N° d'ordre : 05/2012-E/MT

RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITÉ DES SCIENCES ET DE LA TECHNOLOGIE HOUARI BOUMEDIÈNE
FACULTÉ DES MATHÉMATIQUES

THÈSE

Présentée pour l'obtention du grade de Docteur d'Etat en Mathématiques
Option : Algèbre et Théorie des Nombres

Par
Rachid MECHIK

THÈME

Constante d'Eisenstein et Diagonales de Fractions Rationnelles

Soutenue publiquement le 19/07/2012 devant le jury composé de :

M.	**B. BENZAGHOU**	Professeur	à l'USTHB	Président
M.	**G. CHRISTOL**	Professeur	à l'Université Paris 6	Directeur de Thèse
M.	**A. SALINIER**	Professeur	à l'Université de Limoges	Examinateur
M.	**D. BEHLOUL**	Maître de Conférences A	à l'USTHB	Examinateur
M.	**A. DERBAL**	Maître de Conférences A	à l'ENS Kouba	Examinateur
M.	**M. REZAOUI**	Maître de Conférences A	à l'USTHB	Examinateur

SOMMAIRE

Résumé

Dans cette thèse, nous commençons par étudier les points suivants :

1- Constantes d'Eisenstein d'une fonction algébrique.

2- Une méthode effective de calcul d'une constante d'Eisenstein pour une fonction algébrique.

3- Lien entre fonctions algébriques et diagonales de fractions rationnelles :

soit $\mathbb{k}$ un corps. Une fonction f du corps $\mathbb{k}((x))$ est algébrique sur le corps $\mathbb{k}(x)$ si et seulement si elle est diagonale d'une fraction rationnelle F de l'anneau $\mathbb{k}(x, y) \cap \mathbb{k}((x, y))$.

4- Calcul de constantes d'Eisenstein pour les fonctions $(1-x)^r$, où r est un nombre rationnel.

5- Constante d'Eisenstein et optimisation linéaire : une méthode de calcul efficace.

Nous donnons ensuite une nouvelle démonstration d'un théorème de Dwork et van der Poorten.

Remerciements

Le point de départ de notre parcours dans la recherche est le thème des Diagonales de Fractions Rationnelles. Le Professeur B. Benzaghou, le premier, nous y a initié dans notre thèse de Magister dont il était le Directeur. Encore une fois, et avec la bonté et le sens de responsabilité du Professeur, il consent à notre sollicitation et accepte de présider le jury de soutenance de notre thèse de doctorat.
Alors que nous achevions notre travail de Magister, un contact eut lieu entre nous et le Professeur G. Christol. Ayant appris notre intérêt aux Diagonales et remarqué que la Constante d'Eisenstein pouvait y faire suite, Christol nous proposa d'étudier cette constante, dans le but de préparer la thèse présente. Depuis, il nous a accompagné de très près : Chercheur patient et averti, il a orienté nos efforts et nous a prêté main forte dans les situations difficiles.
Les résultats de ce travail sont le fruit de son patronage modèle.
Nous avons fait la connaissance du Professeur A. Salinier lors d'une rencontre à l'université de Limoges. Nous le trouvâmes accueillant et disposé à coopérer.
Sollicité pour prendre part à notre jury, il accepte sans hésitation.
Les Professeurs D. Behloul, F. Bencherif, S. Bouroubi, A. Derbal et M.S. Rezaoui nous font voisinage immédiat. Nous n'allons pas énumérer les occasions et la nature des soutiens qu'ils nous ont apportés : collègues depuis toujours, l'échange mutuel d'idées et de moyens s'est fait tout naturellement.
Soulignons cependant l'effort particulier de Behloul, Bouroubi et Rezaoui dans la mise en forme de cette thèse.
Que tous les collègues qui ont contribué, tant soit peu, à la réalisation de ce travail veuillent trouver ici l'expression de notre sincère gratitude.

Introduction

Le but de ce travail est d'étudier la constante d'Eisenstein des fonctions algébriques.

La méthode générale est de regarder séparément les facteurs de la forme p^h de ces constantes lorsque p parcourt l'ensemble des nombres premiers. Ces facteurs sont appelés constantes d'Eisenstein $p-$adiques et sont effectivement donnés par le rayon de convergence $p-$adique de la fonction considérée.

La thèse se compose de deux parties.

Dans la première, nous étudions la constante d'Eisenstein ainsi que certaines de ses variantes, en utilisant le fait que les fonctions algébriques sont des diagonales de fractions rationnelles (de deux variables). Notre méthode a consisté à minorer la constante d'Eisenstein sur des exemples " bien choisis", contrairement à Dwork et van der Poorten qui ont entrepris de la majorer en le degré et la hauteur du polynôme minimal de la fonction algébrique étudiée..

Si on compare nos résultats à ceux de Dwork et van der Poorten, la différence peut sembler frappante. Cependant, nous devons regarder cet "exploit "avec prudence : les valeurs "beaucoup trop grandes " de Dwork et van der Poorten, par rapport aux nôtres dans le cas régulier, reflètent la difficulté qu'il y a à contrôler la constante d'Eisenstein dans le processus de séparation des conjugués de la fonction algébrique correspondante, qui permet de se ramener aux fonctions algébriques régulières. Dans le cas des constantes calculées par l'optimisation linéaire, notre méthode se généralise sans difficulté à plus de deux variables (bien évidemment, les calculs deviennent délicats). Ceci pourrait être intéressant car les diagonales de fractions rationnelles apparaissent assez systématiquement en physique comme solutions de certaines équations de Calabi Yau (Tables of Calabi Yau Equations Alkmvist and Co ArXivmathg/0507430).

Le texte de la première partie contient essentiellement trois résultats .

Le premier : une "fonction" de $k[[x]]$ est algébrique sur $k(x)$ si et seulement si elle est la diagonale d'une fraction rationnelle à deux variables : dans la littérature,on n'en trouve pas de preuve aussi explicite que celle donnée ici, le point nouveau étant la caractérisation des polynômes $P(x, y)$ de l'anneau $\mathbb{Q}((x))[y]$ pour lesquels la série $P(xy, y)$ est inversible dans l'anneau $\mathbb{Q}((x, y))$, à partir de leur polygone de Newton $x-$adique. Ce résultat est intéressant en lui-même.

