T H E S E présentée

pour l'obtention

du

DIPLOME de DOCTEUR de 3e CYCLE

à

L'UNIVERSITÉ PIERRE ET MARIE CURIE
- Paris 6 -

spécialité : MATHEMATIQUES

mention : THEORIE DES NOMBRES

par M Pierre DEBES

Sujet de la thèse :

VALEURS ALGEBRIQUES DE FONCTIONS ALGEBRIQUES ET THEOREME D'IRREDUCTIBILITE DE HILBERT.

soutenue le 2 Juillet 1984 devant la Commission composée de :

M Daniel BERTRAND Président

M Daniel BARSKY examinateur

M Peter BUNDSCHUH «

M Michel WALDSCHMIDT «

M ..... «

M ..... «

M ..... invité

Avant toute chose, je tiens à remercier D. Barsky, D. Bertrand, P. Bundschuh et M. Waldschmidt de l'honneur qu'ils me font de participer au jury de ma thèse.

Je voudrais aussi employer ces quelques lignes pour témoigner toute ma gratitude aux personnes qui m'ont aidé dans ce travail.

Je pense en premier lieu à M. Waldschmidt, qui depuis mes premiers pas en Théorie des Nombres a su guider ma progression avec une grande justesse ; sa clairvoyance, sa rigueur et son enthousiasme ont été un soutien constant durant ces années.

Je veux parler également de D. Bertrand qui me fait le plaisir de présider le jury de ma thèse ; en de nombreuses occasions, ses remarques, ses explications et ses suggestions se sont révélées une aide précieuse.

Bien d'autres personnes, par leurs indications, leurs conseils et leurs encouragements ont stimulé mes efforts ; parmi elles, D. Barsky, S. Lang, P. Ribenboim, P. Robba, V-G Sprindzuk et bien sûr tous les membres de l'ERA 979 ; qu'ils soient sûrs de ma reconnaissance et de mon estime.

Je remercie enfin M. Blin qui a effectué le tirage de ce mémoire.

R E S U M E

Soient k un corps de nombres et P un polynôme irréductible dans $k[X,Y]$; le théorème d'irréductibilité de Hilbert montre que l'ensemble $H_{P,k}$ constitué des éléments x de k tels que P(x,Y) soit irréductible dans $k[Y]$, est un ensemble infini.

Inspirés par ce théorème, qui joue un rôle essentiel en Théorie des Nombres, les résultats que nous donnons ici, sont plus qualitatifs. Le théorème 2 de ce mémoire (Ch II Th2), qui généralise des travaux de P. Bundschuh et de V-G Sprindzuk, relie a priori, la structure arithmétique d'un élément x de k à celle du polynôme P(x,Y).

Dans certains cas, cette relation est particulièrement simple ; on obtient ainsi, sous certaines conditions, portant entre autres sur la loi de décomposition du nombre premier p dans une certaine extension K de k, l'irréductibilité dans $k[Y]$ des polynômes $P(p^m, Y)$.

Le cas général, s'il est plus complexe, conduit cependant à une nouvelle version du théorème d'irréductibilité de Hilbert (Ch VI Th 5).

Géométriquement, on peut voir le théorème 2 comme un énoncé sur les points rationnels d'une courbe algébrique plane (Ch VII Th 6). Plus généralement, on démontre, en s'appuyant sur un travail de Bombieri, un résultat sur les valeurs d'une fonction rationnelle d'une courbe projective lisse (Ch VII Th 7).

Enfin, on montre en appendice que la méthode transcendante de Gel'fond, qui est à la base de la démonstration du théorème 2, permet également une nouvelle approche du résultat de Bombieri sur les G-fonctions.

S O M M A I R E

INTRODUCTION

Soient k un corps de nombres et P un polynôme irréductible dans $k[X,Y]$. Considérons l'ensemble $H_{P,k}$ des éléments x de k tels que $P(x,Y)$ soit irréductible dans $k[Y]$. D. Hilbert a démontré en 1892 [Hi] que $H_{P,k}$ est un ensemble infini dès que $\deg_Y P \geq 1$ (Théorème d'irréductibilité de Hilbert). Ce résultat s'est révélé depuis, un auxiliaire précieux en Théorie des Nombres (voir [Se]), suscitant de multiples travaux ([Dö], [Si] [Schi], [Fr] entre autres). Grâce au théorème de Siegel [Si], on sait par exemple majorer par un $O(\sqrt{N})$ pour $k = \mathbb{Q}$, le nombre des entiers x qui ne sont pas dans $H_{P,\mathbb{Q}}$ et tels que $|x| \leq N$.

Les fonctions algébriques constituent un outil privilégié pour aborder ce type de résultat. Si Y est une fonction algébrique solution de $P(x,Y) = 0$, le problème consiste à montrer que, pour x dans k, $Y(x)$ est "souvent" de degré sur k égal à $\deg_Y P$. Posé ainsi, il rappelle certains énoncés de transcendance, du genre : si f est une fonction transcendante, alors $f(3)$ est "souvent" transcendant quand 3 est algébrique ; par exemple, si f est l'application exponentielle, c'est le théorème de Hermite-Lindemann, "souvent" signifiant alors 3 non nul. Cette analogie suggère l'idée d'essayer d'adapter au cadre des fonctions algébriques des méthodes développées initialement en transcendance (méthodes de Gel'fond, Siegel, Schneider, Mahler ...)

Ces méthodes suivent schématiquement le modèle suivant.

-1- La construction d'une fonction auxiliaire non nulle possédant de nombreux zéros — elle sera dans notre étude du type $\Phi(X,Y)$, avec $\Phi \in k[X,Y]$ et $\deg_Y \Phi < \deg_Y P$ —

-2- Les minoration et majoration d'une quantité non nulle convenablement choisie — l'inégalité obtenue, qui en général fournit la contradiction d'un raisonnement par l'absurde dans le cas des fonctions transcendantes, constituera pour nous le résultat désiré —

Les fonctions transcendantes, auxquelles on s'intéresse, satisfont habituellement,

soit des équations différentielles (méthodes de Gel'fond, Siegel), soit des équations fonctionnelles (méthode de Mahler). Une fonction algébrique satisfait l'équation fonctionnelle $P(x,y)=0$ il est facile, en outre, d'en déduire une équation différentielle linéaire dont elle soit solution. Ceci a pour effet d'imposer des conditions de croissance, nécessaires dans ce genre de méthode aux coefficients de son développement de Taylor, tant aux places archimédiennes qu'aux places finies : plus précisément, les fonctions algébriques sont des G- fonctions. Enfin, dans le cas des fonctions algébriques, des arguments élémentaires permettent d'obtenir des "lemmes de zéros", dernier ingrédient d'une démonstration de transcendance, qui sert à majorer le nombre de zéros de la fonction auxiliaire : par exemple, la norme par rapport à $k(x)$ d'une fonction algébrique non nulle ou encore le résultant de P et de Φ par rapport à la variable Y, sont des fractions rationnelles, non nulles, et n'admettent donc qu'un nombre fini de racines.

Les fonctions algébriques sont donc a priori tout à fait susceptibles d'être étudiées au moyen de telles méthodes. Les premiers efforts dans ce sens, qui seront déterminants, remontent à Siegel qui en 1929, évoquait à la fin de son article sur les E- fonctions [Si], la possibilité d'utiliser sa méthode pour les G- fonctions. Ses idées se concrétiseront cinquante ans plus tard, avec les travaux de T. Schneider [Schn1] [Schn2], P. Bundschuh [Bu] et de V.G Sprindzuk [Sp1], [Sp2], [Sp3], [Sp4] sur les valeurs de fonctions algébriques, et ceux de E. Bombieri, notamment, sur les valeurs de G- fonctions [Bo1].

Les premiers résultats obtenus sont des énoncés "locaux" : ils montrent qu'un nombre algébrique non nul appartient nécessairement à l'ensemble $H_{P,k}$ s'il est suffisamment petit par rapport à sa hauteur et son degré pour une place v donnée. T. Schneider et P. Bundschuh traitent le cas d'une place archimédienne, V.G Sprindzuk celui d'une place finie. Peu après, Sprindzuk ([Sp2] puis [Sp4]) donnera un énoncé plus général, tenant compte à la fois des points de vue archimédiens et p-adiques. Le résultat central de ce mémoire que nous donnons au chapitre II (§2.1 Théorème 2) améliore cet énoncé de Sprindzuk. De nature "globale" en ce sens qu'ils font intervenir simultanément plusieurs places, ces résultats mettent en évidence une relation entre la structure arithmétique d'un élément x de k (sa "décomposition" dans l'anneau des entiers d'un certain corps de nombres K attaché au polynôme P) à celle du polynôme $P(x,Y)$ (sa décomposition en irréductibles de l'anneau principal $k[Y]$). Du théorème 2, il est facile de déduire un énoncé local (Ch II §1.1 Th 1) qui contient alors tous ceux cités plus haut.

La démonstration du théorème 2, préparée au chapitre III, fait l'objet du chapitre IV. Notre approche, également "transcendante", diffère cependant quelque peu de celle de Sprindzuk

la ligne directrice de sa démarche est d'adapter la méthode de Siegel aux fonctions algébriques ; notre démonstration, qui généralise celle de P. Bundschuh, s'appuie elle sur la méthode de Gel'fond [Wa].

Au chapitre V, on fait le lien avec le résultat de Bombieri sur les valeurs de G- fonctions [Bo1]. La méthode, cinquante ans après, s'inspire encore des idées de Siegel. On en rappelle les grandes lignes dans un premier temps ; on donne ensuite à partir du résultat de Bombieri, qui s'applique au cas particulier des fonctions algébriques, une nouvelle démonstration du théorème 2.

Dans certains cas, le théorème 2 est particulièrement facile à utiliser ; on en donne plusieurs exemples au chapitre II, à la suite des énoncés des théorèmes 1 et 2 : on obtient ainsi, sous certaines conditions portant, entre autres, sur la loi de décomposition dans K du nombre premier p, l'irréductibilité dans $k[Y]$ des polynômes $P(p^m, Y)$ où $m \geq 0$.

Le chapitre VI s'occupe lui du cas général. A. Schinzel en 1965 [Schi1] et un peu plus tard, M. Fried [Fr] ont montré que l'ensemble $H_{P,k}$ contenait une progression arithmétique $(am+b)_{m\geq 0}$; il contient donc également une progression géométrique $((b(a+1)^m)_{m\geq 0})$. On démontre au chapitre VI une nouvelle version du théorème d'irréductibilité de Hilbert qui précise ce dernier résultat.

Le chapitre VII est plus géométrique. On regarde le polynôme P comme une courbe algébrique plane et on déduit alors du théorème 2 un énoncé sur ses points rationnels. En 1983, dans son article sur le théorème de décomposition de Weil [Bo4], E. Bombieri a donné un énoncé plus général sur les valeurs de fonctions rationnelles sur une courbe projective lisse. Ce résultat cependant présente une inexactitude. Au second paragraphe du chapitre VII, nous indiquons comment on doit modifier son énoncé ; nous en donnons ensuite deux démonstrations, qui reprennent pour l'essentiel celles de Bombieri : l'une, de nature algébrique, est basée sur la théorie des Hauteurs, l'autre, de nature arithmétique, utilise le théorème 2.

Nous faisons quelques dernières remarques au chapitre VIII. En appendice enfin, nous montrons que la méthode de Gel'fond, qui est à la base de notre étude, permet également une nouvelle approche du résultat de Bombieri sur les G- fonctions.

CHAPITRE I

Notations et rappels préliminaires

§1. VALEURS ABSOLUES ET HAUTEURS

1.1 Valeurs absolues d'un corps de nombres. [Am] [La2]

On se fixe une fois pour toutes une clôture algébrique de $\mathbb{Q}$ notée $\overline{\mathbb{Q}}$. Les valeurs absolues v d'un corps de nombres F sont normalisées de telle façon que:

si v/p (c'est-à-dire si v prolonge la métrique p-adique sur $\mathbb{Q}$, p étant un nombre premier)

$$|p|_v = p^{-1}$$

si v/∞ (c'est-à-dire si v est archimédienne)

$$|x|_v = |x| \quad \text{pour tout nombre rationnel } x$$

($|\ |$ désignant la valeur absolue usuelle sur $\mathbb{Q}$).

M_F désignera l'ensemble des valeurs absolues normalisées (ou places) de F. Si v est une place de F, nous noterons F_v le complété de F pour la métrique v et d_v^F le degré local de la place v par rapport à $\mathbb{Q}$ défini par :

$$d_v^F = [F_v : \mathbb{Q}_v]$$

Si v est archimédienne, $d_v^F = 1$ ou 2 selon que v est réelle ou imaginaire ; si v est une place finie au dessus de p (c'est-à-dire si v/p), $d_v^F = e_v f_v$, e_v étant l'exposant de l'idéal premier $\mathfrak{P}_v$ associé à v dans la décomposition de l'idéal engendré par p dans $\mathcal{O}_F$, l'anneau des entiers de F, f_v étant la

dimension sur $\mathbb{Z}/p\mathbb{Z}$ du corps $O_F/\mathfrak{P}_v$.

Rappelons que, pour toute place w de $\mathbb{Q}$ on a :

$$\sum_{\substack{v \in M_F \\ v/w}} d_v^F = [F:\mathbb{Q}]$$

et que pour tout x dans F non nul, on a :

$$\prod_{v \in M_F} |x|_v^{d_v^F} = 1 \qquad \text{(Formule du produit)}$$

M_F - constantes [La3] (Ch10 §1)

On note $M_{\bar{\mathbb{Q}}}$ l'ensemble des places de $\bar{\mathbb{Q}}$. Soit F un corps de nombres ; nous dirons qu'une application

$$\gamma : M_{\bar{\mathbb{Q}}} \longrightarrow \mathbb{R}$$

est une M_F - constante si

a) pour tout $v \in M_{\bar{\mathbb{Q}}}$, γ_v ne dépend que de la restriction de v à F.

b) $\gamma_v = 0$ pour tout $v \in M_{\bar{\mathbb{Q}}}$ sauf au dessus d'un nombre fini de places de F.

Nous dirons qu'une application $\Gamma : M_{\bar{\mathbb{Q}}} \longrightarrow \mathbb{R}_+^*$ est une M_F-constante multiplicative si la fonction $\gamma = -\operatorname{Log}\Gamma$ est une M_F - constante. Nous utiliserons fréquemment la notation $\gamma = (\gamma_v)_{v \in M_F}$ (resp. $\Gamma = (\Gamma_v)_{v \in M_F}$) pour désigner une M_F-constante γ (resp. une M_F - constante multiplicative Γ).

Soit X un ensemble. Une fonction

$$\alpha : X \times M_{\bar{\mathbb{Q}}} \longrightarrow \mathbb{R}$$

sera dite M - majorée s'il esciste une M_F - constante γ telle que l'on ait

$$\alpha(x,v) \leq \gamma_v \qquad \text{pour tout } (x,v) \text{ dans } X \times M_{\bar{\mathbb{Q}}}$$

Il est clair que cette définition ne dépend pas du corps de nombres F choisi. On définit de même, les notions de fonctions M - minorées, M - bornées.

Si X est une variété algébrique, α sera dite M- continue si pour tout $v \in M_{\bar{\mathbb{Q}}}$, la fonction

$$\alpha_v : X \longrightarrow \mathbb{R}$$

définie par $\alpha_v(x) = \alpha(x,v)$ est continue pour la v- topologie [La3] (Ch 10 §1 p 250).

1.2 Hauteurs [La3]

Nous noterons h la hauteur logarithmique absolue qui est définie sur $\bar{\mathbb{Q}}^m$ de la façon suivante :

- si m est un entier supérieur ou égal à 2 et $\underline{x} = (x_1, \ldots, x_m)$ un élément non nul de $\bar{\mathbb{Q}}^m$

$$h(\underline{x}) = \frac{1}{[F:\mathbb{Q}]} \sum_{v \in M_F} d_v^F \operatorname{Log}\left(\operatorname*{Max}_{1 \le i \le m} |x_i|_v\right)$$

où F est un corps de nombres contenant $x_1, \ldots, x_m$.

(Il est classique que cette définition ne dépend pas du corps de nombres F contenant $x_1, \ldots, x_m$)

- si x est un nombre algébrique :

$$h(x) = h((1, x))$$

H désignera la hauteur absolue, définie par $H = \exp \circ h$. Nous utiliserons fréquemment les propriétés suivantes, de h, qui sont élémentaires.

- Pour tout $m \geq 2$, pour tout $\underline{x}$ dans $\overline{\mathbb{Q}}^m$, non nul, pour tout α dans $\overline{\mathbb{Q}}$, non nul :

$$h(\alpha \underline{x}) = h(\underline{x})$$

h induit donc une fonction sur $\mathbb{P}^{m-1}(\overline{\mathbb{Q}})$ encore appelée hauteur logarithmique absolue (sur $\mathbb{P}^{m-1}(\overline{\mathbb{Q}})$)

- h est à valeurs positives ou nulles.
- pour tout nombre algébrique x non nul :

$$h(x) = -\frac{1}{[F:\mathbb{Q}]} \sum_{v \in M_F} d_v^F \operatorname{Log} \min(1, |x|_v)$$

où F est un corps de nombres auquel x appartient.

$$h(x^{-1}) = h(x)$$

- pour tout nombre algébrique x non nul, et pour tout nombre rationnel r

$$h(x^r) = |r| \, h(x)$$

Dans ce type d'étude, on a généralement le choix entre plusieurs définitions de hauteur; ici nous emploierons essentiellement la hauteur logarithmique absolue. Les raisons de ce choix sont techniques : l'utilisation de h semble bien plus appropriée dès que l'on travaille avec plusieurs places puisque sa définition comme somme de facteurs locaux permet de déduire des résultats globaux d'analyses locales qui sont souvent plus naturelles.

Rappelons cependant les relations liant h aux autres hauteurs usuelles, principalement, la hauteur polynômiale H définie sur $\overline{\mathbb{Q}}$ par :

$$H(x) = \operatorname*{Max}_{0 \le i \le n} |a_i|$$

où le polynôme $a_0 X^n + a_1 X^{n-1} + \ldots + a_n$ est irréductible dans $\mathbb{Z}[X]$, de degré n, et annule x et la mesure de Mahler M définie sur $\overline{\mathbb{Q}}$ par

$$M(x) = |a_0| \prod_{1 \le i \le n} \operatorname{Max}(1, |x_i|_\infty)$$

où $|\ |_\infty$ est une place archimédienne de $\mathbb{Q}(x_1, \ldots, x_n)$ et $x_1, \ldots, x_n$ sont les

différents conjugués de x sur $\mathbb{Q}$.
Il est bien connu que :

$$(1+n)^{-1} \leq \frac{H(x)}{M(x)} \leq 2^n$$

et que :

$$h(x) = \frac{1}{n} \operatorname{Log} M(x)$$

Hauteurs de polynômes. Par hauteur logarithmique absolue $h(\underline{P})$ (resp. hauteur absolue $\mathcal{H}(\underline{P})$) d'un n-uple $\underline{P} = (P_1, \ldots, P_n)$ de polynômes P_i à coefficients dans $\overline{\mathbb{Q}}$, nous entendrons la hauteur logarithmique absolue (resp. la hauteur absolue) du vecteur formé par l'ensemble des coefficients des P_i, $i = 1, 2, \ldots, n$.

D'autre part, si F est un corps de nombres contenant les coefficients $(a_\lambda)_{\lambda \in \Lambda}$ des polynômes P_i, $i = 1, 2, \ldots, n$ et v une place de F, on définit la v-hauteur de $\underline{P}$ et la v-hauteur logarithmique de $\underline{P}$, respectivement par

$$H_v(\underline{P}) = \max_{\lambda \in \Lambda} |a_\lambda|_v \qquad h_v(P) = \operatorname{Log} H_v(\underline{P})$$

Notons qu'alors si $\underline{P} \neq 0$, on a :

$$\mathcal{H}(\underline{P}) = \left[\prod_{v \in M_F} H_v(\underline{P})^{d_v^F} \right]^{1/[F:\mathbb{Q}]}$$

1.3 Inégalité de Liouville

Le résultat suivant, qui est classique, permet de comparer la hauteur d'un polynôme aux valeurs absolues de ses racines.

INÉGALITÉ DE LIOUVILLE — *Soient F un corps de nombres, v une place de F, et $P = a_0 X^n + a_1 X^{n-1} + \cdots + a_n$ un polynôme à coefficients dans F de degré $n \geq 0$. Si x est une racine de P dans $\overline{\mathbb{Q}}$ et w un prolongement quelconque de v à $F(x)$ alors*

a) *si v est archimédienne :*

$$|x|_w < \frac{H_v(P) + |a_0|_v}{|a_0|_v}$$

si v est ultramétrique :

$$|x|_w \leq \frac{H_v(P)}{|a_0|_v}$$

b) *de plus si $x \neq 0$ on a :*

si v est archimédienne :

$$|x|_w > \frac{|P(0)|_v}{H_v(P) + |P(0)|_v}$$

si v est ultramétrique :

$$|x|_w \geq \frac{|P(0)|_v}{H_v(P)}$$

Démonstration. a) Le résultat est trivial si $|x|_w \leq 1$. Supposons donc $|x|_w > 1$
De l'égalité $a_0x^n + a_1x^{n-1} + \cdots + a_n = 0$ on déduit :
si v est archimédienne :

$$|a_0|_v \leq H_v(P)\left(\frac{1}{|x|_w} + \frac{1}{|x|_w^2} + \cdots + \frac{1}{|x|_w^{n-1}}\right) < \frac{H_v(P)}{|x|_w - 1}$$

ce qui donne la première inégalité annoncée.
si v est ultramétrique :

$$|a_0|_v |x|_w^n \leq H_v(P)\left(\mathrm{Max}(1, |x|_w)^{n-1}\right)$$

Comme on a aussi :

$$|a_0|_v \leq H_v(P)\left(\mathrm{Max}(1, |x|_w)^{n-1}\right)$$

on obtient :

$$|a_0|_v \,\mathrm{Max}(1, |x|_w)^n \leq H_v(P)\left(\mathrm{Max}(1, |x|_w)^{n-1}\right)$$

et donc.

$$\mathrm{Max}(1, |x|_w) \leq \frac{H_v(P)}{|a_0|_v}$$

b) Pour le b) on remarque que x^{-1} est racine du polynôme $\hat{P} = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0$
et on applique le a) □

Remarque. Du a), on déduit aisément que :

$$\mathcal{H}(x) \leq 2\,\mathcal{H}(P)$$

Nous utiliserons également cette inégalité ; précisons cependant que ce n'est pas la meilleure possible ; par exemple, on peut montrer que $\mathcal{H}(x)^{[F(x):F]} \leq (1+\deg P)\,\mathcal{H}(P)$.

§2. IRRÉDUCTIBILITÉ ABSOLUE

Si F est un corps, nous noterons $\bar{F}$ sa clôture algébrique. Dans ce paragraphe, k désigne un corps quelconque.

DÉFINITION 1 — Si F est une extension finie de $k(X)$, on appelle corps des constantes de F sur k, le corps $k_F = \bar{k} \cap F$.

DÉFINITION 2 — Soit $P \in k[X,Y]$ un polynôme irréductible dans $k(X)[Y]$, on appelle corps des constantes de P sur k, que l'on note k_P, le corps des constantes sur k du corps $R_P = k(X)[Y] / P\,k(X)[Y]$

L'objet de ce paragraphe est la démonstration de la proposition suivante.

PROPOSITION 1 — Supposons k de caractéristique 0 ; soit P un polynôme irréductible dans $k[X,Y]$ de degré partiel en Y $\deg_Y P \geq 1$; les propositions suivantes sont équivalentes.

i) P est irréductible sur $\bar{k}$

ii) P est irréductible sur toute extension finie de k

iii) P est irréductible sur k_p

iv) $k_p = k$

DEFINITION 3 — Un polynôme P ayant ces propriétés est dit absolument irréductible

Nous avons dégagé quelques résultats algébriques qui constituent les arguments essentiels de la partie non triviale de la démonstration.

LEMME 1 — Soit K une extension de k telle que $\bar{k} \cap K = k$. Alors si P est un polynôme irréductible dans $k[Y]$, P est irréductible dans $K[Y]$

Remarques. 1) D'après ce lemme, un polynôme $P \in k[X,Y]$, absolument irréductible et tel que $\deg_Y P \geq 1$, est, considéré comme polynôme en Y à coefficients dans $k(X)$, également irréductible sur tout corps K contenant $\bar{k}(X)$ et vérifiant $\overline{k(X)} \cap K = \bar{k}(X)$.

2) Si K est une extension transcendante pure de k, l'hypothèse du lemme 1 est vérifiée. (La réciproque est fausse : soit C une courbe algébrique définie par un polynôme $P \in \bar{\mathbb{Q}}[X,Y]$ absolument irréductible, de genre non nul ; alors si K est le corps des fonctions sur $\bar{\mathbb{Q}}$ de la courbe C, on a évidemment $K \cap \bar{\mathbb{Q}} = \bar{\mathbb{Q}}$ et pourtant K n'est pas une extension transcendante pure de $\bar{\mathbb{Q}}$).

Démonstration du lemme 1. On peut supposer que P est unitaire et que $\deg P \geq 2$.

Si P n'est pas irréductible dans $K[Y]$, on peut écrire :

$$P = QR$$

où $Q, R \in K[Y]$, Q et R sont unitaires, $\deg Q \geq 1$ et $\deg R \geq 1$.

P étant irréductible dans $k[Y]$, l'un au moins des coefficients de R ou de Q, disons x, n'appartient à k. Q et R étant unitaires, x est algébrique sur k (c'est une fonction symétrique élémentaire des racines de Q ou de R), ce qui contredit l'hypothèse faite sur K : en effet $x \in K \cap \bar{k} = k$ □

COROLLAIRE 1 — Soit P un polynôme irréductible dans $k[Y]$, alors P est irréductible dans $k(X)[Y]$.

En effet $k(X)$ est une extension transcendante pure de k.

COROLLAIRE 2 — Pour tout α algébrique sur k, on a :

$$[k(\alpha, X) : k(X)] = [k(\alpha) : k]$$

COROLLAIRE 3 — Soient F une extension finie de $k(X)$ et α un élément de $\bar{k}$, alors

$$[F(\alpha) : F] = [k_F(\alpha) : k_F] .$$

L'inégalité $[F(\alpha) : F] \leq [k_F(\alpha) : k_F]$ vient de $k_F \subset F$. Ensuite, comme $\bar{k}_F = \bar{k}$ on a $\bar{k}_F \cap F = k_F$. Le lemme 1 s'applique donc à l'extension F / k_F : le polynôme minimal de α sur k_F est donc irréductible dans $F[Y]$, ce qui fournit l'inégalité restante □

LEMME 2 — Soit F une extension finie et séparable de $k(X)$; alors k_F est une extension finie et séparable de k, et :

$$[k_F : k] \leq [F : k(X)]$$

Soit α un élément de k_F ; en utilisant le corollaire 2 du lemme 1 et l'inclusion $k(\alpha, X) \subset F$, on obtient :

$$[k(\alpha) : k] = [k(\alpha, X) : k(X)] \leq [F : k(X)] ;$$

d'autre part α est séparable sur k car d'après le corollaire 1 du lemme 1, ses conjugués sur k sont les mêmes que ses conjugués sur $k(X)$ qui sont distincts par hypothèse.

Donc k_F est une extension séparable de k dont tous les éléments ont un degré sur k majoré par $[F : k(X)]$; il est classique qu'une telle extension est de degré fini sur k et inférieur à $[F : k(X)]$ □

Démonstration de la proposition 1. i) ⇒ ii) est évident ; ii) ⇒ iii) est une conséquence du lemme 2 (la séparabilité de l'extension $R_p / k(X)$ est assurée par l'hypothèse faite sur la caractéristique de k).

iii) ⇒ iv) : On a évidemment $k \subset k_p$; inversement, soit α un élément quelconque de k_p. Par hypothèse, P est irréductible dans $k_p[X, Y]$; comme $k(\alpha) \subset k_p$, il l'est également dans $k(\alpha)[X, Y]$. On a donc :

$$[R_p : k(X)] = [R_p : k(\alpha, X)] = \deg_Y P$$

La première égalité donne :

$$[k(\alpha,X) : k(X)] = 1$$

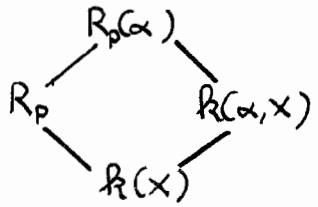
ce qui, d'après le corollaire 2 du lemme 1, signifie que α appartient à k □

iv) ⇒ i) : Supposons que $P = AB$ avec A et B appartenant à $\bar{k}[X,Y]$. Soit E le corps engendré par k et les coefficients de A et de B. D'après le théorème de l'élément primitif, il existe α dans $\bar{k}$ tel que $E = k(\alpha)$.

Par hypothèse, $k_p = k$; le corollaire 3 du lemme 1 donne donc :

$$[R_p(\alpha) : R_p] = [k(\alpha) : k]$$

Le corollaire 2 du lemme 1 et le diagramme suivant



montrent alors que :

$$[R_p(\alpha) : k(\alpha)(X)] = [R_p : k(X)]$$

ce qui signifie que P est irréductible dans $k(\alpha,X)[Y]$ (on le voit bien en écrivant $R_p = k(X,y)$ où y est un élément primitif de R_p sur $k(X)$).

D'autre part, P vu comme polynôme à coefficients dans $k(\alpha)[X]$ est primitif : sinon il serait divisible dans $k(\alpha)[X,Y]$ par un polynôme dans $k(\alpha)[X]$ de degré plus grand que 1 ; il existerait alors un élément a de $\bar{k}$ tel que

$$P(a,Y) = 0$$

et P serait divisible dans $k[X,Y]$ par le polynôme minimal de a sur k, ce qui est absurde puisque P est supposé irréductible dans $k[X,Y]$

Finalement, P est irréductible dans $k(\alpha)[X,Y] = E[X,Y]$ et l'écriture $P = AB$ avec A et B dans $E[X,Y]$ n'est donc possible que si $\deg A = 0$ ou $\deg B = 0$.

C.Q.F.D

§3 SÉRIES FORMELLES ALGÉBRIQUES

Si F est un corps et u une indéterminée, $F[[u]]$ désignera l'anneau des séries formelles en l'indéterminée u à coefficients dans le corps F et $F((u))$ son corps des fractions.

Soit $P \in \bar{\mathbb{Q}}[X,Y]$ un polynôme tel que $\deg_Y P \geq 1$. Nous noterons $e(P)$ (resp. $f(P)$) le plus petit entier strictement positif c tel que P considéré comme

polynôme en l'indéterminée Y et à coefficients dans $\bar{\mathbb{Q}}(X)$ ait une racine dans $\bar{\mathbb{Q}}((X^{\frac{1}{e}}))$ (resp. ait toutes ses racines dans $\bar{\mathbb{Q}}((X^{\frac{1}{e}}))$).

L'existence des entiers $e(P)$ et $f(P)$ est assurée par le théorème de Puiseux ([Ei] ChIII §1.6 ou [Ch] Ch VIII §1 & 8.2). Il est facile, ensuite, de voir que

$$e(P) \mid f(P) \quad \text{et que} \quad f(P) \leq \deg_Y P$$

Soit ξ_0 un élément de $\bar{\mathbb{Q}}$, nous noterons P_{ξ_0} le polynôme défini par :

$$P_{\xi_0}(X - \xi_0, Y) = P(X, Y)$$

et $e(P, \xi_0)$ (resp. $f(P, \xi_0)$) la quantité définie par

$$e(P, \xi_0) = e(P_{\xi_0}). \qquad (\text{resp. } f(P, \xi_0) = f(P_{\xi_0}))$$

HYPOTHÈSE H_{ξ_0} — *Nous dirons que* P *vérifie l'hypothèse* H_{ξ_0} *s'il existe une série formelle* $\underset{\sim}{Y} = \sum_{m \geq 0} \gamma_m (X - \xi_0)^m$ *à coefficients* γ_m *dans* $\bar{\mathbb{Q}}$ *vérifiant*

$$P(X, \underset{\sim}{Y}) = 0.$$

HYPOTHÈSE H'_{ξ_0} — *Nous dirons que* P *vérifie l'hypothèse* H'_{ξ_0} *si le polynôme* $P(\xi_0, Y)$ *possède une racine simple dans* $\bar{\mathbb{Q}}$

Enfin, si R désigne le résultant par rapport à la variable Y des polynômes P et P'_Y, nous dirons que ξ_0 est un point régulier de P si $R(\xi_0) \neq 0$ et singulier sinon. La proposition suivante relie entre elles ces différentes définitions.

PROPOSITION 2 — *Soient* a), b), c), d) *les assertions suivantes.*

a) ξ_0 *est un point régulier de* P.

b) P *vérifie l'hypothèse* H'_{ξ_0}

c) P *vérifie l'hypothèse* H_{ξ_0}

d) $e(P, \xi_0) = 1$

On a alors : a) $\Rightarrow$ b) $\Rightarrow$ c) $\Rightarrow$ d).

En particulier si $R \neq 0$ *(par exemple si* P *est irréductible sur un corps contenant ses coefficients) alors*

P *vérifie l'hypothèse* H_{ξ_0} *pour tout* $\xi_0 \in \bar{\mathbb{Q}}$ *sauf un nombre fini.*

Il s'agit de résultats classiques. Si $R(\xi_0) \neq 0$ alors le polynôme $P(\xi_0, Y)$ possède $\deg_Y P$ racines distinctes (et donc simples) ([La1] Ch V §10) et donc a) $\Rightarrow$ b). Pour la seconde implication, on utilise le lemme de Cauchy ([Ei] ChIII §1.1). La troisième est évidente.

Remarques. 1) Les implications réciproques sont fausses toutes les trois (Considérer les

polynômes Y^3+Y^2+X pour la première, $Y^2-X^2(1+X)$ pour la seconde et $XY-1$ pour la troisième, au point $\xi_0 = 0$)

2) On peut préciser l'implication b) ⇒ c) : en fait si $\gamma_0 \in \overline{\mathbb{Q}}$ est une racine simple de $P(\xi_0, Y)$, il existe une unique série formelle $\underset{\sim}{Y}$ de premier terme γ_0 vérifiant $P(X, \underset{\sim}{Y}) = 0$; l'existence résulte du lemme de Cauchy, l'unicité est, par exemple, une conséquence de la proposition suivante, qui est immédiate.

PROPOSITION 3 — *Soit k un corps de nombres contenant ξ_0 et les coefficients de P. Soit $\underset{\sim}{Y} = \sum_{m\geq 0} \gamma_m (X-\xi_0)^m$ une série formelle vérifiant $P(X, \underset{\sim}{Y}) = 0$. Alors pour tout entier $m \geq 1$ il existe un polynôme R_m dans $k[X_0, X_1, \ldots, X_m]$ vérifiant :*

$$P'_Y(\xi_0, \gamma_0).\, \gamma_m = R_m(\xi_0, \gamma_0, \gamma_1, \ldots, \gamma_{m-1})$$

Dans la plupart de nos résultats, nous supposerons que P vérifie l'hypothèse Hl_{ξ_0} ceci, cependant, ne restreindra pas la généralité de notre travail : nous verrons en effet (CF remarque 3 suivant l'énoncé du théorème 2 (Ch II § 2)) comment on peut réduire l'étude du cas général à celle de ce cas particulier.

Supposons maintenant que P soit irréductible dans $k[X,Y]$, k étant un corps de nombres contenant les coefficients de P et qu'il vérifie l'hypothèse Hl_{ξ_0}. Soit alors K le corps $K = k((\gamma_m)_{m\geq 0})$. Nous avons réuni dans la proposition 4 les résultats concernant le corps K, dont nous aurons besoin.

PROPOSITION 4 — *a) K est un corps de nombres de degré sur k inférieur ou égal à $\deg_Y P$ et contenant k_p, le corps des constantes sur k du polynôme P.*

b) si $K = k$ alors P est absolument irréductible.

c) si P vérifie l'hypothèse Hl'_{ξ_0}, avec $\xi_0 \in k$, si γ_0 est une racine simple de $P(\xi_0, Y)$ et $\underset{\sim}{Y}$ l'unique série formelle en $X-\xi_0$ de premier terme γ_0 vérifiant $P(X, \underset{\sim}{Y}) = 0$, alors

$$K = k(\gamma_0)$$

Démonstration. Si σ est un k-homomorphisme de corps de K dans $\overline{\mathbb{Q}}$ alors on a $P(X, \underset{\sim}{Y}^\sigma) = 0$ où $\underset{\sim}{Y}^\sigma = \sum_{m\geq 0} \sigma(\gamma_m)(X-\xi_0)^m$. Les $\underset{\sim}{Y}^\sigma$ où σ décrit l'ensemble des k-homomorphismes de K dans $\overline{\mathbb{Q}}$ sont donc des racines de P ; par définition de K, elles sont distinctes alors nécessairement K est de degré fini sur k et son degré est inférieur à $\deg_Y P$.

A un k-isomorphisme près, k_p est le corps des constantes sur k du corps $k(X, \underset{\sim}{Y})$. Comme on a $k(X, \underset{\sim}{Y}) \subset K((X-\xi_0))$ on obtient

$$k_p = k(X, \underset{\sim}{Y}) \cap \overline{\mathbb{Q}} \subset K((X-\xi_0)) \cap \overline{\mathbb{Q}} = K$$

Ceci achève la démonstration de a)

b) Si $K = k$ alors d'après le a) on a $k_p = k$; l'assertion iv) de la proposition est donc vérifiée.

c) C'est encore une conséquence de la proposition 3 □

Remarque. L'inclusion $k_p \subset K$ est stricte en général ; prenons par exemple $k = \mathbb{Q}$ et $P = Y^2 + (1+X)$, alors $\mathbb{Q}_p = \mathbb{Q}$ car P est absolument irréductible et $K = \mathbb{Q}(i)$.

