008), p. 87-108.

<http://ambp.cedram.org/item?id=AMBP_2008__15_1_87_0>

Publication éditée par le laboratoire de mathématiques
de l'université Blaise-Pascal, UMR 6620 du CNRS
Clermont-Ferrand — France

Annales mathématiques Blaise Pascal **15**, 87-108 (2008)

Sur la constante d'Eisenstein

Rachid Mechik

Résumé

On cherche à donner une méthode effective de calcul de la constante d'Eisenstein [3] d'une fonction algébrique. On commence en précisant les liens entre cette constante et les rayons de convergence p-adiques de la fonction pour les différents nombres premiers p. Puis on donne une démonstration entièrement effective du résultat bien connu liant fonctions algébriques et diagonales de fractions rationnelles. Enfin on explique comment en déduire une méthode de calcul générale. On illustre la méthode en l'appliquant aux fonctions $(1-x)^r$. On termine en montrant que le calcul de la constante d'Eisenstein de la diagonale d'une fraction rationnelle se ramène à un nombre fini de problèmes d'optimisation linéaire.

On the Eisenstein Constant

Abstract

We try to give an efficient method for calculating the Eisenstein constant [3] of an algebraic function. We begin by specifying the ties between this constant and the p-adic convergence radius of the function for different prime numbers p. Then we give an entirely efficient proof of the very known result joining algebraic functions and diagonal of rational fractions. Finally we explain how to deduct a general calculation method. We illustrate the method by applying it to the functions $(1-x)^r$. We finish by showing that the calculation of the Eisenstein constant of the diagonal of a rational fraction amounts to a finite number of linear optimization problems.

1. Introduction

En 1852, G. Eisenstein introduisit la constante a que la littérature a baptisée en son nom : "Si une série entière

$$u = \sum \alpha_n z^n$$

Mots-clés : Diagonale de fraction rationnelle, constante d'Eisenstein.
Classification math. : 11S05,13J05.

à coefficients rationnels représente une fonction algébrique, alors il existe un entier a tel que les nombres $a^n\alpha_n$, $n \geq 0$ soient entiers [3]. Schmidt donna, le premier, en 1989 [9] des valeurs précises à la constante d'Eisenstein et Dwork et Van der Poorten [4] la majorèrent en 1991 en utilisant la théorie des équations différentielles p-adiques. Nous contribuons à l'étude de cette constante en adoptant une approche arithmétique.

Nous étendons la définition de la constante d'Eisenstein (§ 2) en introduisant les notions de constante d'Eisenstein radicale (en prenant a dans les puissances fractionnaires d'entiers naturels) et de constante d'Eisenstein p-adique entière ou radicale (en prenant a dans les puissances entières ou fractionnaires d'entiers p-adiques) ; puis nous en donnons quelques propriétés (§ 3).

Nous donnons une démonstration très détaillée de la coïncidence entre l'ensemble des fonctions algébriques et celui des diagonales des fractions rationnelles en deux variables (§ 4).

Nous utilisons ensuite ce résultat pour déterminer une constante d'Eisenstein pour les fonctions algébriques régulières (§ 5.1). Nous illustrons cette technique en l'appliquant dans le cas des fonctions $(1-x)^{n/m}$, où m et n sont des entiers naturels premiers entre eux (§ 5.2). Plus généralement, nous montrons que le calcul d'une constante d'Eisenstein p-adique radicale pour une diagonale de fraction rationnelle se ramène à un problème d'optimisation linéaire (§ 5.3). Nous pouvons en déduire une constante d'Eisenstein radicale puis, quitte à perdre de l'information, une constante d'Eisenstein entière.

2. Définitions et premières propriétés

2.1. Notations

On désigne par $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$ les ensembles des entiers naturels, des entiers relatifs, des nombres rationnels, des nombres réels et des nombres complexes respectivement, munis de leurs structures algébriques habituelles. Si E désigne l'un des ensembles cités ci-dessus, on posera $E^{\neq 0} = E \setminus \{0\}$.
On notera $\bar{\mathbb{Z}}$ la clôture intégrale de l'anneau $\mathbb{Z}$ dans le corps $\mathbb{C}$. Si p désigne un nombre premier, on notera $\mathbb{Z}_p$ l'anneau des entiers p-adiques et $\bar{\mathbb{Z}}_p$ l'anneau des entiers d'une clôture algébrique du corps des fractions $\mathbb{Q}_p$ de $\mathbb{Z}_p$.

Si $\Bbbk$ désigne un anneau, on notera $\Bbbk[x]$ l'anneau des polynômes en x, à coefficients dans $\Bbbk$, par $\Bbbk[[x]]$ l'anneau des séries entières formelles en x, à coefficients dans $\Bbbk$ et par $\Bbbk((x))$ le corps des fractions de l'anneau $\Bbbk[[x]]$.

2.2. Constantes d'Eisenstein

Dans la suite, on appellera fonction toute série entière f de $\mathbb{Q}[[x]]$; on dira que la fonction f est algébrique si elle est algébrique sur le corps $\mathbb{Q}(x)$

Définition 2.1. On dit que l'entier naturel non nul a est une constante d'Eisenstein entière (ou constante d'Eisenstein) pour la fonction f s'il existe un entier naturel non nul c tel que la fonction $cf(ax)$ ait des coefficients entiers, c'est-à-dire appartienne à $\mathbb{Z}[[x]]$.

Définition 2.2. Soit p un nombre premier. On dit que le nombre $a = p^h$, avec h entier naturel, est une constante d'Eisenstein entière p-adique (ou une constante d'Eisenstein p-adique) pour la fonction f s'il existe un entier naturel non nul c (en fait une puissance de p) tel que la fonction $cf(ax)$ ait des coefficients entiers p-adiques, c'est-à-dire appartienne à $\mathbb{Z}_p[[x]]$.

Définition 2.3. On dit que le nombre $a = n^{1/d}$, avec n et d entiers naturels non nuls, est une constante d'Eisenstein radicale pour la fonction f s'il existe un entier naturel non nul c tel que la fonction $cf(ax)$ ait des coefficients entiers algébriques, c'est-à-dire appartienne à $\bar{\mathbb{Z}}[[x]]$.

Définition 2.4. Soit p un nombre premier. On dit que le nombre $a = p^h$, avec h nombre rationnel ≥ 0, est une constante d'Eisenstein radicale p-adique pour la fonction f s'il existe un entier naturel non nul c (en fait une puissance de p) tel que la fonction $cf(ax)$ ait des coefficients entiers algébriques p-adiques, c'est-à-dire appartienne à $\bar{\mathbb{Z}}_p[[x]]$.

Proposition 2.5. *Soient f et g deux fonctions de $\mathbb{Q}[[x]]$. Si l'entier naturel a est une constante d'Eisenstein pour f et g, alors :*

(1) *pour tout entier $b \geq 1$, l'entier ab est une constante d'Eisenstein pour f,*

(2) *l'entier a est une constante d'Eisenstein pour toute fonction h de l'anneau $\mathbb{Q}[x, f, g]$.*

Démonstration. Par définition, il existe des entiers naturels non nuls c et c' tels que les fonctions $cf(ax)$ et $c'g(ax)$ appartiennent à $\mathbb{Z}[[x]]$.

