

Werk

Titel: Seminaire de Théorie des Nombres de Bordeaux

Jahr: 1980-1981

Kollektion: Mathematica

Digitalisiert: Niedersächsische Staats- und Universitätsbibliothek Göttingen

Werk Id: PPN320141322_0010

PURL: http://resolver.sub.uni-goettingen.de/purl?PPN320141322_0010

Übergeordnetes Werk

Werk Id: PPN320141322

PURL: <http://resolver.sub.uni-goettingen.de/purl?PPN320141322>

Terms and Conditions

The Goettingen State and University Library provides access to digitized documents strictly for noncommercial educational, research and private purposes and makes no warranty with regard to their use for other purposes. Some of our collections are protected by copyright. Publication and/or broadcast in any form (including electronic) requires prior written permission from the Goettingen State- and University Library.

Each copy of any part of this document must contain there Terms and Conditions. With the usage of the library's online system to access or download a digitized document you accept the Terms and Conditions.

Reproductions of material on the web site may not be made for or donated to other repositories, nor may be further reproduced without written permission from the Goettingen State- and University Library.

For reproduction requests and permissions, please contact us. If citing materials, please give proper attribution of the source.

Contact

Niedersächsische Staats- und Universitätsbibliothek Göttingen
Georg-August-Universität Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen
Germany
Email: gdz@sub.uni-goettingen.de

université de bordeaux I

l.r. de mathématiques et d'informatique

**séminaire
de
théorie
des
nombres**

AAO

1980-1981

ZB 48515:1980/1981

g1

université de bordeaux I
u.e.r. de mathématiques et d'informatique

séminaire
de
théorie des nombres

1980-1981

laboratoire de théorie des nombres
laboratoire de recherche associé au C.N.R.S. n° 226
351, cours de la libération
33405 Talence-cédex



TABLE DES MATIÈRES
-:-:-:-

Exposé n°	Nombre de pages
1. - Bernard de MATHAN, Quelques remarques sur la conjecture de Littlewood (en approximations diophantiennes simultanées)	20
2. - Marc LABORDE, Presque-premiers dans les petits intervalles (non rédigé)	
3. - Benedict H. GROOS, The annihilation of divisor classes in abelian extensions of the rational function field	5
4. - Eric REYSSAT, Transcendance et fonctions elliptiques	14
5. - Jean-Marc DESHOUILLERS, Théorie additive et géométrie des nombres	3
6. - Michel MATIGNON et Marc REVERSAT, Sur les automorphismes d'extensions transcendantes de corps valués	16
7. - Marius van der PUT, Groupes discrets de quaternions	14
8. - B. DWORK, Hypergeometric functions as p-adic analytic functions	6
9. - François GRAMAIN, Sur le théorème de Fukasawa-Gel'fond	10

10. - F. BEUKERS, Padé-approximations in number theory	9
11. - Gérard VIENNOT, Interprétations combinatoires des nombres d'Euler et de Genocchi (à paraître dans le Séminaire de Théorie des Nombres 1981-1982)	
12. - A. WILES, La conjecture principale de la théorie d'Iwasawa (non rédigé)	
13. - Gérald TENENBAUM, Sur la densité divisorielle d'une suite d'entiers	6
14. - Daniel BERTRAND, Représentations des corps de nombres et théorie de Baker	6
1. - Christophe SOULÉ, K-théorie et corps cyclotomiques	6
16. - Henri COHEN, Accélération de la convergence de certaines réurrences linéaires	2
17. - Jacques PEYRIÈRE, Substitutions aléatoires itérées	9
18. - Martin HUXLEY, Estimating $\liminf (p_{n+r} - p_n) / \log p_n$	10
19. - Gérard RAUZY, Nombres algébriques et substitutions (non rédigé)	
20. - S.M.J. WILSON, Extensions with identical wild ramification	7
21 - Jean-François JAULENT, Théorie d'Iwasawa des tours méta- béliennes	16
22. - Pierrette CASSOU-NOGUÈS, Séries de Dirichlet	14
23. - Hyman BASS, Applications polynômiales à jacobienne constante	6
24. - John TATE, Brumer-Stark-Stickelberger	16
25. - Lawrence C. WASHINGTON, Zeros of p-adic L-functions	4
26. - André WEIL, Sur l'histoire des équations indéterminées de genre 1 depuis Diophante	3
27. - Mohan NAIR, A new method in the elementary theory of primes ...	7
28. - Kunrui YU, Two results in metrical diophantine approximation	8
29. - R. TIJDEMAN, Multiplicities of binary recurrences	11

- 30. - Iekata SHIOKAWA, On irrationality of the values of certain series .. 13
- 31. - F. M. DEKKING, On the structure of selfgenerating sequences..... 6
- 32. - David GOSS, The arithmetic of function fields 11

QUELQUES REMARQUES SUR LA CONJECTURE DE LITTLEWOOD
(EN APPROXIMATIONS DIOPHANTIENNES SIMULTANÉES)

par

Bernard de MATHAN

-:-:-:-

1. - La conjecture de Littlewood

Il a été conjecturé par Littlewood que pour tout couple (α, β) de nombres réels, et tout $\varepsilon > 0$, il existe un entier $n > 0$ tel que

$$n \|\alpha\| \|\beta\| \leq \varepsilon$$

(où $\|x\| = \min_{m \in \mathbb{Z}} |x - m|$ pour tout $x \in \mathbb{R}$).

On ne sait pas actuellement la réponse à ce problème. Un lien a été trouvé par J. W. S. Cassels et H. P. F. Swinnerton-Dyer ([3]) avec les nombres cubiques : Si α et β sont deux nombres d'un même corps cubique, ils satisfont à la conjecture de Littlewood.

Nous étudions la conjecture de Littlewood dans un corps de séries formelles :

Soit K un corps (commutatif !), et soit $K(T)$ le corps des fractions rationnelles à une indéterminée sur K . Munissons $K(T)$ de la valeur absolue telle que pour tout polynôme non nul $f(T) \in K[T]$, on ait $|f(T)| = q^{\deg f(T)}$ où q est une constante réelle > 1 (lorsque le corps K est fini, on prendra $q = \text{card } K$).