Note. On peut donner des définitions et des résultats analogues à ceux qui précèdent en prenant pour ξ_0 le point à l'infini dans $\mathbb{P}^1(\overline{\mathbb{Q}})$. Ainsi, nous dirons que le polynôme P vérifie l'hypothèse H_∞ s'il existe une série formelle en X^{-1}

$$\underset{\sim}{Y} = \sum_{m \geq 0} \upsilon_m X^{-m}$$

à coefficients $\upsilon_m \in \overline{\mathbb{Q}}$, vérifiant

$$P(X, \underset{\sim}{Y}) = 0$$

Soit $\hat{P}$ le polynôme $\hat{P} = X^{\deg_X P} P(X^{-1}, Y)$; l'hypothèse H_∞ est vérifiée si $\hat{P}(0, Y)$ admet une racine simple dans $\overline{\mathbb{Q}}$, ce qui est réalisé si 0 n'est pas une racine du résultant par rapport à Y des polynômes $\hat{P}$ et $\hat{P}'_Y$.

CHAPITRE II

Présentation des principaux résultats

Commençons cette présentation des résultats par un premier énoncé à la fois simple et spectaculaire démontré par V.G Sprindzuk dans son article de 1979 [Sp1].

THÉORÈME 0 (Sprindzuk) — *Soit P un polynôme dans $\mathbb{Q}[X,Y]$, absolument irréductible et vérifiant :*

$$P(0,0) = 0 \quad \text{et} \quad P'_Y(0,0) \neq 0$$

Alors il existe une constante $C > 0$ ne dépendant que de P vérifiant : pour tout nombre premier p et pour tout entier m tels que $p^m > C$ $P(p^m, Y)$ est irréductible dans $\mathbb{Q}[Y]$.

Le théorème 0 s'applique donc sous la condition " p^m grand " ou ce qui revient au même " p^m petit pour la métrique p-adique sur $\mathbb{Q}$". Nous allons la remplacer dans le théorème 1 par une condition plus générale du type :

$$\xi \in \overline{\mathbb{Q}} \quad \text{et} \quad 0 < |\xi|_v < f(\text{Hauteur de } \xi, \text{ degré de } \xi)$$

où $f : \mathbb{R}_+ \times \mathbb{N} \longrightarrow \mathbb{R}_+$ sera une fonction ne dépendant que de P, et v une place de $\overline{\mathbb{Q}}$.

§1 LE RÉSULTAT LOCAL

1.1 Enoncé du théorème 1

Soient k un corps de nombres, ξ_0 un élément de k et P un polynôme irréductible dans $k[X,Y]$. On suppose que P vérifie l'hypothèse H_{ξ_0} (Cf Ch 1 §3) et comme au §3 du chapitre 1, K désigne le corps engendré par k et les coefficients de la série formelle donnée par l'hypothèse H_{ξ_0}. On démontre alors le résultat suivant.

THÉORÈME 1 — *Il existe deux constantes, $a>0$ et $b\geq 0$ ne dépendant que de P, ξ_0 telles que:*
si ξ est un nombre algébrique différent de ξ_0, d un entier positif et v une place du corps $K(\xi)$ et si :

$$(1)\quad |\xi-\xi_0|_v^{d_v^{K(\xi)}/[K(\xi):\mathbb{Q}]} < a\exp\left\{-\frac{d[k(\xi):k]}{\deg_Y P}h(\xi-\xi_0)-b\sqrt{h(\xi-\xi_0)}\right\}$$

alors $P(\xi,Y)$ est divisible dans $k(\xi)[Y]$ par un polynôme irréductible dans $k(\xi)[Y]$ de degré strictement supérieur à d.
De plus si P est absolument irréductible, on peut omettre le terme $[k(\xi):k]$ dans le membre de droite de la condition (1).

Les constantes a et b de l'énoncé sont effectives ; nous donnons leur valeur au paragraphe 3 de ce chapitre.

Pour conclure à l'irréductibilité du polynôme $P(\xi,Y)$ dans $k(\xi)[Y]$, il suffit de vérifier que la condition (1) du théorème 1 est réalisée pour $d=\deg_Y P-1$. Cette valeur de l'entier d est d'ailleurs, à cause de l'inégalité triviale :

$$\frac{d_v^{K(\xi)}}{[K(\xi):\mathbb{Q}]}\operatorname{Log}|\xi-\xi_0|_v \geq -h(\xi-\xi_0)$$

la valeur maximale de d pour laquelle la condition (1) peut être réalisée.

Le théorème 1 généralise simultanément deux résultats, l'un de P. Bundschuh ([Bu] Théorème 1), l'autre de V.G Sprindzuk ([Sp1] Théorème 1) ; dans l'énoncé de P. Bundschuh, v est archimédienne, $k=\mathbb{Q}$ et les constantes a, b dépendent aussi du degré de ξ sur $\mathbb{Q}$; quant à l'énoncé de V.G Sprindzuk, il correspond au cas particulier du théorème 1 où $k=K=\mathbb{Q}$, P est absolument irréductible, ξ est un nombre rationnel, v une place finie de $\mathbb{Q}$ et $d=\deg_Y P-1$; en outre, dans ces

deux énoncés. Leurs auteurs supposent que P vérifie l'hypothèse H'_{ξ_0}.

1.2 Premiers corollaires

Notation. Soient F un corps de nombres et ξ un élément de F, nous noterons désormais $M_F(\xi)$ l'ensemble des places v de F telles que $|\xi|_v < 1$.

Soit ξ un élément de k non nul tel que l'ensemble $M_K(\xi)$ possède exactement un élément v_0. On a alors :

$$h(\xi) = -\frac{d_{v_0}^K}{[K:\mathbb{Q}]} \operatorname{Log}|\xi|_{v_0}$$

et la condition (1) du théorème 1 avec $d = \deg_Y P - 1$ et $\xi_0 = 0$ s'écrit simplement :

$$-\frac{h(\xi)}{\deg_Y P} + b\sqrt{h(\xi)} - \operatorname{Log} a < 0$$

On obtient donc le résultat suivant. Les hypothèses sont celles du théorème 1, avec de plus $\xi_0 = 0$

COROLLAIRE 1 — *Soit ξ un élément de k non nul tel que* $\operatorname{Card} M_K(\xi) = 1$
Si $h(\xi) > h_1$ *où h_1 est une constante positive ne dépendant que de P*
alors $P(\xi, Y)$ *est irréductible dans* $k[Y]$.

Ce corollaire contient en particulier le théorème 0 de V.G Spindzuk que nous avons mentionné au début de ce chapitre. Plus généralement, on a le résultat suivant.

COROLLAIRE 2 — *Sous les hypothèses du corollaire 1, il existe une constante C positive ne dépendant que de P vérifiant :*

1) *pour tout nombre premier p non décomposé dans K et pour tout entier m*
si $p^m > C$ *alors* $P(p^m, Y)$ *est irréductible dans* $k[Y]$
2) *si K est inclus dans un corps quadratique imaginaire, pour tout entier* $m \neq 0$
si $|m| > C$ *alors* $P\left(\frac{1}{m}, Y\right)$ *est irréductible dans* $k[Y]$

DÉFINITION — *Un nombre premier p est dit non décomposé dans un corps de nombres F s'il n'existe qu'une seule place de F au dessus de p, ou ce qui est équivalent si l'idéal pO_F est une puissance d'un idéal premier de O_F, l'anneau des entiers de F.*

Dans l'énoncé de Spindzuk, on a $k = K = \mathbb{Q}$ et tout nombre premier p est évidemment non décomposé dans $\mathbb{Q}$.

Démonstration du corollaire 2. Si p est un nombre premier non décomposé dans K, l'unique place de K au dessus de p est le seul élément de $M_K(p^m)$ si $m \geq 1$; si K est inclus dans un corps quadratique imaginaire, il n'existe dans K qu'une seule place archimédien qui est l'unique élément de $M_K(\frac{1}{m})$ si $|m| > 1$. Le corollaire 1 s'applique donc dans ces deux cas. La constante C vaut $\exp h_1$ □

Il faut cependant noter que le corollaire 2 ne garantit pas l'existence en toute généralité d'un élément ξ de k tel que $P(\xi, Y)$ soit irréductible dans $k[Y]$: il existe en effet des corps qui ne sont pas inclus dans un corps quadratique imaginaire et où il n'existe pas de nombres premiers non décomposés ; en voici un exemple.

Exemple. Prenons $K = \mathbb{Q}(\sqrt{13}, \sqrt{17})$; on a $[K : \mathbb{Q}] = 4$ donc K n'est pas inclus dans un corps quadratique imaginaire.

Soit p un nombre premier distinct de 2, 13 et 17 ; l'un des trois nombres $\left(\frac{13}{p}\right), \left(\frac{17}{p}\right), \left(\frac{13.17}{p}\right)$ est égal à 1 ; p est donc décomposé dans l'un des trois sous corps non triviaux de K, $\mathbb{Q}(\sqrt{13})$, $\mathbb{Q}(\sqrt{17})$, $\mathbb{Q}(\sqrt{13.17})$ et donc est décomposé dans K. Ensuit 2 est décomposé dans $\mathbb{Q}(\sqrt{17})$ car $17 \equiv 1 \pmod 8$, donc dans K. Enfin $\left(\frac{13}{17}\right) = \left(\frac{17}{13}\right) = 1$ donc 17 (resp. 13) est décomposé dans $\mathbb{Q}(\sqrt{13})$ (resp. $\mathbb{Q}(\sqrt{17})$) et donc dans K. Finalement, tous les nombres premiers sont décomposés dans le corps K.

Terminons ce paragraphe par un dernier corollaire qui permet d'obtenir dans un cas particulier une borne effective pour l'une des coordonnées des points entiers de la courbe associée à P, précisant ainsi dans ce cas le théorème de Siegel [Si] sur la finitude de l'ensemble des points entiers d'une courbe algébrique affine.

COROLLAIRE 3 — *Soient* $s \geq 0$ *un entier et* $P = P_s X^s + \cdots + P_0$, *les* P_i *étant des éléments de* $\mathbb{Q}[Y]$ *pour* $0 \leq i \leq s$, *un polynôme irréductible dans* $\mathbb{Q}[X, Y]$. *On suppose que* P_s *possède une racine simple* δ_0 *rationnelle ou quadratique imaginaire. Alors il existe une constante* $m_0 \geq 0$ *telle que pour tout entier* m *on ait :*

si $|m| > m_0$ *alors* $P(m, Y)$ *est irréductible dans* $\mathbb{Q}[Y]$

En particulier si $\deg_Y P \geq 2$, *l'équation* $P(x, y) = 0$ *n'a qu'un nombre fini de solutions en nombres entiers* x, y : *si* (x, y) *est l'une d'elles, alors* $|x| \leq m_0$

Démonstration. Soit $\hat{P}$ le polynôme $\hat{P} = X^s P(X^{-1}, Y) = P_0 X^s + \cdots + P_s$.
La transformation $\wedge$ est un isomorphisme involutif du monoïde multiplicatif des polynômes $A \in \mathbb{Q}[X,Y]$ tels que $A(0,Y) \neq 0$; $\hat{P}$ est donc irréductible sur $\mathbb{Q}$
D'autre part, $\hat{P}$ vérifie l'hypothèse H'_0 (η_0 est une racine simple de $\hat{P}(0,Y) = P_s$) et donc l'hypothèse H_0 (Ch I Prop. 2) avec $K = \mathbb{Q}(\eta_0)$ (Ch I Prop 4) qui par hypothèse est inclus dans un corps quadratique imaginaire. On peut donc appliquer le corollaire 2 au polynôme $\hat{P}$: soit $\hat{C}$ la constante du corollaire 2 associée au polynôme $\hat{P}$; d'après la partie 2) de ce résultat on a :

si $m \in \mathbb{Z}$ et $|m| > \hat{C}$ alors $\hat{P}(m^{-1}, Y)$ est irréductible dans $\mathbb{Q}[Y]$.

ce qui donne le résultat désiré puisque :

$$\hat{P}\left(\frac{1}{m}, Y\right) = \frac{1}{m^s} P(m, Y)$$

Et on peut donc prendre $m_0 = \hat{C}$ □

Intuitivement, le résultat du corollaire 1 signifie que si un nombre ξ est "arithmétiquement simple" alors $P(\xi, Y)$ est un polynôme également "arithmétiquement simple" dans $k[Y]$. Le théorème 2, plus général que le théorème 1, va mettre en évidence un lien entre la structure arithmétique de ξ (la décomposition de l'idéal fractionnaire engendré par ξ dans l'anneau des entiers de K (qui interviendra par l'intermédiaire de l'ensemble $M_K(\xi)$)) et celle de $P(\xi, Y)$ (la décomposition de $P(\xi, Y)$ en irréductibles de l'anneau principal $k[Y]$).

Son énoncé est un énoncé global en ce sens qu'il fait intervenir simultanément plusieurs places, tenant compte ainsi, à la fois des points de vue archimédiens et p-adiques.

§2 LE RÉSULTAL GLOBAL

2.1 Enoncé du théorème 2

Soient k, ξ_0 et P comme dans le paragraphe 1.1. On suppose toujours que P vérifie l'hypothèse H_{ξ_0} ; on note $\underset{\sim}{Y} = \sum_{m \geq 0} \eta_m (X - \xi_0)^m$ la série formelle donnée par cette hypothèse, vérifiant $P(X, \underset{\sim}{Y}) = 0$ et K le corps $k((\eta_m)_{m \geq 0})$.

Pour toute place v de K, nous noterons R_v le rayon de convergence de la série formelle $\sum_{m \geq 0} \eta_m X^m$ pour la métrique v. A cause du choix des normalisations des valeurs absolues que nous avons fait, R_v ne dépend pas du corps k contenant

Q et les coefficients de P.

D'autre part, pour toute place v de K, R_v est strictement positif. Si P vérifie l'hypothèse H'_{ξ_0}, c'est simplement une conséquence du théorème des fonctions implicites ; dans le cas où P vérifie seulement l'hypothèse H_{ξ_0} (ce qu'on suppose), il faut recourir à des résultats plus sophistiqués : le théorème d'Eisenstein (CF Ch III §2.2) pour les places finies et le théorème de Frobenius-Malgrange [Ma] pour les places archimédiennes (il est classique que la série formelle $\underset{\sim}{Y}$, étant algébrique sur $k(x)$, est solution, formelle, d'une équation différentielle linéaire à coefficients dans $k(x)$ à points singuliers réguliers ; d'après le théorème de Frobénius-Malgrange, c'est une solution convergente). (Pour une justification plus élémentaire du cas archimédien, voir [Ch] (Ch VIII Th 8.6.1

La série formelle $\underset{\sim}{Y}$ induit donc sur la boule ouverte $B(\xi_0, R_v) = \{x \in K_v / |x - \xi_0|_v < R_v\}$ une fonction Y_v, strictement analytique ([Am] Ch 4) sur toute boule fermée de la boule $B(\xi_0, R_v)$ et vérifiant :

. pour tout x dans $B(\xi_0, R_v)$ $\quad P(x, Y_v(x)) = 0$

Le théorème suivant est le résultat principal de ce mémoire.

THÉORÈME 2 — *Soient ξ un élément de k, différent de ξ_0, Q un polynôme divisant $P(\xi, Y)$ dans $k[Y]$ et $S(\xi_0, \xi, Q)$ l'ensemble des places v de K vérifiant :*

$$|\xi - \xi_0|_v < R_v \quad \text{et} \quad Q(Y_v(\xi)) = 0$$

Alors

$$\left| \frac{1}{[K:Q]} \sum_{v \in S(\xi_0, \xi, Q)} d_v^K \operatorname{Log} \min(1, |\xi - \xi_0|_v) + \frac{\deg Q}{\deg_Y P} h(\xi - \xi_0) \right| \leq A + B\sqrt{h(\xi - \xi_0)}$$

où A et B sont deux constantes positives ne dépendant que de P, ξ_0 et $\underset{\sim}{Y}$.

Valeur des constantes. De façon précise, pour $\xi_0 = 0$, on peut prendre A et B égaux à

$$A = \operatorname{Log}\left[e^{8sq^2+5q^2+15sq+5\delta q+12q+1} (1+s)^{2q(q+3)} (1+q)^{3q} (1+\delta)\, T^{2q+1}\, \mathcal{H}(P)^{q(2q+5)}\, \mathcal{H}(R)^{3q+1} \right]$$

$$B = \operatorname{Log}\left[e^{4sq^2+2q^2+6sq+2\delta q+3q}\, T^{q^2}\, \mathcal{H}(P)^{q^2}\, \mathcal{H}(R)^{q^2} \right]$$

où R est le résultant par rapport à la variable Y des polynômes P et P_Y', T est la constante d'Eisenstein de $\underset{\sim}{Y}$ (CF Ch III §2.2), $s = \deg_X P$, $q = \deg_Y P$ et $\delta = \deg R$.

Dans le cas général, on obtient la valeur des constantes A et B en remplaçant dans les formules précédentes le polynôme P par le polynôme P_{ξ_0} (CF Ch I §3).

Notons que quitte à les grossir un peu, on peut demander à ces constantes de ne dépendre que de P et ξ_0 : il n'y a en effet qu'un nombre fini de séries formelles $\underset{\sim}{Y}$ en $X - \xi_0$

(au plus $\deg_Y P$) vérifiant $P(X, \underset{\sim}{Y}) = 0$.

Le théorème 2 améliore le résultat principal de [Sp4], démontré par V.G Sprindzuk en 1982 et où le polynôme P est absolument irréductible et vérifie $P(\xi_0, \eta_0) = 0$ et $P'_Y(\xi_0, \eta_0) \neq 0$, c'est à dire l'hypothèse H'_{ξ_0} avec de plus $\eta_0 \in k$ (et donc $K = k$ d'après la proposition 4 du chapitre I). (En fait, l'hypothèse d'irréductibilité absolue est superflue dans son énoncé, comme dans celui du théorème 0, puisqu'elle résulte de $K = k$ (Ch I Proposition 4)). D'autre part, dans l'énoncé de Sprindzuk, les constantes A et B dépendent également du corps k.

Remarques et commentaires. 1) On peut remarquer tout d'abord que, dès que $h(\xi - \xi_0)$ est suffisamment grand (supérieur à une constante ne dépendant que de P, ξ_0 et $\underset{\sim}{Y}$), si Q divise $P(\xi, Y)$ dans $k[Y]$, alors $\deg Q$ est nécessairement déterminé par l'inégalité du théorème 2. Ceci montre par exemple que si $h(\xi - \xi_0)$ est assez grand (au sens précédent) et si les $Y_v(\xi)$ qui sont définis sont conjugués sur k, alors $P(\xi, Y)$ est irréductible sur k (la réciproque étant, elle, évidente).

En effet, notons Q le polynôme minimal sur k des $Y_v(\xi)$ qui sont définis ; l'inégalité du théorème 2 est vérifiée pour $\deg Q = \deg_Y P$ (car comme $R_v \geqslant 1$ pour presque tout $v \in M_K$ (CF Ch III §2.2), on a $\sum_{v \in M_K} d_v^K \left| \operatorname{Log} \min(1, R_v) \right| < +\infty$) ; sous notre hypothèse $h(\xi - \xi_0)$ assez grand, on a donc nécessairement : $\deg Q = \deg_Y P$.

2) On peut interpréter le théorème 2 comme un résultat sur la distribution des $Y_v(\xi)$ qui sont définis, à l'intérieur de l'ensemble des racines de $P(\xi, Y)$. En effet, d'après la formule du produit, on a :

$$h(\xi - \xi_0) = -\frac{1}{[K:Q]} \sum_{v \in M_K} d_v^K \operatorname{Log} \min(1, |\xi - \xi_0|_v) \quad ;$$

et l'inégalité du théorème 2 signifie donc qu'à un $O\left(\sqrt{h(\xi - \xi_0)}^{-1}\right)$ près, la probabilité (selon la loi image $v \longmapsto d_v^K \operatorname{Log} |\xi - \xi_0|_v$) qu'a une place v dans $M_K(\xi - \xi_0)$, d'appartenir à un ensemble du type $S(\xi_0, \xi, Q)$, Q étant un diviseur de $P(\xi, Y)$, c'est-à-dire, grossièrement la probabilité qu'a un $Y_v(\xi)$ d'être une racine de Q, est égale à $\deg Q / \deg_Y P$, ce qui est, somme toute, relativement naturel.

Disons aussi, qu'à la lumière de cette interprétation, on comprend bien pourquoi le résultat du théorème 2 est banal dans les cas extrêmes $Q \in k^*$ et $Q = P(\xi, Y)$.

3) L'hypothèse H_{ξ_0}. Dans l'énoncé du théorème 2, on suppose qu'il existe une série formelle $\underset{\sim}{Y}$ vérifiant $P(X, \underset{\sim}{Y}) = 0$. Cette restriction n'est en réalité pas fondamentale : voici comment se ramener à cette hypothèse.

Soit P un polynôme irréductible dans $k[X,Y]$ tel que $\deg_Y P \geqslant 1$. Pour alléger les notations, supposons que $\xi_0 = 0$. Par définition de $e(P)$ (Ch I § 3), il existe un entier m et une série formelle $\underset{\sim}{Y} \in \overline{\mathbb{Q}}[[X]]$ tels que l'élément de $\overline{\mathbb{Q}}((X^{1/e(P)}))$, $\underset{\sim}{Z} = X^{-m/e(P)}\, \underset{\sim}{Y}(X^{1/e(P)})$ vérifie $P(X, \underset{\sim}{Z}) = 0$.

Considérons alors le polynôme $\check{P}$ appartenant à $k[X,Y]$ défini par :

$$\check{P} = X^{a}\, P(X^{e(P)}, X^{-m}Y)$$

où $(-a)$ est la valuation X-adique dans $k[Y](X)$ de $P(X^{e(P)}, X^{-m}Y)$.
On vérifie facilement que si $P(X^{e(P)}, Y)$ est irréductible dans $k[X,Y]$ alors $\check{P}$ l'est aussi. D'autre part $\check{P}$ vérifie évidemment l'hypothèse H_0, puisque

$$\check{P}(X, \underset{\sim}{Y}) = 0 .$$

Et on peut donc, si $P(X^{e(P)}, Y)$ est irréductible dans $k[X,Y]$ (nous verrons au chapitre V (Prop 7 et § 2 d)) comment se dispenser de cette hypothèse supplémentaire) appliquer le théorème 2 au polynôme $\check{P}$. Nous utiliserons cette réduction au chapitre VI.

4) Dans le cas où ξ_0 est le point à l'infini dans $\mathbb{P}^1(k)$, l'énoncé du théorème 2 est un peu différent.

Soit P un polynôme irréductible dans $k[X,Y]$ vérifiant l'hypothèse H_∞ (CF Ch I § 3); on note $\underset{\sim}{Y} = \sum_{m \geqslant 0} \gamma_m X^{-m}$ l'élément de $\overline{\mathbb{Q}}[[X^{-1}]]$ vérifiant $P(X, \underset{\sim}{Y}) = 0$ et K le corps $k((\gamma_m)_{m \geqslant 0})$. Soit v une place de K, si R_v désigne le rayon de convergence de la série formelle $\sum_{m \geqslant 0} \gamma_m X^m$ pour la métrique v, $\underset{\sim}{Y}$ induit sur la couronne $C(R_v) = \{x \in K / |x|_v > R_v^{-1}\}$ une fonction Y_v vérifiant :

$$\text{pour tout } x \text{ dans } C(R_v) \quad P(x, Y_v(x)) = 0 .$$

THÉORÈME 2 ($\xi_0 = \infty$) — *Soient ξ un élément de k, Q un polynôme divisant $P(\xi, Y)$ dans $k[Y]$ et $S(\infty, \xi, Q)$ l'ensemble des places v de K vérifiant :*

$$|\xi|_v > R_v^{-1} \quad \text{et} \quad Q(Y_v(\xi)) = 0$$

Alors

$$\left| \frac{1}{[K:\mathbb{Q}]} \sum_{v \in S(\infty, \xi, Q)} d_v^K \operatorname{Log} \max(1, |\xi|_v) - \frac{\deg Q}{\deg_Y P}\, h(\xi) \right| \leqslant A_\infty + B_\infty \sqrt{h(\xi)}$$

où A_∞ et B_∞ sont deux constantes positives ne dépendant que de P et $\underset{\sim}{Y}$.

2.2 Corollaires

Le résultat suivant généralise le corollaire 1 du théorème 1 et corrobore l'idée que l'on en avait dégagée selon laquelle plus un nombre ξ est "arithmétiquement simple", moins la structure arithmétique de $P(\xi,Y)$ est complexe. Les hypothèses sont celles du théorème 2, avec de plus $\xi_0 = 0$.

COROLLAIRE 1 — *Soient ξ un élément non nul de k et $P(\xi,Y) = u\, Q_1^{\alpha_1} \cdots Q_r^{\alpha_r}$ la décomposition de $P(\xi,Y)$ en polynômes irréductibles distincts Q_i de l'anneau $k[Y]$.*
Si $h(\xi) > h_2$ où h_2 est une constante positive ne dépendant que de P et $\underset{\sim}{Y}$, alors

$$r \leqslant \operatorname{Card} M_K(\xi).$$

En effet, on déduit facilement du théorème 2 que, dès que

$$\frac{h(\xi)}{\deg_Y P} - B\sqrt{h(\xi)} - A > 0$$

c'est-à-dire dès que $h(\xi)$ est assez grand, si Q est un polynôme divisant $P(\xi,Y)$ dans $k[Y]$ tel que $\deg Q \geqslant 1$, alors on a nécessairement

$$S(0,\xi,Q) \cap M_K(\xi) \neq \emptyset$$

L'application $\begin{cases} M_K^0(\xi) = \{v \in M_K \,/\, |\xi|_v < \operatorname{Min}(1, R_v)\} \longrightarrow \{1,2,\dots,r\} \\ v \longmapsto i(v) \end{cases}$

$i(v)$ étant défini par $Q_{i(v)}(Y_v(\xi)) = 0$, est donc surjective. L'inégalité demandée en résulte □

On avait déduit du corollaire 1 du théorème 1 un résultat sur l'irréductibilité des polynômes spécialisés $P(p^m,Y)$ et $P(m^{-1},Y)$; le corollaire suivant, qui reprend dans un cadre plus général un résultat de Sprindzuk [Sp4] (7.5), fournit des conclusions semblables mais sous des hypothèses différentes.

COROLLAIRE 2 — *Sous les hypothèses du corollaire 1, pour tout nombre premier p et tout entier m tels que $p^m > C'$ (resp. $|m| > C'$), où C' est une constante ne dépendant que de P et $\underset{\sim}{Y}$, on a :*

1) *Si $([K:\mathbb{Q}], \deg_Y P) = 1$ alors $P(p^m,Y)$ (resp. $P(\frac{1}{m},Y)$) est irréductible sur k.*

2) *Si $[K:\mathbb{Q}] < \deg_Y P$ alors $P(p^m,Y)$ (resp. $P(\frac{1}{m},Y)$) n'a pas de racines dans k.*

Démonstration. Soient p un nombre premier et m un entier vérifiant $p^m > C' = \mathrm{Max}(\exp k_1^2, k_2)$ où k_1 est une constante vérifiant

$$x > k_1 \Rightarrow \frac{x^2}{\deg_Y P \cdot [K:\mathbb{Q}]} - Bx - A > 0$$

et k_2 la plus grande racine rationnelle du coefficient (qui est dans $k[x]$) de $Y^{\deg_Y P}$ dans P (ou $-\infty$ si ce polynôme n'a pas de racine rationnelle)
Soit Q un polynôme dans $k[Y]$ de degré minimal non nul, divisant $P(p^m, Y)$ dans $k[Y]$; un tel polynôme existe car la condition $p^m > k_2$ assure que $\deg P(p^m, Y) \geqslant 1$.
L'ensemble $S(0, p^m, Q)$ n'étant constitué que de places au dessous de p, le théorème 2 donne :

$$\left| \frac{1}{[K:\mathbb{Q}]} \sum_{v \in S(0,p^m,Q)} d_v^K - \frac{\deg Q}{\deg_Y P} \right| \mathrm{Log}\, p^m \leqslant A + B\sqrt{\mathrm{Log}\, p^m}$$

ce qui, joint à $\mathrm{Log}\, p^m > k_1^2$ impose :

$$\frac{1}{[K:\mathbb{Q}]} \sum_{v \in S(0,p^m,Q)} d_v^K - \frac{\deg Q}{\deg_Y P} = 0$$

soit

$$\deg_Y P \left(\sum_{v \in S(0,p^m,Q)} d_v^K \right) = \deg Q \cdot [K:\mathbb{Q}]$$

1) Si $([K:\mathbb{Q}], \deg_Y P) = 1$, l'égalité précédente donne nécessairement $\deg_Y P = \deg Q$ c'est-à-dire $P(p^m, Y)$ irréductible dans $k[Y]$
2) Si $[K:\mathbb{Q}] < \deg_Y P$, elle donne $\deg Q \geqslant \frac{\deg_Y P}{[K:\mathbb{Q}]} > 1$, ce qui signifie que $P(p^m, Y)$ n'a pas de racines dans k.
La démonstration des résultats où p^m est remplacé par $\frac{1}{m}$ est identique □

Remarque. L'égalité qui a permis de conclure la démonstration conduit en fait à la minoration de $\deg Q$;

$$\deg Q \geqslant \frac{\deg_Y P}{(\deg_Y P, [K:\mathbb{Q}])}$$

qui contient à la fois 1) et 2)

COROLLAIRE 3 — Soit s un entier et $P = P_s X^s + \cdots + P_0$, les P_i étant des éléments de $\mathbb{Q}[Y]$ pour $0 \leqslant i \leqslant s$, un polynôme irréductible dans $\mathbb{Q}[X,Y]$. Supposons que P_s possède une racine simple de degré sur $\mathbb{Q}$, $r < \deg_Y P$.
Alors l'équation $P(x,y) = 0$ n'a qu'un nombre fini de solutions en nombres entiers x, y : si (x,y) est l'une d'elles, alors $|x| \leqslant m'_0$ où m'_0 est une constante ne dépendant que de P

La démonstration est analogue à celle du corollaire 3 du théorème 1 ; la seule différence est qu'ici, on utilise le corollaire 2 (2)) du théorème 2 à la place du corollaire 2 du théorème 1. On peut aussi, ce qui revient au même, utiliser la forme du théorème 2 où $\xi_0 = \infty$ (Remarque 4)).

2.3 Etude d'un exemple.

Nous allons voir dans ce paragraphe, comment on peut, concrètement, sur un exemple précis, utiliser le théorème 2 et à quel type de résultats on peut aboutir.

Soient p un nombre premier impair et P le polynôme $P = Y^p + X - 1$
P est absolument irréductible et 1 est une racine simple de $P(0,Y)$. P vérifie donc les hypothèses du théorème 2. La série formelle vérifiant $P(X, \underset{\sim}{Y}) = 0$ et de premier terme égal à 1 est $\underset{\sim}{Y} = \sum_{m \geq 0} \delta_m X^m$ avec :

$$\delta_m = \binom{\frac{1}{p}}{m} = \frac{\prod_{i=1}^{m-1} (1 - ip)}{m!\, p^m}$$

Prenons $k = \mathbb{Q}$; on a alors également $K = \mathbb{Q}$. Il est classique que le rayon de convergence archimédien de $\underset{\sim}{Y}$ est $R_\infty = 1$. D'après les résultats du chapitre III (§2.2 Rem 1 p 3) la constante d'Eisenstein de $\underset{\sim}{Y}$ divise p^2 ; de $R_v \geq |T|_v$ si v est finie (Ch III §2.2 Ca) on déduit alors que :

(1) si $q \neq p$ $\quad R_q \geq 1$

Enfin si v_p désigne la valuation p-adique, on a

$$v_p(\delta_m) = -v_p(m!) - m \geq -\frac{m}{p-1} - m = -\frac{mp}{p-1}$$

(pour la majoration de $v_p(m!)$ voir [Am] 3.5 p102)
On obtient donc que :
pour tout entier $m \geq 1$ $\quad |\delta_m|^{\frac{1}{m}} \leq p^{\frac{p}{p-1}}$
ce qui donne :

(2) $\qquad R_p \geq p^{-\frac{p}{p-1}}$

Soient maintenant x, y, c trois entiers rationnels vérifiant :

$$y > 0 \; ; \; x \neq 0 \; ; \; (x,y) = 1 \; ; \; y^p - x^p = c$$

Posons $\xi = c/y^p$ et $\eta = x/y$; on a alors $\xi + \eta^p = 1$; nous avons donc construit un couple (ξ, η) de nombres rationnels tels que $P(\xi, \eta) = 0$ et nous allons maintenant appliquer le théorème 2 à la donnée $P, \underset{\sim}{Y}, \xi$ et $Q = Y - \eta$. Pour cela il nous reste à déterminer l'ensemble $S = S(0, \xi, Q) \cap M_Q(\xi)$, c'est-à-dire

l'ensemble des places v de $\mathbb{Q}$ telles que $|\xi|_v < \mathrm{Min}(1, R_v)$ et que $\gamma_v(\xi) = \eta$. En général, il s'agit du point le plus délicat dans l'application du théorème 2. La remarque suivante en est ici la clé : soit v une place de $\mathbb{Q}$ telle que $|\xi|_v < R_v$ alors $\gamma_v(\xi)$ est défini et vérifie $\xi + \gamma_v(\xi)^p = 1$; de $\xi + \eta^p = 1$ on déduit alors que

(3) $\dfrac{\gamma_v(\xi)}{\eta}$ est une racine p-ième de l'unité dans $\mathbb{Q}_v$.

Nous allons l'utiliser pour montrer que si c vérifie la condition suivante :

(4) Pour tout nombre premier q, différent de p, si q/c alors $q \not\equiv 1 \pmod p$

alors on a $S = M_K(\xi)$.

L'inclusion $S \subset M_K(\xi)$ est triviale ; inversement soit donc v une place de $\mathbb{Q}$ dans $M_K(\xi)$ c'est à dire vérifiant $|\xi|_v < 1$

i) Le cas archimédien : $v = \infty$.

Comme $R_\infty = 1$, $\gamma_\infty(\xi)$ est défini. Le complété $\mathbb{Q}_\infty$ de $\mathbb{Q}$ est $\mathbb{R}$; comme $p \neq 2$, (3) impose que $\gamma_v(\xi) = \eta$ c'est-à-dire $v \in S$

ii) Le cas fini : $v = q$, q un nombre premier.

a) $q \neq p$. D'après (1), $\gamma_q(\xi)$ est défini. D'autre part, $|\xi|_q < 1$ entraîne nécessairement que q/c ; d'après (4), on a donc $q \not\equiv 1 \pmod p$; 1 est alors l'unique racine p-ième de l'unité dans $\mathbb{Q}_q$ ([Am] 2.4 p 53) et (3) impose donc que $\gamma_q(\xi) = \eta$ c'est-à-dire $q \in S$

b) $q = p$. Si $|\xi|_p < 1$ alors p/c. Or si p/c alors p^2/c. En effet : si p/c alors nécessairement $p/y-x$ car $c = y^p - x^p \equiv y - x \pmod p$; or si $p/y-x$ on a aussi $p/y^{p-1} + y^{p-2}x + \cdots + yx^{p-2} + x^{p-1}$ et finalement on a donc bien p^2/c puisque $c = (y-x)(y^{p-1} + y^{p-2}x + \cdots + x^{p-1})$.

Comme $(c, y) = 1$, on a $|\xi|_p = |c|_p = p^{-2}$; d'après (2), $\gamma_p(\xi)$ est donc défini ; 1 étant la seule racine p-ième de l'unité dans $\mathbb{Q}_p$ (car $p \neq 2$), $\gamma_p(\xi) = \eta$ d'après (3) ce qui signifie que $p \in S$.

L'égalité $S = M_K(\xi)$ est donc démontrée et le théorème 2 donne alors l'inégalité suivante

$$\left(1 - \frac{1}{p}\right) R(\xi) - B\sqrt{R(\xi)} - A \leqslant 0$$

Notons γ_p la racine positive du trinôme $\left(1 - \frac{1}{p}\right)X^2 - BX - A$ et $\beta_p = \exp \gamma_p^2$. Nous avons montré la proposition suivante.

PROPOSITION — Soient p un nombre premier impair et x, y deux entiers non nuls, premiers entre eux tels que $\max(|x|^p, |y|^p, |y^p - x^p|) > \beta_p$. Alors $y^p - x^p$ est divisible par un nombre premier congru à 1 modulo p.

COROLLAIRE — Soient p un nombre premier impair et a, b, c trois entiers rationnels premiers entre eux vérifiant $a^p + b^p = c^p$ et $\max(|a|^p, |b|^p, |c|^p) > \beta_p$. Alors a, b, c sont tous trois divisibles par un nombre premier congru à 1 modulo p.

Bien sûr, on peut obtenir ces résultats par des voies élémentaires, (voir par exemple [Bi] ou [Ri] Lecture IV pour une synthèse de résultats de ce type et une liste complète de références) mais il est cependant intéressant d'avoir pu les retrouver par de tels procédés.

§ 3. DÉMONSTRATION DU THÉORÈME 1

Dans ce paragraphe, nous montrons comment le théorème 1 se déduit du théorème 2. La démonstration du théorème 2, fera elle l'objet du chapitre IV.