Nous caressons l'espoir de pouvoir généraliser cette caractérisation, dans un travail à venir, au cas des polynômes de plus de deux variables

Le second **:** le calcul d'une constante d'Eisenstein pour les fonctions $(1-x)^r$, avec r rationnel, est une illustration de la méthode utilisant le théorème de Furstenberg.

Le troisième **:** le calcul d'une constante d'Eisenstein pour la diagonale d'une fraction rationnelle à deux variables (ou plus) se ramène à un nombre fini de problèmes d'optimisation linéaire. Pour ce calcul, les valuations $p-$adiques se sont avérées adéquates.

Dans la deuxième partie, faisant appel à la théorie des corps stables, nous proposons une nouvelle démonstration, plus simple et beaucoup plus courte, du théorème fondamental de Dwork et van der Poorten : " Let M be a subfield of W_1 with discrete valuation. Let L be an extension of degree n (of M). Then $L \subset W_{|n\pi|}$." ([5], paragraphe 2, théorème 2). Nous introduisons le point générique pour caculer le rayon de convergence $p-$adique d'une fonction algébrique quelconque. Ainsi, une étape décisive, dans la généralisation du cas particulier des fonctions algébriques régulières , se trouve franchie.

Il ne reste plus, pour finir ladite généralisation, qu'à transférer en zéro les calculs faits ici près du point générique. Ceci fera l'objet d'un travail ultérieur dans lequel nous souhaitons améliorer, et en tout cas, complèterons le théorème de Dwork et van der Poorten, en utilisant une version plus raffinée du théorème de transfert. Par exemple, le théorème de transfert de Kedlaya (" $p-$adic Differential Equations", chap. 18, Cambridge Studies in Advanced Mathematics 125, Cambridge Univ.Press, 2010) serait un outil approprié pour atteindre ce but.

L'initiative de remanier la démonstration du théorème en question nous a été dictée par les consultations répétées de l'article à portée fondamentale de Dwork et van der Poorten, qui représente la référence de base écrite sur la constante d'Eisenstein et par la justification, jugée nécessaire, de l'introduction, par Dwork et van der Poorten, des ensembles U_c [5, §2].

Un point important de l'étude au voisinage du point générique est le lemme 1.2 de l'article [4] que Dwork et van der Poorten ont utilisé de manière essentielle. Ce lemme, en liaison étroite avec le théorème en question, s'énonce : " Let M_0 be a complete subfield of W (i.e. W_1). Let M be an extension of M_0 of degree n prime to p. Then M (as subfield of M_0^{alg} and hence by the lemma 1.1 (of [4]) identified with a subfield of $\mathbf{O}_t$) lies in W, i.e. each element of M converges on the disk $\mathbf{D(t,1^-)}$. This is automatically valid if $p = 0$." . La démonstration élégante de ce théorème, donnée par Dwork et Robba, est relativement facile à comprendre et nous ne l'avons pas reprise, préférant nous consacrer au cas où p divise le degré de l'extension, dont la compréhension dans l'article de Dwork et van der Poorten demande nettement plus d'efforts.

Le recours à la théorie des corps stables nous a autorisé du reste, dans la deuxième partie, à nous passer, dans nos calculs, de l'hypothèse restrictive de valuation discrète faite dans l'énoncé du théorème de Dwork et van der Poorten.

La théorie des nombres $p-$adiques est le cadre de ce travail et, à travers le texte, valeurs absolues et valuations $p-$adiques régissent les raisonnements. Nous n'avons toutefois rien rappelé de cette théorie, estimant qu'elle est devenue aujourd'hui chose classique.

Néanmoins, signalons pour les intéressés une introduction concise à la théorie $p-$adique. Il s'agit d'un cours nouveau, accessible, rédigé par S. Katok dans son livre : $p-$adic analysis in comparison with real // MASS selecta / Ed. by S. Katok, A. Sossinsky, and S. Tabachnikov. Providence, AMS, 2003, P.11-87

Pour finir, reconnaissons que nous ne saurions remercier suffisamment le professeur G. Christol de nous avoir recommandé le livre de S. Siegfried, U.Güntzer et R. Remmert (voir [1], bibliographie de la deuxième partie), document clé dans l'élaboration d'une partie de ce travail.

Partie 1

Sur la Constante d'Eisenstein

1.1 Présentation

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

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

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 [7] des valeurs précises à la constante d'Eisenstein et Dwork et Van der Poorten [5] 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 (§1) 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 (§ 2).

Nous donnons une démonstration très détaillée de la cïncidence entre l'ensemble des fonctions algébriques et celui des diagonales des fractions rationnelles en deux variables (§ 3).

Ensuite, nous utilisons ce résultat pour déterminer une constante d'Eisenstein pour les fonctions algébriques régulières (§ 4.1). 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 (§ 4.2). 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 (§ 4.3). On peut en déduire une constante d'Eisenstein radicale puis, quitte à perdre de l'information, une constante d'Eisenstein entière.

1.2 Définitions et premières propriétés

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

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 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 *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 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 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 $\bar{\mathbb{Z}}_p[[x]]$.*

1.2.2 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 $1/|a|$ (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 $P(f, x) = 0$, les zéros de f sont des racines de l'équation $P(0, x) = 0$). D'après un résultat classique sur les fonctions analytiques, on en déduit que la fonction f est bornée dans son disque de convergence.

Remarque 5 *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 [3], 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.*

Proposition 6 *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 $cf(bax) \in \mathbb{Z}[[x]]$.

(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 $\mathbb{Z}[[x]]$.

Remarque 7 *La proposition ci-dessus s'étend de manière évidente aux trois autres variantes de constantes d'Eisenstein pour une fonction algébrique f de $\mathbb{Q}[[x]]$.*

Exemple 8 *Considérons la fonction*

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

on trouve

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

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 $g(x) = 1/(x+3)$, donc aussi l'entier $2 \cdot 3 = 6$. Par conséquent, l'entier 6 est une constante d'Eisenstein pour la fonction

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

Théorème 9 (Eisenstein) *Toute fonction algébrique $f(x) \in \mathbb{Q}[[x]]$ possède une constante d'Eisenstein.*

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

1.3 Relations entre les différentes constantes d'Eisenstein

Proposition 10 *Les conditions suivantes sont équivalentes :*

1. *La fonction $f(x) \in \mathbb{Q}[[x]]$ 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 l'implication directe.

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 $f(x) \in \mathbb{Q}[[x]]$.