Le complété de $K(T)$ pour cette valeur-absolue est le corps $K((T^{-1}))$ des séries formelles de Laurent en $1/T$, la valeur absolue d'une série formelle $\sum_{n=-n_0}^{+\infty} a_n T^{-n}$, où $a_{-n_0} \neq 0$, étant q^{n_0} . Soit $\mathfrak{m}_0$ l'idéal maximal de l'anneau de valuation de

$K((T^{-1}))$, i.e. que $\mathfrak{m}_0$ est l'ensemble des séries formelles de la forme $\sum_{n=1}^{+\infty} a_n T^{-n}$ ($a_i \in K$), on a la décomposition en somme directe de groupes additifs:

$$K((T^{-1})) = K[T] \oplus \mathfrak{m}_0.$$

On désigne par E et $\mathcal{K}_0$ respectivement les projections correspondantes sur $K[T]$ et $\mathfrak{m}_0$ ("partie entière", "partie fractionnaire"). Pour $X \in K((T^{-1}))$, on pose $\|X\| = |\mathcal{K}_0(X)|$. Le problème correspondant à la conjecture de Littlewood est alors le suivant : existe-t-il pour tout couple (α, β) d'éléments de $K((T^{-1}))$, et pour toute constante entière positive c , un polynôme non nul $f \in K[T]$ tel que :

$$|f| \|\alpha f\| \|f\beta\| \leq q^{-c}.$$

Il a été démontré par H. Davenport et J.S. Lewis que la réponse est négative si le corps K est infini, puis A. Baker a fourni un contre-exemple explicite dans le cas où $K = \mathbb{Q}$: on a :

$$|f| \|f e^{1/T}\| \|f e^{2/T}\| \geq q^{-5}$$

pour tout polynôme $f \neq 0$ ([4], [1]).

Le problème reste cependant entier si le corps K est fini, ce qui est bien entendu le cas le plus profond, et le plus proche de celui de $\mathbb{R}$. Il est probable que l'équivalent du résultat de J.W.S. Cassels et H.P.F. Swinnerton-Dyer ([3]), concernant les corps cubiques, -sur $K(T)$ - reste vrai dans ce cas, il est sans doute aisé de transcrire ce travail.

Nous établissons ici un lien de nature différente avec les corps cubiques. Les corps cubiques qui s'introduisent naturellement dans le point de vue que nous allons développer sont d'ailleurs ceux dont tous les conjugués sont dans $K((T^{-1}))$ -i.e. l'équivalent des corps cubiques totalement réels-.

Nous étudions en fait la conjecture "duale" (bien que ce point de vue ne soit peut-être pas indispensable) grâce au résultat suivant que nous avons précédemment établi ([5]). Nous supposons que K est le corps fini $\mathbb{F}_q$ à q éléments, et désignons pour simplifier l'écriture, par $\mathcal{L}$ l'anneau $K[T]$, $\mathfrak{F}$ le corps $K(T)$, et $\mathfrak{F}_0$ le corps $K((T^{-1}))$.

THÉORÈME 1. - Soient c et N des entiers, $c \geq 0$, $N \geq -1$. Soit (α, β) un couple d'éléments de $\mathfrak{F}_0$. Les conditions suivantes sont équivalentes :

(i) l'inéquation

$$\|h\alpha\| \|h\beta\| \leq q^{-(N+c+3)}$$

n'a pas de solution $h \in \mathcal{L}$, telle que $0 < |h| \leq q^N$;

(ii) le $\mathbb{F}_q$ -espace vectoriel des polynômes $f \in \mathcal{L}$, tels que $|f| \leq q^{N+c}$ et $\|f\alpha\| \leq q^{-(N+2)}$ est de dimension c , et pour tout entier k , $0 \leq k \leq N+c$, il existe un couple de polynômes (f_k, g_{N+c-k}) tel que

$$|f_k| = q^k, \quad |g_{N+c-k}| = q^{N+c-k},$$

et

$$\|f_k\alpha + g_{N+c-k}\beta\| \leq q^{-(N+2)}.$$

Dans le même article, nous établissons également l'équivalence dans $\mathfrak{F}_0$, entre la conjecture de Littlewood, et l'énoncé suivant :

Pour toute constante c' entière ≥ 0 , il existe un couple de polynômes $(f, g) \in \mathcal{L} \times \mathcal{L}$, non tous deux nuls, tel que :

$$\max(1, |f|) \max(1, |g|) \|f\alpha + g\beta\| \leq q^{-(c'+3)}.$$

Y. Taussat nous a d'ailleurs fait remarquer que la méthode de Davenport et Lewis permet également de démontrer ce résultat, ainsi que le théorème 1, sans supposer que le corps de base soit fini.

2. - Conjecture de Littlewood et récurrences linéaires de longueur 3

LEMME 1. - Soit (α, β) un couple d'éléments de $\mathfrak{F}_0$, supposons qu'il existe une constante c entière ≥ 0 , telle que pour tout polynôme non nul $f \in \mathfrak{F}$, on ait :

$$|f| \|f\alpha\| \|f\beta\| \geq q^{-(c+2)}.$$

Soit c' entier ≥ 0 tel que pour tout couple de polynômes $(f, g) \neq (0, 0)$, on ait :

$$\max(|f|, 1) \max(|g|, 1) \|f\alpha + g\beta\| \geq q^{-(c'+2)}.$$

Pour tout entier N tel que $N+c \geq 3$, soit $(f_{k,N}, g_{N+c-k,N})$ un couple de polynômes, de degrés respectifs k et $N+c-k$, tels que

$$\|f_{k,N}\alpha + g_{N+c-k,N}\beta\| \leq q^{-(N+2)}.$$

Pour chaque entier k , $0 \leq k \leq N+c-3$, il existe des polynômes $P_{0,k,N} = P_0, \dots, P_{3,k,N} = P_3$, non tous nuls, tels que

$$\sum_{i=0}^3 P_i f_{k+i,N} = 0$$

$$\sum_{i=0}^3 P_i g_{N+c-k-i,N} = 0$$

et

$$|P_i| \leq q^{c+c'+1}.$$

Preuve. - Ecrivons pour simplifier $f_k = f_{k,N}$ et $g_k = g_{k,N}$. Posons $\gamma_k = \mathcal{K}_0(f_k\alpha + g_{N+c-k}\beta)$. Pour tout quadruplet (P_0, P_1, P_2, P_3) de polynômes de degrés au plus $d = c+c'+1$, on a :

$$\left| \sum_{i=0}^3 P_i \gamma_{k+i} \right| \leq q^{-(N+2-d)}.$$

Puisque la boule $|X| \leq q^{-(N+3d+5)}$ est un sous-espace de la boule $|X| \leq q^{-(N+2-d)}$, de codimension $4d+3$, il existe un quadruplet non nul de polynômes $(P_i)_{0 \leq i \leq 3}$ tel que

$$\left| \sum_{i=0}^3 P_i \gamma_{k+i} \right| \leq q^{-(N+3d+5)}.$$

Posons :

$$F = \sum_{i=0}^3 P_i f_{k+i}$$

$$G = \sum_{i=0}^3 P_i g_{N+c-k-i}$$

puisque

$$\max(1, |F|) \max(1, |G|) \leq q^{N+c+2d+3}$$

et que

$$\|F\alpha + G\beta\| \leq q^{-(N+3d+5)}$$

donc

$$\max(1, |F|) \max(1, |G|) \|F\alpha + G\beta\| \leq q^{c-d-2} = q^{-(c'+3)},$$

on a donc :

$$F = G = 0$$

c. q. f. d.