Soient k, P, ξ_0, K comme dans l'énoncé du théorème 1 et $\underset{\sim}{Y}$ la série formelle vérifiant $P(X, \underset{\sim}{Y}) = 0$ donnée par l'hypothèse H_{ξ_0}. Notons $\mathcal{D}$ l'ensemble des diviseurs de P dans $\overline{\mathbb{Q}}[X,Y]$ vérifiant l'hypothèse H_{ξ_0} ; soient alors

$$\mathcal{A} = \max_{D \in \mathcal{D}} \max_{\substack{\underset{\sim}{z} \in \overline{\mathbb{Q}}[[X-\xi_0]] \\ D(X, \underset{\sim}{z}) = 0}} A_{D, \underset{\sim}{z}}$$

$$\mathcal{B} = \max_{D \in \mathcal{D}} \max_{\substack{\underset{\sim}{z} \in \overline{\mathbb{Q}}[[X-\xi_0]] \\ D(X, \underset{\sim}{z}) = 0}} B_{D, \underset{\sim}{z}}$$

où nous notons $A_{D,\underset{\sim}{z}}$ et $B_{D,\underset{\sim}{z}}$ les constantes du théorème 2 associées à la donnée de D, ξ_0 et $\underset{\sim}{z}$. $\mathcal{A}$ et $\mathcal{B}$ sont bien définis car, modulo les éléments de k^*, $\mathcal{D}$ est un ensemble fini, et ne dépendent que de P et ξ_0.

Nous allons démontrer le théorème 1 pour les valeurs suivantes de a et de b :

$$a = \min\left(\min_{v \in M_K} R_v \,,\, \exp(-\mathcal{A})\right)$$
$$b = \mathcal{B}$$

où R_v est le rayon de convergence v-adique de $\underset{\sim}{Y}$. a et b sont 2 constantes positives ne dépendant que de P et ξ_0, et $a \neq 0$ car $R_v \geqslant |T|_v$ si v est finie (CF Ch III §2.2 Cor 2)

Soient donc ξ un nombre algébrique différent de ξ_0, d un entier positif et v une place du corps $K(\xi)$, vérifiant la condition (1) du théorème 1 c'est-à-dire :

$$(1) \quad |\xi - \xi_0|_v^{d_v^{K(\xi)} / [K(\xi):\mathbb{Q}]} < a \exp\left\{ - \frac{d[k(\xi):k]}{\deg_Y P} h(\xi - \xi_0) - b\sqrt{h(\xi - \xi)} \right\}$$

Comme $a \leqslant 1$, on a :

$$|\xi - \xi_0|_v \leqslant |\xi - \xi_0|_v^{d_v^{K(\xi)}/[K(\xi):\mathbb{Q}]} < R_v$$

$Y_v(\xi)$ est donc défini ; c'est un nombre algébrique sur $k(\xi)$ puisque $P(\xi, Y_v(\xi)) =$ soit Q son polynôme minimal sur le corps $k(\xi)$.

Ensuite soit $\mathcal{P}$ le polynôme, irréductible dans $k(\xi)[X,Y]$ et vérifiant $\mathcal{P}(X,\underset{\sim}{Y}) =$ ($\mathcal{P}$ est défini à un élément de $k(\xi)^*$ près). Alors, d'une part, $\mathcal{P}$ divise P dans $k(\xi)[X,Y]$, et d'autre part Q divise $\mathcal{P}(\xi, Y)$ dans $k(\xi)[Y]$.

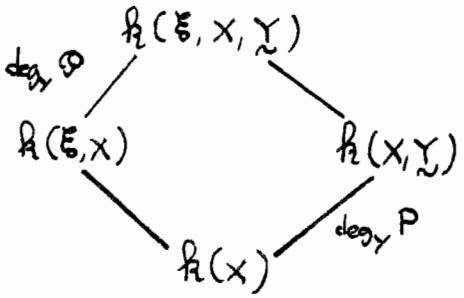
En appliquant le théorème 2 à la donnée $\mathcal{P}, \xi, Q$ et en remarquant que $\mathcal{P} \in \mathcal{D}$, on obtient :

$$|\xi - \xi_0|_v^{d_v^{K(\xi)}/[K(\xi):\mathbb{Q}]} \geqslant \prod_{v \in S(\xi_0, \xi, Q)} \min(1, |\xi - \xi_0|_v)^{d_v^{K(\xi)}/[K(\xi):\mathbb{Q}]} \geqslant \exp\left\{ -A - \frac{\deg Q}{\deg_Y \mathcal{P}} h(\xi - \xi_0) - B\sqrt{h(\xi - \xi_0)} \right.$$

et donc

$$(2) \quad |\xi - \xi_0|_v^{d_v^{K(\xi)}/[K(\xi):\mathbb{Q}]} \geqslant a \exp\left\{ - \frac{\deg Q}{\deg_Y P} [k(\xi) : k]\, h(\xi - \xi_0) - b\sqrt{h(\xi - \xi_0)} \right\}$$

puisque d'après le diagramme suivant :



on a :

$$\frac{1}{\deg_Y \mathcal{P}} \leqslant \frac{[k(\xi, X) : k(X)]}{\deg_Y P} = \frac{[k(\xi) : k]}{\deg_Y P}$$

En comparant (1) et (2), on obtient $\deg Q > d$. Q est donc le polynôme irréductible dans $k(\xi)[Y]$ divisant $P(\xi, Y)$ désiré.

Si P est absolument irréductible, on peut omettre dans le membre de droite de (2) et donc dans celui de la condition (1) le terme $[k(\xi) : k]$ qui provient de la minoration de $\deg_Y \mathcal{P}$. En effet, dans ce cas, on a $\deg_Y \mathcal{P} = \deg_Y P$.

C. Q. F. D

CHAPITRE III

Les outils de la méthode

Nous donnons dans ce chapitre plusieurs résultats qui seront les clés de la méthode que nous utiliserons pour démontrer le théorème 2 au chapitre suivant.

Le premier pas de cette méthode, dont nous avons esquissé les grands traits dans l'introduction, prévoit la construction d'une fonction auxiliaire possédant de nombreux zéros. Pour le mener à bien, nous utiliserons le résultat suivant, nous elle variante du lemme de Siegel, démontré par E. Bombieri dans [Bo3].

§1 LEMME DE SIEGEL

Soient k et E deux corps de nombres tels que $k \subset E$. Soient d'autre part $L_i = \sum_{j=1}^{N} a_{ij} X_j$, $i = 1, 2, \ldots, M$ M formes linéaires en les N variables $X_1, \ldots, X_N$, à coefficien a_{ij} dans E. Posons $r = [E : k]$. On a :

LEMME DE SIEGEL — Il existe une constante γ ne dépendant que des corps k et E ayant la propriété suivante :
Si $N > rM$, alors il existe une solution $\underline{x} = (x_1, \ldots, x_N) \in k^N$, $\underline{x} \neq 0$ au système

$$L_i(\underline{x}) = 0 \qquad i = 1, 2, \ldots, M$$

vérifiant

$$H(\underline{x}) \leq \gamma (\gamma N)^{rM/N - rM} \left[\prod_{i=1}^{M} H(L_i) \right]^{r/N - rM}$$

Dans le paragraphe suivant, nous établissons plusieurs résultats qui nous permettron notamment de majorer les termes $H(L_i)$, c'est-à-dire les hauteurs des formes linéaires définissant le système que nous aurons à résoudre pour construire la fonction auxiliaire.

§2 MAJORATIONS DES COEFFICIENTS D'UNE SÉRIE FORMELLE ALGÉBRIQUE

Soient F un corps de nombres et $A \in F[X,Y]$ un polynôme non nul. On suppose qu'il existe une série formelle $y = \sum_{m \geq 0} y_m X^m$ à coefficients y_m dans F, vérifiant $A(X, y) = 0$.

Soit v une place de F; l'objet de ce paragraphe est d'obtenir des majorations des $|y_m|_v$ du type :

$$|y_m|_v \leq \gamma_{1,v}\, \gamma_{2,v}^{m} \qquad \text{pour } m \geq 0$$

$\gamma_{1,v}$ et $\gamma_{2,v}$ étant deux constantes ne dépendant que de A et de v.

Dans tout le paragraphe 2, nous utiliserons les notations suivantes :

$A = A_{d_2} Y^{d_2} + \cdots + A_1 Y + A_0$ où $A_j = \sum_{i=1}^{d_1} a_{ij} X^i$ pour $j = 1, 2, \ldots, d_2$

et $d_1 = \deg_X A$ $d_2 = \deg_Y A$.

2.1 Le cas archimédien

Dans cette partie, v est une place archimédienne de F; nous supposons de plus que $R = R_Y(A, A'_Y)$ le résultant par rapport à l'indéterminée Y des polynômes A et A'_Y est un polynôme (en X) non nul.

Notons r_v le rayon de convergence de la série formelle y pour la place v; c'est un nombre réel strictement positif (CF Ch II §2.1), un raisonnement classique montre alors que

(1) $\quad r_v \geq \Delta_v = \operatorname{Inf} \{ |x|_w \,/\, x \neq 0 \text{ et } R(x) = 0 \}$

où w est un prolongement quelconque de v à $\overline{\mathbb{Q}}$.

Soit y_w la fonction analytique induite par y sur le disque ouvert $D(0, r_v)$ de $\mathbb{C}_w$, le complété de $\overline{\mathbb{Q}}$ pour la place w; on va obtenir les majorations désirées en utilisant les inégalités de Cauchy :

pour tout $m \geq 0$ $\quad |y_m|_v \leq \dfrac{M_w(r)}{r^m}$ $\quad$ où $\quad 0 < r < r_v$

et $\qquad M_w(r) = \sup_{|x|_w = r} |y_w(x)|_w$

Estimation de $M_w(r)$. Soient δ l'ordre du polynôme A_{d_2} en 0 et

$$r_{1,v} = \frac{|a_{\delta, d_2}|_v}{2(1+d_1)\, H_v(A)} \qquad \text{(Notons que } r_{1,v} \leq 1\text{)}$$

On a alors :

PROPOSITION 1 — Pour tout r tel que $0<r<r_v$ et $r \leq r_{1,v}$, on a :

$$M_w(r) \leq \frac{4(1+d_1)H_v(A)}{|a_{D,d_2}|_v\, r^D} .$$

Démonstration. Soit x tel que $|x|_w < r_v$ et que $A_{d_2}(x) \neq 0$. Alors $X_w(x)$ est défini et c'est une racine du polynôme $A(x,Y)$. En utilisant l'inégalité de Liouville, on obtient :

$$(2) \qquad |X_w(x)|_w \leq \frac{2(1+d_2)H_v(A)\ \mathrm{Max}(1,|x|_w)^{d_1}}{|A_{d_2}(x)|_w}$$

Nous allons maintenant minorer A_{d_2} sur un cercle centré en 0. Par définition de D, on peut écrire :

$$A_{d_2} = X^D a_{D,d_2}(1+xA) \quad \text{où} \quad a_{D,d_2} \neq 0 \quad \text{et} \quad A = \sum_{i>D} \frac{a_{i,d_2}}{a_{D,d_2}} X^{i-D-1}$$

Soit r tel que $0<r \leq r_{1,v} = \dfrac{|a_{D,d_2}|_v}{2(1+d_1)H_v(A)}$ et x tel que $|x|_v = r$

On a alors :

$$|xA(x)|_w \leq \frac{r\, d_1\, H_v(A)}{|a_{D,d_2}|_v} \leq \frac{1}{2}$$

et donc

$$(3) \qquad |A_{d_2}(x)|_w \geq \frac{|a_{D,d_2}|_v\, r^D}{2}$$

Si maintenant $0<|x|_w<r_v$ et $|x|_w<r_{1,v}$, alors (2) et (3) sont valides ; la majoration de $M_w(r)$ en résulte aussitôt. □

Minoration de r_v. Soient μ l'ordre du polynôme R en 0, δ_μ le coefficient (non nul) du terme en X^μ dans le polynôme R $\left(\delta_\mu = \dfrac{R^{(\mu)}(0)}{\mu!}\right)$ et

$$r_{2,v} = \frac{|\delta_\mu|_v}{2H_v(R)}$$

PROPOSITION 2 — On a : $r_v > r_{2,v}$.

Démonstration. Notons tout d'abord que l'inégalité à démontrer est triviale si $r_v = +\infty$ (on déduit facilement de (2), en utilisant la formule de Cauchy que ceci ne peut arriver que si y est un polynôme). Supposons donc $r_v < +\infty$; dans ce cas, (1) s'écrit

$$(4) \qquad r_v \geq \Delta_v = \mathrm{Min}\left\{ |x|_w \,/\, x \neq 0 \text{ et } R(x) = 0 \right\}$$

Pour minorer Δ_v, on utilise encore l'inégalité de Liouville, mais cette fois sous sa forme permettant de minorer les racines d'un polynôme. On l'applique, non

pas au polynôme R dont 0 peut être une racine — et en ce cas l'inégalité qu'on obtient est inintéressante —, mais au polynôme $\tilde{R} = \frac{R}{X^{\mu}}$

Comme $H_v(\tilde{R}) = H_v(R)$ et que $\tilde{R}(0) = \delta_\mu$, on obtient

$$\Delta_v \geq \frac{|\delta_\mu|_v}{2\, H_v(R)}$$

et donc la minoration annoncée de r_v □

Ecrivons maintenant les inégalités de Cauchy pour $r = r_{1,v}\, r_{2,v}$ $(r \leq \mathrm{Min}(r_{1,v}, r_{2,v}))$, en utilisant les résultats des propositions 1 et 2, on obtient alors :

PROPOSITION 3 — *Pour tout entier* $m \geq 0$, *on a* :

$$|\gamma_m|_v \leq \gamma_{1,v}\, \gamma_{2,v}^{m+D}$$

où $\gamma_{1,v} = \dfrac{4(1+d_1)\, H_v(A)}{|a_{D,d_2}|_v}$

et

$$\gamma_{2,v} = \frac{4(1+d_1)\, H_v(A) H_v(R)}{|a_{D,d_2}|_v\, |\delta_\mu|_v}$$

Notes. 1) Si 0 est un point régulier du polynôme A, c'est-à-dire si $R(0) \neq 0$, on a :

$$\mu = D = 0 \qquad a_{D,d_2} = A_{d_2}(0) \quad \text{et} \quad \delta_\mu = R(0)$$

Dans le cas général, on peut majorer D et μ respectivement par d_1 et $\deg R$.

2) On ne peut pas employer la méthode précédente si v est une place finie car dans ce cas la minoration $r_v \geq \Delta_v$ est fausse en général (Prendre par exemple le polynôme $A = Y^p - (1+X)$)

2.2 Le cas fini

Dans cette partie, v désigne une place finie de F. Nous commencons par un résultat élémentaire qui donne les majorations souhaitées sous l'hypothèse supplémentaire $A'_Y(0, y_0) \neq 0$.

PROPOSITION 4 — *Supposons que* A *vérifie* $A(0,0) = 0$ *et* $A'_Y(0,0) \neq 0$. *Alors pour tout entier* $m \geq 1$, *on a* :

$$|\gamma_m|_v \leq \left[\frac{H_v(A)}{|A'_Y(0,0)|_v}\right]^{2m-1}.$$

La démonstration se fait par récurrence sur l'entier m. De $A(X, y) = 0$, on

déduit $a_{10} + a_{01} y_1 = 0$, ce qui donne $|y_1|_v \leq \frac{H_v(A)}{|a_{01}|_v}$ c'est-à-dire, le résultat demandé pour $m = 1$.

Supposons le résultat vrai jusqu'à l'entier m. En égalant à 0 le coefficient de X^{m+1} dans $A(X, y)$, on obtient :

$$\sum_{i=0}^{\min(m+1,d_1)} \sum_{j=1}^{\min(m+1,d_2)} a_{ij} \sum_{\alpha_1 + \cdots + \alpha_j = m+1-i} y_{\alpha_1} \cdots y_{\alpha_j} + a_{m+1} = 0$$

où $$a_{m+1} = \begin{cases} a_{m+1,0} & \text{si } m+1 \leq d_1 \\ 0 & \text{si } m+1 > d_1 \end{cases}$$

ce qui donne :

$$a_{01} y_{m+1} = -\left[\sum_{(i,j) \in I_{m+1}} a_{ij} \sum_{\alpha_1 + \cdots + \alpha_j = m+1-i} y_{\alpha_1} \cdots y_{\alpha_j} + a_{m+1} \right]$$

où I_{m+1} est l'ensemble des couples (i,j) vérifiant :

$$0 \leq i \leq \min(m+1, d_1) \quad ; \quad 1 \leq j \leq \min(m+1, d_2) \quad ; \quad (i,j) \neq (0,1)$$

Les indices α_i intervenant dans le membre de droite de l'égalité précédente sont tous inférieurs à m ; en utilisant l'hypothèse de récurrence, on obtient :

pour tout $(i,j) \in I_{m+1}$ tel que $\alpha_1 + \cdots + \alpha_j = m+1-i$

$$|y_{\alpha_1} \cdots y_{\alpha_j}| \leq \left[\frac{H_v(A)}{|a_{01}|_v} \right]^{\beta_{ij}}$$

où $\beta_{ij} = \sum_{z=1}^{j} (2\alpha_z - 1) = 2(m+1-i) - j$

Comme $i + j \geq 2$ pour les couples d'indices considérés, on a $\beta_{ij} \leq 2m$ ce qui donne :

$$|y_{m+1}|_v \leq \frac{H_v(A)}{|a_{01}|_v} \left[\frac{H_v(A)}{|a_{01}|_v} \right]^{2m} = \left[\frac{H_v(A)}{|a_{01}|_v} \right]^{2m+1} \qquad \square$$

Le moyen classique de majorer les $|y_m|_v$ lorsque v est une place finie (ce qui revient à majorer les dénominateurs des y_m) est d'utiliser le théorème d'Eisenstein. C'est ce que nous ferons quand A ne vérifiera pas l'hypothèse $A'_Y(0, y_0) \neq 0$.

THÉORÈME D'EISENSTEIN — *Soit $y = \sum_{m \geq 0} y_m X^m$ une série formelle à coefficients dans $\overline{\mathbb{Q}}$, algébrique sur $\mathbb{Q}(X)$. Alors l'ensemble $\mathcal{J}(y)$ des entiers rationnels t tels que, pour tout $m \geq 1$, $t^m y_m$ soit un entier algébrique est un idéal de $\mathbb{Z}$, non nul.*

DÉFINITION — *On appelle constante d'Eisenstein de la série formelle y, que l'on note T_y, le générateur positif de l'idéal $\mathcal{J}(y)$.*

COROLLAIRE 1 — Sous les hypothèses du §2, si v est une place finie de F, alors pour tout $m \geq 1$ $\quad |y_m|_v \leq |T_y|_v^{-m}$.

Ce sont bien des majorations des $|y_m|_v$ du type demandé au début du paragraphe 2. Du corollaire 1, on déduit le résultat suivant que nous avons déjà utilisé plusieurs fois au chapitre II.

COROLLAIRE 2 — Si v est une place finie de F et r_v le rayon de convergence de la série formelle y pour la métrique v, alors :

$$r_v \geq |T_y|_v .$$

Nous déduirons le théorème d'Eisenstein de la proposition suivante qui, en outre, permet de déterminer explicitement T_y. La démonstration que nous allons en donner s'inspire de l'une des preuves du théorème d'Eisenstein que proposent B. Dwork et P. Robba dans [D-R].

PROPOSITION 5 — Gutre les hypothèses du §2, nous supposons que A est un polynôme à coefficients dans O_F, l'anneau des entiers de F et que $A'_Y(X, y) \neq 0$. Il existe donc un entier $s \geq 0$ et un élément de F non nul b_0 tels que :

$$A'_Y(X, y) \equiv b_0 X^s \mod X^{s+1}$$

Soient m_0, m_1, m les dénominateurs respectifs de y_0, des y_j, $j = 1, 2, \ldots, s+1$ et de b_0^{-1} ; soit aussi M le p.p.c.m de m_0 et de m_1. Alors les 2 nombres

$$t_1 = m_0^{\deg_Y A} m_1^{s+1} m \quad \text{et} \quad t_2 = M^{\deg_Y A} m$$

appartiennent à l'ensemble $\mathfrak{I}(y)$.

Démonstration. Supposons tout d'abord que les y_j, $j = 0, 1, \ldots, s+1$ sont des entiers de F. Nous reviendrons au cas général à la fin de la démonstration. Nous avons donc $m_0 = m_1 = M = 1$ et $t_1 = t_2 = m$. Et il s'agit de montrer que $m \in \mathfrak{I}(y)$.
Nous noterons $|\ |_x$ la valeur absolue x-adique définie sur $F[[x]]$ de la façon suivante : si $f \in F[[x]]$ et $f \neq 0$ alors

$$|f|_x = a^{-\nu} \quad \text{où } \nu \in \mathbb{N} \text{ est défini par } f \equiv 0 \mod x^\nu \text{ et } f \not\equiv 0 \mod x^{\nu+1}$$

a étant un nombre réel strictement plus grand que 1, fixé.
Rappelons que, muni de cette valeur absolue, $F[[x]]$ est un espace métrique complet.

Pour tout entier rationnel $\delta \geq 1$, soit L_δ l'ensemble des séries formelles $z = \sum_{m \geq 0} z_m x^m$ à coefficients dans F vérifiant :
pour tout entier $m \geq 0$ $\quad \delta^m z_m$ est un élément de O_F.
Il est facile de vérifier le lemme suivant :

LEMME 1 — Pour tout entier $\delta \geq 1$, L_δ est un sous-anneau fermé de $F[[x]]$; de plus : $z = \sum_{m \geq 0} z_m x^m$ appartient à L_δ et si $z_0 = 1$ alors z est inversible dans L_δ.

La démonstration de la proposition 5 va consister à montrer que y est la limite d'une suite de L_m.

Construction d'une suite convergeant vers y. Soit B la boule fermée de $F[[x]]$ de centre y et de rayon $a^{-(s+1)}$. Vérifions tout d'abord le lemme suivant.

LEMME 2 — Soit $\eta \in B$; alors on a :

$$A(x, \eta) \equiv 0 \mod x^{2s+1}$$
$$A'_y(x, \eta) \equiv b_0 x^s \mod x^{s+1}.$$

Dém. La seconde formule provient de $\eta \equiv y \mod x^{s+1}$. En utilisant la formule de Taylor on obtient :

(5) $\quad A(x, \eta) \equiv (\eta - y) A'_y(x, \eta) \mod x^{2s+2}$

ce qui donne la première formule □

Du lemme 2, on déduit que la correspondance $\eta \mapsto \varphi(\eta) = \eta - \frac{A(x,\eta)}{A'_y(x,\eta)}$ définit une application de B dans B.

LEMME 3 — L'application $\varphi : B \to B$ est contractante.

Dém. D'après la formule de Taylor, on a :

$$A(x, y) = A(x, \eta) + (y - \eta) A'_y(x, \eta) + (y - \eta)^2 a(\eta)$$

où $a(\eta) \in F[[x]]$.

Puisque $A(x, y) = 0$, on obtient que :

si $\eta \in B$ alors $\quad \varphi(\eta) - y = \frac{(y-\eta)^2}{x^s} a'(\eta)$

où $a'(\eta) = a(\eta) \frac{x^s}{A'_y(x,\eta)} \in F[[x]]$

Soient maintenant η_1 et η_2, 2 éléments de B ; d'après ce qui précède, on a

$$\varphi(\eta_1) - \varphi(\eta_2) = (\eta_1 - \eta_2)\left(y - \frac{\eta_1 + \eta_2}{2}\right) \frac{2a'(\eta)}{x^s}$$

ce dont on déduit

$$|\varphi(\eta_1) - \varphi(\eta_2)|_x \leq a^{-1} |\eta_1 - \eta_2|_x \quad \square$$

B étant complet, l'application φ possède un unique point fixe η_∞ dans B ; de plus la suite $(\eta_j)_{j \geq 0}$ définie par :

$$\eta_{j+1} = \varphi(\eta_j) \quad \text{pour } j \geq 0$$

et $\eta_0 = a_0 + a_1 x + \dots + a_s x^s$

converge vers η_∞. Or comme η est un point fixe de φ dans B, on a nécessairement $\eta_\infty = \eta$.
Montrons maintenant que les η_j que nous venons de construire appartiennent à L_m.
D'après le lemme 2, pour tout $j \geq 0$, $\frac{A(X,\eta_j)}{b_0 X^{2s+1}}$ et $\frac{A'_Y(X,\eta_j)}{b_0 X^s}$ sont des séries formelles; appelons les respectivement $\varphi_{1,j}$ et $\varphi_{2,j}$. Le lemme suivant nous donnera le résultat désiré

LEMME 4 — Pour tout entier $j \geq 0$, η_j, $\varphi_{1,j}$ et $\varphi_{2,j}$ appartiennent à L_m.

Dem. La démonstration se fait par récurrence sur l'entier j.

a) $j = 0$. Par hypothèse η_0 appartient à $O_F[X]$ (et donc à L_m). $\frac{A(X,\eta_0)}{X^{2s+1}}$ et $\frac{A'_Y(X,\eta_0)}{X^s}$ sont donc des séries formelles à coefficients dans O_F. Pour obtenir que

$$\varphi_{1,0} = \frac{A(X,\eta_0)}{b_0 X^{2s+1}} \quad \text{et} \quad \varphi_{2,0} = \frac{A'_Y(X,\eta_0)}{b_0 X^s}$$

appartiennent à L_m, il reste donc à montrer que le premier terme de ces deux séries formelles est un entier de F : c'est clair pour $\varphi_{2,0}$ puisque d'après le lemme 2 son premier terme vaut 1 ; et d'après (5), celui de $\varphi_{1,0}$ est égal à $-\gamma_{s+1}$ qui est supposé entier.

b) Supposons le résultat vrai pour l'entier j. $\varphi_{2,j}$ appartient donc à L_m; d'autre part, son premier terme vaut 1 (Lemme 2). D'après le lemme 1, $\varphi_{2,j}$ est inversible dans l'anneau L_m; on en déduit que la série formelle $A(X,\eta_j) / A'_Y(X,\eta_j)$ appartient à L_m. En effet :

$$\frac{A(X,\eta_j)}{A'_Y(X,\eta_j)} = X^{s+1} \varphi_{1,j} (\varphi_{2,j})^{-1} \tag{6}$$

Ensuite, en utilisant la formule de Taylor, on obtient

$$\frac{A(X,\eta_{j+1})}{b_0 X^{2s+1}} = \sum_{h \geq 2} \left[\frac{A(X,\eta_j)}{A'_Y(X,\eta_j)}\right]^h \frac{\psi_{j,h}}{b_0 X^{2s+1}}$$

et

$$\frac{A'_Y(X,\eta_{j+1})}{b_0 X^s} = \frac{A'_Y(X,\eta_j)}{b_0 X^s} + \sum_{h \geq 1} \left[\frac{A(X,\eta_j)}{A'_Y(X,\eta_j)}\right]^h \frac{(h+1)\psi_{j,h+1}}{b_0 X^s}$$

où $\psi_{j,h} = \frac{A^{(h)}_{Yh}(X,\eta_j)}{h!}$ $\quad j \geq 0$, $h \geq 0$, $A^{(h)}_{Yh}$ désignant la dérivée partielle h-ième d'ordre h en Y.

Les $\psi_{j,h}$ sont des éléments de L_m puisque $A^{(h)}_{Yh} / h!$ est un polynôme à coefficients dans O_F. Et d'après (6)

$$\left[\frac{A(X,\eta_j)}{A'_Y(X,\eta_j)}\right]^h \frac{1}{b_0 X^{2s+1}} \qquad \left(\text{resp.} \quad \left[\frac{A(X,\eta_j)}{A'_Y(X,\eta_j)}\right]^h \frac{1}{b_0 X^s}\right)$$

appartient à L_m si $h \geq 2$ (resp. si $h \geq 1$). Finalement donc, $\varphi_{1,j+1}$ et $\varphi_{2,j+1}$ s'écrivant comme sommes de produits d'éléments de L_m sont eux aussi des éléments de L_m □

L'ensemble L_m étant fermé (Lemme 1), η, limite d'une suite d'éléments de L_m est lui aussi dans L_m. Ceci achève la démonstration du cas où les η_j $j = 0, 1, \ldots, s+1$ sont dans O

Retour au cas général. Revenons maintenant au cas général où les η_j, $j = 0, 1, \ldots, s+1$ ne sont pas nécessairement des entiers de F. On peut se ramener au cas précédent de 2 façons.

Première réduction. La série formelle $\hat{\eta} = M\eta$ vérifie l'hypothèse du cas précédent et c'est une racine du polynôme $\hat{A} \in \mathcal{O}_F[X,Y]$ défini par:

$$\hat{A} = M^{\deg_Y A} A\left(X, \frac{Y}{M}\right)$$

On a :

$$\hat{A}'_Y(X, \hat{\eta}) \equiv M^{(\deg_Y A - 1)} b_0 X^s \mod X^{s+1}$$

On déduit donc du cas précédent que

pour tout $j \geq 0$ $\quad M\left(M^{\deg_Y A - 1} m\right)^j \eta_j$ est un entier de F,

ce qui montre que t_2 appartient à $\mathfrak{d}(\eta)$

Seconde réduction. La série formelle $\check{\eta} = \eta(m_1 X) - \eta_0$ vérifie l'hypothèse du cas précédent et c'est une racine du polynôme $\check{A} \in \mathcal{O}_F[X,Y]$ défini par:

$$\check{A} = m_0^{\deg_Y A} A\left(m_1 X, Y + \eta_0\right)$$

On a :

$$\check{A}'_Y(X, \check{\eta}) \equiv m_0^{\deg_Y A} b_0 m_1^s X^s \mod X^{s+1}$$

On déduit donc du cas précédent que

pour tout $j \geq 1$ $\quad \left(m_0^{\deg_Y A} m_1^{s+1} m\right)^j \eta_j$ est un entier de F,

ce qui montre que t_1 appartient à $\mathfrak{d}(\eta)$.

C.Q.F.D.

Démonstration du théorème d'Eisenstein. Pour voir que l'ensemble $\mathfrak{d}(\eta)$ est un idéal, il suffit de remarquer que c'est l'ensemble des entiers rationnels t vérifiant:

pour tout $m \geq 1$ et pour toute place finie v de F

$$|t|_v \, |\eta_m|_v^{1/m} \leq 1$$

F étant un corps de nombres contenant les coefficients de η (on sait qu'il en existe un d'après la proposition 4 du chapitre I).

Le point essentiel du théorème d'Eisenstein est que cet idéal est non nul. Soit A le polynôme (défini au signe près) irréductible dans $\mathbb{Z}[X,Y]$ vérifiant $A(X, \eta) = 0$. A étant irréductible dans $\mathbb{Z}[X,Y]$, on a $A'_Y(X, \eta) \neq 0$. La proposition 5 montre alors que $\mathfrak{d}(\eta) \neq \{0\}$. Plus précisément, les notations étant celles de la proposition 5, on a

$$T_\eta \mid \left(m_0^{\deg_Y A} m_1^{s+1}, M^{\deg_Y A}\right) m \qquad \square$$

Remarques. 1) Supposons, en plus des hypothèses de la proposition 5, que $A'_Y(0, y_0) \neq 0$ et que y_0 soit un entier algébrique. On a alors $m_0 = 1$, $s = 0$, $m_1 = m = \operatorname{den}(A'_Y(0,y_0)^{-1})$ ce qui donne $t_1 = m^2$ et donc T_y / m^2. On retrouve dans ce cas l'estimation classique de la constante d'Eisenstein, estimation que nous avons d'ailleurs utilisée au chapitre II (§2

2) Dans la remarque précédente, t_1 divise $t_2 = m^{\deg_X A + 1}$ et T_y / t_1 est donc une meilleure "majoration" que T_y / t_2. Il peut se produire l'inverse : prenons pour A le polynôme $A = Y^2 - X^{2n}(1+X)$ et pour y la série formelle $y = X^n \sum_{j \geq 0} \binom{\frac{1}{2}}{j} X^j$. On a $A(X,y) = 0$ et $A'_Y(X,y) \equiv 2X^n \mod X^{n+1}$ ce qui donne $m_0 = 1$ $s = n$ $m_1 = M = m = 2$ et donc $t_2 = 8$ divise $t_1 = 2^{n+2}$ dès que $n \geqslant 1$.

Maintenant que nous savons explicitement déterminer la constante d'Eisenstein d'une série formelle algébrique, nous pouvons donner un ordre de grandeur des constantes A et B du théorème 2. Pour simplifier les calculs, supposons que les coefficients de P sont des entiers algébriques, que $D_0 = 0$ (et donc $P(0,0) = 0$) et que $P'_Y(0,0) \neq 0$. D'après la remarque 1, on a : $T / (\operatorname{den} P'_Y(0,0)^{-1})^2$ et donc :

$$T \leqslant \operatorname{den} P'_Y(0,0)^{-2} \leqslant \mathcal{H}(P'_Y(0,0))^2 \leqslant \mathcal{H}(P)^2 .$$

Il est facile d'obtenir les majorations suivantes de $\deg R$ et de $\mathcal{H}(R)$

$$\deg R \leqslant (2q-1)s$$

$$\mathcal{H}(R) \leqslant (2q-1)!\,(1+s)^{2q-2}\, q^q\, \mathcal{H}(P)^{2q-1}$$

Tous calculs faits, on obtient :

$$A \leqslant a_1 h(P) + a_2$$

$$B \leqslant b_1 h(P) + b_2$$

où a_1, a_2, b_1, b_2 sont 4 constantes ne dépendant que de $s = \deg_X P$ et de $q = \deg_Y P$. Précisément on peut prendre

$$\begin{cases} a_1 = 8q^2 + 8q + 1 \\ a_2 = 9q^3 + 26sq^2 + 11q^2 + 12sq + 7q - s \end{cases} \quad \text{et} \quad \begin{cases} b_1 = 2q^3 \\ b_2 = 3q^4 + 2sq^3 + 6sq^2 + 4sq + 3q \end{cases}$$

CHAPITRE IV

Démonstration du théorème 2

Le but de ce chapitre est de démontrer le théorème 2 énoncé au paragraphe 2 du chapitre II. Nous conserverons les notations que nous avions introduites alors, y compris celles que nous avions définies à la fin de l'énoncé du théorème 2 pour donner la valeur des constantes A et B.

Donnons nous donc k, P, ξ_0, $\underset{\sim}{Y}$, K, ξ et Q vérifiant les hypothèses du théorème 2. Notre objectif est de montrer l'inégalité :

(1) $$|\varphi(\xi_0, \xi, Q)| \leqslant A + B\sqrt{k(\xi - \xi_0)}$$

où A et B sont les constantes définies dans le théorème 2 et $\varphi(\xi_0, \xi, Q)$ la quantité donnée par

$$\varphi(\xi_0, \xi, Q) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in S(\xi_0, \xi, Q)} d_v^K \operatorname{Log}\min(1, |\xi_1 - \xi_{0,1}|_v) + \frac{\deg Q}{\deg P} k(\xi - \xi_0)$$

Nous avons divisé la démonstration en deux parties : dans la première, nous établissons le résultat, ou plutôt une moitié du résultat, à savoir la minoration de l'expression $\varphi(\xi_0, \xi, Q)$ sous certaines hypothèses supplémentaires, précisées au début du paragraphe 1 ; c'est l'essentiel de la démonstration et le gros du travail. Nous montrons ensuite dans la seconde partie comment en déduire le résultat complet du théorème 2.

Avant d'aborder la première partie, remarquons que l'on a :

$$|\varphi(\xi_0, \xi, Q)| \leqslant k(\xi - \xi_0)$$

L'inégalité (1) est donc claire si $k(\xi - \xi_0) \leqslant A$. Nous supposerons donc désormais que

(2) $$k(\xi - \xi_0) > A$$

§1 PREMIÈRE PARTIE DE LA DEMONSTRATION

Nous supposons dans cette partie que $\xi_0 = 0$ et que Q est un polynôme irréductible dans $k[Y]$. Pour alléger les écritures, nous noterons d le degré de Q (on a $d>0$), $S(\xi, Q)$ l'ensemble $S(0,\xi,Q)$ et $\varphi(\xi, Q)$ la quantité $\varphi(0,\xi,Q)$.

Notons d'autre part, qu'à cause de l'inégalité de Liouville (Ch I §1.3 Remarque le nombre ξ est, sous l'hypothèse (2), nécessairement un point régulier de P : en effet, il est manifeste que $A \geq \mathrm{Log}\, 2 + h(R)$.

1.1 1ère étape : Construction d'une fonction auxiliaire

Notre objectif dans cette première étape est la démonstration de la proposition suivant

PROPOSITION 1 — *Soient $L>0$ un entier et p l'entier défini par $p = L[\sqrt{h(\xi}$ ($[\ ]$ désigne la partie entière). Alors il existe un polynôme non nul $\Phi = \sum_{i,j} \Phi_{i,j} X^i Y^j$ à coefficients dans k, vérifiant :*

(a) $\deg_X \Phi < p$, $\deg_Y \Phi < q$

(b) *Si $v \in S(\xi, Q)$ alors*
$\Phi_v = \Phi(X, Y_v)$ *a un zéro d'ordre supérieur ou égal à L au point ξ*

(c) $h(\Phi) \leq L\left(\frac{d}{q} h(\xi) + c_1 \sqrt{h(\xi)} + c_2 + o(1)\right)$

où $c_1 = \mathrm{Log}\, 2 + 2 + 2(2q+3)s + 2\delta$

$c_2 = \mathrm{Log}\left(2^{5q+3s+\delta+2}(1+s)^{2(q+2)}(1+q)^3(1+\delta)\mathcal{H}(P)^{2q+3}\mathcal{H}(R)\right) + 4 + 4(2q+3)s + 4\delta$

et $o(1)$ est une fonction de L tendant vers 0 quand L tend vers $+\infty$.

Démonstration. La condition (b) signifie que les L premiers termes du développement de Taylor au point ξ des fonctions Φ_v où $v \in S(\xi, Q)$ sont nuls. Calculons les a priori.