(1) Pour tout entier naturel non nul b, il est clair que $cf\left(bax\right) \in \mathbb{Z}\left[\left[x\right]\right]$.
(2) Soit $h = \sum h_{ijk} x^i f^j g^k$ un polynôme en x, f et g à coefficients h_{ijk} dans $\mathbb{Q}$. Si on note δ le ppcm des dénominateurs des nombres rationnels h_{ijk} et d (resp. d') le degré de h en f (resp. g), on constate que $\delta c^d c'^{d'} h(ax)$ appartient à $\mathbb{Z}\left[\left[x\right]\right]$. □

Remarque 2.6. La proposition ci-dessus s'étend de manière évidente aux trois autres variantes de constantes d'Eisenstein pour une fonction algébrique f de $\mathbb{Q}\left[\left[x\right]\right]$.

Exemple 2.7. Considérons la fonction

$$f\left(x\right) = \frac{1}{2+x} = \frac{1}{2}\frac{1}{1+x/2};$$

on trouve

$$2f\left(2x\right) = \frac{1}{1+x} \in \mathbb{Z}\left[\left[x\right]\right].$$

L'entier 2 est une constante d'Eisenstein pour f, donc aussi l'entier $3{\cdot}2 = 6$. On voit de même que l'entier 3 est une constante d'Eisenstein pour la fonction $g\left(x\right) = 1/\left(x+3\right)$, donc aussi l'entier $2 \cdot 3 = 6$. Par conséquent, l'entier 6 est une constante d'Eisenstein pour la fonction

$$f^2\left(x\right) g\left(x\right) = \frac{1}{\left(2+x\right)^2\left(3+x\right)}.$$

Théorème 2.8 (Eisenstein)**.** *Toute fonction algébrique $f\left(x\right) \in \mathbb{Q}\left[\left[x\right]\right]$ possède une constante d'Eisenstein.*

Démonstration. En fait, le travail que nous réalisons revient à une démonstration effective du théorème d'Eisenstein. □

2.3. Constante d'Eisenstein et rayon de convergence

Il est immédiat de constater qu'un nombre réel $a = p^h$, où h est rationnel positif, est une constante d'Eisenstein radicale p-adique pour une fonction f si et seulement si la fonction f est analytique et bornée dans le disque (d'un corps p-adique suffisamment gros) de centre 0 et de rayon $1/\left|a\right|$ (qui est égal à a en vertu de la normalisation $|p| = 1/p$).

Maintenant, si on suppose que la fonction f est algébrique, elle ne peut avoir qu'un nombre fini de zéros dans son disque de convergence (car si $P\left(f,x\right) = 0$, les zéros de f sont des racines de l'équation $P\left(0,x\right) = 0$).

D'après un résultat classique sur les fonctions analytiques, on en déduit que la fonction f est bornée dans son disque de convergence.

Remarque 2.9. Il semble donc que l'on puisse facilement définir "la meilleure constante d'Eisenstein radicale p-adique" comme étant le rayon de convergence de la fonction f, mais cela suppose, avec nos conventions, que le rayon soit une puissance rationnelle de p (ce que l'on conjecture (Christol)). D'après [6], à chaque fonction algébrique est attaché un rayon de convergence "naturel" (qui, contrairement à ce qui se passe dans le cas complexe, n'est pas en général la distance de 0 à la première singularité, comme le montre la fonction $(1+x)^{1/p}$). Par construction, ce rayon de convergence naturel est bien une puissance rationnelle de p. Dwork et Robba ont démontré que le rayon de convergence réel est au moins égal à ce rayon naturel. Le point délicat est de montrer qu'il n'y a pas de fonction algébrique dont le rayon de convergence réel est strictement supérieur à ce rayon naturel.

3. Relations entre les différentes constantes d'Eisenstein

Proposition 3.1. *Les conditions suivantes sont équivalentes :*

(1) *La fonction algébrique $f(x) \in \mathbb{Q}[[x]]$ a une constante d'Eisenstein a.*

(2) *Pour tout nombre premier p, la fonction $f(x)$ a une constante d'Eisenstein p-adique a_p et, si c_p est l'entier attaché à a_p, on a $a_p = c_p = 1$ pour presque tout p.*

Dans ces conditions, on a $a = \prod_p a_p$.

Démonstration. Si $f(x) = \sum_n \alpha_n x^n$ a une constante d'Eisenstein a, il existe un entier naturel non nul c tel que $cf(ax) \in \mathbb{Z}[[x]]$, c'est-à-dire $c\alpha_n a^n \in \mathbb{Z}$,pour tout n. Soit p un nombre premier arbitraire. Ecrivons $a = p^r q$, $c = p^{r'} q'$,avec
$$(p,q) = (p,q') = 1$$
et posons $a_p = p^r$, $c_p = p^{r\prime}$. Alors $c_p\alpha_n a_p^n \in \mathbb{Z}/q'q^n$ et puisque q et q' sont inversibles dans $\mathbb{Z}_p$, il s'ensuit que $c_p\alpha_n a_p^n \in \mathbb{Z}_p$. Donc a_p est une constante d'Eisenstein p-adique pour $f(x) \in \mathbb{Q}[[x]]$ d'où (1)$\Longrightarrow$(2).

Faisant parcourir à p l'ensemble des nombres premiers dans $\mathbb{N}$, on obtient la relation $a = \prod_p a_p$ qui relie la constante d'Eisenstein a et les constantes d'Eisenstein p-adique a_p associées à une fonction algébrique $f(x) \in \mathbb{Q}[[x]]$.

Réciproquement, supposons qu'il existe, pour tout nombre premier p, deux nombres a_p et c_p dans $\mathbb{Z}_p^{\neq 0}$ tels que $c_p f(a_p x) \in \mathbb{Z}_p[[x]]$. Quitte à les multiplier par des nombres inversibles de $\mathbb{Z}_p$, on peut supposer qu'ils appartiennent en fait à $p^{\mathbb{N}} \subset \mathbb{N}^*$. Compte tenu de la condition $a_p = c_p = 1$ pour presque tous les nombres premiers p, les nombres $a = \prod a_p$ et $c = \prod c_p$ sont bien définis et appartiennent à $\mathbb{N}^*$. Si $f(x) = \sum_n \alpha_n x^n$, par hypothèse, $c_p \alpha_n a_p^n$ appartient à $\mathbb{Z}_p$ pour tout p. On constate que l'entier $c\alpha_n a^n$, appartenant à $\mathbb{Z}_p$ pour tout p appartient à $\mathbb{Z}$. Autrement dit, $a = \prod_p a_p$ est une constante d'Eisenstein pour la fonction f.

$$f(x) = \sum_n \alpha_n x^n \in \mathbb{Q}[[x]].$$

Ceci prouve (2)$\Longrightarrow$(1). □

Remarque 3.2. Dans la condition 2) de la proposition 3.1, les hypothèses $a_p = 1$ et $c_p = 1$ pour presque tout p sont nécessaires comme le montrent les deux contre-exemples ci-dessous.

Exemple 3.3. Considérons la fonction $f(x) = \sum_n x^n/n!$.
Si v_p désigne la valuation p-adique de $\mathbb{Q}$ et si $n \in \mathbb{N}$ on a $v_p(n!) \leq \dfrac{n}{p-1}$

$$v_p(p^n/n!) = v_p(p^n) - v_p(n!) = n - v_p(n!) \geq n\,\frac{p-2}{p-1} \geq 0.$$

Donc $f(px) = \sum_n (p^n/n!)x^n \in \mathbb{Z}_p[[x]]$. Autrement dit, pour tout nombre premier p, $a_p = p$ est une constante d'Eisenstein p-adique pour f (avec $c_p = 1$). Cependant, $f(x) = \sum_n x^n/n!$ n'a pas de constante d'Eisenstein car, quelques soient $a \in \mathbb{N}^{\neq 0}$ et $c \in \mathbb{Z}^{\neq 0}$, pour n assez grand, le dénominateur $n!$ du nombre rationnel $ca^n/n!$ contient des nombres premiers qui ne sont ni dans a ni dans c et le nombre $c\alpha_n a^n$ n'appartient pas à $\mathbb{Z}$.