Remarque. - Il n'existe bien entendu pas de relation non triviale de la forme :

$$P_0 f_k + P_1 f_{k+1} = 0$$

$$P_0 g_{N+c-k} + P_1 g_{N+c-k-1} = 0$$

(pour une raison évidente de degré).

Supposons maintenant qu'on ait une relation non triviale :

$$(1) \quad \begin{cases} P_0 f_k + P_1 f_{k+1} + P_2 f_{k+2} = 0 \\ P_0 g_{N+c-k} + P_1 g_{N+c-k-1} + P_2 g_{N+c-k-2} = 0 \end{cases}$$

et donc :

$$(2) \quad P_0 \gamma_k + P_1 \gamma_{k+1} + P_2 \gamma_{k+2} = 0 .$$

Les relations (1) impliquent que :

$$(3) \quad \left\{ \begin{array}{l} |P_1| > |P_0| \\ \text{et} \\ |P_1| > |P_2| \end{array} \right. .$$

En effet, si par exemple $|P_0| = \max_{0 \leq i \leq 2} |P_i|$, on a :

$$|P_0 g_{N+c-k} + P_1 g_{N+c-k-1} + P_2 g_{N+c-k-2}| = q^{N+c-k} |P_0|$$

donc

$$P_0 g_{N+c-k} + P_1 g_{N+c-k-1} + P_2 g_{N+c-k-2} \neq 0 .$$

Compte tenu de (3), la relation (2) montre alors que :

$$|\gamma_{k+1}| < |\gamma_k| \quad \text{ou} \quad |\gamma_{k+1}| < |\gamma_{k+2}| .$$

Supposons maintenant que les triplets de polynômes $(f_\ell, f_{\ell+1}, f_{\ell+2})$ ainsi que $(g_{N+c-\ell}, g_{N+c-\ell-1}, g_{N+c-\ell-2})$ vérifient des relations du type (1) pour tout entier ℓ , $k-r \leq \ell \leq k+r$ (pour un entier N fixé). Si par exemple, $|\gamma_{k+1}| < |\gamma_{k+2}|$, alors $|\gamma_{k+2}| < |\gamma_{k+3}|$, etc... donc :

$$|\gamma_{k+1}| \leq q^{-(r+1)} |\gamma_{k+r+2}| \leq q^{-(N+r+3)} .$$

De même, si $|\gamma_{k+1}| < |\gamma_k|$, alors $|\gamma_k| < |\gamma_{k-1}|$, etc..., donc :

$$|\gamma_{k+1}| \leq q^{-(r+1)} |\gamma_{k-r}| \leq q^{-(N+r+3)} .$$

On a donc :

$$r \leq c+c'-1 .$$

Ceci montre qu'on ne peut avoir toujours des relations du type (1). Les relations mises en évidence au lemme 1 sont donc essentiellement de longueur 3, i. e. font effectivement intervenir des quadruplets de polynômes (P_0, P_1, P_2, P_3) avec $P_0 P_3 \neq 0$.

Nous allons maintenant étudier la situation pour des relations cubiques entières, i.e. lorsque pour un entier N donné, les polynômes (f_k) et (g_{N+c-k}) vérifient pour tout k :

$$f_{k+3} + P f_{k+2} + Q f_{k+1} + \lambda f_k = 0$$

$$g_{N+c-k-3} + P g_{N+c-k-2} + Q g_{N+c-k-1} + \lambda g_{N+c-k} = 0$$

où P et Q sont des polynômes, et $\lambda \in \mathbb{F}_q^*$.

Nous supposons de plus le polynôme de $\mathbb{F}[X]$, $X^3 + P X^2 + Q X + \lambda$ irréductible sur $\mathbb{F}$. Nous dirons alors que les polynômes (f_k) et (g_{N+c-k}) satisfont à une relation de récurrence cubique entière irréductible.

THÉORÈME 2. - Supposons q pair ou premier. Soit (α, β) un couple d'éléments de $\mathbb{F}_0$, supposons qu'il existe c , entier ≥ 0 , tel que

$$|f| \|f\alpha\| \|f\beta\| \geq q^{-(c+2)}$$

pour tout $f \in \mathbb{F}$, $f \neq 0$.

Soient alors pour tout entier $N \geq 0$, et tout entier k , $0 \leq k \leq N+c$, des polynômes $f_{k,N}$ et $g_{N+c-k,N}$, de degrés respectifs k et $N+c-k$, tels que :

$$\|f_{k,N}^\alpha + g_{N+c-k,N}^\beta\| \leq q^{-(N+2)}.$$

Il n'existe qu'un nombre fini d'entiers N tels que les polynômes $(f_{k,N})$ et $(g_{N+c-k,N})$ satisfassent une relation de récurrence cubique entière irréductible.

Preuve. Si les polynômes $(f_{k,N}) = (f_k)$ et $(g_{N+c-k,N}) = (g_{N+c-k})$ satisfont à une récurrence

$$f_{k+3} + P f_{k+2} + Q f_{k+1} + \lambda f_k = 0$$

$$g_{N+c-k-3} + P g_{N+c-k-2} + Q g_{N+c-k-1} + \lambda g_{N+c-k} = 0,$$

on a nécessairement $|P| = |Q| = q$. La première relation montre en effet que si $|P| > q$, on doit avoir $|Q| = q|P|$, ce qui est incompatible avec la seconde relation. Si $|P| < q$, on doit avoir $|Q| = q^2$, ce qui est également impossible, compte tenu de la seconde relation. Donc $|P| = q$, et de même $|Q| = q$.

LEMME 2. - Le polynôme $X^3 + PX^2 + QX + \lambda$ a trois racines θ , θ' , θ'' , dans $\mathfrak{F}_0$, telles que :

$$|\theta| = q \quad |\theta'| = q^{-1} \quad |\theta''| = 1.$$

Preuve. - Le polynôme $\frac{X^3}{P} + X^2 + \frac{Q}{P}X + \frac{\lambda}{P}$ a pour image dans le corps résiduel $X^2 + \mu X$ (où $\mu \neq 0$ est l'image de Q/P) donc d'après le lemme de Hensel, admet une racine θ'' de valeur absolue 1, et une racine θ' de valeur absolue $|\theta'| < 1$. Il admet donc une racine θ de valeur absolue $|\theta| = \frac{1}{|\theta'|} > 1$. Comme $|\theta + \theta' + \theta''| = q$, on a donc $|\theta| = q$, $|\theta'| = \frac{1}{q}$.