Soient $v \in S(\xi, Q)$ et $Y_{v,\xi} = \sum_{m \geq 0} \eta_{m,v} (X-\xi)^m$ le développement de Taylor de la fonction Y_v au point ξ. Soient, d'autre part, η une racine du polynôme Q dans $\overline{\mathbb{Q}}$ et $Y_\xi = \sum_{m \geq 0} \eta_m(\xi)(X-\xi)^m$ l'unique série formelle, qui est à coefficient dans $k(\eta)$ (car ξ est régulier (CF Ch1 §3)) vérifiant :

$P(X, Y_\xi) = 0$ et $\eta_0(\xi) = \eta$.

Puisque Q est irréductible dans $k[Y]$, il existe un k-isomorphisme de corps σ_v de $k(\eta)$ sur $k(\eta_{0,v})$ tel que :

$$\sigma_v(\eta) = \eta_{0,v} .$$

On démontre alors facilement par récurrence, en utilisant l'hypothèse que ξ est régulier et la proposition 3 du chapitre I que

$$\sigma_v(\eta_m(\xi)) = \eta_{m,v} \qquad \text{pour } m \geq 0 .$$

Le polynôme Φ étant à coefficients dans k, les coefficients du développement de Taylor en ξ de Φ_v sont conjugués (sous le k-isomorphisme σ_v) à ceux du développement en série de puissances de $X-\xi$ de $\Phi(X, Y_\xi)$. On calcule facilement ce dernier développement et on obtient :

$$\Phi(X, Y_\xi) = \sum_{m \geq 0} \Big(\sum_{i,j} A_{i,j;m}\, \Phi_{i,j} \Big) (X-\xi)^m$$

où

$$A_{i,j;m} = \sum_{\kappa=0}^{\min(m,i)} \binom{i}{\kappa} \xi^{i-\kappa} \sum_{d_1+\cdots+d_j = m-\kappa} \Big(\prod_{\tau=1}^{j} \eta_{d_\tau}(\xi) \Big) \qquad \text{pour } 0 \leq i < p,\ 0 \leq j < q \text{ et } m \geq 0$$

Finalement, la condition (b) de la proposition 1 ne dépend pas de $v \in S(\xi, Q)$ et est équivalente au système d'équations linéaires

$$L_\ell\big((\Phi_{i,j})_{i,j}\big) = 0 \qquad \ell = 1, 2, \ldots, L$$

où

$$L_\ell = \sum_{i,j} A_{i,j;\ell-1}\, X_{i,j} \qquad \text{pour } \ell = 1, 2, \ldots, L .$$

C'est un système de L équations à pq inconnues ; pour le résoudre, nous allons utiliser le lemme de Siegel énoncé au chapitre III (§1). Les formes linéaires L_ℓ ont leurs coefficients dans le corps $k(\eta)$. Donc, en adoptant les notations du paragraphe 1 du chapitre III, on a $E = k(\eta)$ et $r = d$.

De $k(\xi) \geq A \geq 4$ et $d \leq q$, on déduit que

$$(3) \qquad q\,[\sqrt{k(\xi)}] - d \geq q$$

Ceci assure que la condition de résolubilité du système $pq > Ld$ est réalisée ; d'après le lemme de Siegel, il existe donc un polynôme non nul Φ dans $k[X, Y]$ vérifiant les conditions (a) et (b) de la proposition 1 et

$$(4) \qquad \mathcal{H}(\Phi) \leq \Big[\prod_{\ell=1}^{L} \mathcal{H}(L_\ell)^{d/pq - Ld} \Big] \cdot \exp(O(L))$$

Nous allons maintenant majorer la hauteur des formes linéaires L_ℓ et en déduire grâce à (4) que le polynôme Φ vérifie aussi la condition (c) de la proposition 1

Soit v une place du corps $k(\eta)$. Si v est archimédienne, en appliquant la proposition 3 du chapitre III au polynôme $A = P_\xi$ et à la série formelle $y = \sum_{m\geq 0} \eta_m(\xi) X^m$, on obtient que, pour tout entier $m \geq 0$,

$$|\eta_m(\xi)|_v \leq \frac{4(1+\delta) H_v(P_\xi)}{|P_q(\xi)|} \left[\frac{4(1+\delta) H_v(P_\xi) H_v(R_\xi)}{|P_q(\xi)|_v \, |R(\xi)|_v}\right]^m$$

où R_ξ est le polynôme défini par $R_\xi(X-\xi) = R(X)$ et $P_q \in k[X]$ désigne le coefficient de Y^q dans P (précisément $P_q = \frac{1}{q!} P^{(q)}_{Y^q}$).

On en déduit les majorations suivantes : pour $i = 0,1,\ldots,p-1$ $\quad j = 0,1,\ldots,q-1$ et $\ell \geq 0$

$$(5) \quad |A_{i,j,\ell}|_v \leq 2^p \operatorname{Max}(1,|\xi|_v)^p \, \ell^{q-1} \left[\frac{4(1+\delta) H_v(P_\xi)}{|P_q(\xi)|_v}\right]^{q-1} \left[\frac{4(1+\delta) H_v(P_\xi) H_v(R_\xi)}{|P_q(\xi)|_v \, |R(\xi)|_v}\right]^\ell .$$

Si v est une place finie, en appliquant la proposition 4 du chapitre III au polynôme $A = P_\xi$, défini par $P_{\xi,\eta}(X-\xi, Y-\eta) = P(X,Y)$ et à la série formelle $y = \sum_{m\geq 1} \eta_m(\xi) X^m$, on obtient que pour tout entier $m \geq 1$

$$|\eta_m(\xi)|_v \leq \left[\frac{H_v(P_{\xi,\eta})}{|P'_Y(\xi,\eta)|_v}\right]^{2m-1} .$$

On en déduit les majorations suivantes : pour $i = 0,\ldots,p-1$ $\quad j = 0,\ldots,q-1$ et $\ell \geq 0$

$$(6) \quad |A_{i,j,\ell}|_v \leq \operatorname{Max}(1,|\xi|_v)^p \operatorname{Max}(1,|\eta|_v)^{q-1} \left[\frac{H_v(P_{\xi,\eta})}{|P'_Y(\xi,\eta)|_v}\right]^{2\ell}$$

De (5) et (6) on déduit finalement que pour $\ell = 1,2,\ldots,L$

$$(7) \quad \mathcal{H}(L_\ell) \leq 2^p \left[4(1+\delta) \mathcal{H}(P_\xi) \mathcal{H}(R_\xi) \mathcal{H}(P_{\xi,\eta})^2\right]^L \mathcal{H}(\xi)^p \exp(O(L))$$

Il reste à majorer la hauteur des polynômes P_ξ, R_ξ et $P_{\xi,\eta}$. D'après la formule de Taylor, on a

$$P_{\xi,\eta}(X,Y) = \sum_{i,j\geq 0} \frac{1}{i!\,j!} P^{(i+j)}_{X^i Y^j}(\xi,\eta) \, X^i Y^j$$

Soit v une place du corps $k(\eta)$.

si $v \nmid \infty$ $\quad H_v(P_{\xi,\eta}) \leq H_v(P) \operatorname{Max}(1,|\xi|_v)^\delta \operatorname{Max}(1,|\eta|_v)^q$

si $v \mid \infty$ $\quad H_v(P_{\xi,\eta}) \leq 2^{\delta+q}(1+\delta)(1+q) H_v(P) \operatorname{Max}(1,|\xi|_v)^\delta \operatorname{Max}(1,|\eta|_v)^q$

ce qui donne

$$\mathcal{H}(P_{\xi,\eta}) \leq (1+\delta)(1+q) 2^{\delta+q} \mathcal{H}(P) \mathcal{H}(\xi)^\delta \mathcal{H}(\eta)^q$$

D'après l'inégalité de Liouville (ch I § 1.3) on a :

$$\mathcal{H}(\eta) \leq 2 \mathcal{H}(P(\xi,Y)) \leq 2(\delta+1) \mathcal{H}(\xi)^\delta \mathcal{H}(P)$$

On obtient donc finalement

$$\mathcal{H}(P_{\xi,\eta}) \leq 2^{\delta+2q} (1+\delta)^{q+1} (1+q) \mathcal{H}(P)^{q+1} \mathcal{H}(\xi)^{\delta(1+q)}$$

De même, on montre aisément que

$$\mathcal{H}(P_\xi) \leq (1+s)(1+q)2^{s+q}\,\mathcal{H}(P)\mathcal{H}(\xi)^s$$
$$\mathcal{H}(R_\xi) \leq (1+\delta)2^\delta\,\mathcal{H}(R)\mathcal{H}(\xi)^\delta$$

En reportant ces résultats dans (7), on obtient

(8) $\quad \mathcal{H}(L_\ell) \leq 2^p\, c_3^L\, \mathcal{H}(\xi)^{p+c_4 L}\, \exp(o(L)) \qquad$ pour $\ell = 1,2,\ldots,L$

où $\quad c_3 = 2^{5q+3s+\delta+2}(1+s)^{2(q+2)}(1+q)^3(1+\delta)\,\mathcal{H}(P)^{2q+3}\,\mathcal{H}(R)$

$\quad c_4 = (2q+3)s + \delta$.

Nous pouvons maintenant conclure la démonstration de la proposition 1. De (4) et de (8), on déduit que

$$h(\Phi) \leq L\left(\frac{pd}{pq-Ld}\operatorname{Log}2 + \frac{Ld}{pq-Ld}\operatorname{Log}c_3 + \frac{(p+c_4L)d}{pq-Ld}\,h(\xi) + o(1)\right).$$

En utilisant que $pq - Ld \geq Lq$ (d'après (3)) et que $p = L[\sqrt{h(\xi)}]$, on obtient

$$h(\Phi) \leq L\left(\operatorname{Log}c_3 + \operatorname{Log}2\sqrt{h(\xi)} + \frac{d\,h(\xi)}{q - d/[\sqrt{h(\xi)}]} + \frac{c_4 q\, h(\xi)}{q[\sqrt{h(\xi)}] - d} + o(1)\right)$$

On écrit ensuite

$$\frac{h(\xi)}{q - d/[\sqrt{h(\xi)}]} = \frac{h(\xi)}{q} + \frac{d\,h(\xi)}{q(q[\sqrt{h(\xi)}] - d)}$$

et

$$\frac{h(\xi)}{q[\sqrt{h(\xi)}] - d} \leq \frac{16}{9}\frac{[\sqrt{h(\xi)}]^2}{q[\sqrt{h(\xi)}] - d} = \frac{16}{9}\left(\frac{[\sqrt{h(\xi)}]}{q} + \frac{d}{q^2} + \frac{d^2}{q^2(q[\sqrt{h(\xi)}] - d)}\right)$$

la dernière inégalité provenant de $h(\xi) > A \geq 9$

ce qui donne finalement le (c) de la proposition 1 c'est-à-dire

$$h(\Phi) \leq L\left(\frac{d}{q}h(\xi) + c_1\sqrt{h(\xi)} + c_2 + o(1)\right)$$

où $c_1 = \operatorname{Log}2 + 2 + 2c_4$ et $c_2 = \operatorname{Log}c_3 + 4 + 4c_4$ sont les constantes annoncées dans la proposition 1.

C.Q.F.D.

1.2 2nde étape : Minoration d'une quantité non nulle

Par construction, Φ est à coefficients dans le corps k et $\deg_Y \Phi < \deg_Y P$; P étant irréductible dans $k[X,Y]$, on a

$$\Phi(X, Y) \neq 0$$

Par conséquent $\ell = v_x(\Phi(X,Y)) < +\infty$. ($v_x$ désigne la valuation X-adique dans $\bar{\mathbb{Q}}[[X]]$)

Notons γ le coefficient de $X^{\bar{\ell}}$ dans $\Phi(X, Y)$. Alors γ est un élément non nul du corps K. A ce niveau de la méthode, on utilise un argument arithmétique, ici, la formule du produit :

$$(9) \qquad \prod_{v \in M_K} |\gamma|_v^{d_v^K} = 1$$

Dans l'étape suivante, nous allons majorer les $|\gamma|_v$. De l'inégalité ainsi obtenue nous déduirons le résultat voulu.

1.3 3ème étape : Majoration des $|\gamma|_v$

Pour retrouver les notations du paragraphe 2 du chapitre III dont nous allons utiliser les résultats, nous désignons par ν (resp. μ) l'ordre du polynôme P_q (resp. R) en 0 et par $p_{\nu,q}$ (resp. s_μ) le coefficient de X^ν (resp. X^μ) dans P_q (resp. R)
Soit alors, pour v place archimédienne de K, t_v la quantité définie par

$$t_v = \frac{|p_{\nu,q}|_v \, |s_\mu|_v}{4(1+\delta) H_v(P) H_v(R)} \qquad \left(\text{On a } t_v \leq 1 \text{ et } t_v < R_v \text{ (Ch III Prop 2)} \right)$$

Définissons enfin l'ensemble A_ξ comme l'ensemble des places v de K vérifiant

si v est archimédienne $\quad |\xi|_v < \frac{t_v}{2}$

si v est finie $\quad |\xi|_v < |T|_v$.

Nous allons distinguer deux types de majorations suivant que v appartient ou non à $S(\xi, Q) \cap A_\xi$. Pour les places v qui n'y sont pas, nous utiliserons la proposition suivante.

PROPOSITION 2 — *Soit v une place du corps K. Alors*

si v est finie $\quad |\gamma|_v \leq H_v(\Phi) \, \mathrm{Max}(1, |\nu_0|_v)^{q-1} \, |T|_v^{-\bar{\ell}}$

si v est archimédienne $\quad |\gamma|_v \leq pq \, H_v(\Phi) \, \bar{\ell}^{q-1} \left[\frac{4(1+\delta) H_v(P)}{|p_{\nu,q}|_v} \right]^{q-1} t_v^{-(\bar{\ell}+q-1)\nu}$

Démonstration. Ces inégalités s'obtiennent facilement à partir de la formule

$$\gamma = \sum_{i,j} \Phi_{i,j} \left(\sum_{d_1 + \cdots + d_q = \bar{\ell} - i} \prod_{\sigma=1}^{q} \nu_{d_\sigma} \right)$$

et de, la proposition 3 du chapitre III si v est archimédienne, du corollaire 1 du théorème d'Eisenstein (Chap III §2.2) si v est finie □

Pour majorer les $|\gamma|_v$ où $v \in S(\xi, Q) \cap A_\xi$, nous allons utiliser un argument

analytique, le principe du maximum. Le résultat est le suivant.

PROPOSITION 3 — *Soit* $v \in S(\xi, Q) \cap A_\xi$. *Alors*

si v *est finie* $\quad |\gamma|_v \leqslant |\xi|_v^L \; |T|_v^{-(\bar\ell+L)} \; H_v(\Phi) \; \mathrm{Max}(1, |b_0|_v)^{q-1}$

si v *est archimédienne* $\quad |\gamma|_v \leqslant |\xi|_v^L \; 2^L \; t_v^{-(\bar\ell+L)} \; pq \; H_v(\Phi) \left[\dfrac{4(1+\delta) H_v(P)}{|p_{\delta,q}|_v \; t_v^\delta}\right]^{q-1}$

Démonstration. Soient $v \in S(\xi, Q) \cap A_\xi$, w un prolongement quelconque de v à $\bar{\mathbb{Q}}$ et $\mathbb{C}_w$ le complété de $\bar{\mathbb{Q}}$ pour la place w. Notons γ_w la fonction (qui prolonge γ_v sur K_v) induite par $\underline{\gamma}$ sur la boule ouverte $B_w = \{x \in \mathbb{C}_w / |x|_w < R_v\}$ et Φ_w la fonction $\Phi(X, \gamma_w)$ (qui prolonge donc Φ_v).
Par construction du polynôme Φ, la fonction

$$G_w : x \longmapsto \frac{\Phi_w(x)}{x^{\bar\ell}(x-\xi)^L}$$

est strictement analytique sur toute boule fermée de B_w et prend la valeur $G_w(0) = \gamma(-\xi)^{-L}$ en 0. Le principe du maximum donne

(10) si v est archimédienne $|\gamma|_v \leqslant |\xi|_v^L \; 2^L \; t_v^{-(\bar\ell+L)} \; pq \; H_v(\Phi) \; \mathrm{Max}(1, M_w(t_v))^{q-1}$

(11) si v est finie $\quad |\gamma|_v \leqslant |\xi|_v^L \; (|T|_v - \varepsilon_v)^{-(\bar\ell+L)} \; H_v(\Phi) \; \mathrm{Max}(1, M_w(|T|_v - \varepsilon_v))^{q-1}$

où l'on note $M_w(r) = \underset{|x|_w = r}{\mathrm{Max}} \; |\gamma_w(x)|_w$ pour tout r tel que $0 < r < R_v$ et où ε_v désigne, si v est une place finie, un nombre rationnel vérifiant $0 < \varepsilon_v < |T|_v - |\xi|_v$.
D'après la proposition 1 du chapitre III, on a :

si v est archimédienne $\quad M_w(t_v) \leqslant \dfrac{4(1+\delta) H_v(P)}{|p_{\delta,q}|_v \; t_v^\delta}$

D'autre part, il est facile de vérifier que

si v est finie $\quad M_w(|T|_v - \varepsilon_v) \leqslant \mathrm{Max}(1, |b_0|_v)$

On obtient le résultat annoncé en reportant ces deux dernières inégalités dans (10) et (11) et en faisant tendre ε_v vers 0 dans le cas fini □

De (9) et des résultats des propositions 2 et 3, on déduit maintenant l'inégalité suivante.

$$(12) \qquad 1 \leqslant \left[\prod_{v \in S(\xi,Q) \cap A_\xi} |\xi|_v^{d_v}\right]^{L/[K:\mathbb{Q}]} \mathcal{H}(\Phi) \; \bar\ell^{\,q-1} \; c_5^{\bar\ell} \; (2c_5)^L \exp(o(L))$$

où

$$c_5 = 4(1+\delta) \mathcal{H}(P) \mathcal{H}(R) T .$$

1.4 4ème étape : Lemme de zéros et conclusion

La proposition suivante donne une majoration de $\bar{\ell}$.

PROPOSITION 4 — On a $\bar{\ell} \leq (p-1)q + (q-1)s$.

Démonstration. P étant irréductible dans $k[X,Y]$ et ne divisant pas Φ dans $k(X)[Y]$, Δ le résultant par rapport à la variable Y des polynômes P et Φ est un élément non nul de $k[X]$. En outre, il est classique qu'il existe des polynômes A et B dans $k[X,Y]$ tels que

$$AP + B\Phi = \Delta$$

On obtient donc :

$$B(X,Y)\,\Phi(X,Y) = \Delta$$

ce dont on déduit

$$\bar{\ell} \leq V_X(\Delta) \leq \deg \Delta \leq (p-1)q + (q-1)s$$

la dernière inégalité s'obtenant facilement en écrivant Δ comme un déterminant. □

En reportant ce résultat dans (12) et en utilisant le (c) de la proposition 2, c'est-à-dire la majoration de $h(\Phi)$ on obtient :

$$0 \leq L\left[\frac{1}{[K:\mathbb{Q}]} \sum_{v \in S(\xi,Q) \cap A_\xi} d_v^K \operatorname{Log}|\xi|_v + \frac{d}{q} h(\xi) + c_6 \sqrt{h(\xi)} + c_7 + o(1)\right]$$

où

$$c_6 = c_1 + q \operatorname{Log} c_5$$
$$c_7 = c_2 + \operatorname{Log} 2c_5 .$$

En divisant par L et en le faisant tendre vers $+\infty$, on obtient

$$(13)\quad \frac{1}{[K:\mathbb{Q}]} \sum_{v \in S(\xi,Q) \cap A_\xi} d_v^K \operatorname{Log}|\xi|_v + \frac{d}{q} h(\xi) \geqslant -c_6 \sqrt{h(\xi)} - c_7 .$$

Mais d'autre part,

$$(14)\quad \frac{1}{[K:\mathbb{Q}]} \sum_{v \in S(\xi,Q) \setminus A_\xi} d_v^K \operatorname{Log} \min(1, |\xi|_v) \geqslant \frac{1}{[K:\mathbb{Q}]} \left[\sum_{\substack{v \in M_K \\ v/\infty}} d_v^K \operatorname{Log} \frac{t_v}{2} + \sum_{\substack{v \in M_K \\ v \text{ finie}}} d_v^K \operatorname{Log}|T|_v \right] \geqslant -\operatorname{Log} 2c_5 .$$

Finalement (13) et (14) donnent

$$(15)\qquad \varphi(\xi, Q) \geqslant -c_6 \sqrt{h(\xi)} - c_8$$

où $c_8 = c_7 + \operatorname{Log} 2c_5$.

Ceci achève la première partie de la démonstration du théorème 2.

§2 SECONDE PARTIE DE LA DÉMONSTRATION

Rappelons que nous avons établi l'inégalité (15) dans le cas $\xi_0 = 0$ et sous l'hypothèse Q irréductible dans $k[Y]$. Restons dans le cas $\xi_0 = 0$, mais supposons maintenant que Q soit, comme dans l'énoncé du théorème 2 un diviseur quelconque de $P(\xi, Y)$ dans $k[Y]$.

Soit $Q = Q_1 \cdots Q_r$ la décomposition du polynôme Q en polynômes irréductible Q_i de $k[Y]$. Nous avons déjà remarqué que sous l'hypothèse (2), le nombre ξ est un point régulier de P. On en déduit que les polynômes Q_i sont deux à deux non associés. Il est clair alors que l'ensemble $S(\xi, Q)$ est égal à la réunion disjointe des ensembles $S(\xi, Q_i)$ où $i = 1, 2, \ldots, r$ de sorte que

$$\varphi(\xi, Q) = \sum_{i=1}^{r} \varphi(\xi, Q_i)$$

Il résulte de la première partie de la démonstration que

$$(16) \quad \varphi(\xi, Q) \geqslant -q c_8 - q c_6 \sqrt{h(\xi)}$$

Montrons maintenant comment on déduit de (16) la majoration de $\varphi(\xi, Q)$, la seconde inégalité annoncée dans le théorème 2.

Puisque le polynôme Q divise le polynôme $P(\xi, Y)$ dans $k[Y]$, il existe un polynôme R dans $k[Y]$ tel que :

$$P(\xi, Y) = QR$$

Comme ξ est un point régulier de P, on a :

$$(17) \quad \varphi(\xi, Q) + \varphi(\xi, R) = \varphi(P(\xi, Y))$$

Or (16) étant valable pour tout diviseur du polynôme $P(\xi, Y)$ dans $k[Y]$, on a

$$(18) \quad \varphi(\xi, R) \geqslant -q c_8 - q c_6 \sqrt{h(\xi)}$$

Mais d'autre part il est évident que

$$\varphi(\xi, P(\xi, Y)) = -\frac{1}{[K:\mathbb{Q}]} \sum_{\substack{v \in M_K \\ |\xi|_v \geqslant R_v}} d_v^K \operatorname{Log} \min(1, |\xi|_v)$$

et donc d'après le corollaire 2 du théorème d'Eisenstein et la proposition 2 du chapitre III, on obtient :

$$(19) \quad \varphi(\xi, P(\xi, Y)) \leqslant -\frac{1}{[K:\mathbb{Q}]} \left[\sum_{\substack{v \in M_K \\ v \text{ finie}}} d_v^K \operatorname{Log} |T|_v + \sum_{\substack{v \in M_K \\ v \neq \infty}} d_v^K \operatorname{Log} \frac{|\delta_v|_v}{2 H_v(R)} \right] \leqslant \operatorname{Log} c_9$$

où $c_9 = 2T\,\mathcal{H}(R)$

Et on déduit donc de (17), (18) et de (19)

(20) $\qquad \varphi(\xi, Q) \leqslant qc_8 + \mathrm{Log}\, c_9 + qc_6\sqrt{h(\xi)}$.

Finalement, en regroupant (16) et (20), on obtient le résultat suivant : si Q est un polynôme divisant le polynôme $P(\xi, Y)$ dans $k[Y]$ alors

$$|\varphi(\xi, Q)| \leqslant A + B\sqrt{h(\xi)} .$$

où $A = qc_8 + \mathrm{Log}\, c_9$ et $B = qc_6$ sont les constantes annoncées dans l'énoncé du théorème

Le théorème 2 est donc démontré dans le cas $\xi_0 = 0$. Reste à montrer comment on se ramène à ce cas particulier.

Plaçons-nous donc sous les hypothèses générales du théorème 2. Considérons alors le polynôme P_{ξ_0}, qui rappelons-le est défini par $P_{\xi_0}(X - \xi_0, Y) = P$ et la série formelle $Y_{\xi_0} = \sum_{m \geqslant 0} b_m X^m$. P_{ξ_0} et Y_{ξ_0} ont respectivement leurs coefficients dans les corps k et K et il est clair que :

$$P_{\xi_0}(X, Y_{\xi_0}) = 0$$

D'autre part, si Q est un diviseur donné de $P(\xi, Y)$ dans $k[Y]$, alors Q divise $P_{\xi_0}(\xi - \xi_0, Y) = P(\xi, Y)$ dans $k[Y]$. On peut donc appliquer le résultat démontré dans le cas $\xi_0 = 0$ à la donnée $(P_{\xi_0}, Y_{\xi_0}, \xi - \xi_0, Q)$, ce qui donne :

$$|\varphi(\xi_0, \xi, Q)| \leqslant A + B\sqrt{h(\xi - \xi_0)}$$

où A et B sont les constantes du cas $\xi_0 = 0$ associées au polynôme P_{ξ_0} et à la série formelle Y_{ξ_0}.

C. Q. F. D

Note. La réduction du problème au cas $\xi_0 = 0$ ne présentant aucune difficulté, afin de simplifier les énoncés, nous prendrons dans toute la suite ξ_0 égal à 0.

CHAPITRE V

G-fonctions

Définies par C.L Siegel en même temps que les E-fonctions, en 1929, les G-fonctions sont beaucoup plus délicates à étudier. Cependant, depuis le travail de E. Bombieri [Bo1], on dispose d'un énoncé général sur les valeurs de G-fonctions, qui, même s'il n'est pas aussi satisfaisant, peut être comparé aux résultats de Siegel sur les E-fonctions [Si].

L'esprit du résultat principal de Bombieri est le suivant : soient $Y_1, \ldots, Y_n$ n G-fonctions à coefficients dans un corps de nombres F, vérifiant des équations différentielles linéaires ; alors si $Y_1, \ldots, Y_n$ sont $F(x)$ linéairement indépendantes, il ne peut exister "trop" de relations linéaires liant les valeurs des fonctions Y_i en un point ξ de F. Or si on prend $Y_i = \underset{\sim}{Y}^{i-1}$, $i = 1, 2, \ldots, q$ où $\underset{\sim}{Y}$ est une série formelle algébrique de degré q sur $F(x)$, cela signifie que le degré de $\underset{\sim}{Y}(\xi)$ sur le corps F. ne peut être trop petit, ce qui est un résultat tout à fait analogue à ceux des théorèmes 1 et 2.

Nous allons maintenant préciser tout ceci et voir qu'en fait, on peut déduire le théorème 2 du résultat de Bombieri.

§1 LE RÉSULTAT DE BOMBIERI

DEFINITION — *Soit* $\underset{\sim}{Y} = \sum_{m \geq 0} \nu_m X^m$ *une série formelle à coefficients dans un corps de nombres* F ; *nous dirons que* $\underset{\sim}{Y}$ *est une* G-fonction *si*

$$\overline{\lim_{m \to +\infty}} \ \frac{1}{m} \left[\frac{1}{[F:\mathbb{Q}]} \sum_{v \in M_F} d_v^F \ \mathrm{Log}\left(\max_{h \leq m} |\nu_h|_v \right) \right] < +\infty$$

Remarque Il résulte de la définition qu'une G-fonction a un rayon de convergence R_v strictement positif en toute place v d'un corps de nombres contenant ses coefficients.

1.1 Enoncé du résultat

Soient F un corps de nombres, $n \geq 1$ un entier et A une matrice $n \times n$ à coefficients dans $F(x)$. On suppose que l'opérateur différentiel $L = D - A$, où nous notons $D = \frac{d}{dx}$, est fuchsien de type arithmétique ([Bo1] p 46, [Bo2]).

On se donne également $\underline{Y} = (Y_1, \ldots, Y_n)$ un vecteur solution de $L\underline{Y} = 0$ dont les composantes Y_i, $i = 1, 2, \ldots, n$ sont des G-fonctions à coefficients dans F. Pour toute place v de F, nous notons R_v le plus petit des rayons de convergence des séries formelles Y_i, $i = 1, \ldots, n$ pour la place v et $Y_{1,v}, \ldots, Y_{n,v}$ les fonctions naturellement induites par $Y_1, \ldots, Y_n$ sur la boule ouverte $B(0, R_v) = \{x \in F_v / |x|_v < R_v\}$.

On suppose de plus que les Y_i, $i = 1, \ldots, n$ vérifient les deux conditions suivantes.

(a) Les Y_i, $i = 1, \ldots, n$ sont $F(x)$ linéairement indépendantes

(b) $\frac{1}{[F:\mathbb{Q}]} \sum_{v \in M_F} d_v^F \operatorname{Log} \max(1, R_v^{-1}) < +\infty$

Sous ces hypothèses, on a le résultat suivant.

THÉORÈME 3 (E. Bombieri) — *Soient ξ un élément de F non nul et qui ne soit pas une singularité de L, ρ un entier et $(a_{ij})_{\substack{1 \leq i \leq \rho \\ 1 \leq j \leq n}}$ une matrice à coefficients dans F de rang ρ. Soit enfin S un ensemble de places v de F vérifiant*

$$|\xi|_v < R_v \quad \text{et} \quad \sum_{j=1}^{n} a_{ij} Y_{j,v}(\xi) = 0 \quad \text{pour } i = 1, 2, \ldots, \rho.$$

Alors pour tout nombre réel τ tel que $0 < \tau \leq \frac{1}{2}$, on a :

$$\frac{n - 2\tau}{[F:\mathbb{Q}]} \sum_{v \in S} d_v^F \operatorname{Log} \min(1, |\xi|_v) + (n - \rho + d_1 \tau) h(\xi) \geq -\left(d_2 + \frac{d_3}{\tau} + d_4 \tau\right)$$

où d_1, d_2, d_3, d_4 sont 4 constantes positives ne dépendant que de L et de $\underline{Y}$.

Remarque. Les constantes d_1, d_2, d_3, d_4 dont la valeur est donnée explicitement dans [Bo1] (p 49) ne dépendent pas du corps F. D'autre part, il est facile de voir que, étant à coefficients dans le corps F, les G-fonctions Y_i, $i = 1, \ldots, n$ sont sous l'hypothèse (a) linéairement indépendantes sur $\overline{\mathbb{Q}}(x)$. Le résultat du théorème 3 est donc valable sur tout corps de nombres contenant le corps F.

1.2 Schéma de démonstration (voir [Bo1] pour les détails)

1er pas ([Bo1] Lemme 13 p 39). ζ étant donné dans $]0,1[$, on construit pour tout entier N assez grand, des polynômes $P_1, \dots, P_n$ dans $F[X]$, non tous nuls, de degré inférieur à N, dont on contrôle la hauteur et tels que $\underline{P}.\underline{Y} = P_1 Y_1 + \dots + P_n Y_n$ ait un zéro d'ordre supérieur ou égal à $(n-\zeta)N$ en 0. On utilise pour ceci le lemme de Siegel que nous avons déjà employé au chapitre IV (Ch III §1 ou [Bo1] p 7).

2ème pas. D'après le théorème de Shidlovski ([Bo1] p 15), pour N assez grand ($N \geq \frac{c_1}{1-\zeta}$, où c_1 est une constante ne dépendant que de l'opérateur L), la matrice à coefficients dans $F[X]$, $R = (R_{m,j})_{\substack{1 \leq m \leq n \\ 1 \leq j \leq n}}$ où les $R_{m,j}$ sont définis par :

$$\frac{D^{m-1}(\underline{P}.\underline{Y})}{(m-1)!} = \sum_{j=1}^{n} R_{m,j} Y_j \qquad \text{pour tout entier } m \geq 1$$

est de rang n. On utilise dans cette étape l'hypothèse (a) d'indépendance linéaire sur $F(X)$ des Y_j, $j = 1, 2, \dots, n$, pour assurer que $\underline{P}.\underline{Y} \neq 0$, cela étant l'une des hypothèses du théorème de Shidlovski.

3ème pas Au moyen d'arguments élémentaires ([Bo1] Lemme 6 p 20), on montre alors qu'il existe une constante c_2 ne dépendant que de l'opérateur L et vérifiant : si ξ est un élément de F non nul et qui n'est pas une singularité de l'opérateur L, alors il existe un entier $\ell \leq \zeta N + c_2$ tel que la matrice $(R_{m,j}(\xi))_{\substack{1 \leq m \leq n+\ell \\ 1 \leq j \leq n}}$ soit de rang n.
Soient alors $m_1, \dots, m_{n-p} \in [1, n+\ell]$ tels que la matrice $A(\xi)$ définie par

$$A(\xi) = \left[\begin{array}{c} (a_{i,j})_{\substack{1 \leq i \leq p \\ 1 \leq j \leq n}} \\ \hline (R_{m_i,j}(\xi))_{\substack{1 \leq i \leq n-p \\ 1 \leq j \leq n}} \end{array}\right] \begin{matrix} \updownarrow p \\ \updownarrow n-p \end{matrix}$$

$$\qquad\qquad \longleftrightarrow \; n$$

soit de rang n. Appelons $\Delta(\xi)$ son déterminant ; c'est un élément non nul du corps F.

4ème pas. Lorsque $v \in S$, $(Y_{j,v}(\xi))_{1 \leq j \leq n}$ est l'unique solution du système

$$A(\xi)\cdot\begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ c_{m_1,v} \\ \vdots \\ c_{m_{n-\rho},v} \end{bmatrix} \begin{matrix} \updownarrow \rho \\ \updownarrow n-\rho \end{matrix}$$

où $c_{m,v} = \dfrac{D^{m-1}}{(m-1)!}(P_1 Y_{1,v} + \cdots + P_n Y_{n,v})(\xi)$ pour $m \geqslant 1$

Les formules de Cramer donnent une majoration de $|\Delta(\xi)|_v$. On obtient ([Bo1] p40):

$$\sum_{v\in S} d_v^F \operatorname{Log}|\Delta(\xi)|_v \leqslant (n-\rho-1)\left(\sum_{v\in S} d_v^F \operatorname{Log}\left(\max_{\substack{1\leqslant m\leqslant n+\ell \\ 1\leqslant j\leqslant n}} |R_{m,j}(\xi)|_v\right)\right) + \left(\sum_{v\in S} d_v^F \operatorname{Log}\left(\max_{1\leqslant m\leqslant n+\ell} |c_{m,v}|_v\right)\right) + o(N)$$

Pour $m = 1, \ldots, n+\ell$, la série formelle $\dfrac{D^{m-1}}{(m-1)!}(\underline{P}\cdot\underline{Y})$ a un zéro d'ordre supérieur ou égal à $(n-2\mathcal{Z})N - (c_2+n)$ au point 0. En utilisant le principe du maximum, on obtient des majorations des $|c_{m,v}|_v$ qui font apparaître la quantité $N(n-2\mathcal{Z})\sum_{v\in S} d_v^F \operatorname{Log}|\xi|_v$ dans l'inégalité précédente. ([Bo1] Lemmes 15 & 16 p43.44)

<u>5ème pas</u>. La formule du produit permet d'obtenir la minoration suivante

$$\sum_{v\in S} d_v^F \operatorname{Log}|\Delta(\xi)|_v = \sum_{v\notin S} d_v^F \operatorname{Log}|\Delta(\xi)|_v \geqslant -(n-\rho)\left(\sum_{v\notin S} d_v^F \operatorname{Log}\max_{\substack{1\leqslant m\leqslant n+\ell \\ 1\leqslant j\leqslant n}} |R_{m,j}(\xi)|_v\right) - o(N)$$

En regroupant les résultats des quatrième et cinquième pas, apparaît la hauteur du vecteur $(R_{m,j}(\xi))_{\substack{1\leqslant m\leqslant n+\ell \\ 1\leqslant j\leqslant n}}$ que le théorème de Dwork-Robba [Bo1] (p22) permet de contrôler ([Bo1] Lemme 10 p33) en fonction de $N h(\xi)$ et de quelques autres termes parasites qu'on majore ([Bo1] Lemme 17 p47) en utilisant l'hypothèse faite sur l'opérateur L et le théorème de Katz ([Bo1] p46). Enfin, on divise par N, puis on le fait tendre vers $+\infty$; l'inégalité que l'on obtient constitue le résultat annoncé.

C. Q. F. D.

Dans son principe, cette démonstration est une adaptation de la méthode mise au point par Siegel [Si] et développée par Shidlovski [Sh] pour l'étude des valeurs de E-fonctions. On peut y reconnaître toutes les caractéristiques d'une démonstration de transcendance : construction d'une fonction auxiliaire possédant de nombreux zéros (1er pas) ; construction d'une quantité non nulle associée à la fonction auxiliaire (2ème et 3ème pas) ; minoration et majoration de cette quantité (4ème et 5ème pas) ;

lemme de zéros (3ème pas) etc...

Cependant, il s'agit d'une méthode quelque peu différente de celle de Gel'fond, que nous avons utilisée pour démontrer le théorème 2. En effet, si on examine ces deux démonstrations, on s'aperçoit que les rôles du "point de base", 0, et du "point variable", ξ, y sont, en quelque sorte, échangés, ce qui a pour effet de déplacer les difficultés. Ainsi, dans la démonstration précédente, on construit une fonction auxiliaire ayant un zéro d'ordre élevé au point 0, ce qui ne pose pas de problème majeur; en contre partie, l'étape suivante dont le but est de montrer qu'une certaine quantité, attachée à ξ, est non nulle, est beaucoup moins aisée, puisqu'elle repose notamment sur le théorème de Shidlovski. Dans la méthode de Gel'fond, la quantité non nulle sur laquelle on travaille, est simplement, le premier terme non nul d'un développement de Taylor non nul au point 0. Par contre, nous l'avons vu, la construction de la fonction auxiliaire ayant un zéro d'ordre élevé en ξ, est beaucoup plus délicate.