Exemple 3.4. Considérons la fonction $f(x) = \sum_n \alpha_n x^n$ où,

$$\text{pour } n = p_1^{r_1}...p_k^{r_k}, \text{ on pose } \alpha_n = 1/p_1...p_k.$$

Alors pour tout nombre premier p, $p\alpha_n \in \mathbb{Z}_p$. Donc $a_p = 1$ est une constante d'Eisenstein p-adique pour f (on prendra $c_p = p$). Cependant, $f(x) = \sum_n \alpha_n x^n$ n'a pas de constante d'Eisenstein car, quelques soient $a \in \mathbb{N}^{\neq 0}$ et $c \in \mathbb{Z}^{\neq 0}$, il existe des nombres premiers $n = p$ pour lesquels le dénominateur p du nombre rationnel α_n contient un nombre premier qui ne divise ni a ni c et donc tels que le nombre $c\alpha_n a^n$ n'appartient pas à $\mathbb{Z}$.

4. Fonctions algébriques et diagonales de fractions rationnelles

Soit $\Bbbk$ un corps. On définit une application diag : $\Bbbk((x,y)) \longrightarrow \Bbbk((x))$ en posant

$$\operatorname{diag} \sum_{i,j} a_{ij} x^i y^j = \sum_i a_{ii} x^i.$$

$\operatorname{diag}(F)$ s'appelle alors la diagonale de F.[1]

Le résultat suivant est connu ([7] en caractéristique positive, [1] en caractéristique nulle et [2] pour une généralisation aux fonctions de plusieurs variables). Nous en donnons une démonstration plus complète et explicite que celles que l'on trouve dans la littérature.

Théorème 4.1. *Soit $\Bbbk$ un corps. Une fonction f du corps $\Bbbk((x))$ est algébrique sur le corps $\Bbbk(x)$ si et seulement si elle est diagonale d'une fraction rationnelle F de l'anneau $\Bbbk(x,y) \cap \Bbbk((x,y))$.*

Démonstration. Le point clef pour démontrer que **la diagonale d'une fraction rationnelle est une fonction algébrique** est une description de l'anneau $\Bbbk(x,y) \cap \Bbbk((x,y))$. Pour cela, il faut caractériser les polynômes de $\Bbbk[x,y]$ qui sont inversibles dans $\Bbbk((x,y))$. La réponse à cette question est donnée dans le lemme 4.5.

Lemme 4.2. *Soit P un polynôme de l'anneau $\Bbbk((x))[y]$. On suppose que le polygone de Newton x-adique de P a un seul coté et que celui-ci a une pente $\lambda \geq 0$. Alors la série $P(xy,y)$ est inversible dans l'anneau $\Bbbk((x,y))$.*

Démonstration. Ecrivons $P(x,y) = a_0(x) + a_1(x)y + ... + a_d(x)y^d$. Par hypothèse, on a : $v_x(a_i) - v_x(a_0) \geq \lambda i \geq 0$ pour $0 < i \leq d$ avec égalité pour $i = d$. Posons $v = v_x(a_0)$ et $\tilde{a}_i = x^{-v} a_i$ de telle sorte que $v_x(\tilde{a}_0) = 0$, c'est-à-dire $\tilde{a}_0(0) \neq 0$, et $v_x(a_i) \geq 0$ pour $i > 0$. Il vient

$$\begin{aligned} P(xy,y) &= (xy)^v \Big(\tilde{a}_0(xy) + \tilde{a}_1(xy)\, y + \cdots + \tilde{a}_d(xy) y^d\Big) \\ &= (xy)^v \big(\tilde{a}_0(xy) - y\, u(xy,y)\big). \end{aligned}$$

[1] On peut définir, plus généralement, l'application diagonale sur l'anneau des séries entières en n variables sur le corps $\Bbbk$ mais nous n'aurons à utiliser que le cas $n = 2$.

avec u dans $\mathbb{k}[[x,y]]$. Comme $\tilde{a}_0$ est inversible dans $\mathbb{k}[[x]]$, on constate alors que

$$\frac{1}{P(xy,y)} = \frac{1}{\tilde{a}_0(xy)\,(xy)^v}\sum_{n\geq 0} y^n \frac{u(xy,y)^n}{\tilde{a}_0(xy)^n}$$

appartient à $\mathbb{k}((x,y))$, comme annoncé. $\square$

Lemme 4.3. *Soit P un polynôme de l'anneau $\mathbb{k}((x))[y]$. On suppose que le polygone de Newton x-adique de P a un seul coté et que celui-ci a une pente $\lambda \leq -1$. Alors la série $P(xy,y)$ est inversible dans l'anneau $\mathbb{k}((x,y))$.*

Démonstration. Si $P(x,y) = a_d(x)\,y^d + \cdots + a_0(x)$, on a : $v_x(a_i) - v_x(a_d) \geq \lambda(i-d) \geq (d-i)$ pour $0 \leq i < d$ avec égalité pour $i = 0$. Posons $v = v_x(a_d)$ et $\tilde{a}_i = x^{-v}a_i$ de telle sorte que $v_x(\tilde{a}_d) = 0$, c'est-à-dire $\tilde{a}_d(0) \neq 0$, et $v_x(\tilde{a}_i) \geq d - i$ pour $i < d$, autrement dit $x^{i-d}\tilde{a}_i(x)$ appartient à $\mathbb{k}[[x]]$. On trouve donc que :

$$\begin{aligned} P(xy,y) &= x^v y^{v+d}\Big(\tilde{a}_d(xy) + \cdots + x^{d-i}\,(xy)^{i-d}\tilde{a}_i(xy) + \cdots \\ &\qquad\qquad \cdots + x^d\,(xy)^{-d}\tilde{a}_0(xy)\Big) \\ &= x^v y^{v+d}(\tilde{a}_d(xy) - x\,u(x,xy)). \end{aligned}$$

avec u dans $\mathbb{k}[[x,y]]$. On constate alors que

$$\frac{1}{P(xy,y)} = \frac{1}{\tilde{a}_d(xy)\,x^v y^{v+d}}\sum_{n\geq 0} x^n \frac{u(x,xy)^n}{\tilde{a}_d(xy)^n}$$

appartient à $\mathbb{k}((x,y))$, comme annoncé. $\square$

Lemme 4.4. *Soit P un polynôme de l'anneau $\mathbb{k}((x))[y]$. On suppose que les pentes des cotés du polygone de Newton x-adique de P appartiennent toutes à l'intervalle $(-1,0)$. Alors, la série $P(xy,y)$ n'est pas inversible dans l'anneau $\mathbb{k}((x,y))$.*

Démonstration. Soit $P(x,y) = a_d(x)y^d + \cdots + a_0(x)$ et soit $\lambda_1 \leq \cdots \leq \lambda_\nu$ les pentes du polygone de Newton de P. Par hypothèse on a $-1 < \lambda_1$ et $\lambda_\nu < 0$.
Par définition du polygone x-adique de P, on a :
- $v_x(a_i) - v_x(a_d) \geq (i-d)\lambda_\nu > 0$ pour $i < d$,
- $v_x(a_0) - v_x(a_i) \leq (-i)\lambda_1 < i$ pour $0 < i$.