Il existe donc des coefficients A, A', A'', B, B', B'' , appartenant à $\mathfrak{F}(\theta, \theta')$ tels que :

$$(1) \quad f_k = A \theta^k + A' \theta'^k + A'' \theta''^k$$

$$(2) \quad g_{N+c-k} = B \theta^{k-(N+c)} + B' \theta'^{k-(N+c)} + B'' \theta''^{k-(N+c)}.$$

Comme les restes

$$\mathcal{H}_0(f_k \alpha + g_{N+c-k} \beta) = \gamma_k$$

satisfont également la récurrence :

$$\gamma_{k+3} + P \gamma_{k+2} + Q \gamma_{k+1} + \lambda \gamma_k = 0$$

il existe donc des éléments C, C', C'' , de $\mathfrak{F}_0$, tels que :

$$(3) \quad \gamma_k = C \theta^k + C' \theta'^k + C'' \theta''^k.$$

On cherche un polynôme $\Phi(X) \in \mathfrak{F}[X]$, $\Phi(X) = U + VX + WX^2$ ($U, V, W \in \mathfrak{F}$) tel que, si on pose :

$$F = U f_0 + V f_1 + W f_2$$

$$G = U g_{N+c} + V g_{N+c-1} + W g_{N+c-2}$$

$$\Gamma = U \gamma_0 + V \gamma_1 + W \gamma_2,$$

on ait $F \neq 0$ ou $G \neq 0$, et :

$$\max(|F|, 1) \max(|G|, 1) \|\Gamma\| \leq q^{-(c'+3)}$$

où c' est une constante arbitrairement petite, contrairement à l'hypothèse que (α, β) ne satisfasse pas la conjecture de Littlewood.

Posons $N+c = m$, et écrivons :

$$F = A \Phi(\theta) + A' \Phi(\theta') + A'' \Phi(\theta'')$$

$$G = B \theta^{-m} \Phi(\theta) + B' \theta'^{-m} \Phi(\theta') + B'' \theta''^{-m} \Phi(\theta'')$$

$$\Gamma = C \Phi(\theta) + C' \Phi(\theta') + C'' \Phi(\theta'') .$$

Les égalités (1) et (2) montrent que :

$$|A| = |B'| = 1 .$$

Par ailleurs on a nécessairement

$$|A'| \leq q \quad |A''| \leq q .$$

En effet, sinon l'égalité (1), pour $k=0$, montre que $|A'| = |A''|$, et pour $k=1$, on a alors $|A \theta + A' \theta' + A'' \theta''| = |A''| \geq q^2$, ce qui est contradictoire avec (1).

De même

$$|B| \leq q \quad \text{et} \quad |B''| \leq q .$$

Par ailleurs, un argument évident de théorie de Galois prouve que $A \in \mathfrak{F}(\theta)$, $A' \in \mathfrak{F}(\theta')$ et $A'' \in \mathfrak{F}(\theta'')$, et que A' et A'' sont conjugués de A (par le $\mathfrak{F}$ -isomorphisme de $\mathfrak{F}(\theta)$ sur $\mathfrak{F}(\theta')$ (resp. $\mathfrak{F}(\theta'')$), qui applique θ sur θ' (resp. sur θ'')). Donc $A A' A'' \neq 0$. Comme en outre $A(\theta - \theta')(\theta' - \theta'')(\theta'' - \theta)$ est entier sur $\mathfrak{L}$, on a donc

$$|A A' A''| = |N_{\mathfrak{F}(\theta) : \mathfrak{F}} A| \geq q^{-6}$$

et donc finalement :

$$q^{-7} \leq |A'| \leq q \quad q^{-7} \leq |A''| \leq q .$$

De même

$$q^{-7} \leq |B| \leq q \quad q^{-7} \leq |B''| \leq q .$$

D'autre part, puisque $|\gamma_k| \leq q^{-(N+2)}$ pour tout k , on a donc :

$$|C''| \leq q^{-(m+2-c)}$$

$$|C'| \leq q^{-(m+2-c)}$$

$$|C| \leq q^{-(2m+2-c)}.$$

On se donne alors deux constantes entières $D \geq 0$ et $\delta > 0$, telles que $\delta - D \geq c' + c + 1$, et nous allons montrer que pour un choix convenable de ces constantes, on peut choisir le polynôme $\Phi \neq 0$ tel que :

$$(4) \quad |A \Phi(\theta) + A'' \Phi(\theta'')| \leq q^{-\delta} |\Phi(\theta)|$$

$$(5) \quad |A' \Phi(\theta')| \leq q^{-\delta} |\Phi(\theta)|$$

$$(6) \quad |B \Phi(\theta)| < q^{2m} |\Phi(\theta')|$$

$$(7) \quad |B'' \Phi(\theta'')| < q^m |\Phi(\theta')|$$

$$(8) \quad |\Phi(\theta')| \leq |\Phi(\theta'')|$$

$$(9) \quad |\Phi(\theta)| \leq q^m |\Phi(\theta'')|$$

$$(10) \quad |N_{\mathcal{F}(\theta)} \Phi(\theta)| \leq q^D.$$

Les conditions (4) et (5) montreront que

$$|F| \leq q^{-\delta} |\Phi(\theta)|$$

les conditions (6), (7), que :

$$|G| = q^m |\Phi(\theta')| \neq 0$$

et enfin, (8) et (9), que :

$$|\Gamma| \leq q^{-(m+2-c)} |\Phi(\theta'')|.$$

Comme on assurera également la condition

$$(11) \quad |\Phi(\theta)| \geq q^{\delta}$$

on aura bien :

$$\max(|F|, 1) \max(|G|, 1) |\Gamma| \leq q^{-(c'+3)}.$$

Si (4) est satisfaite, on a

$$|\Phi(\theta)| = |A''| |\Phi(\theta'')|$$

donc :

$$q^{-7} |\Phi(\theta'')| \leq |\Phi(\theta)| \leq q |\Phi(\theta'')|$$

la condition (9) est alors satisfaite.

La condition (5) impliquera alors

$$|\Phi(\theta')| \leq q^{7-\delta} |\Phi(\theta)| \leq q^{8-\delta} |\Phi(\theta'')|$$

ainsi la condition (8) sera satisfaite pourvu que $\delta \geq 8$.

D'autre part, si la condition (4) est satisfaite, on a :

$$|B\Phi(\theta)| \leq q^9 |B''| |\Phi(\theta'')|$$

la condition (6) sera alors incluse dans (7) dès que $m \geq 9$.

Il ne reste donc à satisfaire que les conditions (4), (5), (7), (10), (11).

Si on a les conditions (4) et

$$(10) \quad 1 \leq |\Phi(\theta) \Phi(\theta') \Phi(\theta'')| \leq q^D,$$

comme alors

$$|\Phi(\theta)| = |A''| |\Phi(\theta'')|,$$

on a :

$$|\Phi(\theta')| \leq \frac{q^{D+1}}{|\Phi(\theta)|^2}.$$

La condition (5) sera vérifiée dès que (11) le sera, et que $|\Phi(\theta')| < 1$, donc dès que :

$$|\Phi(\theta)|^2 > q^{D+1},$$

ce qui est impliqué par la condition (11).