Chez V. G Sprindzuk dont le résultat [Sp4] est semblable au nôtre, on sent également l'influence des idées de Siegel. D'ailleurs, il doit faire face au même type de problèmes que Bombieri, notamment à l'une des principales difficultés inhérentes à la méthode de Siegel: les différentiations successives de la fonction auxiliaire font apparaître des factoriels dont il faut se débarasser pour obtenir des estimations satisfaisantes. Le théorème de Dwork-Robba permet d'éviter cet écueil chez Bombieri; l'analogue en est le lemme 4.5 de [Sp4] chez Sprindzuk.

Il n'est pas surprenant que la méthode de Siegel ait permis de traiter le cas des G-fonctions d'une part, et celui des fonctions algébriques d'autre part; en effet, les fonctions algébriques sont un exemple typique de G-fonctions satisfaisant des équations différentielles. Nous allons préciser ce point au paragraphe suivant et en déduire une nouvelle démonstration du théorème 2.

§2 NOUVELLE DÉMONSTRATION DU THÉORÈME 2

Commençons tout d'abord par faire le lien entre fonctions algébriques et G-fonctions.

PROPOSITION — *Soit* $y = \sum_{m \geq 0} y_m x^m \in \bar{\mathbb{Q}}[[x]]$ *une série formelle, algébrique sur* $\mathbb{Q}(x)$; *alors* y *est une G-fonction.*

Démonstration. Remarquons d'abord que le corps $F = \mathbb{Q}((y_m)_{m\geq 0})$ est un corps de nombres d'après la proposition 4 du chapitre I. Ensuite, on sait (Corollaire 1 du théorème d'Eisenstein, Ch III §2.2) que si v est une place finie du corps F, on a

$$(1) \qquad \frac{\mathrm{Log}\,|y_m|_v}{m} \leq \mathrm{Log}\,|T_y|_v^{-1} \quad \text{pour tout } m \geq 1$$

D'autre part, y ayant en toute place archimédienne de F un rayon de convergence strictement positif (CF Ch II § 2.1), on a :

$$(2) \qquad \max_{\substack{v\in M_F \\ v/\infty}} \max_{m\geq 1} \frac{\mathrm{Log}\,|y_m|_v}{m} < +\infty$$

Il est maintenant facile de déduire de (1) et de (2) que y vérifie la condition définissant les G-fonctions. □

Nous sommes maintenant en mesure de démontrer le théorème 2 à partir du résultat de Bombieri. Nous réadoptons les notations des chapitres II et IV. Rappelons les données principales du problème : P est un polynôme irréductible dans $k[X,Y]$, k étant un corps de nombres, $\underset{\sim}{Y} = \sum_{m\geq 0} y_m X^m$ est une série formelle à coefficients dans $\overline{\mathbb{Q}}$ vérifiant $P(X,\underset{\sim}{Y}) = 0$, et K est le corps $k((y_m)_{m\geq 0})$. Nous noterons, de plus, F la clôture normale de K sur k.

Soit $P = P_1 \cdots P_r$ la décomposition du polynôme P en polynômes irréductibles dans $F[X,Y]$. Comme P est irréductible dans $k[X,Y]$, il existe un unique indice $i \in [1,r]$ tel que $P_i(X,\underset{\sim}{Y}) = 0$ et quitte à renuméroter les polynômes P_i, on peut supposer que $i = 1$.

Le polynôme P_1 étant irréductible dans $F[X,Y]$ et donc dans $F(X)[Y]$ puisque $\deg_Y P_1 \geq 1$, le corps $F(X,\underset{\sim}{Y})$ est un $F(X)$ espace vectoriel de dimension $q_1 = \deg_Y P_1$ et la famille $\{1, \underset{\sim}{Y}, \cdots, \underset{\sim}{Y}^{q_1-1}\}$ en constitue une base. D'autre part, à cause de la formule

$$(3) \qquad D\underset{\sim}{Y} = -\frac{(P_1)'_X(X,\underset{\sim}{Y})}{(P_1)'_Y(X,\underset{\sim}{Y})}$$

il est clair que la dérivation D laisse stable le corps $F(X,\underset{\sim}{Y})$. De ces deux dernières remarques, on déduit qu'il existe une matrice $q_1 \times q_1$ à coefficients dans $F(X)$, A, vérifiant :

$$(4) \qquad D\begin{bmatrix} 1 \\ \underset{\sim}{Y} \\ \vdots \\ \underset{\sim}{Y}^{q_1-1} \end{bmatrix} = A \begin{bmatrix} 1 \\ \underset{\sim}{Y} \\ \vdots \\ \underset{\sim}{Y}^{q_1-1} \end{bmatrix}$$

Notons L l'opérateur $L = D - A$; le théorème d'Eisenstein permet de montrer que c'est un opérateur différentiel fuchsien de type arithmétique (CF [Bo1] p 60 et [Bo2])

Le lemme suivant précise où sont les singularités de l'opérateur différentiel L.

LEMME 1 — Soit R_1 le résultant par rapport à la variable Y des polynômes P_1 et $(P_1)'_Y$. Alors la matrice $R_1^{2q_1} A$ a ses coefficients dans l'anneau $F[X]$ et les singularités de l'opérateur L sont donc des racines du polynôme R_1.

Démonstration. Notons $\mathcal{M}$ le $F[X]$ module de base $\{1, \underset{\sim}{Y}, \ldots, \underset{\sim}{Y}^{q_1-1}\}$ et $P_{1q} \in F[X]$ le coefficient de Y^{q_1} dans P_1. C'est un exercice facile de vérifier que pour tout polynôme $\alpha \in F[X,Y]$, on a

$$(5) \qquad P_{1q}^{\max(0, \deg_Y \alpha - q_1 + 1)} \alpha(X, \underset{\sim}{Y}) \in \mathcal{M}$$

D'autre part, il est classique qu'il existe 2 polynômes B et C dans $F[X,Y]$ tels que $\deg_Y B \leq q_1 - 1$ $\deg_Y C \leq q_1 - 2$ et vérifiant

$$B(P_1)'_Y + C P_1 = R_1$$

Cette dernière égalité donne :

$$(6) \qquad \frac{R_1}{(P_1)'_Y(X, \underset{\sim}{Y})} = B(X, \underset{\sim}{Y})$$

On remarque ensuite que P_{1q_1} divise R_1 dans $F[X,Y]$. (3), (5), (6) et $\deg_Y B \leq q_1 - 1$ donnent alors

$$R_1^{q_1+1} D\underset{\sim}{Y} \in \mathcal{M}$$

ce dont il est facile de déduire que

$$R_1^{2q_1} D\underset{\sim}{Y}^i \in \mathcal{M} \qquad \text{pour } i = 0, 1, \ldots, q_1 - 1 \quad \square$$

Ceci étant, (4) signifie que le vecteur $\underline{Y} = (1, \underset{\sim}{Y}, \ldots, \underset{\sim}{Y}^{q_1-1})$ est solution de $L\underline{Y} = 0$; ses composantes sont des G-fonctions à coefficients dans F (il est clair sur la définition que nous avons donnée que l'ensemble des G-fonctions est un anneau). Enfin, la condition (a) du §1.1 est évidemment satisfaite à cause de l'irréductibilité de P_1 dans $F[X,Y]$; quant à la condition (b) c'est encore une conséquence du théorème d'Eisenstein.

Les hypothèses du théorème de Bombieri étant vérifiées, donnons nous, maintenant, comme dans l'énoncé du théorème 2, un élément ξ de k non nul, Q un diviseur dans $k[Y]$ du polynôme $P(\xi, Y)$ et supposons que l'on ait

$$(7) \qquad h(\xi) > A'_0 = \operatorname{Max}\left(\operatorname{Log} 2 + h(R), \frac{4d_3 - d_4}{d_1 + 2}\right)$$

d_1, d_2, d_3, d_4 étant les constantes du théorème 3 associées à L et $\underline{Y}$.

R_1, rappelons-le, désigne le résultant par rapport à la variable Y des polynômes P et P'_Y. C'est un multiple dans $F[X]$ du polynôme R_1 ; par conséquent, à cause de l'inégalité de Liouville (Ch I §1.3 Remarque), sous l'hypothèse (7), le nombre ξ n'est pas une singularité de l'opérateur L.

Dans la suite, nous noterons Q_1 le p.g.c.d dans l'anneau $F[Y]$ des polynômes Q et $P_1(\xi, Y)$, S_1^K (resp. S_1^F) l'ensemble des places v de K (resp. F) vérifiant :

$$|\xi|_v < R_v \quad \text{et} \quad Q_1(Y_v(\xi)) = 0 \ ,$$

$Q_1 = T_1 \cdots T_s$ la décomposition du polynôme Q_1 en polynômes irréductibles (non associés) dans $F[Y]$ et enfin $S_{1,i}$, pour $i = 1, \ldots, s$ l'ensemble des places v de F vérifiant :

$$|\xi|_v < R_v \quad \text{et} \quad T_i(Y_v(\xi)) = 0 \ .$$

Soit $i \in [1, s]$; le polynôme T_i étant irréductible dans $F[Y]$, pour toute place v dans S_{1i}, le corps $F(Y_v(\xi))$ est un F-espace vectoriel de dimension $\deg T_i$. Il existe donc, pour toute place v dans S_{1i}, $q_1 - \deg T_i$ relations linéaires à coefficients dans F, linéairement indépendantes sur F liant $1, Y_v(\xi), \ldots, Y_v(\xi)^{q_1-1}$. En outre, ces relations ne dépendent pas de $v \in S_{1,i}$ puisque les $Y_v(\xi)$ où $v \in S_{1,i}$ sont conjugués sur le corps F. En appliquant le théorème 3 au nombre ξ et à ce système de relations linéaires, on obtient que pour tout nombre réel τ tel que $0 < \tau \leq \frac{1}{2}$

$$(8) \quad \frac{q_1}{[F:\mathbb{Q}]} \sum_{v \in S_{1i}} d_v^F \log \min(1, |\xi|_v) + \deg T_i \, h(\xi) \geqslant -\left(d_2 + \frac{d_3}{\tau} + (d_4 + (d_1+2)h(\xi))\tau\right)$$

A cause de l'hypothèse (7), la valeur $\tau_0 = \sqrt{d_3 / d_4 + (d_1+2)h(\xi)}$ où la fonction de τ du membre de droite de l'inégalité précédente atteint son maximum, est dans l'intervalle $]0, \frac{1}{2}]$; on déduit donc de (8) :

$$(9) \quad \frac{1}{[F:\mathbb{Q}]} \sum_{v \in S_{1i}} d_v^F \operatorname{Log} \min(1, |\xi|_v) + \frac{\deg T_i}{q_1} h(\xi) \geqslant -\left(d_5 + d_6 \sqrt{h(\xi)}\right)$$

où $d_5 = d_2 + \sqrt{4 d_3 d_4}$ et $d_6 = \sqrt{4 d_3 (d_1+2)}$

L'inégalité (9) est valable pour tout $i \in [1, s]$; comme l'ensemble S_1^F est la réunion disjointe des ensembles $S_{1,i}$ $i = 1, \ldots, s$, on a donc :

$$(10) \quad \frac{1}{[F:\mathbb{Q}]} \sum_{v \in S_1^F} d_v^F \operatorname{Log} \min(1, |\xi|_v) + \frac{\deg Q_1}{q_1} h(\xi) \geqslant -\left(q\, d_5 + q d_6 \sqrt{h(\xi)}\right)$$

Il reste à montrer que l'expression de gauche dans (10) est bien égale à $\psi(\xi, Q)$, la quantité dont on cherche à majorer la valeur absolue. Pour ceci, remarquons tout d'abord que, comme $\underset{\sim}{Y}$ a ses coefficients dans K, si w_1 et w_2 sont deux places de F au dessus d'une même place v de K, alors $Y_{w_1}(\xi)$ et $Y_{w_2}(\xi)$ sont conjugués sur K ; Q_1 étant à coefficients dans K, on en déduit que toutes les places de F au dessus d'une place de K dans S_1^K sont dans S_1^F et par conséquent :

$$(11)\quad \frac{1}{[F:\mathbb{Q}]} \sum_{v \in S_1^F} d_v^F \operatorname{Log} \min(1, |\xi|_v) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in S_1^K} d_v^K \operatorname{Log} \min(1, |\xi|_v)$$

D'autre part, puisque Q_1 divise Q dans $K[Y]$, il est clair que $S_1^K \subset S(\xi, Q)$, $S(\xi, Q)$, rappelons-le, étant l'ensemble des places v de K telles que $|\xi|_v < R_v$ et $Q(Y_v(\xi)) = 0$. Mais inversement si $v \in S(\xi, Q)$, comme $P_1(X, \underset{\sim}{Y}) = 0$, on a $P_1(\xi, Y_v(\xi)) = 0$ et donc $v \in S_1^K$ puisque Q_1 est par définition le p.g.c.d de $P_1(\xi, Y)$ et de Q. Finalement on a donc

$$(12)\qquad S_1^K = S(\xi, Q)$$

Pour pouvoir conclure, il nous faut encore montrer que $\frac{\deg Q_1}{q_1} = \frac{\deg Q}{q}$. Cela va résulter du lemme suivant.

LEMME 2 — *Pour tout $i \in [1, r]$, il existe un élément σ_i de G le groupe de Galois de F sur k tel que*

$$P_i = P_1^{\sigma_i} .$$

Démonstration. Soit N le corps engendré par k et les coefficients du polynôme P_1. On a $k \subset N \subset F$.
Les polynômes P_1^σ, où σ décrit G_N, l'ensemble des k-homomorphismes de N dans F, sont des polynômes irréductibles dans $F[X,Y]$, distincts et divisant P dans $F[X,Y]$. Leur produit $\mathcal{P} = \prod_{\sigma \in G_N} P_1^\sigma$ divise donc P dans $F[X,Y]$ et donc aussi dans $k[X,Y]$ puisque $\mathcal{P} \in k[X,Y]$. Par conséquent $P = \mathcal{P}$ (à un élément de k^* près), ce qui achève la démonstration puisqu'on peut prolonger tout élément de G_N en un élément de G □

Du lemme 2, on déduit d'une part, que,

$$\deg_Y P_1 = \frac{\deg_Y P}{r} ,$$

d'autre part, en notant Q_i le p.g.c.d dans l'anneau $F[Y]$ de $P_1^{\sigma(i)}$ et de Q que

$$Q = \prod_{i=1}^{r} Q_i = \prod_{i=1}^{r} Q_1^{\tau(i)}$$

et donc que

$$\deg Q_1 = \frac{\deg Q}{r}$$

ce qui donne bien

$$(13) \qquad \frac{\deg Q_1}{\deg_Y P_1} = \frac{\deg Q}{\deg_Y P}$$

Finalement, en tenant compte de (7), (10), (11), (12) et (13) donnent

$$(14) \qquad \frac{1}{[K:\mathbb{Q}]} \sum_{v \in S(\xi,Q)} d_v^K \operatorname{Log} \min(1, |\xi|_v) + \frac{\deg Q}{\deg_Y P} h(\xi) \geq -(A' + B' \sqrt{h(\xi)})$$

où $A' = \max(A'_0, q\, d_5)$ et $B' = q d_6$ sont des constantes ne dépendant que de P et de $\underset{\sim}{Y}$, ceci étant valable pour tout nombre ξ de k non nul et tout polynôme Q divisant $P(\xi, Y)$ dans $k[Y]$.

Ceci achève la démonstration puisque nous avons déjà montré au chapitre IV (§ 2) comment déduire de (14) la totalité du théorème 2. □

CHAPITRE VI

Théorème d'irréductibilité de Hilbert

Démontré par D. Hilbert en 1892 [Hi], le théorème d'irréductibilité s'énonce ainsi : k un corps de nombres et P un polynôme irréductible dans $k[X,Y]$ étant donnés, si $\deg_Y P \geqslant 1$, l'ensemble, noté $H_{P,k}$, des éléments x de k tels que $P(x,Y)$ soit irréductible dans $k[Y]$ est un ensemble infini.

A. Schinzel en 1965 [Schi1] et plus tard, M. Fried [Fr] ont montré que l'ensemble $H_{P,k}$ contenait une progression arithmétique $(am+b)_{m\geq 0}$. En conséquence, $H_{P,k}$ contient également une progression géométrique ($(b(a+1)^m)_{m\geq 0}$). Dans ce chapitre, on donne une nouvelle version du théorème d'irréductibilité de Hilbert, qui précise ce dernier résultat.

§1 PREMIÈRE APPROCHE

Nous reprenons les notations et les hypothèses du chapitre II. k est un corps de nombres, P un polynôme irréductible dans $k[X,Y]$; on suppose qu'il vérifie l'hypothèse H_0 (CF ChI §3) ; K désigne le corps $k((\gamma_m)_{m\geq 0})$ où les γ_m sont les coefficients de la série formelle $\underset{\sim}{Y}$ solution de $P(X,\underset{\sim}{Y}) = 0$, donnée par l'hypothèse H_0. Rappelons aussi que $M_K(\xi)$ désigne pour tout élément ξ de k, l'ensemble des places v de K telles que $|\xi|_v < 1$.

La proposition suivante, que nous allons déduire du théorème 2, est le résultat-clé de ce chapitre.

PROPOSITION 1 — *Soient ξ un élément non nul de k, $m \geqslant 0$ un entier et Q un diviseur dans $k[Y]$ de $P(\xi^m, Y)$. Alors si m est suffisamment grand (supérieur à un entier m_0 ne dépendant que de P, k et ξ), on a :*

$$(1)\quad \frac{1}{[K:\mathbb{Q}]} \sum_{v \in S(Q)} d_v^K \operatorname{Log} |\xi|_v + \frac{\deg Q}{\deg_Y P}\, h(\xi) = 0$$

où $S(Q)$ est une partie de l'ensemble $M_K(\xi)$.

Démonstration. Considérons la suite $(u_m)_{m\geq 0}$ définie par

$$u_m = \max_{Q\in D_m} \left| \frac{1}{[K:\mathbb{Q}]} \sum_{v\in S(Q)} d_v^K \operatorname{Log}|\xi|_v + \frac{\deg Q}{\deg_Y P}\, h(\xi) \right|$$

où $S(Q) = S(0,\xi^m,Q)\cap M_K(\xi)$ (Cf Not. du Ch II §2.1) et D_m désigne l'ensemble des diviseurs Q dans $k[Y]$ du polynôme $P(\xi^m, Y)$.
En utilisant le fait que $h(\xi^m) = m\, h(\xi)$, on déduit du théorème 2 que pour tout $m>0$

$$(2) \qquad 0 \leqslant u_m \leqslant \frac{A}{m} + \frac{B\sqrt{h(\xi)}}{\sqrt{m}}$$

où A et B sont les constantes du théorème 2.
D'autre part, pour tout $m\geq 0$ et tout polynôme Q dans D_m, on a $S(Q)\subset M_K(\xi)$ et $0\leq \deg Q \leq \deg_Y P$. ξ, P et k étant fixés, la suite $(u_m)_{m\geq 0}$ prend donc un nombre fini de valeurs. Comme, d'après (2), elle tend vers 0, elle est nulle à partir d'un certain rang m_0 □

COROLLAIRE — Supposons en plus des hypothèses de la proposition 1 que ξ vérifie la propriété suivante : il existe une place v_0 dans $M_K(\xi)$ telle qu'aucune puissance non nulle de $|\xi|_{v_0}$ n'appartienne au groupe multiplicatif engendré par les $|\xi|_v$ où $v\in M_K(\xi)\setminus\{v_0\}$ (i.e $|\xi|_{v_0}^{\mathbb{Z}} \cap \prod_{\substack{v\in M_K(\xi)\\ v\neq v_0}} |\xi|_v^{\mathbb{Z}} = \{1\}$).
Alors pour $m\geq m_0$, $P(\xi^m, Y)$ est irréductible dans $k[Y]$.

En effet, soient $m\geq m_0$ et Q est un diviseur dans $k[Y]$ de $P(\xi^m,Y)$. Comme $h(\xi) = \frac{1}{[K:\mathbb{Q}]} \sum_{v\in M_K(\xi)} d_v^K \operatorname{Log}|\xi|_v$, on peut écrire la relation (1)

$$(3) \qquad (\deg_Y P - \deg Q) \sum_{v\in S(Q)} d_v^K \operatorname{Log}|\xi|_v - \deg Q \sum_{v\in M_K(\xi)\setminus S(Q)} d_v^K \operatorname{Log}|\xi|_v = 0$$

Or l'hypothèse faite sur ξ signifie que $\operatorname{Log}|\xi|_{v_0}$ n'appartient pas au $\mathbb{Q}$ espace vectoriel engendré par les $\operatorname{Log}|\xi|_v$ où v décrit $M_K(\xi)\setminus\{v_0\}$. De (3) on déduit donc que soit $\deg Q = \deg_Y P$ (si $v_0\in S(Q)$), soit $\deg Q = 0$ (si $v_0\in M_K(\xi)\setminus S(Q)$) □

Remarque. Le corollaire s'applique en particulier dans les cas suivants.

a) La famille des $|\xi|_v$ où v décrit l'ensemble $M_K(\xi)$ est non vide et multiplicativement libre (cas traité dans [Sp4]). Notons que cette hypothèse est satisfaite si l'ensemble $M_K(\xi)$ n'a qu'un seul élément ; mais dans ce cas, on dispose avec le corollaire 1 du théorème 1 d'un résultat plus précis.

b) $k=\mathbb{Q}$ et il existe un nombre premier p non décomposé dans K tel que $|\xi|_p<1$. (v_0 est dans ce cas l'unique place de K au dessus de p).

c) $k = \mathbb{Q}$, K est inclus dans un corps quadratique imaginaire et $|\xi| < 1$ (v_0 est ici l'unique place archimédienne du corps K).

d) $k = K = \mathbb{Q}$ et $\xi \neq 0, 1, -1$ (cas traité dans [Sp2])

Ceci étant, le problème de l'existence d'un élément ξ de k satisfaisant l'hypothèse du corollaire reste posé. Et nous allons voir malheureusement qu'il a une réponse négative en général (voir exemple ci-dessous). Cependant, moyennant l'hypothèse supplémentaire $K = k$, la réponse devient oui et on obtient alors le résultat suivant.

THEOREME 4 — Soit P un polynôme irréductible dans $k[X,Y]$ possédant une racine dans $k((X))$. Alors l'ensemble $H_{P,k}$ contient une progression géométrique $(b^m)_{m \geq 1}$ non périodique.

Démonstration. On se ramène facilement au cas où P a une racine dans $k[[X]]$ (nous détaillerons ce point au b) de la démonstration du théorème 5) Alors P vérifie l'hypothèse H_0 avec $K = k$. En utilisant par exemple le théorème 0 du Chapitre V (§1) de [La2], qui est une forme faible du théorème de Riemann-Roch, on démontre facilement qu'il existe un élément ξ de k tel que $M_k(\xi)$ n'ait qu'un seul élément. D'après le b) de la remarque, ξ vérifie l'hypothèse du corollaire et l'ensemble $H_{P,k}$ contient donc la progression géométrique $(b^m)_{m \geq 1}$ où $b = \xi^{m_0}$; Enfin, cette progression géométrique n'est pas périodique puisque b n'est ni nul ($M_k(\xi)$ est fini) ni une racine de l'unité ($M_k(\xi) \neq \emptyset$) □

Voici maintenant un exemple où quel que soit l'élément ξ du corps k considéré, la relation (1) a une autre solution que $\deg Q = 0$ et $\deg Q = \deg_Y P$. En particulier, dans cet exemple, aucun élément du corps k ne vérifie l'hypothèse du corollaire.

Exemple. Soit P le polynôme $P = M(Y) - X$ où M est le polynôme minimal sur $\mathbb{Q}$ d'un élément primitif α du corps $\mathbb{Q}(\sqrt{13}, \sqrt{17})$. P est un polynôme irréductible dans $\mathbb{Q}[X,Y]$; prenons $k = \mathbb{Q}$; $\deg_Y P = 4$; enfin P vérifie l'hypothèse H_0 puisque α est une racine simple du polynôme $P(0,Y) = M(Y)$; et donc d'après la proposition 4 du chapitre I, P vérifie l'hypothèse H_0 avec $K = \mathbb{Q}(\sqrt{13}, \sqrt{17})$

Nous avons déjà rencontré le corps $K = \mathbb{Q}(\sqrt{13}, \sqrt{17})$ au chapitre II (§1.2 Exemple). De ce que l'on en avait dit alors résulte que pour toute place v de K on a $d_v^K = 1$ ou $d_v^K = 2$. Donc si p désigne soit un nombre premier soit ∞, il est toujours possible de construire un ensemble S_p de places v de K au dessus de p tel que $\sum_{v \in S_p} d_v^K = 2$.

A maintenant ξ est un nombre rationnel quelconque, considérons l'ensemble S_ξ défini par $S_\xi = \bigcup_{p \in M_{\mathbb{Q}}(\xi)} S_p$. Alors, on a évidemment $S_\xi \subset M_K(\xi)$ et il est facile de vérifier que:

$$\frac{1}{[K:\mathbb{Q}]} \sum_{v \in S_\xi} d_v^K \operatorname{Log} |\xi|_v + \frac{2}{\deg_{\mathbb{Q}} P} h(\xi) = 0 .$$

Par contre, il est tout aussi facile de vérifier que, dès que $M_{\mathbb{Q}}(\xi)$ contient un nombre premier p tel que $\min_{\substack{v \in M_K \\ v/p}} d_v^K \geqslant 2$, alors $\deg_{\mathbb{Q}} = 1$ ne peut pas être solution de la relation (1). Or il existe une infinité de tels nombres premiers, par exemple ceux qui sont inertes dans l'un des trois sous-corps quadratiques de K.

Nous allons voir au paragraphe 2 que ce dernier point est un fait général; et c'est grâce à ce nouvel argument que nous pourrons démontrer le résultat annoncé au début du chapitre.

§2 LE RÉSULTAT DÉFINITIF

Notre objectif est d'établir le résultat suivant.

THÉORÈME 5 — *Soient k un corps de nombres et $P_1, \ldots, P_n$ n polynômes irréductibles dans $k(X)[Y]$. Pour $i = 1, 2, \ldots, n$ on note $H_{P_i,k}$ l'ensemble des éléments x de k tels que $P_i(x, Y)$ soit irréductible dans $k[Y]$. Alors pour toute partie finie S de M_k, l'ensemble $H_{P_1,\ldots,P_n,k} = \bigcap_{i=1}^{n} H_{P_i,k}$ contient une progression géométrique $(ab^m)_{m \geqslant 1}$ dont la raison b vérifie:*

$$|b|_v < 1 \quad \text{pour tout } v \text{ dans } S$$

De plus, si les polynômes P_i, $i = 1, \ldots, n$ sont totalement décomposés dans $\overline{\mathbb{Q}}((X))$, on peut prendre $a = 1$.

Remarques. 1) Pour ce dernier point, il est clair que l'hypothèse "$P_1, \ldots, P_n$ totalement décomposés dans $\overline{\mathbb{Q}}((X))$" n'est pas superflue (Prendre par exemple $P_1 = Y^2 - X$). Par contre, peut-être l'hypothèse "Chacun des polynômes P_i possède une racine dans $\overline{\mathbb{Q}}((X))$" suffirait-elle (Voir Th 4)

2) Pour l'essentiel, le théorème 5 peut s'énoncer plus simplement: toute partie hilbertienne d'un corps de nombres ([La 3] Ch 9) contient une progression géométrique.

2.1 Résultats préliminaires

DÉFINITION — *Soit K un corps de nombres distinct de $\mathbb{Q}$. Nous dirons qu'un nombre premier p est de degré $\geqslant 2$ sur K si* $\min_{\substack{v \in M_K \\ v/p}} d_v^K \geqslant 2$.

PROPOSITION 2 — *Soit K un corps de nombres distinct de $\mathbb{Q}$. Alors il existe une infinité de nombres premiers p de degré $\geqslant 2$ sur K.*

Pour démontrer la proposition 2, on utilise le résultat suivant ([C-F] Ch VIII Th 9 p 229 ou [Schi 3] II.23 Lemme p 192)

PROPOSITION 3 — *Si $f \in \mathbb{Z}[X]$ est un polynôme de degré supérieur à 2 admettant une racine modulo p pour tous les nombres premiers p sauf un nombre fini alors f est réductible dans $\mathbb{Q}[X]$.*

Démonstration de la proposition 2 Soit f le polynôme minimal sur $\mathbb{Q}$ d'un élément primitif entier du corps K. f est un polynôme irréductible dans $\mathbb{Z}[X]$ et comme $K \neq \mathbb{Q}$, $\deg f \geqslant 2$. D'après la proposition 3, l'ensemble $\mathcal{P}_f$ des nombres premiers p tels que f n'a pas de racines modulo p est infini. Or si $p \in \mathcal{P}_f$ a fortiori f n'a pas de racines dans $\mathbb{Q}_p$. Les nombres premiers p dans $\mathcal{P}_f$ sont donc de degré $\geqslant 2$ sur K puisque le degré local d_v^K d'une place v de K au dessus de p est égal au degré de l'un des diviseurs irréductibles de f dans $\mathbb{Q}_p[X]$ □

La proposition 4 montre tout l'intérêt de la définition que nous venons d'introduire

PROPOSITION 4 — *Soit A un polynôme irréductible dans $\mathbb{Q}[X,Y]$ tel que $\deg_Y A \geqslant 2$. On suppose que A vérifie l'hypothèse H_0 et on note K le corps engendré par $\mathbb{Q}$ et les coefficients d'une série formelle $Y \in K[[X]]$ solution de $A(X,Y)=0$. Soit ξ un nombre rationnel non nul. Si l'une des 2 hypothèses suivantes est vérifiée,*

a) $[K:\mathbb{Q}] < \deg_Y A$ *et* $|\xi| \neq 1$.

b) $[K:\mathbb{Q}] \geqslant 2$ *et il existe un nombre premier p de degré $\geqslant 2$ sur K tel que* $|\xi|_p < 1$.

alors pour tout $m \geqslant M$ où M ne dépend que de A et de ξ, le polynôme $A(\xi^m, Y)$ n'a pas de racines dans $\mathbb{Q}$.

Démonstration. Soient $m \geqslant 0$ un entier et Q un diviseur dans $k[Y]$ de $A(\xi^m, Y)$ de degré non nul ; il s'agit de montrer que pour m suffisamment grand, on a $\deg Q > 1$. D'après la proposition 1, si m est supérieur à un entier, qu'on note M, qui ne dépend que de A et de ξ, alors il existe une partie $S(Q)$ de l'ensemble $M_K(\xi)$ telle que

$$\frac{1}{[K:\mathbb{Q}]} \sum_{v \in S(Q)} d_v^K \operatorname{Log} |\xi|_v + \frac{\deg Q}{\deg_Y A} h(\xi) = 0$$

Ecrivons $\xi = \dfrac{\prod_{i \in I} p_i^{\alpha_i}}{s}$ où s est un entier non nul, les p_i des nombres premiers distincts ne divisant pas s et les α_i sont strictement positifs. La relation précédente s'écrit alors

$$\sum_{i \in I} \operatorname{Log} p_i^{\alpha_i} \left[\frac{1}{[K:\mathbb{Q}]} \sum_{\substack{v \in S(Q) \\ v/p_i}} d_v^K - \frac{\deg Q}{\deg_Y A} \right] = 0 \qquad \text{si } |\xi| > 1$$

$$\sum_{i \in I} \operatorname{Log} p_i^{\alpha_i} \left[\frac{1}{[K:\mathbb{Q}]} \left(\sum_{\substack{v \in S(Q) \\ v/p_i}} d_v^K - \sum_{\substack{v \in S(Q) \\ v/\infty}} d_v^K \right) \right] + \operatorname{Log}|s| \left[\frac{1}{[K:\mathbb{Q}]} \sum_{\substack{v \in S(Q) \\ v/\infty}} d_v^K - \frac{\deg Q}{\deg_Y A} \right] = 0 \qquad \text{si } |\xi| < 1$$

Comme les p_i sont distincts et qu'ils ne divisent pas s, on obtient que pour toute place w dans $M_{\mathbb{Q}}(\xi)$ ($w = p_i$ ou $w = \infty$ éventuellement), on a

$$\frac{1}{[K:\mathbb{Q}]} \sum_{\substack{v \in S(Q) \\ v/w}} d_v^K = \frac{\deg Q}{\deg_Y A}$$

et donc, puisque $\deg Q \neq 0$

$$\deg Q \geqslant \frac{\deg_Y A}{[K:\mathbb{Q}]} \min_{\substack{v \in M_K \\ v/w}} d_v^K$$

Il est maintenant facile de conclure. (Il faut juste se rappeler pour le b) qu'on a toujours $[K:\mathbb{Q}] \leqslant \deg_Y A$ (Ch I Prop 4)) □

Hilbert déjà, dans [Hi], avait remarqué que pour estimer le "nombre" d'éléments d'un ensemble $H_{P,k}$, il suffisait de "compter" les points rationnels de certaines courbes algébriques planes (en nombre fini) attachées au polynôme P. C'est cet argument, que nous précisons dans la proposition 5, qui nous permettra au paragraphe suivant de déduire un résultat d'irréductibilité de la proposition 4.

PROPOSITION 5 — *Soit* $P = P_q Y^q + \cdots + P_1 Y + P_0$ *un polynôme irréductible dans* $\mathbb{Q}[X,Y]$ *tel que* $\deg_Y P \geqslant 1$ *et totalement décomposé dans* $\overline{\mathbb{Q}}[[X]]$. *Alors il existe une famille finie de polynômes* A_j, $j = 1, 2, \ldots, l$ *irréductibles dans* $\mathbb{Q}[X,Y]$, *de* $\deg_Y \geqslant 2$, *et vérifiant l'hypothèse* H_0, *qui ont la propriété suivante. Soit* x *un nombre rationnel ; si* $P_q(x) \neq 0$ *et si pour tout* $j \in [1,l]$, *le polynôme* $A_j(x,Y)$ *n'a pas de racines dans* $\mathbb{Q}$ *alors le polynôme* $P(x,Y)$ *est irréductible dans* $\mathbb{Q}[Y]$.

Pour la démonstration de ce résultat, voir la proposition 1.1 du chapitre 9 de [La3] p.227. La seule différence est qu'ici on demande de plus aux polynômes A_i de vérifier l'hypothèse H_0, mais ceci résulte évidemment du fait qu'on a supposé P totalement décomposé dans $\bar{\mathbb{Q}}[[X]]$.

Dans la proposition 4, on se place sur le corps des nombres rationnels, et c'est d'ailleurs une hypothèse essentielle. Pour réduire la démonstration du théorème 5 au cas $k = \mathbb{Q}$, nous utiliserons l'énoncé suivant, qui, lui aussi est classique ([La3] Ch.9. Prop 3.3)

PROPOSITION 6 — *Sous les hypothèses du théorème 5, il existe une partie finie F du corps $\mathbb{Q}$ et une famille finie $P_1, \dots, P_N$ de polynôme irréductibles dans $\mathbb{Q}(X)[Y]$ telles que*

$$H_{P_1,\dots,P_N,\mathbb{Q}} \subset H_{P_1,\dots,P_n,k} \cup F$$

Nous terminons ce paragraphe par un résultat qui, au cours de la démonstration du théorème 5, nous permettra de passer du cas où les P_i sont totalement décomposés dans $\bar{\mathbb{Q}}((X))$ au cas général.

PROPOSITION 7 — *Soient P un polynôme irréductible dans $k[X,Y]$ et $\beta \geq 1$ un entier. Soit $P(X^\beta, Y) = \Pi_1 \cdots \Pi_r$ une décomposition du polynôme $P(X^\beta, Y)$ en produit de polynômes irréductibles dans $\bar{\mathbb{Q}}[X,Y]$. On note alors L le corps engendré par k et les coefficients des polynômes Π_i $i = 1, \dots, r$. Soit enfin α un élément non nul de k tel que le polynôme $T^\beta - \alpha$ soit irréductible dans $L[T]$. Alors le polynôme $P(\alpha X^\beta, Y)$ est irréductible dans $k[X,Y]$.*

Remarque. Le résultat est faux si l'on suppose seulement $T^\beta - \alpha$ irréductible dans $k[T]$ (Prendre $P = Y^4 - 4X$, $\beta = 4$ et $\alpha = -1$)

Démonstration. Soit β un élément de $\bar{\mathbb{Q}}$ tel que $\beta^\beta = \alpha$. Les polynômes Π_i, $i = 1, \dots, r$ étant absolument irréductibles, une décomposition du polynôme $P(\alpha X^\beta, Y)$ en produits d'irréductibles de l'anneau $\bar{\mathbb{Q}}[X,Y]$ est donnée par

$$(4) \quad P(\alpha X^\beta, Y) = \Pi_1(\beta X, Y) \cdots \Pi_r(\beta X, Y)$$

Supposons que l'on ait $P(\alpha X^\beta, Y) = QR$ avec Q et R dans $k[X,Y]$

D'après (4) on a nécessairement

$$\begin{cases} Q = \zeta\, Q_1(\beta X, Y) \\ R = \kappa\, R_1(\beta X, Y) \end{cases}$$

où Q_1 et R_1 sont deux polynômes dans $L[X,Y]$; ζ et κ sont a priori deux éléments de $\bar{\mathbb{Q}}$ mais à cause de $0 \neq Q(0,Y) = \zeta\, Q_1(0,Y)$ (resp. $0 \neq R(0,Y) = \kappa\, R_1(0,Y)$) ils sont aussi nécessairement dans L ; et donc quitte à modifier Q_1 et R_1 on peut supposer que $\zeta = \kappa = 1$.