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 à $p^{\mathbb{N}} \subset \mathbb{N}^{\neq 0}$. 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 $\mathbb{N}^{\neq 0}$. 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 en fait à $\mathbb{Z}$. Autrement dit, $a = \prod_p a_p$ est une constante d'Eisenstein pour la fonction

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

Ce qui prouve l'implication réciproque.

Remarque 11 *Dans la condition 2) de la proposition 10, 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 12 *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, quels que 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 13 *Considérons la fonction $f(x) = \sum_n \alpha_n x^n$ où,*

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

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, quels que soient $a \in \mathbb{N}^{\neq 0}$ et $c \in \mathbb{Z}^{\neq 0}$, il existe un nombre premier p qui ne divise ni a, ni c de sorte que le nombre $c\alpha_p a^p$ n'appartient pas à $\mathbb{Z}$.

1.4 Fonctions algébriques et diagonales de fractions rationnelles

Soit $\mathbb{k}$ un corps. On définit une application diag : $\mathbb{k}((x,y)) \longrightarrow \mathbb{k}((x))$ 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 ([6] 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 14 *Soit $\mathbb{k}$ un corps. Une fonction f du corps $\mathbb{k}((x))$ est algébrique sur le corps $\mathbb{k}(x)$ si et seulement si elle est diagonale d'une fraction rationnelle F de l'anneau $\mathbb{k}(x,y) \cap \mathbb{k}((x,y))$.*

Démonstration : Le point clé pour démontrer que **la diagonale d'une fraction rationnelle est une fonction algébrique** est une description de l'anneau $\mathbb{k}(x,y) \cap \mathbb{k}((x,y))$. Pour cela, il faut caractériser les polynômes de $\mathbb{k}[x,y]$ qui sont inversibles dans l'anneau $\mathbb{k}((x,y)$. La réponse à cette question est donnée dans le lemme 18.

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

Lemme 15 *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

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

avec u dans $\Bbbk[[x, y]]$. Comme $\tilde{a}_0$ est inversible dans $\Bbbk[[x]]$, on constate 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 $\Bbbk((x, y))$, comme annoncé.

Lemme 16 *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 $\lambda \leq -1$. Alors la série $P(xy, y)$ est inversible dans l'anneau $\Bbbk((x, y))$.*

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 $\Bbbk[[x]]$. On trouve donc que :

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

avec u dans $\Bbbk[[x, y]]$. 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 $\Bbbk((x, y))$, comme annoncé.

Lemme 17 *Soit P un polynôme de l'anneau $\Bbbk((x))[y]$. 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 $\Bbbk((x, y))$.*

Démonstration : Soit $P(x,y) = a_d(x)y^d + \cdots + a_0(x)$ et soient $\lambda_1 \leq \cdots \leq \lambda_\nu$ les pentes du polygone de Newton de P. Par hypothèse on a $-1 < \lambda_1$ et $\lambda_\nu < 0$.

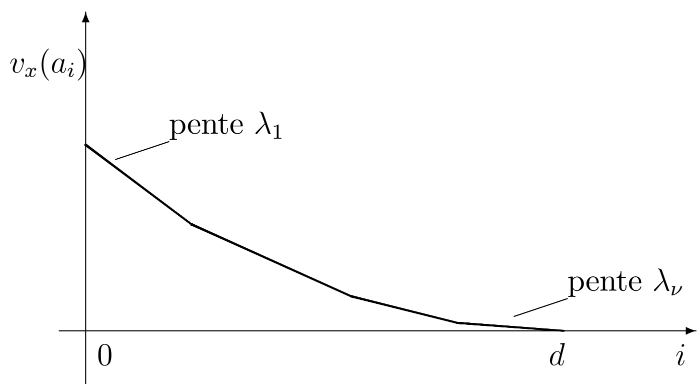


FIG. 1-1 – Polygone de Newton ayant toutes ses pentes dans $(-1, 0)$.

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 $0 < i$.

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 :

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

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

Lemme 18 *La fraction rationnelle F du corps $\mathbb{k}(x,y)$ appartient à l'anneau $\mathbb{k}((x,y))$ si et seulement si la fraction rationnelle*

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

écrite sous forme réduite dans $\mathbb{k}(x)(y)$ a un dénominateur D (dans $\mathbb{k}(x)[y]$), 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 $\mathbb{k}((x))$ 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 $\mathbb{k}((x))[y]$ dont le polygone de Newton x-adique a un seul coté, 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 $\mathbb{k}((x))[y]$ 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.

En vertu des lemmes 15 et 16, $Q(xy, y)$ est le produit d'éléments $P_{\lambda_i}(xy, y)$ inversibles dans l'anneau $\mathbb{k}((x, y))$ et est donc est inversible dans cet anneau. Par conséquent $\dfrac{S}{Q}(xy, y)$ appartient à $\mathbb{k}((x, y))$.

Si $F(xy) = \dfrac{N}{D}(xy, y)$ appartient à $\mathbb{k}((x, y))$, alors $\dfrac{R}{P}(xy, y)$ appartient à $\mathbb{k}((x, y))$. Or, comme $(R, P) = 1$, il existe des polynômes U, V de l'anneau $\mathbb{k}((x))[y]$ tels que $UP+VR = 1$, et donc $\dfrac{1}{P(xy, y)} = \big[U + V\dfrac{R}{P}\big](xy, y)$ appartient aussi à $\mathbb{k}((x, y))$. 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 17, $P(xy, y)$ ne peut être inversible dans l'anneau $\mathbb{k}((x, y))$ 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 15 et 16 assurent que $P(xy, y)$ est inversible dans l'anneau $\mathbb{k}((x, y))$ et la fraction rationnelle $F(xy) = \dfrac{N}{D}(xy, y)$ appartient bien à $\mathbb{k}((x, y))$ 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 (coeffficient 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

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

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 17, cette pente n'appartient pas à l'intervalle $(-1,0)$.

Nous calculons maintenant $\mathrm{diag}\big(\dfrac{yR(xy,y)}{P(xy,y)}\big)$ 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 15 :
on a $P(xy,y) = (xy)^v\big(\tilde{a}_0(xy) - y\,u(xy,y)\big)$ 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 $\mathbb{k}((x))$ 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 $\mathbb{k}((x))$ 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

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

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 :

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

c'est-à-dire :

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

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 19 *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 $G = N/D$:*

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

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 [6].