Ainsi (5) est impliqué par (4), (10) et (11). Les conditions (4) et (10) montrent également que :

$$|\Phi(\theta')| \geq \frac{1}{q |\Phi(\theta'')|^2}$$

la condition (7) est alors satisfaite si

$$|\Phi(\theta'')|^3 \leq q^{m-3}.$$

La condition (11) est impliquée par :

$$|\Phi(\theta'')| \geq q^{\delta+7}.$$

En définitive, les conditions à satisfaire sont donc :

$$(4) \quad |A \Phi(\theta) + A'' \Phi(\theta'')| \leq q^{-\delta} |\Phi(\theta)|$$

$$(10) \quad |N(\Phi(\theta''))| \leq q^D$$

(où N désigne la norme dans l'extension $\mathfrak{F} \rightarrow \mathfrak{F}(\theta'')$)

$$\text{et} \quad (12) \quad q^{3(\delta+7)} \leq |\Phi(\theta'')|^3 \leq q^{m-3}.$$

Pour étudier les conditions, nous allons maintenant nous intéresser à l'arithmétique du corps cubique $\mathfrak{F}(\theta'')$. On a tout d'abord le résultat suivant (analogue au théorème de Minkowski dans $\mathbb{R}^n$) :

LEMME 3. - Soit n un entier positif, et soit μ la mesure de Haar sur $\mathfrak{F}_0^n$, normalisée par $\mu(\mathfrak{M}_0^n) = 1$. Soit U une partie bornée intégrable de $\mathfrak{F}_0^n$, telle que $\mu(U) > 1$. Alors $(U-U) \cap \mathfrak{L}^n \neq \{0\}$.

Preuve. - Pour tout $X = (X_1, \dots, X_n) \in \mathfrak{F}_0^n$ ($X_i \in \mathfrak{F}_0$), posons $|X| = \max_i |X_i|$, et $|U| = \max_{X \in U} |X|$. Soit K un entier ≥ 0 tel que $|U| \leq q^K$. Si $(U-U) \cap \mathfrak{L}^n = \{0\}$, les ensembles $f+U$, où $f \in \mathfrak{L}^n$, sont disjoints deux à deux, et puisque $|f+U| \leq q^K$ pour tout f tel que $|f| \leq q^K$, on a donc :

$$q^{n(K+1)} \mu(U) \leq q^{n(K+1)}$$

soit

$$\mu(U) \leq 1.$$

COROLLAIRE. - Soit U une partie bornée intégrable de $\mathfrak{F}_0^n$. Soit $(e_1, \dots, e_n)$ une base de $\mathfrak{F}_0^n$, on note $\det(e_1, \dots, e_n)$, le déterminant de la matrice des composantes des (e_i) dans la base naturelle. Pour que $(U-U) \cap (\mathfrak{L} e_1 + \dots + \mathfrak{L} e_n)$ ne soit pas réduit à $\{0\}$, il suffit que

$$\mu(U) > |\det(e_1, \dots, e_n)|.$$

Preuve. - Soit φ l'automorphisme de $\mathfrak{F}_0^n$ appliquant la base naturelle sur $(e_1, \dots, e_n)$. La condition $(U-U) \cap (\mathfrak{L} e_1 + \dots + \mathfrak{L} e_n) \neq \{0\}$ équivaut à $(U'-U') \cap \mathfrak{L}^n \neq \{0\}$ où $U' = \varphi^{-1}(U)$. Or $\mu(U') = \frac{\mu(U)}{|\det(e_1, \dots, e_n)|}$.

Nous déduisons tout d'abord de ce corollaire le résultat suivant :

LEMME 4. - Soit $\mathcal{K}$ une extension cubique séparable de $\mathfrak{F}$, ayant tous ses conjugués dans $\mathfrak{F}_0$. Le discriminant de $\mathcal{K}$ est de valeur absolue au moins q^4 .

Remarque. - Toute extension de $\mathfrak{F}$ incluse dans $\mathfrak{F}_0$ est en fait séparable.

Preuve. - Soient $\sigma, \sigma', \sigma''$ les $\mathfrak{F}$ -isomorphismes (distincts) de $\mathcal{K}$ dans $\mathfrak{F}_0$. Soit u l'injection de $\mathcal{K}$ dans $\mathfrak{F}_0^3$:

$$u : X \rightarrow (\sigma(X), \sigma'(X), \sigma''(X)).$$

Soit $(\alpha_1, \alpha_2, \alpha_3)$ une base de $\mathfrak{L}$ -module de l'anneau $\mathcal{A}$, clôture intégrale de $\mathfrak{L}$ dans $\mathcal{K}$. Posons $u(\alpha_i) = \tilde{\alpha}_i$, puisque $\sigma, \sigma', \sigma''$ sont $\mathfrak{F}_0$ -linéairement indépendants, le déterminant

$$\Delta = \begin{vmatrix} \sigma(\alpha_1) & \sigma(\alpha_2) & \sigma(\alpha_3) \\ \sigma'(\alpha_1) & \sigma'(\alpha_2) & \sigma'(\alpha_3) \\ \sigma''(\alpha_1) & \sigma''(\alpha_2) & \sigma''(\alpha_3) \end{vmatrix}$$

est non nul, et $(\tilde{\alpha}_1, \tilde{\alpha}_2, \tilde{\alpha}_3)$ est donc une base de $\mathfrak{F}_0^3$.

Soit V l'ensemble des éléments $(X_1, X_2, X_3) \in \mathfrak{F}_0^3$ tels que $|X_1 X_2 X_3| < 1$, on a $V \cap (\mathfrak{L} \tilde{\alpha}_1 + \mathfrak{L} \tilde{\alpha}_2 + \mathfrak{L} \tilde{\alpha}_3) = \{0\}$ car la norme d'un élément de $\mathcal{K}$, non nul et entier sur $\mathfrak{L}$, est de valeur absolue au moins 1. L'ensemble U des éléments $(X_1, X_2, X_3) \in \mathfrak{F}_0^3$ tels que $|X_1| \leq \frac{1}{q}$, $|X_2| \leq \frac{1}{q}$, $|X_3| \leq q$, est inclus dans V , est bornée et intégrable, de mesure $\mu(U) = q^2$, et de plus $U-U \subset U$. On a donc, d'après le corollaire du lemme 3 : $\Delta \geq q^2$.

Revenant à $\mathfrak{F}(\theta'')$, il en résulte donc que :

LEMME 5. - Les éléments $(1, \theta'', \theta''^2)$ forment une base de $\mathfrak{F}$ -module de l'an-
neau des entiers de $\mathfrak{F}(\theta'')$.