Par hypothèse, $T^b - \alpha$ est irréductible dans $L[T]$; en particulier si j est un entier quelconque, β^j n'appartient à L que si j est dans l'idéal $b\mathbb{Z}$. Comme Q et R sont à coefficients dans $k \subset L$, Q_1 et R_1 sont nécessairement de la forme:

$$\begin{cases} Q_1 = Q_2(X^b, Y) \\ R_1 = R_2(X^b, Y) \end{cases}$$

où Q_2 et R_2 sont dans $L[X,Y]$, ce qui donne

$$\begin{cases} Q = Q_2(\alpha X^b, Y) \\ R = R_2(\alpha X^b, Y) \end{cases}$$

On voit donc que Q_2 et R_2 appartiennent nécessairement à $k[X,Y]$. Or $P(\alpha X^b, Y) = QR$ s'écrit maintenant $P(\alpha X^b, Y) = Q_2(\alpha X^b, Y)\, R_2(\alpha X^b, Y)$; ceci n'est possible que si $P = Q_2 R_2$ ce qui, puisque P est irréductible dans $k[X,Y]$ impose que ou bien Q_2 ou bien R_2, et donc ou bien Q ou bien R soit de degré nul.

C. Q. F. D.

2.2 Démonstration du théorème 5

On se donne donc $P_1, \ldots, P_n$ n polynômes de $\deg_Y \geq 1$, irréductibles dans $k[X,Y]$, où k est un corps de nombres, et S une partie finie de M_k. Pour démontrer le théorème 5, nous allons procéder progressivement.

a) 1er cas : $k = \mathbb{Q}$ et $P_1, \ldots, P_n$ sont totalement décomposés dans $\bar{\mathbb{Q}}[[X]]$

Notons pour $i = 1, 2, \ldots, n$, $(A_{ij})_{1 \leq j \leq l_i}$ la famille de polynômes associée au polynôme P_i dans la proposition 5 et $\mathcal{J}$ l'ensemble des couples (i,j) tels que $1 \leq i \leq n$ et $1 \leq j \leq l_i$, qui indexe la réunion de ces familles.

Chacun des polynômes A_{ij} vérifie l'hypothèse H_0 ; notons pour tout (i,j) dans $\mathcal{J}$, $Y_{ij} = \sum_{m \geq 0} b_{m,ij} X^m$ une série formelle solution de $A_{ij}(X, Y_{ij}) = 0$ et K_{ij} le corps $K_{ij} = \mathbb{Q}((b_{m,ij})_{m \geq 0})$. Soit alors $\mathcal{J}^0$ l'ensemble des indices $(i,j) \in \mathcal{J}$ tels que $[K_{ij} : \mathbb{Q}] = \deg_Y A_{ij}$.

D'après la proposition 2, il existe pour tout (i,j) dans J°, une infinité de nombres premiers de degré ≥ 2 sur K_{ij} ; choisissons en un qu'on note p_{ij}, ceci pour tout indice (i,j) dans J°. Considérons maintenant le nombre rationnel β défini par

$$\beta = 2\cdot\left(\prod_{(i,j)\in J^\circ} p_{ij}\right)\left(\prod_{P \text{ premier dans } S} P\right) \qquad \text{si } \infty \notin S$$

et

$$\beta = \frac{\left(\prod_{(i,j)\in J^\circ} p_{ij}\right)\left(\prod_{P \text{ premier dans } S} P\right)}{p_\infty} \qquad \text{si } \infty \in S$$

où p_∞ est un nombre premier n'appartenant pas à S, distinct des p_{ij} et choisi suffisamment grand pour que $\beta < 1$.

Faisons $A = A_{ij}$ dans la proposition 4, (i,j) étant un indice quelconque dans J. Par construction, le nombre β vérifie toujours l'une des deux hypothèses a) et b). Par conséquent, si m est supérieur à un entier M_{ij}, le polynôme $A_{ij}(\beta^m, Y)$ n'a pas de racines dans le corps $\mathbb{Q}$. D'autre part, comme $\beta \neq 0, 1, -1$, on est sûr qu'en prenant m assez grand, disons supérieur à un entier M_0, β^m ne sera pas une racine de l'un des polynômes $P_{i,q_i} \in \mathbb{Q}[X]$ où $i = 1,2,\ldots,n$, coefficient de $Y^{\deg_Y P_i}$ dans P_i.

Soit alors $m_0 = \operatorname{Max}\left(1, M_0, \operatorname*{Max}_{(i,j)\in J} M_{ij}\right)$; on déduit maintenant facilement de la proposition 5 que si $m \geq m_0$ alors chacun des polynômes $P_i(\beta^m, Y)$, $i = 1,2,\ldots,n$ est irréductible dans $\mathbb{Q}[Y]$.

L'ensemble $H_{P_1,\ldots,P_n,\mathbb{Q}}$ contient donc la progression géométrique $(b^m)_{m\geq 1}$ où $b = \beta^{m_0}$; enfin par construction de β, on a $|b|_v < 1$ pour tout v dans S □

b) <u>2ème cas : $k = \mathbb{Q}$ et $P_1,\ldots,P_n$ sont totalement décomposés dans $\bar{\mathbb{Q}}((X))$</u>

On se ramène au cas précédent en introduisant les polynômes $\check{P}_i$, $i = 1,2,\ldots,n$, définis par $\check{P}_i = X^{a_i} P_i(X, X^{-n_i}Y)$ où a_i et n_i sont deux entiers choisis de telle façon que l'hypothèse du 1er cas soit satisfaite (CF Ch II §2.1 Rem 3). Il suffit ensuite de remarquer que pour tout nombre rationnel x non nul, l'irréductibilité dans $\mathbb{Q}[Y]$ de $P_i(x,Y)$ équivaut à celle de $\check{P}_i(x,Y) = x^{a_i} P_i(x, x^{-n_i}Y)$ □

c) <u>3ème cas : $P_1,\ldots,P_n$ sont totalement décomposés dans $\bar{\mathbb{Q}}((X))$</u>

Il s'agit ici d'étendre le corps de base. En utilisant la proposition 6, on déduit du cas précédent qu'il existe $b \in \mathbb{Q}\setminus\{0,1,-1\}$ vérifiant $|b|_v < 1$ pour tout v dans $S|_{\mathbb{Q}} = \{v|_{\mathbb{Q}} \,/\, v \in S\}$ et $\{b^m / m \geq 1\} \subset H_{P_1,\ldots,P_n,k} \cup F$ où F est

une partie finie de $\mathbb{Q}$.

Comme F est fini, quitte à changer b en l'une de ses puissances, on peut faire en sorte qu'en fait $\{b^m / m \geq 1\} \subset H_{P_1,\ldots,P_n,k}$. Enfin comme $b \in \mathbb{Q}$, on a aussi $|b|_v < 1$ pour tout v dans S. Le théorème 5 est donc complètement démontré dans le cas où les polynômes P_i, $i = 1,2,\ldots n$ sont totalement décomposés dans $\bar{\mathbb{Q}}((X))$ □

d) Cas général

Par définition des entiers $\delta(P_i)$ (CF Ch I §3), les polynômes $P_i(X^{\delta(P_i)}, Y)$ sont totalement décomposés dans $\bar{\mathbb{Q}}((X))$; on est donc ramené au cas précédent, à ceci près qu'il peut arriver que l'un des polynômes $P_i(X^{\delta(P_i)}, Y)$ soit réductible dans $k[X,Y]$ (Penser à $Y^2 - X$). Pour lever cette difficulté, on utilise la proposition 7.

Ecrivons pour tout $i \in [1,n]$, $P_i(X^{\delta(P_i)}, Y) = TZ_{i,1} \times \ldots \times TZ_{i,r_i}$ une décomposition du polynôme $P_i(X^{\delta(P_i)}, Y)$ en produit de polynômes irréductibles dans $\bar{\mathbb{Q}}[X,Y]$. Notons L_i le corps engendré par k et les coefficients des polynômes $TZ_{i,j}$, $j = 1,\ldots,r_i$ et $L = L_1 \ldots L_n$ le corps engendré par les L_i, $i = 1,2,\ldots,n$.

On choisit ensuite α un élément non nul du corps k tel que pour tout $i \in [1,n]$ le polynôme $T^{\delta(P_i)} - \alpha$ soit irréductible dans $L[T]$: on peut prendre par exemple pour α un nombre premier impair qui ne divise pas le discriminant du corps de nombres L ; l'irréductibilité dans $L[T]$ des polynômes $T^{\delta(P_i)} - \alpha$ résulte alors du théorème de Capelli ([Schi3] I.13 Th 21 p 91).

Considérons maintenant les polynômes $P_{i,\alpha}$, définis par

$$P_{i,\alpha} = P_i(\alpha X^{\delta(P_i)}, Y) \qquad \text{pour } i = 1,2,\ldots,n$$

Alors, ces polynômes sont également totalement décomposés dans $\bar{\mathbb{Q}}((X))$; mais d'après la proposition 7, eux sont irréductibles dans $k[X,Y]$.

D'après le cas précédent, l'ensemble $H_{P_{1,\alpha},\ldots,P_{n,\alpha},k}$ contient donc une progression géométrique $(\beta^m)_{m \geq 1}$ avec β dans k vérifiant $|\beta|_v < 1$ pour tout v dans S. Posons $a = \alpha$ et $b = \beta^\delta$ où $\delta = \text{ppcm}(\delta(P_1),\ldots,\delta(P_n))$; alors il est clair que la progression géométrique $(ab^m)_{m \geq 1}$ satisfait la conclusion du théorème 5.

C.Q.F.D.

CHAPITRE VII

Enoncés géométriques

Dans ce chapitre, on adopte un point de vue plus géométrique. On regarde le polynôme P des chapitres précédents comme une courbe algébrique plane. Au premier paragraphe, on déduit du théorème 2 un énoncé sur les points rationnels de cette courbe. Plus généralement, on donne au second paragraphe un énoncé, essentiellement dû à Bombieri, [Bo4] sur les valeurs d'une fonction rationnelle quelconque sur une courbe projective lisse.

L'une des principales difficultés de ce chapitre sera de traduire en termes purement géométriques l'énoncé du théorème 2 : la notion de fonction algébrique, par exemple, devra disparaître; en particulier nous faudra-t-il simplifier la condition "$v \in S(\xi_0, \xi, Q)$". Ce sera l'objet des lemmes 1 et 2 au paragraphe 1 ; au paragraphe 2, nous devrons de surcroît, recourir au Théorème de Décomposition de Weil [We].

Notations. ([Fu] [Ha] pour la géométrie des courbes). C désignera une courbe algébrique définie sur un corps de nombres k. Elle sera toujours supposée absolument irréductible. Si F est un sous-corps de $\bar{\mathbb{Q}}$, nous noterons C(F) l'ensemble des points F-rationnels de la courbe C.

Si F est une extension de k, F(C) désignera le corps des fonctions rationnelles de la courbe C, définies sur F. Un point M de C sera dit régulier si l'anneau local de C en M est un anneau de valuation discrète ; nous noterons alors ord_Q la valuation (surjective) associée.

Si φ est un élément de $\bar{\mathbb{Q}}(C)$, le degré de φ est défini par

$$(1) \qquad \deg \varphi = [\bar{\mathbb{Q}}(C) : \bar{\mathbb{Q}}(\varphi)] \quad ;$$

c'est aussi le nombre de zéros (resp. de pôles) dans $C(\bar{\mathbb{Q}})$ de la fonction φ, comptés

avec multiplicité ; c'est encore le degré de $\varphi : C(\bar{\mathbb{Q}}) \longrightarrow \mathbb{P}^1(\bar{\mathbb{Q}})$ vu comme revêtement (ramifié) de $\mathbb{P}^1$.

Les notions de M_k - constantes, fonctions M-bornées etc... , ont été définies au chapitre I (§1.1)

Pour le Théorème de Décomposition de Weil, comme pour la théorie des Hauteurs, nous prendrons ici comme unique référence le livre de S. Lang, "Fundamentals of Diophantine Geometry" [La3]

Enfin, afin d'éviter la multiplication des constantes, nous préférons utiliser ici, la notation $O(\ldots)$: si f est une fonction positive, $O(f)$ désignera une fonction majorée en module par une quantité du type Af où A est une constante (qui peut dépendre de certains paramètres).

§1 POINTS RATIONNELS SUR UNE COURBE ALGÉBRIQUE PLANE

Dans ce paragraphe, C est une courbe algébrique affine plane définie sur k. On note $k[x,y]$ son anneau de coordonnées. On suppose qu'il existe dans $C(k)$ un point Q qui soit régulier. Quitte à échanger x et y et à leur ajouter une constante (dans le corps k), on peut supposer que x est une uniformisante en Q et que $y(Q) = 0$.

Sous ces conditions, on a le résultat suivant.

THÉORÈME 6 — *Il existe une M_k-constante multiplicative β, ne dépendant que de C et de Q, telle que pour tout point $M \neq Q$ dans $C(k)$, on ait :*

(2) *S'il existe $v \in M_k$ tel que $|y(M)|_v < \beta_v$ alors $x(M) \neq 0$.*

(3) $$\frac{1}{[k:\mathbb{Q}]} \sum_{\substack{v \in M_k, \\ |y(M)|_v < \beta_v}} d_v^k \operatorname{Log} \min(1, |x(M)|_v) = -\frac{1}{\deg x} h(x(M)) + O(1) + O\left(\sqrt{h(x(M))}\right)$$

où les constantes intervenant dans les $O(\ldots)$ ne dépendent que de C et de Q.

Remarque. On a $\beta_v = 1$ pour tout $v \in M_k$ sauf un nombre fini. Mais en général, le résultat devient faux si l'on prend $\beta_v = 1$ pour toute place v de k dans l'énoncé du théorème 6 (Voir l'exemple du §2.1).

Démonstration. Soit $P = \sum_{i,j} p_{ij} X^i Y^j$ le polynôme (défini à un élément de k^* près), irréductible dans $k[X,Y]$ et vérifiant

$$P(x, y) = 0$$

Par définition du degré de x, on a $\deg x = \deg_Y P$; d'autre part $x(Q) = y(Q) = 0$ impose $p_{00} = 0$; enfin x étant une uniformisante en Q, on a

(4) $\qquad p_{01} \neq 0$

Pour toute place v de k, on définit alors le nombre réel β_v par :

$$\begin{cases} \beta_v = \dfrac{|p_{01}|_v}{H_v(P)} & \text{si } v \text{ est finie.} \\ \beta_v = \dfrac{|p_{01}|_v}{2(1+\deg_X P)(\deg_Y P)^2 H_v(P)} & \text{si } v \text{ est archimédienne.} \end{cases}$$

Nous allons démontrer le théorème 6 pour ce choix de la famille β, qui, visiblement, est une M_k - constante multiplicative.

D'après (4), le polynôme P vérifie l'hypothèse H_0' ; on note $\Upsilon = \sum_{m \geq 1} \gamma_m X^m$ l'unique série formelle de premier terme nul, solution de $P(X, \Upsilon) = 0$; Υ est à coefficients dans k ; comme au chapitre II, on note également, pour toute place v de k, R_v le rayon de convergence v-adique de Υ, Υ_v la fonction qu'induit Υ sur k_v etc...

Associons à toute place v de k, le nombre réel ζ_v défini par :

si v est finie, $\zeta_v = \beta_v |T|_v$, où T désigne la constante d'Eisenstein de la série Υ.

si v est archimédienne, ζ_v est un nombre réel choisi assez petit pour que :

$$0 < \zeta_v < \operatorname{Min}(R_v, \beta_v)$$

et que :

pour tout x dans k_v, si $|x|_v < \zeta_v$ alors $|\Upsilon_v(x)|_v < \beta_v$.

Notons ensuite, pour tout point M dans $C(k)$, $S(M)$ (resp. $T(M)$, $A(M)$) l'ensemble des places v de k vérifiant :

$$|x(M)|_v < R_v \quad \text{et} \quad \Upsilon_v(x(M)) = y(M)$$

resp. $\quad |y(M)|_v < \beta_v$

resp $\quad |x(M)|_v \geqslant \zeta_v$.

LEMME 1 — On a :

(a) $\quad S(M) \setminus T(M) \subset A(M)$.

(b) $\quad T(M) \setminus S(M) \subset A(M)$.

Démonstration. Remarquons tout d'abord que

(5) pour tout x dans k_v, si $|x|_v < \zeta_v$ alors $|Y_v(x)|_v < \beta_v$

Si v est une place archimédienne, (5) est inclus dans la définition de ζ_v ; si v est une place finie, on a, si $|x|_v < \zeta_v$

$$|\eta_m x^m| < |T|_v^{-m} (\beta_v |T|_v)^m \leq \beta_v \qquad \text{pour tout } m \geq 1$$

ce qui donne bien :

$$|Y_v(x)|_v < \beta_v .$$

L'inclusion (a) est facile : soit $v \in S(M)$; si $v \notin A(M)$ c'est-à-dire si $|x(M)|_v < \zeta_v$, alors d'après (5) on a

$$|Y_v(x(M))|_v < \beta_v$$

et donc, puisque $v \in S(M)$:

$$|y(M)|_v < \beta_v$$

ce qui signifie bien que $v \in T(M)$ □

Voyons l'inclusion (b). Soit $v \in T(M)$; si $v \notin A(M)$, comme $\zeta_v < R_v$, $Y_v(x(M))$ est défini. Dans k_v on a alors :

$$P(x(M), Y_v(x(M))) = P(x(M), y(M)) = 0 .$$

D'autre part, d'après (5),

$$|Y_v(x(M))|_v < \beta_v .$$

Enfin puisque $v \in T(M)$,

$$|y(M)|_v < \beta_v .$$

Le lemme suivant permet de conclure que, sous ces conditions, on a nécessairement $Y_v(x(M)) = y(M)$ c'est à dire que $v \in S(M)$ □

LEMME 2 — *Soient v une place de k et ξ, η_1, η_2 trois éléments de k_v, vérifiant :*

a) $P(\xi, \eta_1) = P(\xi, \eta_2) = 0$

b) $|\xi|_v < \beta_v$

c) $|\eta_i|_v < \beta_v$ *pour* $i = 1, 2$

Alors $\eta_1 = \eta_2$

Démonstration. On écrit :

$$0 = P(\xi, \eta_2) - P(\xi, \eta_1) = p_{01}(\eta_2 - \eta_1) + \sum_{\substack{j \geq 2 \\ i \geq 0}} p_{ij} \xi^i (\eta_2^j - \eta_1^j) + \sum_{i \geq 1} p_{i1} \xi^i (\eta_2 - \eta_1)$$

Si $\eta_1 \neq \eta_2$, cela donne :

$$0 \neq -P_{01} = \sum_{\substack{j\geq 2\\ i\geq 0}} P_{ij}\,\xi^i\,(\mathcal{D}_2^{j-1} + \mathcal{D}_2^{j-2}\mathcal{D}_1 + \cdots + \mathcal{D}_1^{j-1}) \;+\; \sum_{i\geq 1} P_{i1}\,\xi^i$$

En utilisant b) et c) on obtient alors

si v est une place finie : $\quad 0 < |P_{01}|_v < H_v(P)\,\beta_v \leq |P_{01}|_v$

si v est une place archimédienne : $\quad 0 < |P_{01}|_v < (1+\deg_x P)(\deg_y P)^2 H_v(P)\beta_v + \deg_x P\, H_v(P)\beta_v \leq |P_{01}|_v$

et donc dans les deux cas la contradiction désirée □

Il est maintenant facile de conclure la démonstration du théorème 6. (2) est également une conséquence du lemme 2. Ensuite d'après le lemme 1, on a :

$$(6)\quad \left| \frac{1}{[k:\mathbb{Q}]} \left[\sum_{v\in T(M)} d_v^k \operatorname{Log}\min(1,|x(M)|_v) - \sum_{v\in S(M)} d_v^k \operatorname{Log}\min(1,|x(M)|_v) \right] \right| \leq \frac{1}{[k:\mathbb{Q}]} \sum_{v\in M_k} d_v^k \operatorname{Log} \tau_v^{-1} = O(1)$$

Or d'après le théorème 2, on a

$$(7)\quad \frac{1}{[k:\mathbb{Q}]} \sum_{v\in S(M)} d_v^k \operatorname{Log}\min(1,|x(M)|_v) + \frac{1}{\deg x}\, h(x(M)) = O(1) + O\left(\sqrt{h(x(M))}\right)$$

En regroupant (6) et (7) on obtient donc :

$$\frac{1}{[k:\mathbb{Q}]} \sum_{v\in T(M)} d_v^k \operatorname{Log}\min(1,|x(M)|_v) = -\frac{1}{\deg x}\, h(x(M)) + O(1) + O\left(\sqrt{h(x(M))}\right)$$

C. Q. F. D.

Remarque. En raffinant légèrement la démonstration au niveau du lemme 1, on obtient le théorème 3 de [De 2]. On peut également le déduire directement du théorème 6.

COROLLAIRE — *Supposons, en plus des hypothèses du théorème 6, que C soit de genre non nul. Alors il n'existe qu'un nombre fini de points M sur C vérifiant $x(M) = p^m$, avec p premier et $m \geq 1$, et $y(M) \in \mathbb{Q}$.*

§ 2 AUTOUR DU THÉORÈME DE DECOMPOSITION DE WEIL

Le Théorème de Décomposition de Weil ([La 3] Ch 10 et [We] initialement) montre comment la décomposition arithmétique des valeurs d'une fonction rationnelle φ sur une courbe projective lisse est reliée à la décomposition en diviseurs premiers du diviseur des zéros et pôles de φ. En 1983, E. Bombieri [Bo 4] a énoncé un résultat qui précise la contribution de chacun des pôles dans la relation précédente. Ce résultat, cependant,

présente une inexactitude. Voici comment il faut modifier le "Main Theorem" de [Bo4]

2.1 Enoncé du résultat

Dans tout le §2, C sera une courbe projective lisse plongée dans $\mathbb{P}^n$, l'espace projectif de dimension n ; nous noterons $x_0, \ldots, x_n$ les fonctions coordonnées associées à ce plongement.

Pour $\alpha = 0, 1, \ldots, n$, soit $U_\alpha(k)$ l'ouvert de $C(k)$ constitué des points M de $C(k)$ tels que $x_\alpha(M) \neq 0$. Si v est une place de k, on définit une distance δ_v^α sur $U_\alpha(k)$ en posant :

$$\delta_v^\alpha(M,M') = \max_{\beta \neq \alpha} \left| \frac{x_\beta(M)}{x_\alpha(M)} - \frac{x_\beta(M')}{x_\alpha(M')} \right| \qquad \text{pour } M, M' \text{ dans } C(k)$$

Nous noterons alors δ_v l'application de $C(k) \times C(k)$ dans $[0, +\infty]$ définie par

$$\delta_v(M,M') = \inf_\alpha \delta_v^\alpha(M,M') \qquad \text{pour } M, M' \text{ dans } C(k)$$

où l'Inf est pris sur l'ensemble des indices $\alpha \in [0,n]$ tels que M, M' soient dans $U_\alpha(k)$.

Ceci étant, le résultat est le suivant.

THÉORÈME 7 — *Soient $\varphi : C \to \mathbb{P}^1$ une fonction rationnelle sur C définie sur k et Q un pôle de φ rationnel sur k.*

Alors il existe une M_k-constante multiplicative Δ, ne dépendant que du plongement $C \subset \mathbb{P}^n$ et de la fonction φ, telle que, pour tout point $M \neq Q$ dans $C(k)$, on ait :

(8) S'il existe $v \in M_k$ tel que $\delta_v(M,Q) < \Delta_v$ alors M n'est pas un pôle de φ.

$$(9) \quad \frac{1}{[k:\mathbb{Q}]} \sum_{\substack{v \in M_k \\ \delta_v(M,Q) < \Delta_v}} d_v^k \operatorname{Log}^+ |\varphi(M)|_v = -\frac{\operatorname{ord}_Q \varphi}{\deg \varphi} h(\varphi(M)) + O(1) + O\left(\sqrt{h(\varphi(M))}\right)$$

où les constantes intervenant dans les $O(\ldots)$ ne dépendent que du plongement $C \subset \mathbb{P}^n$ et de la fonction φ.

Remarque. En prenant pour C un modèle lisse de la courbe algébrique plane $P(x,y) = 0$ et φ égal à la fonction rationnelle x^{-1}, on obtient le théorème 6. Inversement, nous déduirons au paragraphe 2.4 le théorème 7 du théorème 6.

Exemple. Voici un exemple où, contrairement à l'énoncé de Bombieri dans [Bo4], on ne peut pas choisir $\Delta_v = 1$ pour tout v dans l'énoncé du théorème 7. On prend $k = \mathbb{Q}$,

C est la courbe de $\mathbb{P}^2$ d'équation $X^2+Y^2+2YZ=0$, on choisit $\varphi(X,Y,Z)=(Z,X)$ et $Q=(0,0,1)$.

On a alors $\mathrm{ord}_Q\varphi=-1$ et $\deg\varphi=2$. Considérons les points $M_h=(x_h,y_h,z_h)$, pour h entier positif, définis par

$$x_h=\frac{2^{h+1}3^h}{2^{2h}+3^{2h}}\quad,\quad y_h=-\frac{2.3^{2h}}{2^{2h}+3^{2h}}\quad,\quad z_h=1\quad.$$

Pour tout $h>0$, on a $M_h\in C(\mathbb{Q})$; pour toute place v de $\mathbb{Q}$, on a

$$\delta_v(M_h,Q)=\delta_v^2(M_h,Q)=\mathrm{Max}\,(|x_h|_v,|y_h|_v).$$

On a donc $\delta_v(M_h,Q)<1$ si et seulement si $v=2$ ou 3. Si l'on choisit $\Delta_v=1$ pour tout v dans l'énoncé du théorème 7, le terme de gauche dans (9) est équivalent, quand h tend vers $+\infty$, à $h\log 6$, celui de droite à $h\log 3$.

Cet exemple montre également qu'on ne peut pas prendre $\beta_v=1$ pour tout v dans l'énoncé du théorème 6.

De son résultat, E. Bombieri donne deux démonstrations. La première, de nature algébrique, est basée sur la Théorie des Hauteurs [La3] ; nous la reprenons en la détaillant au paragraphe 2.3 ; l'erreur de Bombieri se situe au niveau de son lemme p 299 dans [Bo4], qu'il faut remplacer par le lemme 1 du paragraphe 2.3

La seconde, de nature arithmétique, utilise son résultat sur les G-fonctions ([Bo1] ou Ch V Th 3) ; dans celle-ci, l'affirmation p 304, lignes 4-5-6 : "we can replace the condition $v\in S$ by the condition $\delta_v(P,Q)<1$ and introduce a further remainder term $O(1)$" n'est pas correcte (on le vérifie aisément sur l'exemple précédent) ; par contre, elle le devient si l'on remplace "$\delta_v(P,Q)<1$" par "$\delta_v(P,Q)<\Delta_v$" pour Δ_v convenablement choisi. Au paragraphe 2.4, nous proposons une troisième approche, arithmétique également, qui utilise le théorème 2.

Le point commun de ces démonstrations est qu'on utilise dans toutes le Théorème de Décomposition de Weil. Nous rappelons maintenant en quelques lignes les idées essentielles de cet important résultat.

2.2 Le Théorème de décomposition de Weil [La3]

Suivant S. Lang ([La3] Ch 10), nous parlerons de fonctions de Weil plutôt que de distributions de Weil comme Bombieri dans [Bo4].

Soit D un diviseur de Cartier sur C. On note $|D|$ son support. Une fonction de Weil associée au diviseur D est une fonction

$$\lambda : C(\bar{\mathbb{Q}}) \setminus |D| \times M_{\bar{\mathbb{Q}}} \longrightarrow \mathbb{R}$$

telle que

(1) Pour tout point M dans $C(\bar{\mathbb{Q}}) \setminus |D|$ et pour tout $v \in M_{\bar{\mathbb{Q}}}$ ($M_{\bar{\mathbb{Q}}}$ désigne l'ensemble des places de $\bar{\mathbb{Q}}$), $\lambda(M,v)$ ne dépend que de la restriction de v au corps de rationalité de D et de M.

(2) Si (U,f) représente D sur un ouvert (de Zariski) U, alors il existe une fonction M-bornée et M-continue.

$$\alpha : U \times M_{\bar{\mathbb{Q}}} \longrightarrow \mathbb{R}$$

telle que, pour tout point M dans $C(\bar{\mathbb{Q}}) \setminus |D|$, on ait

$$\lambda(M,v) = v \circ f(M) + \alpha(M,v)$$

Notes. 1) Ici, v désigne la valuation associée à la place v, c'est-à-dire

$$v = -\mathrm{Log}\,|\,|_v$$

2) Si λ est une fonction de Weil associée à D, nous noterons Λ qu'on appellera fonction de Weil multiplicative associée à D, la fonction

$$\Lambda = e^{-\lambda}$$

3) Sur une courbe lisse, il existe un isomorphisme (décrit dans [La3] Ch 10 § 2 p 253) entre le groupe des diviseurs de Cartier et le groupe des diviseurs de Weil. La courbe C étant supposée lisse, nous utiliserons plutôt cette dernière notion.

4) Si λ est une fonction de Weil, nous noterons (λ) son diviseur associé.

Fonction de Weil associée à un diviseur principal. Soit f une fonction rationnelle sur C, la fonction $\lambda_f : C(\bar{\mathbb{Q}}) \setminus |(f)| \times M_{\bar{\mathbb{Q}}} \longrightarrow \mathbb{R}$ définie par

$$\lambda_f(M,v) = v \circ f(P)$$

est une fonction de Weil associée au diviseur principal (f).

Dans la suite, nous utiliserons à plusieurs reprises les deux énoncés suivants, qui sont deux des résultats centraux de la théorie des fonctions de Weil. Le premier (CF [La3] Ch 10 Prop 2.2 p 256) est un résultat d'unicité; le second (CF [La3] Ch 10 Prop 3.2 p 259), un résultat d'existence.

PROPOSITION 1 — Soit λ une fonction de Weil dont le diviseur associé est 0. Alors λ est une fonction M-continue et bornée.

PROPOSITION 2 — Soient $d_1, \ldots, d_m$ m fonctions de Weil de diviseurs associés de la forme

$$(d_i) = Y + X_i$$

avec $X_i \geqslant 0$ pour $i = 1, 2, \ldots, m$ et telles que les supports des X_i n'aient pas de points en commun. Alors la fonction $d : C(\bar{\mathbb{Q}}) \setminus |Y| \times M_{\bar{\mathbb{Q}}} \longrightarrow \mathbb{R}$ définie par

$$d(M, v) = \inf_{1 \leq i \leq m} d_i(M, v)$$

est une fonction de Weil dont le diviseur associé est Y.

C'est ce dernier énoncé qui permet de conclure (CF Prop.4) la démonstration du Théorème de Décomposition de Weil qui affirme l'existence pour tout diviseur D sur une courbe projective lisse d'une fonction de Weil associée à D (Voir [La3] Ch10 Th3.5 pour les dimensions supérieures).

Pour tout point Q dans $C(\bar{\mathbb{Q}})$, nous noterons d_Q la fonction de Weil associée au diviseur Q (d'après la proposition 1, on peut parler de la fonction de Weil associée à un diviseur, à une fonction M-bornée près). On peut ([La3] §3 p 258) prolonger M-continument la fonction d_Q au point Q, en posant, pour toute place v de $\bar{\mathbb{Q}}$

$$d_Q(Q, v) = +\infty \qquad \text{c'est à dire} \qquad \Lambda_Q(Q, v) = 0$$

Considérons maintenant une fonction rationnelle φ non nulle sur C ; on note

$$(\varphi) = \sum_Q m_Q Q$$

son diviseur. La fonction de Weil

$$d_\varphi - \sum_Q m_Q d_Q$$

est associée au diviseur nul. D'après la proposition 1, elle est M-bornée ; il existe donc deux $M_{\mathbb{R}}$-constantes γ_1, γ_2 telles que pour tout (M, v) dans $C(\bar{\mathbb{Q}}) \times M_{\bar{\mathbb{Q}}}$, on ait :

$$(10) \qquad \gamma_1(v) + \sum_Q m_Q d_Q(M, v) \leqslant v \circ \varphi(M) \leqslant \sum_Q m_Q d_Q(M, v) + \gamma_2(v)$$

C'est sous cette forme qu'André Weil avait initialement énoncé son Théorème de Décomposition [We].

Des propositions 1 et 2, nous allons maintenant déduire un résultat qui nous permettra, au paragraphe 2.3 de définir la famille $(\Delta_v)_{v \in M_k}$ du théorème 7.

PROPOSITION 3 — Soient Q, Q' 2 points distincts dans $C(k)$. Alors la fonction $\mathrm{Min}(d_Q, d_{Q'})$ est M-majorée. Précisément, il existe une $M_{\mathbb{R}}$-constante $\gamma(Q, Q')$ qui ne dépend que de Q et Q' telle que pour tout (M, v) dans $C(\bar{\mathbb{Q}}) \times M_{\bar{\mathbb{Q}}}$, on ait :

$$\mathrm{Min}(d_Q(M, v), d_{Q'}(M, v)) \leqslant \gamma_v(Q, Q')$$

En effet, d'après la proposition 2, la fonction $\mathrm{Min}(d_Q, d_{Q'})$ est une fonction de Weil dont le diviseur associé est nul (Ecrire $(d_Q) = 0 + Q$ et $(d_{Q'}) = 0 + Q'$). D'après la proposition 1, c'est donc une fonction M-bornée □

Dans la proposition 3, nous n'avons écrit que la majoration de $\mathrm{Min}(d_Q, d_{Q'})$, la minoration n'étant, elle, pas très intéressante : en effet, on sait d'autre part ([La3] Ch 10 Prop 3.1 p258) que pour tout point Q dans $C(\bar{\mathbb{Q}})$, la fonction de Weil d_Q est M-minorée : il existe donc une $M_{\mathbb{R}}$-constante γ_Q telle que

$$\gamma_Q(v) \leq d_Q(M,v) \qquad \text{pour tout } (M,v) \text{ dans } C(\bar{\mathbb{Q}}) \times M_{\bar{\mathbb{Q}}}$$

Et, quitte à modifier un peu d_Q, on peut prendre γ_Q égale à la fonction nulle. Dans la suite, nous supposerons toujours que pour tout (M,v) dans $C(\bar{\mathbb{Q}}) \times M_{\bar{\mathbb{Q}}}$, on a

$$0 \leq d_Q(M,v) \qquad \text{c'est-à-dire} \qquad \Lambda_Q(M,v) \leq 1$$

Terminons ce paragraphe par la démonstration, à partir de la proposition 2 de l'existence d'une fonction de Weil associée au diviseur Q.

PROPOSITION 4 — Soit Q un point de C. Alors la fonction $\Lambda_Q : C(\bar{\mathbb{Q}}) \times M_{\bar{\mathbb{Q}}} \longrightarrow \mathbb{R}$, définie par

$$\Lambda_Q(M,v) = \mathrm{Min}(1, \delta_v(M,Q))$$

est une fonction de Weil multiplicative associée au diviseur Q.

Démonstration. Notons $i = (x_0, \ldots, x_n)$ le plongement de C dans $\mathbb{P}^n$ et pour tout couple d'indices (α,β) dans $[0,n]$ tel que $\alpha \neq \beta$, $f_{\alpha\beta}$ la fonction rationnelle

$$f_{\alpha\beta} = \frac{x_\beta}{x_\alpha}.$$

Soit $\alpha \in [0,n]$ tel que $x_\alpha(Q) \neq 0$. i étant un plongement, Q est le seul zéro commun aux fonctions $\varphi_{\alpha\beta} = f_{\alpha\beta} - f_{\alpha\beta}(Q)$ où β décrit l'ensemble $[0,n] - \{\alpha\}$. De plus, comme la courbe C est supposée lisse, c'est un zéro simple. On peut donc écrire :

$$(\varphi_{\alpha\beta}) = Q - Y_\alpha + X_{\alpha\beta}$$

où $Y_\alpha \geq 0$, $X_{\alpha\beta} \geq 0$ et où les supports des diviseurs $X_{\alpha\beta}$, où $\beta \neq \alpha$, n'ont pas de points en commun.

D'après la proposition 2, pour tout α tel que $x_\alpha(Q) \neq 0$, la fonction

$$d_\alpha = \min_{\beta \neq \alpha} v \circ \varphi_{\alpha\beta}$$

est une fonction de Weil associée au diviseur $Q - \gamma_\alpha$. Ecrivons le de la manière suivante :

$$(\lambda_\alpha) = -Q + \gamma_\alpha$$

D'autre part, on peut également écrire

$$(0) = -Q + Q$$

La proposition 2 montre alors que la fonction

$$-\operatorname{Min}\Big(0, \min_{\substack{\alpha,\\ x_\alpha(Q)\neq 0}} (-\lambda_\alpha)\Big) = \operatorname{Max}\Big(0, \max_{\substack{\alpha,\\ x_\alpha(Q)\neq 0}} \lambda_\alpha\Big)$$

est une fonction de Weil associée au diviseur Q. En revenant à la notation multiplicative, ceci signifie bien que la fonction Λ_Q de l'énoncé de la proposition 4 est une fonction de Weil multiplicative associée au diviseur Q □

2.3 Approche algébrique

Avant d'aborder la première démonstration du théorème 7, remarquons que son résultat demeure inchangé si l'on fait une extension du corps de base ; nous pourrons donc grossir à loisir le corps k au cours des deux paragraphes suivants. Dans celui-ci, nous supposons que k est un corps de définition pour tous les zéros et pôles de la fonction φ.

Dans la suite, Λ_Q désigne la fonction de Weil multiplicative associée à Q de la proposition 4 et λ_Q sa fonction de Weil additive associée ($\lambda_Q = -\operatorname{Log}\Lambda_Q$). Signalons cependant que le raisonnement que l'on va faire reste valable si λ_Q est une fonction de Weil quelconque associée à Q.