Théorème 20 (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 1-2). Il est donc clair que l'équation $P(x,y) = 0$ admet une et une seule racine f telle que $v_x(f) > 0$.

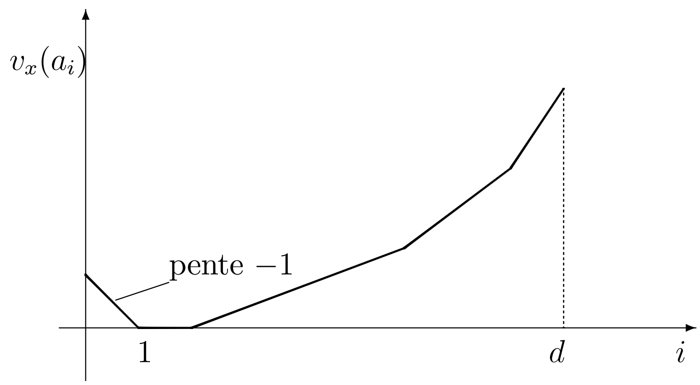


Fig. 1-2 – Polygone de Newton de P.

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 :

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

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 19 donne alors :

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

ce qui achève la démonstration de ce théorème.

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

Le corollaire 20 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 conjuguées à avoir cette propriété. Pour avoir une démonstration générale, il suffit de se ramener à ce cas en "séparant" f de ses conjuguées.

Soit $f = \sum_{n=0}^{\infty} a_n x^n$ 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

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

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 $g_i = x^{-d}(f_i - \sum_{n=0}^{d} a_n x^n)$. Par définition de d, pour $i > 1$, on a

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

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

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

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 $P\big(x, g(x)\big) = 0$, on trouve $P(0, 0) = P\big(0, g(0)\big) = 0$.

Le calcul des valuations x-adiques des racines g_i montre que le polygone de Newton x-adique de P (figure 1-2), 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 20, g

est la diagonale de la fraction rationnelle

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

Donc f est la diagonale de la fraction rationnelle

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

1.5 Calcul d'une constante d'Eisenstein pour une fonction algébrique

1.5.1 Constante d'Eisenstein de fonctions algébriques régulières

Comme on l'a vu à 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 20).

Lemme fondamental 21 *Soit $F(x,y) = P/Q$ une fraction rationnelle de $\mathbb{Q}(x,y)$ où P et Q sont des polynômes de $\mathbb{Q}[x,y]$ 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 $f(x) = diag F(x,y)$.*

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

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

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

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

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

Corollaire 22 *Si le polynôme Q de $\mathbb{Z}[x,y]$ satisfait la condition $Q(0,0) \neq 0$, alors $Q(0,0)^2$ est une constante d'Eisenstein pour la diagonale de P/Q où P est un polynôme de $\mathbb{Q}[x,y]$.*

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

Remarque 23 *Nous allons voir qu' 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 10 donnant alors la constante d'Eisentstein entière (exemple 26). 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 28).*

Corollaire 24 *Soit f une fonction algébrique régulière et soit P dans $\mathbb{Z}[x,y]$ un polynôme minimal de f $\left[\text{on a } P(x,f)=0,\ f(0)=0,\ P(0,0)=0 \text{ et } P'_y(0,0)\neq 0.\right]$ 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 conjuguées 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 particuliers, ce résultat général peut être notablement amélioré. Nous en donnons des exemples dans les paragraphes suivants.

1.5.2 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 25 *Soit m un entier naturel non nul et soit $m = p_1^{m_1} p_2^{m_2} ... p_n^{m_n}$ sa décomposition en produit de facteurs premiers. Posons*

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

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

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

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 alors $|\alpha_m|_p = |p|^{1/(p-1)} < 1$.

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

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

• 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

$$\left| \binom{m}{k} \right|_p = \left| \binom{m'}{k'} \right|_p$$

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

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

ce qui achève la démonstration.

Le lemme montre que, pour $2\leq k\leq m$, les nombres $\dfrac{1}{m}\dbinom{m}{k}\alpha_m^{k-1}$ sont des entiers (algébriques) et donc que le polynôme $\dfrac{1}{m}P\left(mx,\alpha_m y\right)$ est à coefficients entiers (algébriques). Le lemme fondamental montre alors 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 6-2). On en déduit aussitôt que $a'=m^2$ est une constante d'Eisenstein entière pour ces fonctions, ce que l'on aurait pu obtenir directement par le corollaire 24. Toutefois, quand m a des facteurs carrés, le résultat obtenu est meilleur comme le montre l'exemple suivant.

Exemple 26 *Considérons la fonction $f\left(x\right)=\left(1-x\right)^{1/m}$ 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 24 dès que $r>1$ ou $s>1$.

Remarque 27 *Considérons la fonction algébrique $g\left(x\right)=\left(1-x\right)^{1/3}-1$. On a $P\left(x,g\left(x\right)\right)=0$ avec $P\left(x,y\right)=y^3+3y^2+3y+x$. Le degré n de P en y ainsi que sa hauteur H valant 3, la formule de Dwork-van der Poorten [4] 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 en fait la difficulté qu'il y a à contrôler la constante d'Eisenstein dans le processus de séparation des conjuguées qui permet de se ramener au cas des fonctions régulières.

1.5.3 Calcul d'une constante d'Eisenstein par optimisation linéaire

Lorsqu'on utilise 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 15 et 16 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 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. Ce minimum est atteint à 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 l'on peut déduire une constante d'Eisenstein entière.

Nous illustrons cette méthode générale par un exemple.