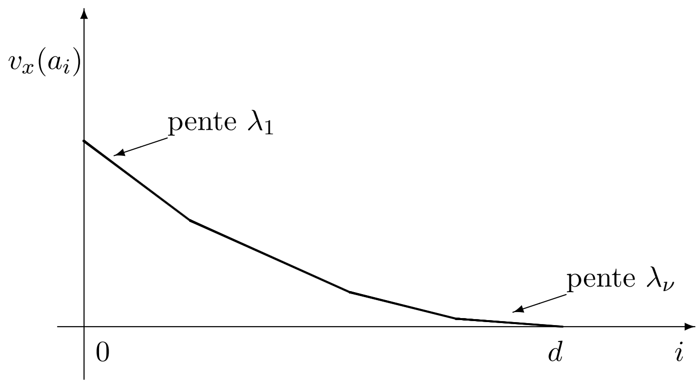


Figure 1. Polygone de Newton ayant toutes ses pentes dans $(-1,0)$.

En particulier $0 < v_x(a_0) - v_x(a_d) < d$. Posons $\tilde{a}_i = x^{-v_x(a_i)}\,a_i$ avec $\tilde{a}_i = 0$ si $a_i = 0$. En particulier $\tilde{a}_0(0) \neq 0$ et $\tilde{a}_d(0) \neq 0$. Par ailleurs, nous posons $r_i = v_x(a_i) - v_x(a_d) > 0$ et $s_i = i + v_x(a_i) - v_x(a_0) > 0$. On trouve :

$$\begin{aligned} P(xy,y) &= x^{v_x(a_d)}y^{v_x(a_0)}\Big(\tilde{a}_d(xy)y^{s_d} + \cdots \\ &\qquad\qquad \cdots + \tilde{a}_i(xy)x^{r_i}\,y^{s_i} + \cdots + \tilde{a}_0(xy)x^{r_0}\Big) \\ &= x^{v_x(a_d)}y^{v_x(a_0)}\Big(\tilde{a}_d(0)y^{s_d} + \tilde{a}_0(0)x^{r_0} + xy\,u(x,y)\Big) \end{aligned}$$

avec u dans $\Bbbk[[x,y]]$. On constate que la série $P(xy,y)$ n'est pas inversible dans l'anneau $\Bbbk((x,y))$. $\square$

Lemme 4.5. *La fraction rationnelle F du corps $\Bbbk(x,y)$ appartient à l'anneau $\Bbbk((x,y))$ si et seulement si la fraction rationnelle*

$$F(\frac{x}{y},y) = \frac{N}{D}$$

écrite sous forme réduite dans $\Bbbk(x)(y)$ a un dénominateur $D \in \Bbbk(x)[y]$, dont le polygone de Newton x-adique, n'a pas de pente dans l'intervalle $(-1,0)$.

Démonstration. D'après le lemme de Hensel, le corps $\Bbbk((x))$ étant complet pour la valuation x-adique, on peut écrire

$$D = \prod_{\lambda_i} P_{\lambda_i}$$

où les λ_i sont les pentes des cotés du polygone de Newton x-adique de D et où P_{λ_i} est un polynôme de $\Bbbk((x))[y]$ dont le polygone de Newton x-adique a un seul coté, celui-ci étant de pente λ_i. Posons :

$$P = \prod_{\lambda_i \in (0,1)} P_{\lambda_i} \quad , \qquad Q = \prod_{\lambda_i \notin (0,1)} P_{\lambda_i}.$$

Par construction, on a $D = PQ$. Comme les polynômes P et Q sont premiers entre eux par construction, il existe des polynômes R et S de $\Bbbk((x))[y]$ tels que $N = R\,Q + S\,P$ avec $\deg R < \deg P$. Comme N est, par hypothèse, premier à $D = PQ$, R et P sont premiers entre eux.
D'après les lemmes 4.2 et 4.3, $Q(xy, y)$ est le produit d'éléments $P_{\lambda_i}(xy, y)$ inversibles dans $\Bbbk((x, y))$ et donc est inversible dans cet anneau. Par conséquent $\dfrac{S}{Q}(xy, y)$ appartient à $\Bbbk((x, y))$.
Si $F(x, y) = \dfrac{N}{D}(xy, y)$ appartient à $\Bbbk((x, y))$, alors $\dfrac{R}{P}(xy, y)$ appartient à $\Bbbk((x, y))$. Or, comme $(R, P) = 1$, il existe des polynômes U, V de l'anneau $\Bbbk((x))[y]$ tels que $UP + VR = 1$, et donc $\dfrac{1}{P(xy, y)} = [U + V\dfrac{R}{P}](xy, y)$ appartient aussi à $\Bbbk((x, y))$. Les pentes des cotés du polygone de Newton de P sont, par construction, les λ_i qui appartiennent à l'intervalle $(-1, 0)$. D'après le lemme 4.4, $P(xy, y)$ ne peut être inversible dans $\Bbbk((x, y))$ que s'il n'y a aucun λ_i dans $(-1, 0)$ (et donc si P est un polynôme constant).

Réciproquement, si le polynôme D n'a pas de pente dans l'intervalle $(-1, 0)$, les lemmes 4.2 et 4.3 assurent que $P(xy, y)$ est inversible dans l'anneau $\Bbbk((x, y))$ et la fraction rationnelle $F(x, y) = \dfrac{N}{D}(xy, y)$ appartient bien à $\Bbbk((x, y))$ comme annoncé. □

Fin de la preuve de la partie directe (la diagonale d'une fraction rationnelle est une fonction algébrique).

Supposons que f est la diagonale de la fraction rationnelle

$$F(x, y) = \sum a_{n,m} x^n y^m$$

et posons : $G(x,y) = \dfrac{1}{y}F(\dfrac{x}{y}, y) = \sum a_{n,m}x^n y^{m-n-1}$. On constate que la forme différentielle

$$G(x,y)dy = F(\frac{x}{y}, y)\frac{dy}{y} = \sum a_{n,m}x^n y^{m-n}\frac{dy}{y},$$

vue comme fonction de y à coefficients dans $\mathbb{k}((x))$, a un résidu en 0 (coefficient de $\frac{dy}{y}$) égal à $\sum a_{n,n}x^n$, c'est-à-dire à la diagonale f de F.
Le principe de la démonstration est que le calcul du résidu d'une fraction rationnelle est une opération algébrique. Toutefois pour mettre cette technique heuristique en forme, il faut soigneusement préciser les anneaux dans lesquels se trouvent les différentes séries. Nous allons faire ce travail en détail.