Ceci étant précisé, on choisit pour Δ une M_k-constante multiplicative vérifiant

$$(11) \qquad \Delta_v \leq \min_{\substack{Q_1,Q_2\in Z(\varphi)\cup P(\varphi)\\ Q_1\neq Q_2}} e^{-\gamma_v(Q_1,Q_2)} \qquad \text{pour tout } v\in M_k$$

où $Z(\varphi)$ (resp $P(\varphi)$) désigne l'ensemble des zéros (resp. des pôles) de φ et $\gamma(Q_1,Q_2)$ la M_k-constante de la proposition 3.

Il est clair, alors, d'après la proposition 3, que la relation (8) du théorème 7 est satisfaite ; nous allons montrer que la relation (9) l'est également.

LEMME 1 — *Soient Q un pôle de φ et v une place de k. Alors, pour tout point M dans $C(k)$ tel que $\Lambda_Q(M,v) < \Delta_v$, on a*

$$(12) \qquad \operatorname{Log}|\varphi(M)|_v = -\operatorname{ord}_Q\varphi\ \lambda_Q(M,v) + O_v(1)$$

$$(13) \qquad \operatorname{Log}^+|\varphi(M)|_v = \operatorname{Log}|\varphi(M)|_v + O'_v(1)$$

où $O_v(1)$ (resp. $O'_v(1)$) est une fonction de M, bornée par une quantité ne dépendant que de C et de φ et nulle pour tout $v\in M_k$ sauf un nombre fini. Précisément, on a $O_v(1)=0$ (resp. $O'_v(1)=0$) pour les places v de k telles que $\gamma_1(v)=\gamma_2(v)=\operatorname{Log}\Delta_v=0$, γ_1 et γ_2 étant les M_k-constantes de (10).

Démonstration. Supposons que $\Lambda_Q(M,v) < \Delta_v$. Alors à cause de la proposition 3 pour tout Q', zéro ou pôle de φ distinct de Q, on a

$$\Lambda_{Q'}(M,v) \geqslant \Delta_v \quad .$$

La relation (10) donne alors :

$$-\gamma_2(v) + \deg\varphi \operatorname{Log}\Delta_v - \operatorname{ord}_Q\varphi\, d_Q(M,v) \leqslant \operatorname{Log}|\varphi(M)|_v \leqslant -\operatorname{ord}_Q\varphi\, d_Q(M,v) + \deg\varphi \operatorname{Log}^+\Delta_v^{-1} - \gamma_2(v)$$

Ceci démontre (12). Pour (13) on écrit

$$0 \leqslant \operatorname{Log}^+|\varphi(M)|_v - \operatorname{Log}|\varphi(M)|_v \leqslant \deg\varphi \operatorname{Log}\Delta_v + \gamma_2(v) \qquad \square$$

Du lemme 1, on déduit que si Q est un pôle de φ alors

$$\frac{1}{[k:\mathbb{Q}]} \sum_{\substack{v\in M_k,\\ \Lambda_Q(M,v)<\Delta_v}} d_v^k \operatorname{Log}^+|\varphi(M)|_v = \frac{-\operatorname{ord}_Q\varphi}{[k:\mathbb{Q}]} \sum_{\substack{v\in M_k\\ \Lambda_Q(M,v)<\Delta_v}} d_v^k d_Q(M,v) + O(1)$$

et donc, quitte à modifier un peu le $O(1)$

$$\frac{1}{[k:\mathbb{Q}]} \sum_{\substack{v\in M_k,\\ \Lambda_Q(M,v)<\Delta_v}} d_v^k \operatorname{Log}^+|\varphi(M)|_v = \frac{-\operatorname{ord}_Q\varphi}{[k:\mathbb{Q}]} \sum_{v\in M_k} d_v^k d_Q(M,v) + O(1)$$

c'est à dire

$$\frac{1}{[k:\mathbb{Q}]} \sum_{\substack{v\in M_k\\ \Lambda_Q(M,v)<\Delta_v}} d_v^k \operatorname{Log}^+|\varphi(M)|_v = -(\operatorname{ord}_Q\varphi)\, h_{d_Q}(M) + O(1)$$

où h_{d_Q} désigne la hauteur associée à la fonction de Weil d_Q ([La3] Ch 10 §4 p 263). Mais, à cause du théorème 4.3 du chapitre 10 de [La3] d'une part et de l'unicité du morphisme vérifiant 4.3.2 ([La3] p 265), de $\operatorname{Pic}(C)$ dans l'espace des fonctions réelles sur C modulo les fonctions bornées d'autre part ([La3] Ch 4 Th 5.1 p 93), on a

$$h_{d_Q} = h_Q + O(1)$$

où h_Q désigne la hauteur associée à la classe du diviseur Q dans $\operatorname{Pic}(C)$, le groupe de Picard de la courbe C.

On obtient donc

$$(14) \qquad \frac{1}{[k:\mathbb{Q}]} \sum_{\substack{v\in M_k,\\ \Lambda_Q(M,v)<\Delta_v}} d_v^k \operatorname{Log}^+|\varphi(M)|_v = -(\operatorname{ord}_Q\varphi)\, h_Q(M) + O(1)$$

où les constantes intervenant dans le $O(\ldots)$ ne dépendent que du plongement $C \subset \mathbb{P}^n$ et de la fonction φ.

Le résultat suivant est le point essentiel de la démonstration.

LEMME 2 — Pour tous points Q, Q' dans C, on a

$$h_{Q'} = h_Q + O(1) + O(\sqrt{h_Q})$$

où les constantes qui interviennent dans les $O(\dots)$ ne dépendent que de C, Q et Q'.

Démonstration. Si la courbe C est de genre $g = 0$, le résultat est évident : en effet, dans ce cas, $Q - Q'$ est un diviseur principal et on a donc :

$$h_{Q'} = h_Q + O(1)$$

Le cas $g \geqslant 1$ est lui, traité dans [La3] (Ch 5 Prop 5.4 p 115). Le résultat y apparaît comme une conséquence de la quadraticité de la hauteur sur les variétés abeliennes. Rappelons rapidement comment.

On plonge la courbe C dans sa jacobienne J. J est une variété abélienne qui de plus est "self duale", ce qui signifie qu'on peut, via un isomorphisme construit à partir d'un certain diviseur δ sur $J \times J$, identifier J et $\mathrm{Pic}_0(J)$ ([La3] Ch 5 Th 5.1 p 113). D'après un théorème de Néron ([La3] Ch 5 Th 3.1 p 106 ou [Ne] Th 5 p 300), h_δ est quadratique sur $J \times J$. Des propriétés du diviseur δ, on déduit ensuite que h_δ est une forme bilinéaire sur J ([La3] Ch 5 Prop 4.3 p 112) et que la forme quadratique $-h_\delta(x,x)$ est symétrique positive ([La3] Ch 5 Th 5.2 p 114).

La démonstration du lemme 2 est maintenant facile. Posons $b = Q - Q'$, l'isomorphisme $S : \mathrm{Pic}_0(J) \longrightarrow J$ donne

$$h_b(x) = h_\delta(x, S(b)) + O(1)$$

On obtient donc, grâce à l'inégalité de Schwarz

$$(15) \quad |h_b(x)| = O(\sqrt{h_\delta(x,x)}) + O(1)$$

Or, le diviseur dont provient $-h_\delta(x,x)$ a une restriction à C de degré positif ; $-h_\delta(x,x)$ est donc, d'après le corollaire 3.5 du chapitre 4 de [La3], quasi-équivalente à un multiple de h_Q. On déduit donc de (15)

$$h_b = h_Q - h_{Q'} = O(\sqrt{h_Q}) \qquad \square$$

On conclut maintenant aisément la démonstration du théorème 7. En remarquant qu'à cause de (10) on a

$$\frac{1}{[k:\mathbb{Q}]} \sum_{\substack{v \in M_k, \\ \forall Q \in \Phi, \lambda_Q(M,v) \geqslant \Delta_v}} d_v^k \, \mathrm{Log}^+ |\varphi(M)|_v = O(1) \quad ,$$

on déduit de (14) que :

$$(16) \qquad -\sum_{Q\in R(\varphi)} \mathrm{ord}_Q\varphi \; h_Q(M) = h(\varphi(M)) + O(1)$$

Le lemme 2 permet alors d'en tirer

$$h_Q(M) = \frac{1}{\deg\varphi}\, h(\varphi(M)) + O(1) + O\left(\sqrt{h(\varphi(M))}\right)$$

Et on peut donc maintenant réécrire (14)

$$\frac{1}{[k:\mathbb{Q}]} \sum_{\substack{v\in M_k,\\ \lambda_Q(M,v)<\Delta_v}} d_v^k \,\mathrm{Log}^+ |\varphi(M)|_v = -\frac{\mathrm{ord}_Q\varphi}{\deg\varphi}\, h(\varphi(M)) + O(1) + O\left(\sqrt{h(\varphi(M))}\right)$$

où l'on vérifie facilement que les constantes qui interviennent dans les $O(\dots)$ ne dépendent que de C et de φ.

C. Q. F. D.

Remarques. 1) Comme le fait remarquer Bombieri dans [B04], si la courbe C est de genre 0, alors on peut supprimer le terme $O\left(\sqrt{h(\varphi(M))}\right)$ dans la relation (9) du théorème 7.

2) Le lemme 1 montre que si la famille $(\Delta_v)_{v\in M_k}$ est choisie vérifiant (11), alors, la relation (9) du théorème 7 reste valide si on y remplace Log^+ par Log.

2.4 Approche arithmétique.

Notre but dans ce paragraphe est de montrer comment on peut éviter l'utilisation du théorème de Néron dans la démonstration précédente et remplacer cet argument algébrique par un argument arithmétique.

A cause de la relation suivante, valable pour toute M_k-constante Δ,

$$(17) \quad \sum_{Q\in R(\varphi)} \left[\frac{1}{[k:\mathbb{Q}]} \sum_{\substack{v\in M_k,\\ \delta_v(M,Q)<\Delta_v}} d_v^k \,\mathrm{Log}^+ |\varphi(M)|_v + \frac{\mathrm{ord}_Q\varphi}{\deg\varphi}\, h(\varphi(M)) \right] = O(1)$$

il suffit, pour obtenir (9), de montrer que si Q est un pôle de φ, on a, pour Δ bien choisi

$$(18) \quad \frac{1}{[k:\mathbb{Q}]} \sum_{\substack{v\in M_k\\ \delta_v(M,Q)<\Delta_v}} d_v^k \,\mathrm{Log}^+ |\varphi(M)|_v \leqslant -\frac{\mathrm{ord}_Q\varphi}{\deg\varphi}\, h(\varphi(M)) + O(1) + O\left(\sqrt{h(\varphi(M))}\right)$$

Nous allons le démontrer dans un cas particulier auquel nous nous ramènerons ensuite.

1er cas : $\mathrm{ord}_Q\varphi = -1$

Posons $z = \frac{1}{\varphi}$. z est alors une uniformisante en Q

LEMME 1 — Il existe ψ, une fonction rationnelle sur C, qui soit un élément primitif de $\bar{\mathbb{Q}}(C)$ sur $\bar{\mathbb{Q}}(z)$, qui ait un zéro au point Q et qui n'ait ni zéros ni pôles aux autres zéros de z.

Démonstration. On se donne tout d'abord θ_1 un élément primitif de $\bar{\mathbb{Q}}(C)$ sur $\bar{\mathbb{Q}}(z)$. Soit ensuite n_0 un entier tel que la fonction $z^{n_0}\theta_1$ n'ait pas de pôles aux zéros de z et soit nulle au point Q. Enfin, en utilisant le théorème de Riemann-Roch, on construit une fonction rationnelle sur C, θ_2, qui soit nulle au point Q et qui prenne des valeurs non nulles aux autres zéros de la fonction z.
Alors, sauf pour un nombre fini de $t \in \bar{\mathbb{Q}}$, la fonction $\psi = z^{n_0}\theta_1 + t\theta_2$ satisfait la conclusion du lemme 1 □

Considérons maintenant le polynôme $P = P_q Y^q + \cdots + P_1 Y + P_0$, irréductible dans $\bar{\mathbb{Q}}[x,Y]$ ($P_i \in \bar{\mathbb{Q}}[x]$ pour $i = 0,1,\ldots,q$) et vérifiant

$$P(z,\psi) = 0$$

Comme on peut grossir le corps de base, on peut supposer que ψ est définie sur k et que P est à coefficients dans k. Par définition du degré (1), on a

$$\deg_Y P = \deg z = \deg \varphi$$

Ensuite, d'après le théorème 8.3 du chapitre 1 de [Fo] (p50), $P_q(0) \neq 0$ et

$$P(0,Y) = P_q(0) \prod_{Q' \in Z(z)} (Y - \psi(Q'))^{\operatorname{ord}_{Q'} z}$$

Par construction de ψ, 0 est donc une racine simple du polynôme $P(0,Y)$ et le couple $(0,0)$ un point régulier de la courbe algébrique plane $P(x,y) = 0$. On applique alors le théorème 6 aux couples $(z(M), \psi(M))$ qui sont des points de cette courbe. On obtient que, pour tout point $M \neq Q$ dans $C(k)$,

(19) S'il existe $v \in M_k$ tel que $|\psi(M)|_v < \beta_v$ alors $z(M) \neq 0$

$$(20)\quad \frac{1}{[k:\mathbb{Q}]} \sum_{\substack{v \in M_k \\ |\psi(M)|_v < \beta_v}} d_v^k \operatorname{Log}^+ |\psi(M)|_v = \frac{1}{\deg \varphi} h(\varphi(M)) + O(1) + O\left(\sqrt{h(\varphi(M))}\right)$$

où β est la M_k-constante du théorème 6 associée à la courbe $P(x,y)=0$ et au point $(0,0)$.
Il reste maintenant à remplacer "$|\psi(M)|_v < \beta_v$" par une condition du type "$\delta_v(M,Q) < \Delta_v$".

Quitte à le composer par un automorphisme de $\mathbb{P}^n$, on peut supposer que le plongement $C \subset \mathbb{P}^n$, donné par les coordonnées $x_0, \ldots, x_n$, est tel que

$$x_0(Q) = 1 \quad \text{et} \quad x_1(Q) = x_2(Q) = \ldots = x_n(Q) = 0$$

Alors pour tout point M dans $C(k)$ tel que $x_0(M) \neq 0$ et pour toute place v de k, on a

$$\delta_v(M,Q) = \delta_v^0(M,Q) = \max_{1 \leq i \leq n} \left| \frac{x_i(M)}{x_0(M)} \right|_v$$

D'autre part, sur un voisinage de Zariski U de Q, ψ est donné par

$$\psi(M) = \frac{a(x_0(M), \ldots, x_n(M))}{b(x_0(M), \ldots, x_n(M))}$$

où $a, b \in k[X_0, \ldots, X_n]$ sont deux polynômes homogènes de même degré avec de plus b non nul sur U. En outre $\psi(Q) = 0$ impose

$$a(1, 0, \ldots, 0) = 0$$

Il est clair, sur cette description de ψ, qu'il existe une M_k-constante Δ telle que pour tout (M,v) dans $C(k) \times M_k$, on ait :

si $\delta_v(M,Q) < \Delta_v$ alors $|\psi(M)|_v < \beta_v$

De (19) et (20), on déduit donc maintenant que, pour tout point M dans $C(k)$

(21) S'il existe $v \in M_k$ tel que $\delta_v(M,Q) < \Delta_v$ alors M n'est pas un pôle de φ.

$$(22) \quad \frac{1}{[k:\mathbb{Q}]} \sum_{\substack{v \in M_k, \\ \delta_v(M,Q) < \Delta_v}} d_v^k \operatorname{Log}^+ |\varphi(M)|_v \leqslant \frac{1}{\deg \varphi} h(\varphi(M)) + O(1) + O\left(\sqrt{h(\varphi(M))}\right)$$

où les constantes intervenant dans les $O(\ldots)$ ne dépendent que de $C \subset \mathbb{P}^n$ et de φ.

Avant d'aborder le cas général, notons que, quitte à modifier un peu Δ, (21) et (22) restent valables si l'on remplace la fonction $(M,v) \mapsto \delta_v(M,Q)$ par n'importe quelle fonction de Weil multiplicative Λ_Q associée au diviseur Q (Voir Prop. 1 et 4). Ceci va nous être utile dans la suite.

2ème cas : cas général.

On se ramène au cas précédent par des arguments essentiellement algébriques. Posons $N = -\operatorname{ord}_Q \varphi$. On remarque tout d'abord que si le théorème 7 est vrai pour une fonction rationnelle φ, alors il est vrai pour toute fonction rationnelle de la forme $a\varphi^m$ où $a \in k^*$ et $m \in \mathbb{N}$. On peut donc supposer que φ n'est pas de la forme $a\psi^m$ avec $a \in k^*$ et $m \geqslant 2$. Alors, d'après le théorème de Capelli ([Schi3] I.13 TH 21 p 91), le corps $\bar{\mathbb{Q}}(C)(\sqrt[N]{\varphi})$ est une extension de degré N du corps $\bar{\mathbb{Q}}(C)$; c'est un corps de fonctions d'une

variable, c'est donc le corps des fonctions rationnelles d'une courbe projective lisse C', qu'on peut supposer définie sur k et qui est un revêtement de degré N de C. On note

$$\pi : C' \longrightarrow C$$

la surjection de ce revêtement.

Soit $\pi^* Q = \sum_{i=1}^{r} m_i Q_i$, le diviseur image réciproque de Q par l'application π. On a évidemment

$$\mathrm{ord}_{Q_i} z^{\frac{1}{N}} = 1 \qquad \text{pour } i = 1, 2, \ldots, r.$$

On peut donc appliquer le résultat du cas précédent à la fonction $\varphi^{\frac{1}{N}}$ sur C' et aux points Q_i qui en sont des pôles simples. En remarquant que, avec des notations évidentes,

$$\deg_C z = \deg_{C'} z^{\frac{1}{N}}$$

on obtient qu'il existe une M_k-constante multiplicative Δ' telle que pour tout indice $i \in [1, n]$ et tout point M dans $C(k)$, si M' désigne un point de la fibre $\pi^{-1}(M)$ et $k(M')$ un corps de définition de M', alors

(23) S'il existe $v \in M_{k(M')}$ tel que $\Lambda'_{Q_i}(M', v) < \Delta'_v$, alors M' n'est pas un pôle de $\varphi^{\frac{1}{N}}$

$$(24)\quad \frac{1}{[k(M'):\mathbb{Q}]} \sum_{\substack{v \in M_{k(M')} \\ \Lambda'_{Q_i}(M', v) < \Delta'_v}} d_v^{k(M')} \mathrm{Log}^+ |\varphi(M')|_v^{\frac{1}{N}} \leqslant \frac{1}{\deg \varphi} h(\varphi(M')^{\frac{1}{N}}) + O(1) + O\left(\sqrt{h(\varphi(M')^{\frac{1}{N}})}\right)$$

Λ'_{Q_i} désignant une fonction de Weil multiplicative associée au diviseur Q_i.

On multiplie ensuite les inégalités (24) par N, puis on les ajoute. En remarquant que $\varphi(M') = \varphi(M)$, on aboutit alors à

$$(25)\quad \frac{1}{[k(M'):\mathbb{Q}]} \sum_{v} d_v^{k(M')} \mathrm{Log}^+ |\varphi(M)|_v \leqslant \frac{N}{\deg \varphi} h(\varphi(M)) + O(1) + O\left(\sqrt{h(\varphi(M))}\right)$$

la sommation portant sur les places v de $k(M')$ telles que, pour un indice $i \in [1, r]$, on ait $\Lambda'_{Q_i}(M', v) < \Delta'_v$.

Posons $\Delta_v = (\Delta'_v)^{\frac{1}{N}}$ pour tout v dans M_k et notons Λ' la fonction de Weil sur C'

$$\Lambda' = \prod_{i=1}^{r} \Lambda'^{m_i}_{Q_i}$$

Alors il est clair que

(26) Si $\Lambda'(M', v) < \Delta_v$ alors il existe un indice $i \in [1, r]$ tel que $\Lambda'_{Q_i}(M', v) < \Delta'_v$

Or Λ' est une fonction de Weil multiplicative associée au diviseur $\pi^* Q$ et d'après la proposition 2.6 du chapitre 10 de [La3] (fonctorialité des fonctions de Weil), la fonction $\Lambda_Q \circ \pi$ en est une autre (Λ_Q désigne ici la fonction de Weil multiplicative sur C associée au diviseur Q de la proposition 4). On peut donc, quitte à modifier un peu la famille $(\Delta_v)_{v \in M_k}$, remplacer Λ' par $\Lambda_Q \circ \pi$ dans (26). De (23), (25) et (26) on déduit alors :

(27) S'il existe $v \in M_k$ tel que $\Lambda_Q(M,v) < \Delta_v$ alors M n'est pas un pôle de φ

(28) $$\frac{1}{[k:\mathbb{Q}]} \sum_{\substack{v \in M_k, \\ \Lambda_Q(M,v) < \Delta_v}} d_v^k \operatorname{Log}^+ |\varphi(M)|_v \leq \frac{N}{\deg \varphi} h(\varphi(M)) + O(1) + O\left(\sqrt{h(\varphi(M))}\right)$$

C. Q. F. D

Notes. 1) Via cette seconde démonstration, le lemme 2 du paragraphe 2.3 devient un corollaire du théorème 7.

2) Dans les théorèmes 6 et 7, les constantes ne dépendent pas du corps k. C'est une remarque importante : en effet, dans le cas contraire, à cause du résultat récent de G. Faltings [Fa], ces théorèmes n'auraient d'intérêt que pour les courbes de genre $g < 2$.

3) Du théorème 7, on peut déduire un résultat intéressant qui généralise un théorème de Runge (Voir [Mo] Ch 28 Th 1) sur la finitude des points entiers de certaines courbes algébriques. (Voir [Bo4] V. Théorème p 305).

CHAPITRE VIII

Problèmes divers

§1 QUESTIONS DE MÉTHODE

En définitive, on peut dégager en gros, trois méthodes, des travaux de ces dernières années sur les valeurs de fonctions algébriques. Les deux premières, de nature arithmétique, sont, à l'origine, des méthodes transcendantes : la méthode de Gel'fond, mise en oeuvre par T. Schneider et P. Bundschuh et qui est développée dans ce mémoire (CF Ch IV) et la méthode de Siegel, adaptée tout d'abord par V.G. Sprindzuk au cadre des fonctions algébriques et reprise ensuite par E. Bombieri dans celui des G- fonctions (CF Ch V).

Nous avons ébauché au chapitre V une rapide comparaison de ces deux méthodes. La première apparaît peut-être plus simple dans sa conception, plus naturelle. Reste que Bombieri aborde avec la seconde un cas plus général, celui des G- fonctions. Mais nous allons voir en appendice, qu'on peut également atteindre ce cas par la méthode de Gel'fond, et qui plus est, d'une manière plus élémentaire, la démonstration que nous proposons, évitant plusieurs arguments délicats utilisés chez Bombieri, entre autres le théorème de Dwork-Robba.

La troisième méthode (CF Ch VII §2), due également à Bombieri, est, elle, d'inspiration purement algébrique. Elle donne essentiellement le même résultat, mais présente l'avantage d'en expliquer l'origine, à savoir la théorie des hauteurs sur les courbes algébriques. On comprend mieux, dès lors, que les méthodes arithmétiques aient abouti toutes deux à ce même résultat, et notamment à

l'estimation du reste en $O(\sqrt{h})$, qui provient en fait de la quadraticité de la hauteur sur les variétés abéliennes; pour cette raison, cette estimation semble d'ailleurs, la meilleure possible.

Cette dernière méthode est évidemment la plus satisfaisante des trois. Il serait très intéressant de voir s'il est possible de l'étendre, elle aussi, aux G-fonctions. Cela exigerait certes, d'introduire un nouveau formalisme généralisant aux systèmes différentiels la notion de fonctions de Weil et de hauteurs sur les courbes algébriques, mais une approche algébrique de ce problème ouvrirait sans doute une nouvelle voie, en expliquant le pourquoi des méthodes arithmétiques.

§2 UNE TENTATIVE INFRUCTUEUSE

Soit P un polynôme irréductible dans $k(X)[Y]$ vérifiant l'hypothèse habituelle H_0; le théorème 2 énonce alors que si ξ est un élément de k non nul et non racine de l'unité et Q un diviseur dans $k[Y]$ de $P(\xi, Y)$, on a alors

$$(1)\qquad \frac{\sum_{v \in S(\xi,Q)} d_v^K \operatorname{Log}\min(1,|\xi|_v)}{\sum_{v \in M_K} d_v^K \operatorname{Log}\min(1,|\xi|_v)} = \frac{\deg Q}{\deg_Y P} + O\left(h(\xi)^{-\frac{1}{2}}\right)$$

On peut se demander si le résultat subsiste si l'on ne tient compte dans les deux sommes du membre de gauche, que des places au dessus d'un nombre premier p fixé possédant au moins un prolongement dans $M_K(\xi)$, précisément si

$$(2)\qquad \frac{\sum_{\substack{v \in S(\xi,Q)\\ v/p}} d_v^K \operatorname{Log}\min(1,|\xi|_v)}{\sum_{\substack{v \in M_K\\ v/p}} d_v^K \operatorname{Log}\min(1,|\xi|_v)} = \frac{\deg Q}{\deg_Y P} + O\left(h(\xi)^{-\frac{1}{2}}\right)$$

pour tout p dans $M_K(\xi)|_{\mathbb{Q}} = \{w \in M_{\mathbb{Q}} \mid \exists v \in M_K(\xi),\ v/w\}$

La relation (2) serait tout aussi naturelle, a priori, que (1); de plus, elle est vraie si ξ est une puissance assez grande d'un nombre rationnel (Utiliser la prop. 1 du Ch VI et le fait que si x est un nombres rationnel non nul, les nombres réels $\operatorname{Log}|x|_v$ où $v \in M_{\mathbb{Q}}(\xi)$ sont linéairement indépendants sur $\mathbb{Q}$). Cependant, l'inégalité (2) est fausse en général. Voici un contre-exemple.

On prend $P = Y^2 + X^2 + 2X$ et $(\xi_k)_{k\geq 1}$ la suite de nombres rationnels donnés par

$$\xi_k = -\frac{2p^{2k}}{1+p^{2k}}$$

où p est un nombre premier fixé. Comme dans cet exemple, on a $K = \mathbb{Q}$, le terme de gauche dans (2) vaut 0 ou 1. Or pour tout $h \geq 1$, on peut prendre Q de degré égal à 1 et donc $\deg Q / \deg_Y P = 1/2$ puisque le polynôme $P(\xi_h, Y)$ admet la solution rationnelle $\quad \vartheta_h = \dfrac{2p^h}{1+p^{2h}}$.

§3 THÉORÈME D'IRRÉDUCTIBILITÉ DE HILBERT

3.1 Progressions géométriques

Les deux premiers paragraphes laissent donc peu d'espoir quant à une amélioration sensible du théorème 2. Le résultat du chapitre VI paraît, lui, par contre, largement perfectible. Pour l'essentiel, le théorème 5 affirme que toute partie hilbertienne d'un corps de nombres k contient beaucoup de progressions géométriques. A notre avis, la conjecture suivante est raisonnable.

CONJECTURE — *Soient P un polynôme irréductible dans $k(X)[Y]$ et possédant une racine dans $k((X))$ et ξ un élément de k non nul et non racine de l'unité. Alors le polynôme $P(\xi^m, Y)$ est irréductible dans $k[Y]$ si m est un entier suffisamment grand.*

Signalons en liaison avec cette conjecture, l'énoncé suivant (Voir [Se] II.1.7.7), qui est une conséquence du théorème de Siegel-Mahler-Lang (Voir par exemple [Se] I.1)

THÉORÈME — *Soit $S = \{p_1, \dots, p_n\}$ un ensemble fini de nombres premiers. Pour tout nombre rationnel α, on note $Q_{\alpha,S}$ l'ensemble des nombres rationnels de la forme*

$$t = \alpha \pm \prod_{i=1}^{n} p_i^{m_i} \quad , \quad m_i \in \mathbb{Z}$$

Alors si Ω est un ensemble mince dans $\mathbb{Q}$ (i.e complémentaire d'une partie hilbertienne de $\mathbb{Q}$), pour tout $\alpha \in \mathbb{Q}$ sauf un nombre fini, l'ensemble

$$\Omega \cap Q_{\alpha,S}$$

est fini.

Un corollaire de ce résultat est que si P est un polynôme irréductible dans $\mathbb{Q}(X)[Y]$, alors sauf pour un nombre fini de $\alpha \in \mathbb{Q}$, la conjecture est vraie pour le polynôme $P_\alpha = P(X+\alpha, Y)$.

3.2 Nombres premiers

Nous supposons dans ce paragraphe P irréductible dans $\mathbb{Q}(X)[Y]$. On sait depuis longtemps que l'ensemble $H_{P,\mathbb{Q}} = \{x \in \mathbb{Q} / P(x,Y) \text{ irréductible dans } \mathbb{Q}[Y]\}$ contient une infinité de nombres premiers. Nous avons montré au chapitre II que sous certaines hypothèses, l'ensemble $H_{P,\mathbb{Q}}$ les contenait tous sauf un nombre fini. (Cf Ch II Th 0 et corollaires 1 & 2 du Th 1). Il est naturel de se demander s'il s'agit d'un résultat général.

La réponse est certainement négative ; cependant, à notre connaissance, on ne dispose que de contre-exemples conjecturaux : le polynôme $P = Y^2 + 1 - X$ en est un ; en effet, le polynôme $P(p,Y)$ se décompose si le nombre premier p s'écrit $p = y^2 + 1$ avec y dans $\mathbb{Z}$; or on pense généralement qu'il existe une infinité de nombres premiers p de cette forme.

Ce dernier problème est un cas particulier d'une conjecture plus générale, appelée hypothèse de Schinzel et qui est la suivante.

HYPOTHÈSE DE SCHINZEL — *Soient s un entier et $f_1, \ldots, f_s$, s polynômes irréductibles dans $\mathbb{Z}[X]$. On suppose qu'il n'existe pas d'irréductible $p \in \mathbb{Z}$ qui divise toutes les valeurs $\prod_{i=1}^{s} f_i(x)$ du polynôme $\prod_{i=1}^{s} f_i$ avec entiers x. Alors l'ensemble des entiers x pour lesquels les $f_i(x)$, $i = 1, 2, \ldots, s$ sont tous des nombres premiers (i.e des irréductibles de $\mathbb{Z}$) est un ensemble infini.*

A. Schinzel, [Schi2], a montré que ce résultat permettrait de résoudre un grand nombre de problèmes arithmétiques classiques, par exemple le problème précédent (Prendre $s=1$ et $f_1 = X^2 + 1$) ou encore le problème des nombres premiers jumeaux (Prendre $s=2$ $f_1 = X$, $f_2 = X+2$).

Malheureusement, cette conjecture semble encore aujourd'hui hors d'atteinte. Et pourtant comme il apparait si l'on remplace l'anneau $A = \mathbb{Z}$ par l'anneau $A = k[Y]$, avec k corps de nombres, il ne s'agit là que (!) d'une version sur $\mathbb{Z}$ du théorème d'irréductibilité de Hilbert, l'hypothèse de non divisibilité des $\prod_{i=1}^{s} f_i(x)$ par un irréductible de A étant automatiquement réalisée pour $A = k[Y]$ ...

APPENDICE : VALEURS DE G-FONCTIONS

Nous proposons ici une nouvelle approche du résultat de Bombieri sur les G-fonctions ([Bo1] ou Ch V §1). La démonstration que nous allons donner est une généralisation au cadre des G-fonctions de la méthode développée pour les fonctions algébriques (Cf Ch IV). Elle évite plusieurs arguments délicats utilisés chez Bombieri, notamment le théorème de Dwork-Robba.

1. G-opérateurs différentiels

Soient k un corps de nombres, n un entier et $A \in M_{n\times n}(k(x))$ une matrice $n\times n$ à coefficients dans $k(x)$. On s'intéresse à l'opérateur différentiel $L = D - A$.

R désignera un dénominateur dans $k[x]$ de la matrice A; on a donc

$$R \in k[x] \quad \text{et} \quad B = RA \in M_{n\times n}(k[x])$$

On notera aussi

$$\delta = \operatorname{Max}\left(\deg R, \operatorname*{Max}_{\substack{1\le i\le n\\ 1\le j\le n}} \deg B_{ij}\right)$$

où les B_{ij}, $i=1,2,\dots,n$, $j=1,2,\dots,n$ sont les coefficients de la matrice B.

PROPOSITION 1 — *Soient Ω une extension de k et z un élément de Ω, ordinaire pour L (i.e. $R(z)\neq 0$). Soit $\underline{y} = \sum_{m\ge 0} \underline{y}_{z,m}(x-z)^m$ un vecteur à composantes dans $\Omega[[x-z]]$ solution de $L\underline{y} = 0$. Alors pour tout entier $M \ge 0$, il existe une famille $(P_{j,m})_{\substack{0\le j\le \delta\\ 0\le m\le M}}$ de matrices $n\times n$ à coefficients dans le corps k vérifiant :*

$$(1) \qquad R(z)\,\underline{y}_{z,M+1} = \sum_{j=0}^{\delta}\left(\sum_{m=0}^{M} P_{j,m}\cdot \underline{y}_{z,m}\right) z^j$$

Note : Ici et dans la suite, on note $\underline{u} = \begin{bmatrix} u_1 \\ | \\ u_n \end{bmatrix}$, soit "verticalement", les vecteurs de Ω^n.

Démonstration. Dire que $\underline{y}$ est une solution de $L\underline{y} = 0$ signifie que

$$(2) \qquad R_z\, D\,\underline{y}_z = B_z\,\underline{y}_z$$

où R_z, B_z et $\underline{y}_z$ sont respectivement définis par $R_z(X-z) = R$, $B_z(X-z) = B$ et $\underline{y}_z(X-z) = \underline{y}$.

(2) s'écrit

$$\left(\sum_{k=0}^{\delta} \frac{R^{(k)}(z)}{k!} X^k\right)\left(\sum_{k\geq 0}(k+1)\,\underline{y}_{z,k+1} X^k\right) = \left(\sum_{k=0}^{\delta} \frac{B^{(k)}(z)}{k!} X^k\right)\left(\sum_{k=0} \underline{y}_{z,k} X^k\right)$$

ce qui, en égalant les termes en X^M, donne

$$(M+1)\,R(z)\,\underline{y}_{z,M+1} = \sum_{h+k=M} \frac{B^{(k)}(z)}{k!}\cdot \underline{y}_{z,h} - \sum_{\substack{h+k=M \\ k\geq 1}} (k+1)\frac{R^{(k)}(z)}{k!}\,\underline{y}_{z,h+1}$$

soit

$$(M+1)\,R(z)\,\underline{y}_{z,M+1} = \sum_{h+k=M} \sum_{j=0}^{\delta} \frac{z^j}{k!\,j!} B^{(k+j)}(0)\cdot \underline{y}_{z,h} - \sum_{\substack{h+k=M \\ k\geq 1}} (k+1) \sum_{j=0}^{\delta} \frac{z^j}{k!\,j!} R^{(k+j)}(0)\,\underline{y}_{z,h+1}$$

et donc, en réordonnant les termes

$$(M+1)\,R(z)\,\underline{y}_{z,M+1} = \sum_{j=0}^{\delta}\left[\sum_{m=0}^{M}\left(\frac{B^{(M-m+j)}(0)}{(M-m)!} + m\,\frac{R^{(M-m+j+1)}(0)}{(M-m+j+1)!}\right)\cdot \underline{y}_{z,m}\right]\frac{z^j}{j!}$$

ce qui est bien de la forme indiquée en (1) □

On déduit aussitôt de la proposition 1 que si z est un point ordinaire et $\underline{\eta}$ un élément de Ω^n, alors il existe une unique solution de (2), qu'on notera

$$\underline{y}_z(\underline{\eta}) = \sum_{m\geq 0} \underline{y}_{z,m}(\underline{\eta})\,X^m$$

qui vérifie

$$\underline{y}_{z,0}(\underline{\eta}) = \underline{\eta}\,.$$

Soit $z \in k$ un point ordinaire ; on définit le coefficient $\sigma(L,z)$ par

$$\sigma(L,z) = \overline{\lim_{L\to+\infty}}\ \frac{1}{L} \sum_{v\in M_k^0} \mathrm{Log}\left[\sup_{\underline{\eta}\in k^n}\ \max_{0\leq m\leq L} \|\underline{y}_{z,m}(\underline{\eta})\|_v\right]$$

où l'on note $\|\underline{y}_{z,m}(\underline{\eta})\|_v = \max_{1\leq i\leq n} |y_{i,z,m}(\underline{\eta})|_v^{d_v^k/[k:\mathbb{Q}]}$

Il est facile de voir que dans cette définition, on peut remplacer "$\sup_{\underline{\eta}\in k^n}$" par "$\max_{\underline{\eta}\in b}$" où b est une base quelconque de k^n.

Au cours de la démonstration du théorème 8, nous aurons besoin de majorations du type

(3) $\qquad \sigma(L,\xi) \leq a\,h(\xi) + b \qquad$ avec $a = a(L)$ et $b = b(L)$

pour tout point ξ de k, ordinaire pour L. Nous allons voir maintenant que pour disposer de telles majorations, il suffit d'imposer une condition du même type au point générique.

Pour toute place finie v de k, on se fixe $\Omega = \Omega_v$ une extension complète et algébriquement close de k_v et qui contient une unité t_v dont l'image dans le corps résiduel de Ω_v soit transcendante sur le corps résiduel de k_v. On définit alors le coefficient $\sigma(L)$ par

(4) $\qquad \sigma(L) = \overline{\lim_{L\to+\infty}}\ \frac{1}{L} \sum_{v\in M_k^0} \mathrm{Log}\left[\sup_{\underline{\eta}\in k^n}\ \max_{0\leq m\leq L} \|\underline{y}_{t_v,m}(\underline{\eta})\|_v\right]$

M_k^0 désignant l'ensemble des places finies du corps k.