Exemple 28 *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*

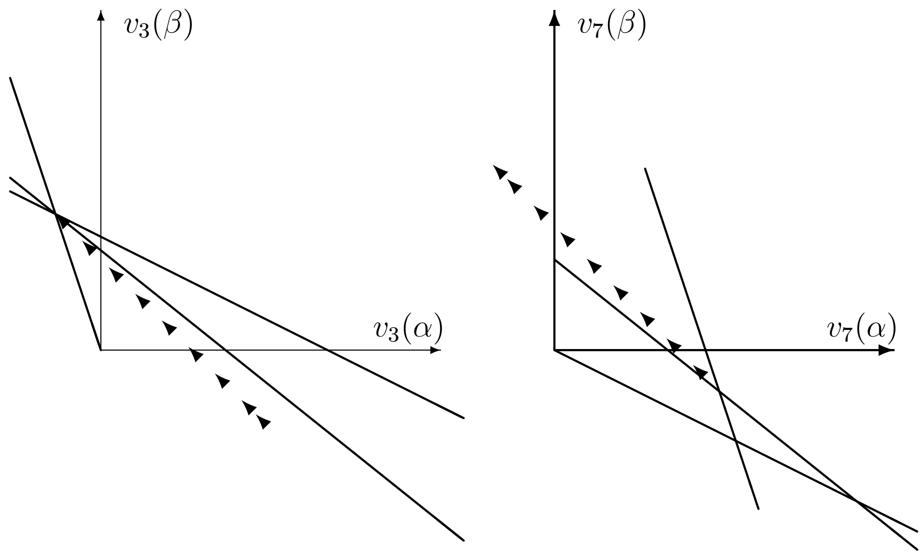
– *divisibles par* 3 *si :*

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

[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.

– *divisibles par* 7 *si :*

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



Pour $p = 3$, *la solution minimale est* $\big(v_3(\alpha), v_3(\beta)\big) = (-1/10, 3/10)$, *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* $\big(v_7(\alpha), v_7(\beta)\big) = (4/11, -1/11)$, *d'où la constante radicale* 7*-adique* $7^{4/11-1/11} = 7^{3/11}$.
Finalement, une constante d'Eisenstein radicale pour $f\left(x\right) = diag\left(\dfrac{R\left(x,y\right)}{S\left(x,y\right)}\right)$ *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 29 *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* $v\left(\alpha\right)$ *et à* $v\left(\beta\right)$ *des valeurs positives ou nulles, les solutions minimales correspondantes sont* $\big(v_3\left(\alpha\right), v_3\left(\beta\right)\big) = (0, 1/4)$ *et* $\big(v_7\left(\alpha\right), v_7\left(\beta\right)\big) = (1/3, 0)$, *ce qui conduit à la constante d'Eisenstein radicale* $3^{1/4}7^{1/3}$.

Remarque 30 *Si* f *est la diagonale d'une fraction rationnelle de plus de deux variables et est algébrique(auquel cas, la diagonale d'une fraction rationnelle algébrique de plus de deux variables n'est pas nécessairement algébrique, d'après* [6] *ou* [7] *), le calcul d'une* *constante d'Eisenstein par la méthode d'optimisation linéaire est théoriquement possible (devenant bien évidemment plus compliqué puisqu'alors on devra travailler dans un espace de dimension plus grande).*

1.6 Bibliographie

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

[2] Denef J & Lipshitz L, Agebraic Power Series and Diagonals, J. Number theory 26 46-67 (1987).

[3] Dienes P, The Taylor Series, Dover, New York (1957).

[4]Dwork B.M & Robba P, On Natural Radii of p-adique Convergence, Transactions of the American Mathematical Society, Volume 256, (1979).

[5] Dwork B.M & Van der Poorten A.J, The Eisenstein Constant, Duke Mathematical Journal, vol.65 N°.1 (1992).

[6] H. Furstenberg, Algebraic functions over finite fields, Journal of Algebra, 7 (1967) 271-277.

[7] Mechik R, Diagonales de fractions rationnelles, Thèse de Magister, U.S.T.H.B Alger (1991).

[8] Schmidt W.M, Eisenstein's Theorem on Power Series Expansions of Algebraic Functions, Acta Arithmetica, 56 (1990).

Partie 2

Une démonstration simplifiée d'un théorème de Dwork et van der Poorten

2.1 Présentation

Dans l'article [5] de Dwork et van der Poorten (voir aussi [6]), la démonstration du théorème 2 page 35 est certainement le point le plus délicat. Elle demande beaucoup d'efforts et occupe une place importante. De plus elle est trés déroutante pour le lecteur. En particulier, elle nécessite l'introduction de définitions surprenantes dont l'intérêt n'apparaît qu'à la fin.

Nous en proposons une démonstration beaucoup plus directe. Celle-ci repose fondamentalement sur la notion de corps stable que l'on trouve exposée de manière élégante dans [1]. Cette démonstration rend l'introduction des ensembles U_c tout à fait naturelle alors que, bien que fondamentale, leur définition paraît très artificielle dans [5].

Au paragraphe 2, nous rappelons les principaux résultats concernant les corps stables tels qu'ils sont développés dans [1]. Rappelons brièvement qu' un corps K est dit stable si toute extension finie L de K a une base "cartésienne" c'est-à-dire pour laquelle l'isomorphisme $L = K^n$ identifie la norme (spectrale) de L à la norme "sup" de K^n. Le résultat principal est que, si le corps K est stable, il en est de même du corps $K(x)$.

Nous complétons ces résultats par un lemme montrant l'existence de bases qui sont à la fois "cycliques" (c'est-à-dire de la forme $1,\, x,\, x^2, \ldots, x^{n-1}$) et cartésiennes.

Dans le paragraphe 3, supposant le corps K muni d'une dérivation, nous étudions le prolongement de cette dérivation à une extension algébrique finie L de K. En particulier, nous majorons la norme de l'opérateur de dérivation agissant sur L à partir de sa norme sur K et du degré de l'extension. Le résultat obtenu est le meilleur possible.

Dans le paragraphe 4, suivant Dwork et van der Poorten, nous identifions (par la formule de Taylor) les éléments d'une extension algébrique L de $K(x)$ à des fonctions analytiques au voisinage du point générique. Le résultat du paragraphe 3 nous permet de minorer leur rayon de convergence. Le résultat obtenu est le meilleur possible si le degré n de l'extension $L/K(x)$ est divisible par p. Par contre, il n'est pas très bon dans le cas "simple" où p ne divise pas n. Ceci est un phénomène bien connu dans l'étude des équations différentielles p-adiques et vient de la non prise en compte, dans nos calculs, d'une simplification du facteur $\frac{1}{n!}$ qui apparaît dans les dérivées supérieures. Ce cas est traité dans [4].

2.2 Préliminaires

Dans ce paragraphe, définitions, propositions et théorèmes sont empruntés à [1].

Définition 31 *Soit K un corps valué et soit L une extension finie de K. On définit la* norme spectrale *sur L par*

$$|y| = \max_{0 \le i \le n-1} |a_i|^{\frac{1}{n-i}}$$

où $P(y) = y^n + a_{n-1}\, y^{n-1} + \cdots + a_0$ est le polynôme unitaire minimal de y sur K.