La décomposition de G en éléments simples dans le corps $\mathbb{k}((x))(y)$ s'écrit :

$$G = Q + \sum \frac{R_k}{P_k}$$

où Q, R_k et P_k sont dans $\mathbb{k}((x))[y]$ et $\deg R_k < \deg P_k$. Il vient

$$\mathrm{diag}F(x,y) = \mathrm{diag}\Big(yQ(xy,y) + \sum \frac{yR_k(xy,y)}{P_k(xy,y)}\Big) = \sum \mathrm{diag}(\frac{yR_k(xy,y)}{P_k(xy,y)})$$

car $\mathrm{diag}(yQ(xy,y)) = 0$, comme on le vérifie facilement.
Par construction, les P_k sont irréductibles dans $\mathbb{k}((x))[y]$ et donc leur polygone de Newton x-adique n'a qu'un seul coté dont la pente est celle d'un coté du polygone de Newton du dénominateur de G. Puisque $G(xy,y) = \frac{1}{y}F(x,y)$ appartient à $\mathbb{k}((x,y))$, d'après le lemme 4.4, cette pente n'appartient pas à l'intervalle $(-1,0)$.

Nous calculons maintenant $\mathrm{diag}(\dfrac{yR(xy,y)}{P(xy,y)})$ en supposant que le polygone de Newton x-adique de P n'a qu'un seul coté, celui-ci ayant une pente $\mathfrak{p}$ qui n'appartient pas à l'intervalle $(-1,0)$.

i) Si $\mathfrak{p} \geq 0$, on est dans la situation du lemme 4.2 :
on a $P(xy,y) = (xy)^v(\tilde{a}_0(xy) - y\,u(xy,y))$ avec $\tilde{a}_0(0) \neq 0$. On trouve alors que

$$\frac{y\,R(xy,y)}{P(xy,y)} = \frac{y\,R(xy,y)}{(xy)^v\tilde{a}_0(xy)}\sum_{n=0}^{\infty} y^n\Big(\frac{u(xy,y)}{\tilde{a}_0(xy)}\Big)^n$$

est de la forme $y\,H(xy,y)$ et a donc une diagonale nulle.

ii) Si $\mathfrak{p} \leq -1$, comme $\Bbbk((x))$ est un corps, on peut supposer le polynôme P unitaire. Notons $f_1 = f, \cdots, f_\nu$ les racines en y du polynôme P dans une extension finie du corps $\Bbbk((x))$ de telle sorte que l'on a

$$P(x,y) = \prod_{i=1}^{\nu} \Big(y - f_i(x)\Big)^{h_i}.$$

La valuation x-adique se prolonge à cette extension. Ecrivons maintenant la décomposition en éléments simples :

$$\frac{R(x,y)}{P(x,y)} = \sum_{i=1}^{\nu}\sum_{j=1}^{h_i} \frac{\alpha_{i,j}(x)}{\big(y - f_i(x)\big)^j}$$

Comme $\mathfrak{p} \leq -1$, les racines f_i du polynôme P ont une valuation x-adique au moins égale à 1. Autrement dit $f_i(x) = x\, g_i(x)$ avec $v_x(g_i) \geq 0$. On trouve

$$\begin{aligned} \sum_{i=1}^{\nu} \frac{y\, \alpha_{i,j}(xy)}{\big(y - f_i(xy)\big)^j} &= \frac{y^{1-j}\alpha_{i,j}(xy)}{\big(1 - x\, g_i(xy)\big)^j} \\ &= \sum_{n=0}^{\infty} \binom{j-1+n}{j-1} x^n y^{1-j} \sum_{i=1}^{\nu} \alpha_{i,j}(xy) g_i^n(xy). \end{aligned}$$

Par un argument galoisien facile, on montre que $\sum_{i=1}^{\nu} \alpha_{i,j} g_i^n$ appartient à $\Bbbk((x))$. On constate que la diagonalisation ne donnera un résultat non nul dans l'expression précédente que si on a $n = 1 - j$ ce qui impose $j = 1$ et $n = 0$. On trouve donc :

$$\operatorname{diag}\Big(\sum_{i=1}^{\nu} \frac{y\, \alpha_{i,j}(xy)}{\big(y - f_i(xy)\big)^j}\Big) = \begin{cases} \sum_{i=1}^{\nu} \alpha_{i,1}(x) & \text{si} \quad j = 1 \\ 0 & \text{si} \quad j > 1 \end{cases}$$

c'est-à-dire :

$$\operatorname{diag}\Big(\frac{y\, R(xy,y)}{P(xy,y)}\Big) = \sum_{i=1}^{\nu} \alpha_{i,1}(x).$$

Pour terminer la démonstration, il suffit de remarquer que les fonctions $\alpha_{i,1}$ appartiennent au corps $\Bbbk(f_1, \ldots, f_\nu)$ et que les f_i, racines d'un polynôme P_k, sont aussi racines du dénominateur de G et donc sont des fonctions algébriques. En fait, $\alpha_{i,1}$ est le résidu de $\dfrac{R}{P}$ (et donc celui de G) au point $y = f_i$.

Remarque 4.6. Lorsque le dénominateur de la fraction rationnelle G n'a que des racines simples, on peut expliciter le calcul précédent car les résidus se calculent facilement. On trouve, si $G = N/D$:

$$\operatorname{diag}\big(y\,F(xy,y)\big) = \sum_{D(f_i)=0\,;\,v_x(f_i)>0} \frac{N(f_i)}{D'(f_i)}$$

le résultat étant une série en x par un argument de Galois, même si ce n'est pas le cas de tous les f_i.

Un cas particulier de cette remarque est le résultat suivant que l'on trouve déjà, dans le cas $n = 1$, dans [7].

Théorème 4.7 (Cauchy- Furstenberg)**.** *Soit P un polynôme de $\mathbb{Q}[x,y]$ tel que $P(0,0) = 0$ et $P'_y(0,0) \neq 0$. Alors l'équation $P(x,y) = 0$ admet une et une seule racine f telle que $v_x(f) > 0$, cette racine appartient à $\mathbb{Q}[[x]]$ et, pour tout $n \geq 0$, on a*

$$(f(x))^n = diag\frac{y^{n+1}\,P'_y(xy,y)}{P(xy,y)}.$$

Démonstration. Par construction, le polygone de Newton de P a une seule pente négative et celle-ci est de longueur 1 (figure 2). Il est donc clair que l'équation $P(x,y) = 0$ admet une et une seule racine f telle que $v_x(f) > 0$.

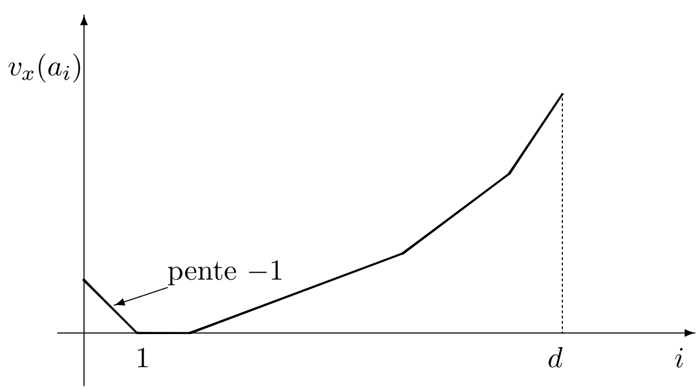


FIGURE 2. Polygone de Newton de P.

On a $P(x,y)=c_0(x)+c_1(x)\,y+\cdots+c_d(x)\,y^d$ avec $c(0)=0$ et $c_1(0)\neq 0$. Posons $Q(x,y)=y-\dfrac{1}{c_1(0)}P(x,y)$. Pour f et g dans $x\mathbb{k}((x))$, on trouve :

$$v_x\big(Q(x,f)-Q(x,g)\big)\geq \max_{i\geq 2}\{v_x(f-g)+1, v_x(f^i-g^i)\}\geq v_x(f-g)+1.$$

Autrement dit, l'application $f\mapsto Q(x,f)$ est une contraction de $x\mathbb{k}((x))$. L'équation $Q(x,f)=f$ a donc une unique solution dans cet ensemble et cette solution est clairement la racine de P qui s'annule en 0.