En effet :

$$\left| \det \begin{pmatrix} 1 & \theta & \theta^2 \\ 1 & \theta' & \theta'^2 \\ 1 & \theta'' & \theta''^2 \end{pmatrix} \right| = q^2$$

donc $\mathfrak{F}(\theta'')$ est de discriminant de valeur absolue q^4 , et $1, \theta'', \theta''^2$ est une base d'entiers.

Les conditions (4), (10), (12), reviennent alors à trouver un élément entier $u \in \mathfrak{F}(\theta'')$, non nul, tel que, σ désignant le $\mathfrak{F}$ -isomorphisme de $\mathfrak{F}(\theta'')$ dans $\mathfrak{F}_0$ appliquant θ'' sur θ , on ait :

$$(4) \quad \left| 1 + \frac{A''u}{\sigma(A''u)} \right| \leq q^{-\delta}$$

$$(10) \quad |Nu| \leq q^D$$

$$(12) \quad q^{3(\delta+7)} \leq |u|^3 \leq q^{m-3}.$$

Nous allons chercher un élément non nul $v \in \mathfrak{F}(\theta'')$, entier sur $\mathfrak{F}$, satisfaisant aux conditions

$$(4') \quad \left| 1 + \frac{v}{\sigma(v)} \right| \leq q^{-\delta}$$

$$(10') \quad |Nv| \leq q^{D'}$$

où $D' = D - 28$ (en supposant $D \geq 28$) et

$$(12') \quad q^{3(\delta+6)} \leq |v|^3 \leq q^{m-30}$$

(en supposant $3(\delta+6) \leq m-30$).

En effet, il existe un élément $h \in \mathfrak{F}$, $h \neq 0$, tel que $\frac{h}{A''}$ soit entier sur $\mathfrak{L}$, et si on a un élément v satisfaisant les conditions (4'), (10'), (12'), il suffit alors de prendre :

$$u = \frac{h}{A''} v.$$

On a bien

$$(4) \quad \left| 1 + \frac{A'' u}{\sigma(A'' u)} \right| \leq q^{-\delta}.$$

D'autre part, on peut écrire A'' sous la forme

$$A'' = \frac{Z}{\Delta}$$

$$\left(\Delta = \begin{vmatrix} 1 & 1 & 1 \\ \theta & \theta' & \theta'' \\ \theta^2 & \theta'^2 & \theta''^2 \end{vmatrix}^2 \right)$$

où Z est entier. Il est clair que $\Delta \in \mathfrak{L}$. On peut prendre :

$$h = \frac{NZ}{\Delta}.$$

On a :

$$N\left(\frac{h}{A''}\right) = \frac{h^3}{NA''} = \left(\frac{NZ}{\Delta}\right)^3 \frac{\Delta^3}{NZ} = (NZ)^2.$$

Or puisque $|A| = 1$ et $|A'| \leq q$, $|A''| \leq q$, on a donc $|NA''| \leq q^2$, donc :

$$|NZ| = |\Delta|^3 |NA''| \leq q^{14}.$$

Ainsi :

$$\left| N\left(\frac{h}{A''}\right) \right| \leq q^{28}$$

donc

$$|Nu| \leq q^{28} |Nv|$$

ainsi (10') implique bien (10).

Enfin, comme

$$\frac{h}{A''} = \frac{NZ}{Z} = \Delta^2 \frac{NA''}{A''} = \Delta^2 AA'$$

on a :

$$\left| \frac{h}{A''} \right| = q^8 |A'|$$

soit

$$q \leq \left| \frac{h}{A''} \right| \leq q^9$$

ainsi la condition (12') implique (12).

Nous allons montrer que trouver un élément v satisfaisant aux conditions (4'), (10') et (12') revient essentiellement à trouver un élément entier $w \in \mathfrak{F}(\theta'')$, non nul, et tel que

$$(13) \quad \left| 1 + \frac{w}{\sigma(w)} \right| < \frac{1}{|N w|}.$$

LEMME 6. - Il existe une unité $\theta_1 \in \mathfrak{F}(\theta'')$ telle que $|\theta_1| = q$ et $|\sigma(\theta_1)| = 1$.

Preuve. - Soient σ, σ' , les $\mathfrak{F}$ -isomorphismes de $\mathfrak{F}(\theta'')$ dans $\mathfrak{F}_0$ appliquant θ'' sur θ et θ' respectivement. L'ensemble U des éléments $(X, Y, Z) \in \mathfrak{F}_0^3$ tels que $|X| \leq q$, $|Y| \leq 1$, et $|Z| \leq \frac{1}{q}$, est de mesure $\mu(U) = q^3$, et est tel que $U - U = U$. D'après le corollaire du lemme 3, il existe donc un entier non nul $\theta_1 \in \mathfrak{F}(\theta'')$, tel que $|\theta_1| \leq q$, $|\sigma(\theta_1)| \leq 1$, et $|\sigma'(\theta_1)| \leq \frac{1}{q}$, ainsi θ_1 est une unité satisfaisant aux conditions du lemme 6. (Naturellement, si l'extension $\mathfrak{F}(\theta'')$ est galoisienne sur $\mathfrak{F}$, il suffit de prendre $\theta_1 = 1/\theta'$.)

Nous pouvons maintenant démontrer le théorème 2 dans le cas où q est une puissance de 2. Puisque $\left| \frac{\theta'' \theta_1}{\sigma(\theta'' \theta_1)} \right| = 1$, on a :

$$\left| 1 + \left(\frac{\theta'' \theta_1}{\sigma(\theta'' \theta_1)} \right)^{q-1} \right| \leq \frac{1}{q}.$$

(en considérant l'image de $\frac{\theta'' \theta_1}{\sigma(\theta'' \theta_1)}$ dans le corps résiduel $\mathbb{F}_q$). Alors, pour tout entier $s \geq 0$:

$$\left| 1 + \left(\frac{\theta'' \theta_1}{\sigma(\theta'' \theta_1)} \right)^{2^s(q-1)} \right| \leq \frac{1}{q^{2^s}}.$$

On prendra donc $v = (\theta'' \theta_1)^{2^s(q-1)}$, avec s suffisamment grand, $D' = 1$, et puisque $|v| = q^{2^s(q-1)}$, il suffira de choisir $m \geq 30 + 3(q-1)2^s$.

Dans le cas où q n'est pas une puissance de 2, on procède de la façon suivante : posons

$$\left| \left(\frac{\theta'' \theta_1}{\sigma(\theta'' \theta_1)} \right)^{q-1} - 1 \right| = q^{-a}.$$

L'entier a est positif. Nous en donnons d'autre part une majoration explicite (bien qu'on puisse se contenter pour la suite de la démonstration du fait que les entiers a ainsi définis sont uniformément majorés puisqu'on ne considère qu'un nombre fini de corps cubiques $\mathfrak{F}(\theta'')$!).