La norme spectrale est une K-norme ([1] théorème 3.3.2/1 page 134). Si K est complet, la norme spectrale est l'unique valeur absolue sur L qui prolonge la valeur absolue de K. Tous les corps que nous allons considérer seront complets à l'exception du corps $K(x)$.

Définition 32 *Soit K un corps valué et soit M un K-espace vectoriel de dimension finie muni d'une K-norme $\|\cdot\|$. L'espace vectoriel M est dit* cartésien *s'il possède une base $\{e_1, \ldots, e_n\}$ (dite* base cartésienne*) telle que*

$$(\forall (a_1, \ldots, a_n) \in K^n) \qquad \Big\| \sum a_i e_i \Big\| = \max |a_i| \, \|e_i\|$$

Définition 33 *On dit qu'un corps valué K est* stable *si toute extension finie L de K, munie de la norme spectrale (définition 31), est un K-espace vectoriel cartésien.*

Par exemple, un corps algébriquement clos est stable car il ne possède qu'une seule extension finie, à savoir lui-même, et la base $\{1\}$ convient évidemment.

Proposition 34 ([1] proposition 3.6.2/3 page 158) *Si un corps valué K est stable alors son complété est stable.*

Proposition 35 ([1] corollaire 3.6.2/7 page 161) *Si K est complet et stable, alors toute extension finie de K est stable (et complète).*

Définition 36 *On dit qu'un corps valué K est* à valuation divisible *si, pour tout entier m et tout a dans K, il existe b dans K tel que $|b^m| = |a|$.*

Si le corps K est un corps valué à valuation divisible, on a évidemment $|K| = |L|$ pour toute extension finie L de K munie de sa norme spectrale.

Proposition 37 ([1] proposition 3.6.2/8 page 161) *Soit K un corps valué à valuation divisible et soit L une extension finie de K (munie de sa norme spectrale). L'extension L est un K-espace vectoriel cartésien si et seulement si $[\overline{L} : \overline{K}] = [L : K]$, où $\overline{K}$ (resp. $\overline{L}$) est le corps des restes de K (resp. L).*

Théorème 38 ([1] proposition 5.3.3/3 page 215) *Soit K un corps valué stable et à valuation divisible, alors le corps $K(x)$ (des fractions rationnelles en x, à coefficients dans K), muni de la norme de Gauss, est stable.*

Lemme 39 *Soit K un corps valué complet, de caractéristique nulle et soit L une extension finie de K. S'il existe $\overline{y}$ dans $\overline{L}$ tel que $\overline{L} = \overline{K}[\overline{y}]$ (c-à-d si $\overline{L}/\overline{K}$ est une extension* simple*) alors, pour tout relèvement y de $\overline{y}$ dans L, on a*

$$\Big(\forall (c_0, \dots, c_{n-1}) \in K^n\Big) \qquad \Big|\sum_{i=0}^{n-1} c_i\, y^i\Big| = \max |c_i| \ .$$

Démonstration : Soit y un relèvement de $\overline{y}$ dans L. Par définition du corps des restes, on a $|y| = 1$. Soit $P(y) = y^m + a_{m-1}y^{m-1} + \cdots + a_0$ le polynôme unitaire minimal de y. En vertu de la définition de la norme spectrale sur L, on a

$$\max_{0 \leq i \leq m-1} |a_i|^{\frac{1}{m-i}} = |y| = 1. \tag{2.1}$$

En passant au corps des restes, on trouve :

$$\sum_{i=0}^{m} \overline{a}_i\, \overline{y}^i = 0,$$

où l'on a noté $\overline{a}_i$ l'image de a_i dans le corps des restes $\overline{K}$. D'après (2.1), les $\overline{a}_i$ ne sont pas tous nuls. Donc, si on note $n = [\overline{L} : \overline{K}]$ le degré de $\overline{y}$ sur $\overline{K}$, on a $n \leq m$.

Comme K est stable, L est un K-espace vectoriel cartésien et, K étant à valuation divisible, la proposition 37, montre que :

$$[L : K] = [\overline{L} : \overline{K}] = n \leq m = [K[y] : K].$$

Mais y appartient à L, donc $L = K[y]$ et $n = m$.

Maintenent, soit $(c_0, \ldots, c_{n-1})$ dans K^n, les c_i n'étant pas tous nuls. Choisissons un élément λ de K tel que $\max |\lambda\, c_i| = 1$. On trouve :

$$\Big| \sum_{i=0}^{n-1} \lambda c_i\, y^i \Big| \leq 1.$$

Si l'inégalité était stricte, en passant au corps des restes, on aurait

$$\sum_{i=0}^{n-1} \overline{\lambda c_i}\, \overline{y}^i = 0.$$

Comme $\overline{y}$ est de degré n sur $\overline{K}$, on aurait $\overline{\lambda c_i} = 0$, soit $|\lambda\, c_i| < 1$, pour tout i, d'où $\max |\lambda c_i| < 1$ ce qui n'est pas.

2.3 Prolongement d'une dérivation aux extensions finies

Proposition 40 *Soit K un corps de caractéristique nulle muni d'une dérivation d et soit L une extension finie de K. La dérivation d se prolonge de manière unique en une dérivation de L, que l'on notera encore d.*

Plus précisément, pour y dans L^*, si $P(y) = y^n + a_{n-1}\, y^{n-1} + \cdots + a_0$ est le polynôme unitaire minimal de y sur K, on a :

$$d(y) = -\frac{\sum_{i=0}^{n-1} d(a_i)\, y^i}{\sum_{i=1}^{n} i\, a_i\, y^{i-1}}. \tag{2.2}$$

Démonstration : Si la dérivation d se prolonge à L, on a

$$0 = d\big(P(y)\big) = d(y)\, P'(y) + d\big(a_{n-1}\big)\, y^{n-1} + \cdots + d\big(a_0\big).$$

Le corps K étant de caractéristique nulle, y est une racine simple de P et $P'(y)$ n'est pas nul. On constate que le prolongement de d est unique et est donné par (2.2).

Le fait que ce prolongement existe effectivement est bien connu. C'est, par exemple, un cas très particulier du théorème 1 de [2].