Le résultat de la remarque 4.6 donne alors :

$$\operatorname{diag}\frac{y^{n+1}\,P'_y\,(xy,y)}{P\,(xy,y)}=\frac{f^n P'_y(x,f)}{P'_y(x,f)}=f^n(x)$$

ce qui achève la démonstration de ce théorème. □

Démonstration de la réciproque (toute fonction algébrique est diagonale d'une fraction rationnelle).

Le théorème 4.7 démontre cette réciproque dans le cas particulier des “fonctions algébriques régulières” c'est-à-dire des fonctions algébriques qui s'annulent à l'origine et sont les seules parmi leurs conjugués à avoir cette propriété. Pour avoir une démonstration générale, il suffit de se ramener à ce cas en “séparant” f de ses conjugués.

Soit $f=\sum_{n=0}^{\infty}a_nx^n$ une fonction algébrique et soit $f_1=f,\ldots,f_\mu$ ses conjugués (sur $\mathbb{k}(x)$) dans une clôture algébrique $\mathbb{k}((x))^{\mathrm{alg}}$ de $\mathbb{k}((x))$. La valuation x-adique v_x de $\mathbb{k}((x))$ se prolonge à $\mathbb{k}((x))^{\mathrm{alg}}$.

On considère la fonction algébrique suivante

$$g=x^{-d}(f-\sum_{n=0}^{d}a_nx^n)=\sum_{n=d+1}^{\infty}a_nx^{n-d}$$

où d est un entier choisi supérieur ou égal au maximum des valuations $v_x(f-f_i)$ pour $2\leq i\leq\mu$. Les conjugués de g sont les $g_i=x^{-d}(f_i-\sum_{n=0}^{d}a_nx^n)$. Par définition de d, pour $i>1$, on a

$$v_x\Big(f-\sum_{n=0}^{d}a_nx^n\Big)\geq d+1>d\geq v_x(f-f_i).$$

On en déduit :

$$v_x(g_1)\geq -d+d+1=1\quad,\qquad v_x(g_i)=-d+v_x(f_i-f)\leq 0\quad(i>1)$$

Soit alors

$$P(x,y) = c_\mu(x)\prod_{i=1}^{\mu}(y-g_i(x)) = \sum_{i=0}^{\mu} c_i(x)y^i$$

un polynôme de $\mathbb{k}[x,y]$ dont g est racine, qui est de degré minimal et dont les coefficients c_i sont des polynômes en x premiers entre eux (ceci définit le polynôme P à un facteur dans $\mathbb{k}^*$ près).
Comme $P(x,g(x)) = 0$, on trouve $P(0,0) = P(0,g(0)) = 0$.
Le calcul des valuations x-adiques des racines g_i montre que le polygone de Newton x-adique de P (figure 2), vu comme un polynôme en y, a une pente strictement négative de multiplicité un et toutes ses autres pentes positives ou nulles. On en déduit que le minimum des valuations est atteint pour c_1. Les c_i ayant été choisis premiers entre eux, ce minimum est forcément nul. Autrement dit $P'_y(0,0) = c_1(0) \neq 0$.

On constate que la fonction algébrique g est régulière et, d'après le théorème 4.7, g est la diagonale de la fraction rationnelle

$$G(x,y) = \frac{y^2P'_y(xy,y)}{P(xy,y)}$$

Donc, f est la diagonale de la fraction rationnelle

$$F(x,y) = (xy)^d\frac{y^2P'_y(xy,y)}{P(xy,y)} + \sum_{n=0}^{d} a_n(xy)^n$$

□

5. Calcul d'une constante d'Eisenstein pour une fonction algébrique

5.1. Constante d'Eisenstein de fonctions algébriques régulières

Comme on l'a vu dans la fin de la démonstration précédente, trouver une fraction rationnelle dont une fonction algébrique donnée est la diagonale peut nécessiter des calculs compliqués. Toutefois, si la fonction algébrique est régulière, on dispose de la formule explicite de Frustenberg (théorème 4.7).

Lemme 5.1. *Soit $F(x,y) = P/Q$ une fraction rationnelle de $\mathbb{Q}(x,y)$ où P et Q sont des polynômes de $\mathbb{k}[x,y]$ et $Q(0,0) \neq 0$ [F appartient à*

$\mathbb{Q}((x,y))]$. *Si, pour des nombres* α *et* β *de* $\mathbb{Q}$ *(resp.* $(\mathbb{N}^{\neq 0})^{\mathbb{Q}}$ *,* $p^{\mathbb{Q}}$*), les coefficients du polynôme* $\frac{1}{Q(0,0)}Q(\alpha x,\beta y)$ *sont des entiers (resp. des entiers algébriques, des entiers p-adiques), alors le nombre* $\alpha\beta$ *est une constante d'Eisenstein entière (resp. radicale, radicale p-adique) pour la fonction* $f\left(x\right)=diagF\left(x,y\right)$.

Démonstration. Il existe un entier γ tel que le polynôme $\gamma P(\alpha x,\beta y)$ soit à coefficients entiers (resp. entiers algébriques, entiers p-adiques). On constate que

$$\gamma Q(0,0)F\left(\alpha x,\beta y\right)=\gamma P(\alpha x,\beta y)\sum_{n=0}^{\infty}\left(\frac{1}{Q(0,0)}Q(\alpha x,\beta y)-1\right)^{n}$$

est une série entière (en deux variables) à coefficients entiers (resp. entiers algébriques, entiers p-adiques). Sa diagonale

$$\operatorname{diag}\gamma Q(0,0)F\left(\alpha x,\beta y\right)=\gamma Q(0,0)f\left(\alpha\beta x\right)$$

est aussi à coefficients entiers (resp. entiers algébriques, entiers p-adiques). D'où le résultat annoncé. □

Corollaire 5.2. *Si le polynôme* $Q\in\mathbb{Z}\left[x,y\right]$ *satisfait la condition* $Q(0,0)\neq 0$, *alors* $Q\left(0,0\right)^{2}$ *est une constante d'Eisenstein pour la diagonale de* P/Q *où* P *est un polynôme de* $\mathbb{Q}\left[x,y\right]$.

Démonstration. C'est le cas particulier $\alpha=\beta=Q(0,0)$ du lemme précédent. □

Remarque 5.3. Nous allons voir que, en général, le résultat du corollaire précédent peut être nettement amélioré. D'une part, on peut utiliser le lemme fondamental pour calculer les constantes d'Eisenstein p-adiques, la proposition 3.1 donnant alors la constante d'Eisentstein entière (exemple 5.6). D'autre part, dans le calcul des constantes d'Eisenstein p-adiques, le résultat optimum peut être obtenu en faisant intervenir, dans le lemme fondamental, des nombres α ou β qui ne sont pas égaux et, en particulier, en prenant l'un d'entre eux non entier (ordinaire, algébrique ou p-adique) (voir exemple 5.8).