DEFINITION — *Nous dirons que* L *est un* G-*opérateur différentiel si* $\tau(L) < +\infty$.

Cette définition est à rapprocher de celle des opérateurs différentiels fuchsiens de type arithmétique chez Bombieri ([Bo1] p 46) : il suffit d'intervertir dans (4) "$\overline{\lim}_{r\to+\infty}$" et "$\sum_v$" pour retrouver le coefficient $\sum_v \mathrm{Log}^+ \frac{1}{r_v}$ de Bombieri. Ce sont donc deux notions très proches qui coincideront dans la plupart des applications du théorème 8. Ainsi, ce sera le cas quand L sera un opérateur différentiel associé à une fonction algébrique (CF Ch5 §2 (4)).

PROPOSITION 2 — *Soit* L *un* G-*opérateur différentiel. Alors il existe 2 constante* a *et* b *ne dépendant que de* L *telles que, pour tout point* ξ *dans* k, *ordinaire pour* L, *on ait*

$$\tau(L,\xi) \leq a\,h(\xi) + b .$$

Remarque. Il résulte de la proposition 2 que si L est un G-opérateur différentiel, alors pour tout point ordinaire ξ dans k, les solutions du système translaté $L_\xi \underline{y}_\xi = 0$ ($L_\xi = R_\xi D - B_\xi$) sont nécessairement toutes des G-fonctions, ce qui justifie la terminologie de G-opérateur.

La proposition suivante, que nous allons utiliser dans la démonstration de la proposition 2 pour majorer les termes correspondant aux places finies dans $\tau(L,\xi)$, montre tout l'intérêt de la notion de point générique.

PROPOSITION 3 — *Soient* v *une place finie de* k, z *un point ordinaire dans* Ω_v *et* $\underline{\eta}$ *un élément de* k^m. *Alors pour tout entier* M *et toute famille de matrices* $Q_0, \dots, Q_M$ *dans* $M_{1\times m}(k)$, *on a :*

$$(5)\qquad \left|\sum_{m=0}^{M} Q_m \cdot \underline{y}_{z,m}(\underline{\eta})\right|_v \leq \left|\sum_{m=0}^{M} Q_m \cdot \underline{y}_{t_v,m}(\underline{\eta})\right|_v \left[\frac{H_v(R)\,\mathrm{Max}(1,|z|_v)^\delta}{|R(z)|_v}\right]^M$$

Remarque. On déduit facilement de la proposition 3 que le coefficient $\tau(L)$ ne dépend pas du choix du point générique t_v (Prendre $z = t'_v$ un second point générique et remarquer que $|R(t'_v)|_v = H_v(R$

Démonstration. On démontre la proposition 3 par récurrence sur M. Pour M = 0, l'inégalité (5) est triviale puisque

$$\underline{y}_{z,0}(\underline{\eta}) = \underline{y}_{t_v,0}(\underline{\eta}) = \underline{\eta}$$

Supposons donc le résultat vrai pour l'entier M et soient $Q_0, \dots, Q_{M+1}$ une famille de matrices $1\times n$ à coefficients dans k. En utilisant la proposition 1, on obtient

$$\sum_{m=0}^{M+1} Q_m \cdot \underline{y}_{z,m}(\underline{\eta}) = \sum_{m=0}^{M} Q_m \cdot \underline{y}_{z,m}(\underline{\eta}) + \frac{Q_{M+1}}{R(z)} \sum_{j=0}^{\delta}\left(\sum_{m=0}^{M} P_{j,m} \cdot \underline{y}_{z,m}(\underline{\eta})\right) z^j$$

soit

$$(6)\qquad \sum_{m=0}^{M+1} Q_m \cdot \underline{y}_{z,m}(\underline{\eta}) = \frac{1}{R(z)} \sum_{j=0}^{\delta}\left[\sum_{m=0}^{M}\left(\frac{R^{(j)}(0)}{j!} Q_m + Q_{M+1} \cdot P_{j,m}\right) \cdot \underline{y}_{z,m}(\underline{\eta})\right] z^j$$

On a donc

$$\left|\sum_{m=0}^{M+1} Q_m \cdot \underline{y}_{z,m}(\underline{z})\right|_v \leq \max_{0\leq j\leq \delta}\left|\frac{1}{R(z)}\sum_{m=0}^{M}\left(\frac{R^{(j)}(0)}{j!}Q_m + Q_{M+1}\cdot P_{j,m}\right)\cdot \underline{y}_{z,m}(\underline{z})\right|_v \max(1,|z|_v)^{\delta}$$

d'où, en utilisant l'hypothèse de récurrence

$$\left|\sum_{m=0}^{M+1} Q_m \cdot \underline{y}_{z,m}(\underline{z})\right|_v \leq \underbrace{\max_{0\leq j\leq \delta}\left|\frac{1}{R(t_v)}\sum_{m=0}^{M}\left(\frac{R^{(j)}(0)}{j!}Q_m + Q_{M+1}\cdot P_{j,m}\right)\cdot \underline{y}_{t_v,m}(\underline{z})\right|_v}_{W}\left[\frac{H_v(R)\max(1,|z|_v)^{\delta}}{|R(z)|_v}\right]^{M+1}$$

Or, comme t_v est générique, le terme noté W vaut

$$W = \left|\sum_{j=0}^{\delta}\frac{1}{R(t_v)}\left[\sum_{m=0}^{M}\left(\frac{R^{(j)}(0)}{j!}Q_m + Q_{M+1}\cdot P_{j,m}\right)\cdot \underline{y}_{t_v,m}(\underline{z})\right]t_v^{j}\right|_v$$

soit, d'après la relation (6),

$$W = \left|\sum_{m=0}^{M+1} Q_m \cdot \underline{y}_{t_v,m}(\underline{z})\right|_v \qquad \square$$

Démonstration de la proposition 2. Notons pour tout point ξ dans k, ordinaire pour L

$$\sigma^{\circ}(L,\xi) = \overline{\lim_{L\to+\infty}}\ \frac{1}{L}\sum_{v\in M_k^{\circ}} \log\left[\sup_{\underline{z}\in k^n}\ \max_{0\leq m\leq L}\|\underline{y}_{\xi,m}(\underline{z})\|_v\right]$$

et

$$\sigma^{\infty}(L,\xi) = \overline{\lim_{L\to+\infty}}\ \frac{1}{L}\sum_{\substack{v\in M_k\\ v/\infty}} \log\left[\sup_{\underline{z}\in k^n}\ \max_{0\leq m\leq L}\|\underline{y}_{\xi,m}(\underline{z})\|_v\right].$$

De la proposition 3, on déduit que

(7) $\quad \sigma^{\circ}(L,\xi) \leq \delta\, h(\xi) + \sigma(L) + h(R) + \log\delta$

Voyons maintenant la contribution des places archimédiennes. C'est un exercice facile de voir que si $(u_m)_{m\in\mathbb{N}}$ est une suite à termes réels positifs non tous nuls, on a

$$\overline{\lim_{L\to+\infty}}\ \max_{0\leq m\leq L} u_m^{\frac{1}{L}} = \max\left(1, \overline{\lim_{L\to+\infty}}\ u_L^{\frac{1}{L}}\right)$$

On en déduit que

(8) $\quad \sigma^{\infty}(L,\xi) \leq \frac{1}{[k:\mathbb{Q}]}\sum_{v\in M_k} d_v^k \log^+\frac{1}{r_v(\xi)}$

où $r_v(\xi)$ est le plus petit des rayons de convergence des solutions de (2) dans $k[[x]]^n$.

Or, v étant archimédienne, $r_v(\xi)$ est supérieur ou égal à la plus petite des distances v-adiques de ξ à l'une des singularités de L. On a donc

$$r_v(\xi) \geq \min_{x,\, R(x)=0}|x-\xi|_v$$

En utilisant l'inégalité de Liouville, on obtient la majoration

$$\max\left(1,\frac{1}{r_v(\xi)}\right) \leq \frac{2\,H_v(R_\xi)}{|R(\xi)|_v}$$

et donc

(9) $\quad \frac{1}{[k:\mathbb{Q}]}\sum_{\substack{v\in M_k\\ v/\infty}} d_v^k \log^+\frac{1}{r_v(\xi)} \leq h(R_\xi) + \log 2 \leq \delta\, h(\xi) + h(R) + (\delta+1)\log 2 + \log(1+\delta)$

Finalement, comme

$$\sigma(L,\xi) \leq \sigma^0(L,\xi) + \sigma^\infty(L,\xi)$$

on obtient le résultat désiré en regroupant (7) (8) et (9) □

Remarque. La proposition 3, permet, de la même façon, de montrer, sans recourir au théorème de Katz, que

$$\frac{1}{[k:\mathbb{Q}]} \sum_{v \in M_k} d_v^k \operatorname{Log}^+ \frac{1}{r_v(\xi)} \leq \frac{1}{[k:\mathbb{Q}]} \sum_{v \in M_\xi} d_v^k \operatorname{Log}^+ \frac{1}{r_v} + \text{cte.}\, h(\xi) \quad \text{(Cf [Bo1] Lemme 17 p47)}$$

2. Le théorème 8

Soient k un corps de nombres, $n \geq 1$ un entier et A une matrice $n \times n$ à coefficients dans $k(x)$. On suppose que l'opérateur $L = D - A$ est un G-opérateur différentiel.

On se donne également $\underline{Y} = (Y_1, \dots, Y_n)$ un vecteur solution de $L\underline{Y} = 0$ dont les composantes Y_i sont des G-fonctions (Cf Ch V) à coefficients dans un corps de nombres K contenant k. Pour toute place v de K, on note R_v le plus petit des rayons de convergence v-adiques des séries Y_i, $i = 1,2,\dots,n$ et $Y_{1,v}, \dots, Y_{n,v}$ les fonctions induites par $Y_1, \dots, Y_n$ sur la boule ouverte $B(0, R_v)$ de K_v.

On suppose de plus que les séries formelles $Y_1, \dots, Y_n$ sont $k(x)$ linéairement indépendantes et que $\frac{1}{[K:\mathbb{Q}]} \sum_{v \in M_K} d_v^K \operatorname{Log}^+ \frac{1}{R_v} < +\infty$.

THÉORÈME 8 — *Soient ξ un élément non nul de k, ρ un entier et $\Lambda = (\lambda_{ij})_{\substack{1 \leq i \leq \rho \\ 1 \leq j \leq n}}$ une matrice à coefficients dans k de rang ρ. Soit enfin $S(\xi, \Lambda)$ l'ensemble des places v de K vérifiant :*

$$|\xi|_v < \operatorname{Min}(1, R_v) \text{ et } \sum_{j=1}^{n} \lambda_{ij} Y_{j,v}(\xi) = 0 \quad \text{pour } i = 1,2,\dots,\rho$$

Alors

$$\frac{1}{[K:\mathbb{Q}]} \sum_{v \in S(\xi,\Lambda)} d_v^K \operatorname{Log} |\xi|_v + \frac{n-\rho}{n} h(\xi) \geq -C_1 \sqrt{h(\xi)} - C_2$$

où C_1 et C_2 sont deux constantes ne dépendant que de L et de $\underline{Y}$.

Remarques. 1) On peut, comme nous l'avons fait pour le théorème 2, donner une valeur explicite pour les constantes C_1 et C_2.

2) A la différence de Bombieri ([Bo1] Main Theorem p 49 ou Ch V Th 3), nous ne supposons pas les séries formelles $Y_1, \dots, Y_n$ à coefficients dans le corps de base k.

Démonstration. Les constantes c_i, $i = 1,2,\dots,15$ qui vont intervenir dans la suite sont des quantités positives ne dépendant que de L et $\underline{Y}$. D'autre part, nous dirons qu'une suite $(u_M)_{M \in \mathbb{N}}$ est un $\bar{o}(1)$ si

$$\overline{\lim_{M \to +\infty}}\, u_M \leq 0$$

Notons qu'à cause du signe $\leq$, on a $\bar{o}(1) + \bar{o}(1) = \bar{o}(1)$.

Soit donc ξ un élément non nul de k. Le terme de gauche dans l'inégalité du théorème 8 étant supérieur à $-h(\xi)$, on peut, quitte à prendre finalement C_2 assez grand, supposer que ξ est un point ordinaire pour L, de hauteur $h(\xi) \geqslant 4$.

On se donne également $\Lambda = (\alpha_{ij})_{\substack{1 \leqslant i \leqslant p \\ 1 \leqslant j \leqslant n}}$ une matrice à coefficients dans k de rang p. Nous noterons $(\underline{e}_\lambda)_{1 \leqslant \lambda \leqslant n-p}$ une base du sous-espace vectoriel V de k^n défini par les équations

$$\sum_{j=1}^{n} \alpha_{ij} x_j = 0 \qquad \text{pour } i = 1, 2, \ldots, p$$

PROPOSITION 4 — *Soient $M > 0$ un entier et p l'entier défini par $p = M[\sqrt{h(\xi)}]$. Alors il existe un n-uple $\Phi = (\Phi_1, \ldots, \Phi_m)$ de polynômes non tous nuls $\Phi_i = \sum_j \Phi_{i,j} X^j$ à coefficients $\Phi_{i,j}$ dans k, vérifiant*

(a) $\deg \Phi_i < p$ *pour* $i = 1, 2, \ldots, n$

(b) *pour* $\lambda = 1, 2, \ldots, n-p$, *la série formelle* $\Phi_\xi \cdot \underline{y}_\xi(\underline{e}_\lambda)$ *a un zéro d'ordre* $\geqslant M$ *en* 0
(Φ_ξ *est défini comme d'habitude par* $\Phi_\xi(X - \xi) = \Phi$)

(c) $$\frac{h(\Phi)}{M} \leqslant \frac{n-p}{n} h(\xi) + c_1 \sqrt{h(\xi)} + c_2 + \bar{o}(1)$$

Démonstration. On a a priori

$$\Phi_\xi \cdot \underline{y}_\xi(\underline{e}_\lambda) = \sum_{m \geqslant 0} \left(\sum_{h+k=m} \frac{\Phi^{(h)}(\xi)}{h!} \cdot \underline{y}_{\xi,h}(\underline{e}_\lambda) \right) X^m$$

La condition (b) de la proposition 4 est donc équivalente au système d'équations

$$L_{\lambda,m}\left((\Phi_{i,j})_{\substack{1 \leqslant i \leqslant n \\ 0 \leqslant j < p}}\right) = 0 \qquad \lambda = 1, 2, \ldots, n-p \quad m = 1, 2, \ldots, M$$

où

$$L_{\lambda,m} = \sum_{i,j} A_{\lambda,m-1,i,j} X_{i,j}$$

et

$$A_{\lambda,m,i,j} = \sum_{h=0}^{\min(m,j)} \binom{j}{h} \xi^{j-h} y_{i,\xi,m-h}(\underline{e}_\lambda)$$

C'est un système de $(n-p)M$ équations à np inconnues. $h(\xi) \geqslant 4$ impose $np - (n-p)M \geqslant nM > 0$. D'après le lemme de Siegel de [Bo1] (i.e celui du Ch III avec $E = k$), il existe un n-uple $\Phi = (\Phi_1, \ldots, \Phi_n)$ de polynômes $\Phi_i \in k[X]$ non tous nuls, vérifiant les conditions (a), (b) et

$$(10) \qquad \mathcal{H}(\Phi) \leqslant \prod_{\substack{1 \leqslant \lambda \leqslant n-p \\ 1 \leqslant m \leqslant M}} \mathcal{H}(L_{\lambda,m})^{\frac{1}{np-(n-p)M}}$$

Reste donc, pour obtenir (c) à majorer la hauteur des formes linéaires $L_{\lambda,m}$. Soit v une place de k. Pour $1 \leqslant i \leqslant n$, $0 \leqslant j < p$ et $0 \leqslant m \leqslant M$ on a

$$|A_{\lambda,m,i,j}|_v \leqslant \max(1, |\xi|_v)^p \max_{\substack{1 \leqslant i \leqslant n \\ 0 \leqslant m \leqslant M}} |y_{i,\xi,m}(\underline{e}_\lambda)|_v \qquad \text{si } v \text{ est finie}$$

$$|A_{\lambda,m,i,j}|_v \leq 2^p \operatorname{Max}(1,|\xi|_v)^p \max_{\substack{1\leq i\leq n\\ 0\leq m\leq M-1}} |y_{i,\xi,m}(e_\lambda)|_v \qquad \text{si } v \text{ est archimédienne}$$

On en déduit que pour $\lambda = 1,\dots,n-\rho$ et $m = 1,2,\dots,M$, on a

$$\mathcal{H}(L_{\lambda,m}) \leq 2^p \mathcal{H}(\xi)^p \prod_{v\in M_k} \sup_{\underline{z}\in k^n} \max_{0\leq m\leq M} \|y_{\xi,m}(\underline{z})\|_v$$

En reportant dans (10), on obtient

$$h(\Phi) \leq \frac{(n-\rho)M}{np-(n-\rho)M}\left[p\operatorname{Log}2 + p h(\xi) + \sum_{v\in M_k} \operatorname{Log}\left[\sup_{\underline{z}\in k^n} \max_{0\leq m\leq M} \|y_{\xi,m}(\underline{z})\|_v\right]\right]$$

et donc

$$\frac{h(\Phi)}{M} \leq \operatorname{Log}2\sqrt{h(\xi)} + \frac{n-\rho}{n-n\rho/[\sqrt{h(\xi)}]}\, h(\xi) + \frac{n-\rho}{n[\sqrt{h(\xi)}]-(n-\rho)}\, \sigma(L,\xi) + \bar{o}(1)$$

On a supposé que L était un G-opérateur. D'après la proposition 2, on a donc

$$\sigma(L,\xi) \leq c_3 h(\xi) + c_4$$

Moyennant ensuite quelques majorations faciles déjà faites au chapitre IV (§1.1 p43) on aboutit au résultat désiré □

Considérons maintenant la solution $\underline{Y} = (Y_1,\dots,Y_m)$ du système différentiel $L\underline{Y} = 0$, donné dans l'énoncé du théorème 8. Les Y_i, $i=1,2,\dots,n$ étant supposés $k(X)$ linéairement indépendants, la série formelle $\Phi.\underline{Y} = \Phi_1 Y_1 + \dots + \Phi_m Y_m$ est non nulle. Le théorème de Shidlovski ([Sh] Ch5 ou [Be]) permet alors de majorer $\bar{\ell}$, l'ordre en 0 de cette série par :

$$(11) \qquad \bar{\ell} \leq np + c_5$$

On note ensuite γ le coefficient de $X^{\bar{\ell}}$ dans $\Phi.\underline{Y}$; c'est un élément non nul du corps K ; on peut donc écrire la formule du produit

$$(12) \qquad \prod_{v\in M_K} |\gamma|_v^{d_v^K} = 1$$

Nous allons maintenant majorer les $|\gamma|_v$. De l'inégalité ainsi obtenue, nous déduirons le résultat voulu. On définit tout d'abord deux ensembles S_1 et S_2 de la manière suivante :

$$S_1 = \left\{ v\in M_K \;/\; v\in S(\xi,\Lambda),\ v\nmid\infty \text{ et } |\xi|_v \geq \frac{R_v}{2}\right\}$$

$$S_2 = S(\xi,\Lambda) \setminus S_1$$

Nous allons distinguer deux types de majoration suivant que v appartient à S_2 ou pas.

PROPOSITION 5 — *On a*

$$\frac{1}{M}\left[\frac{1}{[K:\mathbb{Q}]} \sum_{v\notin S_2} d_v^K \operatorname{Log}|\gamma|_v\right] \leq \frac{1}{M}\left[\frac{1}{[K:\mathbb{Q}]} \sum_{v\notin S_2} d_v^K h_v(\Phi)\right] + c_6\sqrt{h(\xi)} + c_7 + \bar{o}(1)$$

Démonstration. Notons pour $i=1,2,\dots,n$, $Y_i = \sum_{m\geq 0} a_{i,m} X^m$. De la formule

$$\gamma = \sum_{i=1}^{n} \sum_{k_i k_= \bar{\ell}} \Phi_{i,k}\, a_{i,k}$$

on déduit que

$$|\gamma|_v \leqslant H_v(\Phi) \max_{\substack{1\leqslant i\leqslant n \\ 0\leqslant \ell\leqslant \bar{\ell}}} |a_{i,\ell}|_v \qquad \text{si } v \text{ est finie}$$

$$|\gamma|_v \leqslant n(\bar{\ell}+1) H_v(\Phi) \max_{\substack{1\leqslant i\leqslant n \\ 0\leqslant \ell\leqslant \bar{\ell}}} |a_{i,\ell}|_v \qquad \text{si } v \text{ est archimédienne}$$

On obtient donc, en utilisant (11)

$$\frac{1}{[K:\mathbb{Q}]} \sum_{v\notin S_2} d_v^K \operatorname{Log}|\gamma|_v \leqslant \frac{1}{[K:\mathbb{Q}]} \sum_{v\notin S_2} d_v^K h_v(\Phi) + (np+c_5)\left(\frac{1}{np+c_5}\left(\frac{1}{[K:\mathbb{Q}]}\sum_{v\notin S_2} d_v^K \operatorname{Log} \max_{\substack{1\leqslant i\leqslant n \\ 0\leqslant \ell\leqslant np+c_5}} |a_{i,\ell}|_v\right)\right) + O(1)$$

ce qui permet de conclure, puisque les séries $Y_1, \ldots, Y_n$ sont des G-fonctions □

PROPOSITION 6 — *Pour $\varepsilon > 0$ assez petit, on a*

$$\frac{1}{M}\left[\frac{1}{[K:\mathbb{Q}]}\sum_{v\in S_2} d_v^K \operatorname{Log}|\gamma|_v\right] \leqslant \frac{1}{[K:\mathbb{Q}]}\sum_{v\in S(\xi,\Lambda)} d_v^K \operatorname{Log}|\xi|_v + \frac{1}{M}\left[\frac{1}{[K:\mathbb{Q}]}\sum_{v\in S_2} d_v^K h_v(\Phi)\right] + \frac{(1+n\sqrt{R(\xi)})}{[K:\mathbb{Q}]}\left[\sum_{v\in S_2} d_v^K \operatorname{Log}^+ \frac{1}{R_v - 2\varepsilon}\right] + c_8 + o(1)$$

Démonstration. Soit v une place de $S(\xi,\Lambda)$. $\underline{Y}_v = {}^t(Y_{1,v}, \ldots, Y_{m,v})$ est une solution de $L\underline{Y}_v = 0$, définie au voisinage de ξ et par définition de l'ensemble $S(\xi,\Lambda)$, le vecteur $\underline{Y}_v(\xi)$ appartient à $V\otimes_k K_v$ dont $(\underline{e}_\lambda)_{1\leqslant\lambda\leqslant m-p}$ est une base sur K_v. ξ étant ordinaire pour L, il existe une famille unique $(\mu_{v,\lambda})_{1\leqslant\lambda\leqslant m-p}$ d'éléments de K_v vérifiant

$$\underline{Y}_v(x) = \sum_{\lambda=1}^{m-p} \mu_{v,\lambda}\ \underline{y}_{\xi,v}(\underline{e}_\lambda)(x-\xi) \tag{13}$$

pour tout x dans un voisinage v-adique de ξ. Dans (13), nous avons évidemment noté $\underline{y}_{\xi,v}(\underline{e}_\lambda)$ la fonction naturellement induite par $\underline{y}_\xi(\underline{e}_\lambda)$ au voisinage de ξ.

On en déduit qu'au voisinage de ξ, on a

$$(\Phi.\underline{Y}_v)(x) = \sum_{\lambda=1}^{m-p} \mu_{v,\lambda}\left(\Phi(x).\ \underline{y}_{\xi,v}(\underline{e}_\lambda)(x-\xi)\right)$$

ce qui s'écrit encore

$$(\Phi.\underline{Y}_v)(x) = \sum_{\lambda=1}^{m-p} \mu_{v,\lambda}\left(\Phi_\xi.\ \underline{y}_{\xi,v}(\underline{e}_\lambda)\right)(x-\xi)$$

Par construction de Φ, la fonction $\Phi.\underline{Y}_v$ admet donc en ξ un zéro d'ordre $\geqslant M$.

Supposons maintenant v dans l'ensemble $S_2 \subset S(\xi,\Lambda)$. On note w un prolongement de v à $\bar{\mathbb{Q}}$, $\mathbb{C}_w$ le complété de $\bar{\mathbb{Q}}$ pour la place w et $\underline{Y}_w$ la fonction, qui prolonge $\underline{Y}_v$, induite par $\underline{Y}$ sur la boule ouverte $B_w = B(0,R_v)$ de $\mathbb{C}_w$. D'après ce qui précède, la fonction

$$G_w : x \longmapsto \frac{(\Phi.\underline{Y}_w)(x)}{x^\ell (x-\xi)^M}$$

est strictement analytique sur toute boule fermée de B_w et prend la valeur $G_w(0) = \gamma(-\xi)^{-M}$ en 0. Choisissons $\varepsilon > 0$ assez petit pour que

$$R_v - 2\varepsilon > |\xi|_v \qquad \text{pour tout } v \text{ dans } S_2$$

En appliquant le principe du maximum sur la boule $B(0, R_v - \varepsilon)$, on obtient

$$|\gamma|_v \leqslant |\xi|_v^M (R_v-\varepsilon)^{-(\bar{\ell}+M)} H_v(\Phi)\, M_W(R_v-\varepsilon) \qquad \text{si } v \text{ est finie}$$

$$|\gamma|_v \leqslant |\xi|_v^M (R_v-2\varepsilon)^{-(\bar{\ell}+M)} 2^L H_v(\Phi)\, np\, M_W(R_v-\varepsilon) \qquad \text{si } v \text{ est archimédienne}$$

où nous avons noté $M_W(r) = \max_{1\le i\le n} \max_{|x|_v = r} |Y_{i,W}(x)|_W$ pour $0 < r < R_v$

En utilisant (11) on en déduit :

$$(14)\quad \frac{1}{M}\left[\frac{1}{[K:\mathbb{Q}]}\sum_{v\in S_2} d_v^K \operatorname{Log}|\gamma|_v\right] \leqslant \frac{1}{[K:\mathbb{Q}]}\sum_{v\in S_2} d_v^K \operatorname{Log}|\xi|_v + \frac{1}{M}\left[\frac{1}{[K:\mathbb{Q}]}\sum_{v\in S_2} d_v^K h_v(\Phi)\right]$$
$$+ \frac{(n\sqrt{h(\xi)}+1)}{[K:\mathbb{Q}]}\left[\sum_{v\in S_2} d_v^K \operatorname{Log}^+\frac{1}{R_v-2\varepsilon}\right] + \operatorname{Log} 2 + o(1)$$

D'autre part, il est évident que

$$(15)\quad -\frac{1}{[K:\mathbb{Q}]}\sum_{v\in S_1} d_v^K \operatorname{Log}|\xi|_v \leqslant \frac{1}{[K:\mathbb{Q}]}\sum_{\substack{v\in M_K\\ v\neq\infty}} d_v^K \operatorname{Log}^+\frac{1}{R_v} + \operatorname{Log} 2 = c_8$$

En joignant (14) et (15), on obtient le résultat annoncé □

Reportons maintenant dans (12) les résultats des propositions 5 et 6. On obtient que, pour $\varepsilon > 0$ assez petit.

$$0 \leqslant \frac{1}{[K:\mathbb{Q}]}\sum_{v\in S(\xi,\Lambda)} d_v^K \operatorname{Log}|\xi|_v + \frac{h(\Phi)}{M} + (1+n\sqrt{h(\xi)})\left[\frac{1}{[K:\mathbb{Q}]}\sum_{v\in S_2} d_v^K \operatorname{Log}^+\frac{1}{R_v-2\varepsilon}\right] + c_{10} + c_{11}\sqrt{h(\xi)} + \bar{o}(1)$$

et donc, en tenant compte de la majoration (c) de la proposition 4

$$0 \leqslant \frac{1}{[K:\mathbb{Q}]}\sum_{v\in S(\xi,\Lambda)} d_v^K \operatorname{Log}|\xi|_v + \frac{n-\rho}{n} h(\xi) + (1+n\sqrt{h(\xi)})\left[\frac{1}{[K:\mathbb{Q}]}\sum_{v\in S_2} d_v^K \operatorname{Log}^+\frac{1}{R_v-2\varepsilon}\right] + c_{12} + c_{13}\sqrt{h(\xi)} + \bar{o}(1)$$

On passe ensuite à la limite sup en M, puis on fait tendre ε vers 0 ; enfin on majore

$$\frac{1}{[K:\mathbb{Q}]}\sum_{v\in S_2} d_v^K \operatorname{Log}^+\frac{1}{R_v} \quad \text{par} \quad \frac{1}{[K:\mathbb{Q}]}\sum_{v\in M_K} d_v^K \operatorname{Log}^+\frac{1}{R_v}$$

On obtient finalement

$$\frac{1}{[K:\mathbb{Q}]}\sum_{v\in S(\xi,\Lambda)} d_v^K \operatorname{Log}|\xi|_v + \frac{n-\rho}{n} h(\xi) + c_{14}\sqrt{h(\xi)} + c_{15} \geqslant 0$$

C.Q.F.D.

3. Applications

En adaptant les techniques du chapitre VI, il est facile de démontrer les résultats suivants. Nous gardons les hypothèses du théorème 8.

COROLLAIRE — *On suppose ici de plus que* $k = K = \mathbb{Q}$. *Soit* ξ *un nombre rationnel*

distinct de $0, 1, -1$ et $m \geq 0$ un entier. Alors si m est suffisamment grand (supérieur à un entier m_0 ne dépendant que de L et $\underline{Y}$), le vecteur $\underline{Y}_v(\xi^m)$ est défini et ses composantes sont linéairement indépendantes sur $\mathbb{Q}$, ceci pour toute place v dans $M_{\mathbb{Q}}(\xi)$.

Le corollaire 1 est un cas particulier du corollaire 2 où nous supposons seulement $k = \mathbb{Q}$. Si ξ est un nombre rationnel non nul et v une place où $|\xi|_v < R_v$, nous notons $n_v(\xi)$ la dimension sur $\mathbb{Q}$ du $\mathbb{Q}$ espace vectoriel $\mathbb{Q}Y_{1,v}(\xi) + \cdots + \mathbb{Q}Y_{m,v}(\xi)$.

COROLLAIRE 2 — Si $\xi \neq 0, 1, -1$ et si m est un entier suffisamment grand ($m \geq m_0$), alors pour toute place v dans $M_K(\xi)$, le vecteur $\underline{Y}_v(\xi^m)$ est défini et

$$n_v(\xi^m) \geq \frac{n \underset{w \in M_K(\xi)}{\operatorname{Min}} d_w^K}{[K : \mathbb{Q}]}$$

RÉFÉRENCES

[Am] AMICE (Y) : Les nombres p-adiques. Collection Sup. Le Mathématicien 14. Presses universitaires de France (1975).

[Be] BERTRAND (D): Sur les lemmes de zéros. Les journées de Saint-Etienne. Algorithmique, Calcul formel, Arithmétique (1983). Publ. Univ. St. Etienne. Exp N° XXXI

[Bi] BIRKHOFF (G-D): On the integral divisors of $a^n - b^n$. Annals of Math (2). 5 (1904) p 173-180

[Bo1] BOMBIERI (E): On G-functions. Recent progress in analytic number theory. H. Halberstam and C. Hooley ed., Academic Press (1981) Vol 2 p. 1-67.

[Bo2] BOMBIERI (E) & SPERBER (S): On the p-adic analyticity of solutions of linear differential équations. Ill. J. of Math. (1982.) Vol 26 N°1.

[Bo 3] BOMBIERI (E): On the Thue-Siegel-Dyson theorem. Acta Math. Uppsala. (1982) t. 148 p. 255-296.

[Bo4] BOMBIERI (E): On Weil's "théorème de décomposition". Amer. J. Math. 105 (1983) p 295-308.

[Bu] BUNDSCHUH (P): Une nouvelle application de la méthode de Gel'fond. Sem. Delange-Pisot-Poitou. Théorie des Nombres. 19ème année (1977-78) N°42

[C-F] CASSELS (J.W.S) & FRÖLICH (A): Algebraic number theory. Academic Press London and New-York (1967)

[Ch] CHENCINER (P): Courbes algebriques planes. Publ. Math. de l'Univ. Paris VII (1978)

[De1] DÈBES (P): Une version effective du théorème d'irréductibilité de Hilbert. Sem. Anal. Ultrametrique. Amice-Christol-Robba. 10ème année. (1982/83) N°10. Ou Les journées de St-Etienne. Algorithmique. Calcul formel, Arithmétique (1983). Publ. Univ. St-Etienne. Exp. N° XXIX

.../...

[De2] DÈBES (P) : Spécialisations de polynômes. Math. rep. Acad. Sci.; Royal. Soc. Canada, Vol V N°6 Décembre 1983

[Dö] DÖRGE (K) : Einfacher Beweis des Hilbertschen Irreduzibilitätssatzes. Math. Ann. 96 (1927) p. 176-182.

[D-R] DWORK (B) & ROBBA (P) : On natural radii of p-adic convergence. Trans. Amer. Math. Soc. 256 (1979) p. 199-213.

[Ei] EICHLER (M) : Introduction to the theory of algebraic numbers and functions. Pure and applied Math. A series of monographs and textbooks. 23. Acad. Press (1966)

[Fa] FALTINGS (G) : Endlichkeitssätzes für abelsche Varietäten über Zahlkörpen. Invent. Math., 73 (1983), p. 349-366.

[Fo] FORSTER (O) : Lectures on Riemann surfaces. Springer-Verlag N° 81 (1981).

[Fr] FRIED (M) : On Hilbert's Irreducibility theorem. J. Number Theory. 6. (1974) p. 211-231.

[Fu] FULTON (W) : Algebraic curves. An introduction to algebraic geometry. New-York, Amsterdam. W.A. Benjamin (1969)

[Ha] HARTSHORNE (R) : Algebraic geometry. Springer-Verlag N°52 (1977)

[Hi] HILBERT (D) : Über die Irreduzibilität ganzer rationaler Funktionen mit ganzzahligen Koeffizienten. Gesammelte Abhandlungen. Springer-Verlag (1933) [réimpression Chelsea (1965)] Vol 2, N°18 p. 264-286. Ou J. für die reine und angew. Math. (1892) t. 110 p. 104-129

[La1] LANG (S) : Algebra. Addison-Wesley publishing company (1965)

[La2] LANG (S) : Algebraic number theory. Addison-Wesley publishing company (1970)

[La3] LANG (S) : Fundamentals of diophantine geometry. Springer-Verlag (1983)

[Ma] MALGRANGE (B) : Sur les points singuliers des équations différentielles linéaires. Enseign. Math. 20 (1970) p 147-176

.../...

[Mo] MORDELL (L.J): Diophantine equations. Pure and applied Math. A series of monographs and textbooks. 30. Acad. Press (1969)

[Ne] NERON (A): Quasi-fonctions et hauteurs sur les variétés abéliennes. Annals of Math. 53 (1951) p.412-444.

[Ri] RIBENBOIM (P): 13 Lectures on the last Fermat's theorem. Springer-Verlag. (1980)

[Schi1] SCHINZEL (A): On Hilbert's ireducibility theorem. Acta Arithmetica. 16 (1965) p.334-340

[Schi2] SCHINZEL (A): Sur certaines hypothèses concernant les nombres premiers. Acta Arithmetica 4. (1958) p.185-208 et 5. (1959) p.259.

[Schi3] SCHINZEL (A): Selected topics on polynomials. Ann Arbor. The university of Michigan Press (1982)

[Schn1] SCHNEIDER (T): Rationale Punkte über einer algebraischen Kurve. Sem. Delange-Pisot-Poitou. Théorie des Nombres. 15ème année (1973/74) N°20.

[Schn2] SCHNEIDER (T): Eine Bemerkung zu einem Satz von C.L. Siegel. Comm. pure and applied Math. (1976) t.29 p.775-782.

[Se] SERRE (J-P): Autour du théorème de Mordell-Weil. II. Cours au collège de France (1980/81). Notes rédigées par M. Waldschmidt.

[Sh] SHIDLOVSKI (A-B): Approximations diophantiennes et nombres transcendants. Publ. Univ. Moscou (1982)

[Si] SIEGEL (C.L): Über Einige Anwendungen diophantischer Approximationen. Abhandlungen der Preussischen Akademie der Wissenschaften. Phys. Math. Klasse 1929 N°1. Ou Gessamelte Abhandlungen. Springer-Verlag (1966) Vol 1 N°16 p.209-266

[Sp1] SPRINDŽUK (V-G): Hilbert's ireducibility theorem and rational points on algebraic curves. Doklady. Acad. Nauk. SSSR 247 (1979) p285-289.

[Sp2] SPRINDŽUK (V-G): Reducibility of polynomials and rational points on algebraic curves. Doklady. Acad. Nauk. SSSR 250 (1980) p. 1327-1330.

[Sp 3] SPRINDŽUK (V-G) : Diophantine equations involving unknown primes. Trudy M.IAN S.S.S.R 158 (1981) p 180-196.

[Sp4] SPRINDŽUK (V-G) : Arithmetic specializations in polynomials. J. Reine und angew. Math. 340 (1983) p 26-52

[Wa] WALDSCHMIDT (M) : Nombres transcendants. Lecture notes in Math. 402. Springer-Verlag (1976)

[We] WEIL (A) : Arithmetic on algebraic varieties. Annals of Math. 53. (1951) p. 412-443. Ou Gesammelte Abhandlungen. Springer-Verlag (1968).