Définition 41 *Soit K un corps valué de caractéristique nulle. On suppose que K est muni d'une dérivation d, on note d_K la norme de la dérivation d vue comme opérateur sur K :*

$$d_K = \sup_{y \in K^{\neq 0}} \frac{\left|d(y)\right|}{|y|}$$

Une extension finie L de K étant donnée, on se propose maintenant de calculer la norme d_L en fonction de la norme d_K et du degré $[L : K]$.

Théorème 42 *Soit K un corps valué complet de caractéristique nulle à valuation divisible et muni d'une dérivation d. Soit L une extension algébrique de degré fini n de K. On note d_K (resp. d_L) la norme de la dérivation (resp. du prolongement de la dérivation) d agissant sur K (resp. L). On a alors la majoration :*

$$d_L \leq |n|^{-1} d_K.$$

Démonstration : **a) Cas d'une extension simple**. Dans ce cas $\overline{L} = \overline{K}[\overline{y}]$ et, d'après le lemme 39, si y est un relèvement de $\overline{y}$ alors $L = K[y]$ et $1, \dots, y^{n-1}$ est une base cartésienne de L sur K. Puisque $|y| = 1$, si $P(y) = y^n + a_{n-1}\, y^{n-1} + \cdots + a_0$ est le polynôme unitaire minimal de y sur K, on a $\max_{0 \leq i \leq m-1} |a_i| = 1$ (en fait, le corps K étant complet, le lemme de Hensel montre que $|a_0| = 1$). Il vient

$$\Big|\sum_{i=0}^{n-1} d(a_i)\, y^i\Big| = \max \left|d(a_i)\right| \leq d_K \, \max |a_i| = d_K,$$

$$\Big|\sum_{i=0}^{n} i a_i \, y^{i-1}\Big| = \max |i\, a_i| \geq |n\, a_n| = |n|.$$

Et finalement on trouve :

$$\left|d(y)\right| = \left|\frac{\sum_{i=0}^{n-1} d(a_i)\, y^i}{\sum_{i=1}^{n} i\, a_i\, y^{i-1}}\right| \leq \frac{1}{|n|} d_K.$$

Maintenant, pour n'importe quel élément $x = \sum_{i=0}^{n-1} c_i\, y^i$ de L, on a :

$$d(x) = \sum_{i=0}^{n-1} d(c_i)\, y^i + i\, c_i\, d(y)\, y^{i-1} = \sum_{i=0}^{n-1} \Big(d(c_i) + (i+1)\, c_{i+1}\, d(y) \Big)\, y^i,$$

ce qui donne

$$\big|d(x)\big| = \max \Big\{ \big|d(c_i) + (i+1)\, c_{i+1}\, d(y)\big| \Big\} \leq \max \big\{ d_K |d(y)| \big\} \max |c_i| = \frac{1}{|n|}\, d_K\, |x|.$$

On obtient finalement $d_L \leq \dfrac{1}{|n|}\, d_K$ comme annoncé.

b) Cas général. On passe de K à L par une succession d'extensions L_i telles que les extensions résiduelles $\overline{L}_i/\overline{L}_{i-1}$ soient simples. Le résultat s'en déduit car évidemment

$$[L = L_m : L_{m-1}] \cdots [L_1 : L_0 = K] = [L : K].$$

2.4 Corps de fonctions analytiques près du point générique

2.4.1 Anneau de fonctions analytiques bornées près du point générique

Dans ce paragraphe, K est un corps valué qui contient $\mathbb{Q}_p$, stable et à valuation divisible. On peut prendre, par exemple, $K = \mathbb{C}_p$ (complété de la clôture algébrique de $\mathbb{Q}_p$).

On considère aussi un corps Ω "suffisamment gros", qui contient K. Plus précisément, on suppose que Ω est algébriquement clos, sphériquement complet et de corps des restes transcendant sur celui de K.

On choisit un “point générique”t, c'est-à-dire un nombre de Ω tel que $|t| = 1$ et que le disque $D(t, 1^-)$ ne contienne pas de point de la clôture algébrique de K. Soit $Q = \sum a_i\, x^i$ un polynôme de $K[x]$. Soit $\overline{Q}$ le polynôme de $\overline{K}[x]$ obtenu en passant au corps des restes après normalisation. On a $\overline{Q}(\overline{t}) \neq 0$ (sinon, le lemme de Hensel montrerait que le disque $D(t, 1^{-1})$ contient une point de la clôture algébrique de K). Donc $\big|Q(t)\big| = 1$. Autrement dit,

$$\big(\forall (a_0,\ldots,a_m)\in K^m\big) \qquad\qquad \Big|\sum_{i=0}^{m} a_i\, t^i\Big| = \max |a_i|.$$

Définition 43 *Pour $r \leq 1$, on note W_r l'anneau des fonctions analytiques à coefficients dans Ω, qui convergent et sont bornées dans le disque $D(t, r^-)$:*

$$W_r = \Big\{ \sum_{s=0}^{\infty} a_s\,(x-t)^s a_s \in \Omega,\ r^s\,|a_s|\ \textit{bornés}\Big\}.$$

On munit cet anneau de la valeur absolue "borne supérieure dans le disque $D(t, r^-)$" :

$$\Big|\sum a_s\,(x-t)^s\Big|_r = \sup |a_s|\,r^s.$$

Remarque 44 *Pour $r > \varrho$, le plongement $W_r \hookrightarrow W_\varrho$ n'est pas une isométrie. Autrement dit, il y a des fonctions f dans W_r telles que $|f|_r > |f|_\varrho$. En fait, cela se produit si et seulement si $\big|f(t)\big| < |f|_r$. Or, les fonctions particulières qui nous intéresseront ne s'annulant pas dans le disque $D(t, r^-)$, on aura $\big|f(t)\big| = |f|_r$.*

Soit M un corps contenu dans l'anneau $\Omega[[x-t]]$. Le corps M est naturellement muni de la dérivation $d = \frac{d}{dx}$ et il est facile de vérifier que $|f| = |f(t)|$ est bien une valeur absolue sur M ([4] page 200) : il suffit de remarquer que, si $|f(t)| = 0$, alors f est un élément non inversible dans l'anneau $\Omega[[x-t]]$, donc non plus dans le corps M. Autrement dit, $f = 0$.