LEMME 7. - On a $0 < a \leq 3q-5$.

Preuve. - Puisque la valeur absolue du discriminant de $\mathfrak{F}(\theta)$ est q^4 , on a :

$$|(\theta'' \theta_1)^{q-1} - \sigma(\theta'' \theta_1)^{q-1}| |(\theta'' \theta_1)^{q-1} - \sigma'(\theta'' \theta_1)^{q-1}| |(\sigma(\theta'' \theta_1)^{q-1} - \sigma'(\theta'' \theta_1)^{q-1}| \geq q^2$$

et puisque $|\theta'' \theta_1| = |\sigma(\theta'' \theta_1)| = q$ et $|\sigma'(\theta'' \theta_1)| = \frac{1}{q}$, on a donc :

$$|(\theta'' \theta_1)^{q-1} - \sigma(\theta'' \theta_1)^{q-1}| \geq q^{-2q+4}$$

et ainsi :

$$\left| 1 - \frac{(\theta'' \theta_1)^{q-1}}{\sigma(\theta'' \theta_1)^{q-1}} \right| \geq q^{-3q+5}.$$

LEMME 8. - Il existe un élément non nul $w \in \mathfrak{F}(\theta'')$, entier sur $\mathfrak{f}$, tel que :

$$|w + \sigma(w)| \leq q^{-a}$$

$$|w| \leq 1$$

$$|\sigma'(w)| \leq q^a.$$

Preuve. - Soit U l'ensemble des éléments $(w_1, w_2, w_3) \in \mathfrak{F}_0^3$, tels que

$$|w_1 + w_2| \leq q^{-a}$$

$$|w_1| \leq 1$$

$$|w_3| \leq q^a.$$

On a $\mu(U) = q^3$ et il suffit d'appliquer le corollaire du lemme 3.

LEMME 9. - Il existe un élément non nul $v_0 \in \mathfrak{F}(\theta'')$, entier sur $\mathfrak{L}$, tel que :

$$\left| 1 + \frac{v_0}{\sigma(v_0)} \right| < \frac{1}{N v_0}$$

et

$$|N v_0| \leq q^a.$$

Preuve. - Soit w satisfaisant aux conditions du lemme 8. Deux cas se présentent, selon que $|w| < 1$ ou $|w| = 1$.

Si $|w| < 1$, soit $|w| = q^{-t}$, avec $t > 0$. Comme on ne peut avoir simultanément $|w| \leq q^{-a}$ et $|\sigma(w)| \leq q^{-a}$, puisque $|\sigma'(w)| \leq q^a$, on a donc $|w| = |\sigma(w)| = q^{-t}$, donc $|Nw| \leq q^{a-2t}$ et $\left| 1 + \frac{w}{\sigma(w)} \right| \leq q^{-a+t}$. On peut donc dans ce cas prendre $v_0 = w$.

Si $|w| = 1$ on a :

$$\left| 1 + \frac{w}{\sigma(w)} \right| \leq q^{-a}$$

et

$$|Nw| \leq q^a.$$

Or, pour tout entier $k > 0$, soit H_k le groupe multiplicatif des éléments $h \in \mathfrak{F}_0$ tels que $|h-1| \leq q^{-k}$. Pour tout $k > 0$, le quotient H_k/H_{k+1} est isomorphe au groupe additif de $\mathbb{F}_q$ (par l'application $\mu \mapsto 1 + \mu T^{-k} \pmod{H_{k+1}}$). Puisque par définition, l'élément $\left(\frac{\theta'' \theta_1}{\sigma(\theta'' \theta_1)} \right) q^{-1}$ appartient à H_a , mais n'appartient pas à H_{a+1} , et puisque q est premier, cet élément engendre H_a/H_{a+1} .

Puisque $-\frac{w}{\sigma(w)} \in H_a$, il existe donc un entier ν tel que

$$\left| 1 + \frac{(\theta'' \theta_1)^{\nu(q-1)} w}{\sigma((\theta'' \theta_1)^{\nu(q-1)} w)} \right| \leq q^{-(a+1)}$$

et puisque $|N((\theta'' \theta_1)^{\nu(q-1)} w)| = |Nw| \leq q^a$, on peut donc prendre :

$$v_o = (\theta'' \theta_1)^{\nu(q-1)} w.$$

Fin de la démonstration

Soit v_o satisfaisant aux conditions du lemme 9. Puisque $\left| \left(\frac{\theta'' \theta_1}{\sigma(\theta'' \theta_1)} \right)^{q(q-1)} - 1 \right| < q^{-a}$, quitte à multiplier v_o par une puissance entière de $(\theta'' \theta_1)^{q(q-1)}$, ce qui ne change pas $|N v_o|$, on peut supposer que $q \leq |v_o| \leq q^{q(q-1)}$.

Puisque $\lim_{s \rightarrow +\infty} \left| N v_o \right|^{q^s} \left| 1 + \frac{v_o^{q^s}}{\sigma(v_o^{q^s})} \right| = 0$, on trouvera pour m suffisamment grand, un élément $v \in \mathfrak{F}(\theta'')$, non nul, entier sur $\mathfrak{L}$, satisfaisant aux conditions (4'), (10'), (12'), de la forme $v = v_o^{q^s}$.

-:-:-:-

BIBLIOGRAPHIE

- [1] A. BAKER, On an analogue of Littlewood's diophantine approximation problem, Michigan Math. J. (11) (1964), 247-250.
- [2] J.W.S. CASSELS, An introduction to the geometry of numbers, Springer-Verlag-Berlin.
- [3] J.W.S. CASSELS and H.P.F. SWINNERTON-DYER, On the product of three homogeneous linear forms and indefinite ternary quadratic forms, Philos. Trans. Roy. Soc. London, ser. A, 248 (1955), 73-96.
- [4] H. DAVENPORT and D.J. LEWIS, An analogue of a problem of Littlewood, Michigan Math. J. 10 (1963), 157-160.

- [5] B. de MATHAN, Quelques remarques sur la conjecture de Littlewood (en approximations diophantiennes simultanées), Séminaire de Théorie des Nombres de Bordeaux (1978-1979) exposé n° 5.

(texte reçu le 6 mars 1981)

-:-:-:-

Bernard de MATHAN
U.E.R. de Mathématiques
et d'Informatique
Université de Bordeaux I
F 33405 TALENCE CEDEX

THE ANNIHILATION OF DIVISOR CLASSES IN ABELIAN EXTENSIONS OF THE RATIONAL FUNCTION FIELD

by

Benedict H. GROSS

-:-:-:-

§.1. - Abelian extensions

Let F be the finite field with q elements, let $A = F[x]$ be the ring of polynomials over F , and let $k = F(x)$ be the field of rational functions over F . The following construction of abelian extensions of k is due to Carlitz [1].