Corollaire 5.4. *Soit* f *une fonction algébrique régulière et soit* P *dans* $\mathbb{Z}[x,y]$ *un polynôme minimal de* f $\Big[$*on a* $P(x,f)=0$, $f\left(0\right)=0$, $P\left(0,0\right)=$

0 et $P'_y(0,0) \neq 0.$] Alors $\left(P'_y(0,0)\right)^2$ est une constante d'Eisenstein entière pour la fonction f.
Si on suppose en outre que P n'a pas de pente nulle (les conjugués de f sont de valuation x-adique strictement négative), alors $P'_y(0,0)$ est une constante d'Eisenstein entière pour la fonction f.

Démonstration. Grâce aux hypothèses faites sur le polynôme P, on peut écrire $P(x,y) = yP'_y(0,0) + xQ(x,y) + y^2R(x,y)$ avec Q et R dans $\mathbb{Z}[x,y]$ (Q de degré 1 en y). Le théorème de Furstenberg assure que f est la diagonale de la fraction rationnelle

$$F(x,y) = y^2 \frac{P'_y(xy,y)}{P(xy,y)} = y \frac{P'_y(xy,y)}{P'_y(0,0) + xQ(xy,y) + yR(xy,y)}$$

et on applique le lemme fondamental avec $\alpha = \beta = P'_y(0,0)$.
Si P n'a pas de pente nulle, alors R est divisible par x et on applique le lemme fondamental avec $\alpha = P'_y(0,0)$ et $\beta = 1$. □

Dans les cas particulier, ce résultat général peut être notablement amélioré. Nous en donnons des exemples dans les paragraphes suivants.

5.2. Calcul d'une constante d'Eisenstein pour la fonction $(1-x)^r$

Considérons la fonction

$$f(x) = (1-x)^{1/m},$$

où m est un entier naturel non nul. La méthode exposée au paragraphe précédent s'applique à la fonction algébrique régulière $g = f - 1$. Partant de la relation $x + (g+1)^m - 1 = 0$, le théorème de Furstenberg montre que g est la diagonale d'une fraction rationnelle de dénominateur :

$$P(x,y) = m + x + \binom{m}{2} y + \binom{m}{3} y^2 + \cdots + \binom{m}{m} y^{m-1}.$$

Nous commençons par établir un lemme.

Lemme 5.5. *Soit m un entier naturel non nul et soit $m = p_1^{m_1} p_2^{m_2} \ldots p_n^{m_n}$ sa décomposition en produit de facteurs premiers. Posons*

$$\alpha_m = p_1^{1/(p_1-1)} p_2^{1/(p_2-1)} \ldots p_n^{1/(p_n-1)}.$$

Alors, pour tout entier k, $1 \leq k \leq m$, le nombre

$$\beta_{m,k} = \frac{1}{m}\binom{m}{k}\alpha_m(m)^{k-1}$$

est un entier algébrique.

Démonstration. Il suffit de montrer que l'on a $|\beta_{m,k}|_p \leq 1$ pour tout nombre premier p. Si p ne divise pas m, le résultat est évident puisqu'alors $|\alpha_m|_p = |m|_p = 1$.

Nous supposons maintenant que p divise m. On a $|\alpha_m|_p = |p|^{1/(p-1)} < 1$.

• Si p ne divise pas k alors : $\displaystyle\binom{m}{k} = \frac{m}{k}\binom{m-1}{k-1}$

et on trouve $\displaystyle |\beta_{m,k}|_p = \Big|\frac{1}{k}\binom{m-1}{k-1}\alpha_m^{k-1}\Big|_p \leq |\alpha_m^{k-1}|_p < 1.$

• Si p divise k, on fait une récurrence sur le nombre m (plus précisément sur la puissance de p qui divise à la fois k et m). On pose $m = pm'$ et $k = pk'$ et on part de la relation classique

$$\Big|\binom{m}{k}\Big|_p = \Big|\binom{m'}{k'}\Big|_p$$

comme $k - k' = k'(p-1)$ et $k' \geq 1$, on obtient :

$$|\beta_{m,k}|_p = \Big|\frac{1}{p}\,\beta_{m',k'}\alpha_m^{k-1-k'+1}\Big|_p \leq |p|^{-1+k'} \leq 1$$

ce qui achève la démonstration. □

Le lemme montre que, pour $2 \leq i \leq m$, les nombres $\displaystyle\frac{1}{m}\binom{m}{k}\alpha_m^{k-1}$ sont des entiers (algébriques) et donc que le polynôme $\displaystyle\frac{1}{m}P(mx, \alpha_m y)$ est à coefficients entiers (algébriques). Le lemme fondamental montre que $a = m\alpha_m$ est une constante d'Eisenstein radicale pour g donc pour toutes les fonctions $(1-x)^{n/m} = (g+1)^n$ (proposition 2.5-2). On en déduit immédiatement que $a' = m^2$ est une constante d'Eisenstein entière pour ces fonctions ce que l'on aurait pu obtenir directement par le corollaire 5.4. Toutefois, quand m a des facteurs carrés, le résultat obtenu est meilleur comme le montre l'exemple suivant.

Exemple 5.6. Considérons la fonction $f(x) = (1-x)^{1/m}$ avec $m = 2^r\,3^s$. D'après ce qui précède, le nombre

$$a = m\alpha_m = m\ 2^{1/(2-1)}\ 3^{1/(3-1)} = 2\sqrt{3}\,m$$

est une constante d'Eisenstein radicale pour la fonction f. Autrement dit le nombre $6m$ est une constante d'Eisentstein entière pour la fonction f. Ceci améliore le résultat m^2 donné par le corollaire 5.4 dès que $r > 1$ ou $s > 1$.

Remarque 5.7. Considérons la fonction algébrique $g(x) = (1-x)^{1/3} - 1$. On a $P(x, g(x)) = 0$ avec $P(x, y) = y^3 + 3y^2 + 3y + x$. Le degré n de P en y ainsi que sa hauteur H valant 3, la formule de Dwork-van der Poorten [6] et [5] donne, pour la constante d'Eisenstein a de $f = g + 1$, la majoration

$$a \leq 4,8\left(3e^{-3}3^{4+2,74\log 3}e^{3\times 1,22}\right)^3 3^{2\times 3-1} \sim 4,7\times 10^{16}.$$

Cette majoration, comparée aux deux valeurs $a = 3^{3/2}$ (constante radicale) et $a = 9$ (constante entière) fournies par le théorème de Furstenberg, peut sembler très grande mais elle reflète la difficulté qu'il y a à contrôler la constante d'Eisenstein dans le processus de séparation des conjugués qui permet de se ramener au cas des fonctions régulières.

5.3. Calcul d'une constante d'Eisenstein par optimisation linéaire

Lorsque l'on veut utiliser les résultats du paragraphe précédent pour trouver une constante d'Eisenstein pour une fonction algébrique f, on ne s'intéressera qu'au "dénominateur" $Q \in \mathbb{Z}[x, y]$ d'une fraction rationnelle dont f est la diagonale : le "numérateur" $P \in \mathbb{Q}[x, y]$ de cette fraction ne peut qu'améliorer cette constante. [2]

Il résulte des calculs des lemmes 4.2 et 4.3 que, quitte à multiplier P par un "monôme" $x^r y^s$ (r et s entiers relatifs), ce qui ne change pas la constante d'Eisenstein, on peut toujours se ramener au cas où le dénominateur Q vérifie $Q(0,0) \neq 0$. D'après le lemme fondamental, il suffit alors

[2] L'exemple le plus extrême est celui où ce numérateur est égal au dénominateur ! En fait nous conjecturons que la constante d'Eisenstein radicale que nous trouvons par le procédé décrit ci-dessous est la meilleure possible si on veut qu'elle soit valable pour tous les numérateurs possibles.

de trouver des entiers algébriques α, β tels que le polynôme $Q(\alpha x, \beta y)$ ait des coefficients multiples, dans l'anneau des entiers algébriques, du nombre $Q(0,0)$. On va étudier, pour chaque facteur premier p de $Q(0,0)$, les contraintes que cette condition impose aux valuations p-adiques de α et β.
On obtient, pour chaque facteur premier p un système d'inéquations linéaires, à deux variables $v_p(\alpha), v_p(\beta)$, dont le rang est au plus égal au nombre de termes non constants du polynôme $Q(x,y)$. Nous cherchons alors le minimum de $v_p(\alpha) + v_p(\beta)$ sur le domaine convexe ainsi défini. Il est atteint pour l'un des sommets de ce domaine. On obtient ainsi une constante d'Eisenstein radicale p-adique $\alpha\beta = p^{v_p(\alpha)+v_p(\beta)}$ pour f.