La proposition suivante relie la norme d_M de la dérivation $\frac{d}{dx}$ opérant sur M et le rayon de convergence des éléments de M ; elle justifie aussi l'introduction des ensembles U_c de Dwork-van der Poorten ([5] paragraphe 2) :

$$U_c = \Big\{\theta \in W_{\omega\,|p|^c}\,;\ \text{pour } |x-t| < \omega\,|p|^c, \quad \Big|\frac{\theta(x)-\theta(t)}{\theta(t)}\Big| < |p|^{-c}\,|x-t|\Big\}$$

où, pour simplifier, on a posé $\omega = |p|^{\frac{1}{p-1}}$ (ω est la valeur absolue du "π de Dwork").

Proposition 45 *Soit M un sous corps de l'anneau $\Omega[[x-t]]$. Si on le munit de la valeur absolue $|f| = |f(t)|$ et de la dérivation $d = \frac{d}{dx}$, on a $M \subset W_r$ avec $r\,d_M = \omega$. Inversement, si $M \subset W_r$, alors $r\,d_M \leq 1$.*

Démonstration : Pour f dans le corps M, on a $|f^{(s)}(t)| = |d^s(f)| \leq d_M^s|f| = d_M^s|f(t)|$. Comme $|\dfrac{1}{s!}| \leq \omega^{-s}$, la formule de Taylor $f = \displaystyle\sum_{s=0}^{\infty} \frac{1}{s!}\, f^{(s)}(t)(x-t)^s$ permet de constater que

f est contenue dans $W_{\omega\, d_M^{-1}}$. Inversement, si f appartient à $M \subset W_r$, alors, f et f^{-1} appartenant à W_r, la fonction f ne peut avoir de zéro dans le disque $D(t, r^-)$ et la fonction $x \mapsto \big|f(x)\big|$ est constante dans ce disque. En particulier $|f| = |f(t)| = \sup \big|f(x)\big| = |f|_r$. Alors on trouve :

$$\big|d(f)\big| = \Big|\frac{df}{dx}\Big|_r \leq \frac{1}{r}|f|_r = \frac{1}{r}|f|.$$

D'où la majoration $d_M \leq r^{-1}$.

Remarque 46 *Il y a, a priori, un facteur ω perdu dans la manœuvre...*
En fait, en utilisant la majoration plus fine

$$|\frac{1}{s!}| \leq \omega^{1-s} \qquad \textit{pour } s \geq 1$$

on trouve, en définissant le nombre c par $d_M^{-1} = |p|^c$:

$$M \subset \Big\{ f \in W_{\omega\,|p|^c} |f - f(t)|_{\omega\,|p|^c} \leq \omega\,|f(t)| \Big\} = U_c.$$

Inversement, f et $f - f(t)$ ayant la même dérivée, si f appartient à U_c, il vient

$$|f'(t)| \leq \frac{1}{\omega\, d_M^{-1}}\,|f - f(t))|_{\omega\, d_M^{-1}} \leq d_M\,|f(t)|,$$

sans perte de facteur.

2.4.2 Corps de fonctions algébriques

On munit le corps $K(x)$ de la norme de Gauss. Autrement dit, pour f dans $K(x)$, on pose : $|f| = |f(t)|$. D'après le théorème 38 des préliminaires, $K(x)$ est un corps stable. Par ailleurs, il est à valuation divisible car évidemment $\big|K(x)\big| = |K|$.

On note E le complété du corps $K(x)$ pour la norme de Gauss. C'est un corps stable, d'après la proposition 2.4 des préliminaires.

Proposition 47 ([3] proposition2.5.1) *Le corps des fractions rationnelles $K(x)$ se plonge dans l'anneau W_1 par la formule de Taylor*

$$f \hookrightarrow \sum_{s=0} f^{(s)}(t)\,\frac{(x-t)^s}{s!}.$$

Ce plongement est une isométrie pour la norme de Gauss et la valeur absolue $|\cdot|_1$.
Il se prolonge donc en un plongement du corps E dans l'anneau W_1.

On peut maintenant démontrer le résultat suivant.

Théorème 48 *Soit L une extension algébrique de degré fini n de E, contenue dans l'anneau $\Omega[[x-t]]$. Alors L est contenue dans l'anneau $W_{\omega\,|n|}$.*
Si p ne divise pas n, elle est contenue dans l'anneau $W_1 = W_{|n|}$.

Démonstration : Comme E est inclus dans W_1, on a $d_E = 1$. (voir proposition 45). Le corps E est stable et à valuation divisible car $|E| = \left|K(x)\right|$. On peut lui appliquer le théorème 42. On trouve $d_L \leq |n|^{-1}\, d_E = |n|^{-1}$. La proposition 45 affirme alors que l'extension L est contenue dans $W_{\omega\,|n|}$.

Le cas où p ne divise pas n est exactement le lemme 1.2 de [4].

Remarque 49 *La fonction*

$$f(x) = x^{p^{-h}} = \sum_{n=0}^{\infty} \binom{p^{-h}}{n} (x-t)^n$$

a un rayon de convergence égal à $\omega|p|^h$. Elle montre que le résultat du théorème 48 ne peut être amélioré.

2.5 Bibliographie

[1] S. Bosch, U. Güntzer, & R. Remmert - Non -Archimedean analysis. A Systematic approach to rigid analytic geometry, Grundlehren der Mathematischen Wissenschaften, 261. Berlin etc. : Springer Verlag.Xll , 436 p. ,1984.
[2] P. Cartier.-" Dérivations dans les corps. ", Sém. H. Cartan et C. Chevaley Exp. 13, 13 pp., 8 ème année (1955/1956), 1956.
[3] G. Christol.-Differential modules and P-adic differential equations. (Modules différentiels et équations différentielles p-adiques), Queen's Papers in Pure and Applied Mathematics, 66. Kingston, Ontario, Canada, : Queen's University. Vl, 218 p. , 1983.
[4] B. M. Dwork. & P. Robba. -" On natural radii of p-adic convergence .", Trans. Am. Math. Soc. 256 (1979), p. 199-213.
[5] B. M. Dwork. & A. J. Van der Poorten.-"The Eisenstein constant.", Duke.Math. J. 65 (1992), no.1, p. 23-43.
[6] __________,-"Corrections to "The Eisenstein constant".", Duke. Math. J. 76 (1994), no.2, p. 669-672.

[7] R. Mechik.-“Sur la constante d’Eisenstein.”, Ann. Math. Blaise Pascal 15 (2008), no. 1, p. 87-108.