Le produit des constantes d'Eisenstein p-adiques ainsi calculées donne une constante d'Eisenstein radicale pour f d'où on peut déduire une constante d'Eisenstein entière.

Nous illustrons cette méthode générale par un exemple.

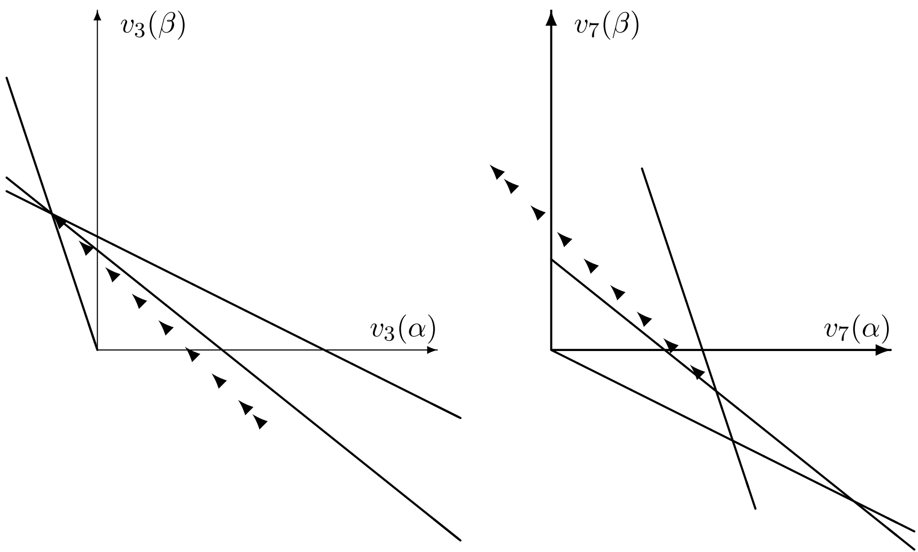
Exemple 5.8. Considérons le polynôme $Q(x,y) = 21 + 3x^3y + 7x^2y^4 + 5x^4y^5$. Les coefficients du polynôme $Q(\alpha x, \beta y)$ sont

– divisible par 3 si :

- $v_3(3\alpha^3\beta) \geq 1$ c'est-à-dire $3v_3(\alpha) + v_3(\beta) \geq 0$,
- $v_3(7\alpha^2\beta^4) \geq 1$ c'est-à-dire $2v_3(\alpha) + 4v_3(\beta) \geq 1$,
- $v_3(5\alpha^4\beta^5) \geq 1$ c'est-à-dire $4v_3(\alpha) + 5v_3(\beta) \geq 1$.

– divisible par 7 si :

- $v_7(3\alpha^3\beta) \geq 1$ c'est-à-dire $3v_7(\alpha) + v_7(\beta) \geq 1$,
- $v_7(7\alpha^2\beta^4) \geq 1$ c'est-à-dire $2v_7(\alpha) + 4v_7(\beta) \geq 0$,
- $v_7(5\alpha^4\beta^5) \geq 1$ c'est-à-dire $4v_7(\alpha) + 5v_7(\beta) \geq 1$.



Pour $p = 3$ la solution minimale est $\left(v_3(\alpha), v_3(\beta)\right) = (-1/10, 3/10)$ ce qui donne la constante d'Eisenstein radicale 3-adique $3^{-1/10+3/10} = 3^{1/5}$. Pour $p = 7$ la solution minimale est $\left(v_7(\alpha), v_7(\beta)\right) = (4/11, -1/11)$, d'où la constante radicale 7-adique $7^{4/11-1/11} = 7^{3/11}$.
Finalement, une constante d'Eisenstein radicale pour la fonction $f(x) = \operatorname{diag}\left(\dfrac{R(x,y)}{S(x,y)}\right)$ est $3^{1/5}7^{3/11}$ et une constante entière est $21 = Q(0,0)$ ce qui n'était pas difficile à obtenir directement en utilisant le lemme fondamental avec $\alpha = 21$ et $\beta = 1$ par exemple !

Remarque 5.9. Dans l'exemple précédent, le fait d'autoriser pour α ou β une valuation p-adique négative améliore effectivement le résultat obtenu pour la constante d'Eisenstein radicale : En imposant à $v(\alpha)$ et à $v(\beta)$ des valeurs positives ou nulles, les solutions minimales correspondantes sont $\left(v_3(\alpha), v_3(\beta)\right) = (0, 4)$ et $\left(v_7(\alpha), v_7(\beta)\right) = (1/3, 0)$ ce qui conduit à trouver $3^{1/4}7^{1/3}$ comme constante d'Eisenstein radicale.

Remarque 5.10. Si f est la diagonale d'une fraction rationnelle de plus de deux variables (donc f n'est pas nécessairement algébrique [8]), le calcul d'une constante d'Eisenstein par la méthode d'optimisation linéaire reste possible même si elle devient plus ardue puisque l'on devra travailler dans un espace de dimension plus grande.

Références

[1] G. Christol – « Limites uniformes p-adiques de fonctions algébriques », Thèse de Doctorat d'Etat, Univ. Paris 6, 1977.

[2] J. Denef et L. Lipshitz – « Agebraic Power Series and Diagonals », *J. Number theory* **26** (1987), p. 46–67.

[3] P. Dienes – *The taylor series. an introduction to the theory of functions of a complex variable.*, Dover Publications Inc., New York, 1957.

[4] B. Dwork et A. Van der Poorten – « The Eisenstein Constant », *Duke Math. J.* **65** (1992), p. 23–43.

[5] ———, « Correction to "the Eisenstein Constant" », *Duke Math. J.* **76** (1994), p. 669–672.

[6] B. Dwork et P. Robba – « On Natural Radii of p-adique Convergence », *Trans. Am. Math. Soc* **256** (1979), p. 199–213.

[7] H. Furstenberg – « Algebraic functions over finite fields », *J. of Algebra* **7** (1967), p. 271–277.

[8] R. Mechik – « Diagonales de fractions rationnelles », Thèse de Magister, U.S.T.H.B Alger, 1991.

[9] W. Schmidt – « Eisenstein's Theorem on Power Series Expansions of Algebraic Functions », *Acta Arithmetica* **56** (1990), p. 161–179.

Rachid Mechik
Université des Sciences et de la
Technologie Houari Boumédiène
Faculté de mathématiques
B.P. 32, El Alia Bab Ezzouar, Alger
16111
Algérie
mechikrachid@yahoo.fr