Let U be an A -algebra. Then there is a unique homomorphism of F -algebras $A \xrightarrow{f} \text{End}_F(U^+)$ which takes x to the endomorphism $f_x(u) = xu + u^q$. Via the map f , U^+ inherits a new A -module structure; we write this action as $u \mapsto f_m(u)$ for $m \in A$. Then $f_{m+n}(u) = f_m(u) + f_n(u)$ and $f_{mn}(u) = f_m(f_n(u))$. If m has degree d , then

$$(1.1) \quad f_m(u) = \begin{bmatrix} m \\ 0 \end{bmatrix} u + \begin{bmatrix} m \\ 1 \end{bmatrix} u^q + \dots + \begin{bmatrix} m \\ d-1 \end{bmatrix} u^{q^{d-1}} + \begin{bmatrix} m \\ d \end{bmatrix} u^{q^d}$$

where $\begin{bmatrix} m \\ i \end{bmatrix}$ is a polynomial in x of degree $q^i(d-i)$, $\begin{bmatrix} m \\ 0 \end{bmatrix} = m$ and $\begin{bmatrix} m \\ d \end{bmatrix}$ is the leading coefficient of m .

Now let $U = \bar{k}$, the algebraic closure of k . Fix a monic polynomial m of $\deg d \geq 1$ and let $\Lambda_m = \{u \in U : f_m(u) = 0\}$. Since the polynomial $f_m(u)$ is separable, Λ_m is a finite A -module of cardinality q^d . In fact, Λ_m is isomorphic (non-canonically) to A/m .

Let $K = k(\Lambda_m)$; then K is a finite Galois extension of k and

$$(1.2) \quad G = \text{Gal}(K/k) \hookrightarrow \text{Aut}(\Lambda_m) \simeq (A/m)^*.$$

One can show that the map in (1.2) is an isomorphism; for $a \in (A/m)^*$ we denote the corresponding element of G by σ_a .

Since $f'_m(u) \neq 0$, the extension K/k is unramified at all finite places which do not divide m . At the infinite place, the inertia subgroup of G is the image of $A^* = F^*$ under the natural map $A^* \hookrightarrow (A/m)^*$. We denote this subgroup by J ; it is cyclic of order $(q-1)$. In fact, J is the full decomposition group of ∞ in G : the infinite place splits completely in the subfield $K^+ = (K)^J$.

$$(1.3) \quad G \simeq (A/m)^* \begin{array}{c} K \\ / \\ K^+ \\ / \\ k \end{array} \begin{array}{l} J \simeq A^* \\ \\ G/J \end{array}$$

For more details on the fields K and K^+ , the reader should consult Carlitz [1], Hayes [3], and Rosen-Galovich [2].

§.2. - The divisor class group

Let D denote the group of divisors of K , D_0 the subgroup of divisors of degree 0, and P the subgroup of principal divisors. Then P is a subgroup of D_0 ; the quotient $C = D_0/P$ is the divisor class group of K . The group C is a finite module for the integral group ring $\mathbb{Z}[G]$; similarly the divisor class group C^+ of K^+ is a finite module for $\mathbb{Z}[G/J]$.

For any class $a \in (A/m)^*$, let $\langle a \rangle$ be the unique representative of a in A with $\deg \langle a \rangle < \deg m$. Notice that the elements σ_a in G with $\langle a \rangle$ monic form a set of coset representatives for the subgroup J . Also the integer $\deg \langle a \rangle$ depends only on the image of σ_a in G/J .

PROPOSITION 2.1. - a) The element $\eta = \sum_{\langle a \rangle \text{ monic}} \sigma_a^{-1}$ of $\mathbb{Z}[G]$ annihilates C .

b) The element $\eta^+ = \sum_{G/J} \deg \langle a \rangle \sigma_a^{-1}$ of $\mathbb{Z}[G/J]$ annihilates C^+ .

The results in (2.1) are analogs of Stickelberger's theorem on the annihilation of ideal classes in cyclotomic fields. They were suggested by Tate's formulation of Stark's conjectures for functions fields, and are special cases of a more general pattern.

Let k be a function field in one variable with field of constants F , the finite field with q elements. Let K be an abelian extension of k with Galois group G . Let S denote a finite, non-empty set of primes of k which includes all primes which ramify in K/k , and let $w = q^n - 1$ be the number of roots of unity in K . For $\sigma \in G$, let $\zeta(\sigma, s)$ be the partial zeta-function of σ relative to the set S ; then $\zeta(\sigma, s)$ is regular at $s=0$ and $w\zeta(\sigma, 0)$ is a rational integer. Let $\theta = \sum_G \zeta(\sigma, 0) \sigma^{-1}$; then $w\theta$ is an element of $\mathbb{Z}[G]$ and acts on C , the divisor class group of K .

PROPOSITION 2.2. - a) (Tate) - The element $w\theta$ of $\mathbb{Z}[G]$ annihilates $C = D_0/P$.

b) (Deligne) - If we write $a^{w\theta} = \text{div}(\epsilon_a)$ for $a \in D_0$, then $K(\sqrt[w]{\epsilon_a})$ is an abelian extension of k .

The proof of (2.2) involves the geometry of the curve $\overline{X} = X \otimes_F \overline{F}$, where X is the non-singular complete curve with function field K . The key ingredient is Weil's formula for the L -functions of K/k in terms of the generalized Jacobian of $\overline{X}$.

The relationship between (2.1) and (2.2) is the following. Let $k = F(x)$; by an explicit calculation of the partial zeta-functions for $K = k(\Lambda_m)$ and K^+ one finds :

$$(2.3) \quad \begin{cases} \theta = \eta - \frac{1}{q-1} \sum_G \sigma \\ \theta^+ = -\eta^+ + (d-1 - \frac{1}{q-1}) \sum_{G/J} \sigma \end{cases}$$

In this case $w = q-1$ and the norm annihilates the class group (as k has class number 1). From part a) of (2.2) it follows that $w\eta$ annihilates C and $w\eta^+$ annihilates C^+ . One can remove the w by looking at Tate's proof more carefully and using the "Riemann hypothesis" for K . Then (2.1) yields a simple proof of part b) : in this case ε_a is congruent (modulo K^{*w}) to an element of k^* .

Finally, we should note that Tate and Deligne have a similar result for the action of $w\theta$ on D . For the field K^+ , their result is related to the "circular units" of Rosen and Galovich [2].

§. 3. - Hecke characters

If ω_1 is any place of K dividing ω , then $(\omega_1)^\eta = \frac{1}{q-1}(\omega)$. If we combine this with (2.1. a) we see that for any divisor $a \in D$ we have

$$(3.1) \quad a^\eta = \text{div}(\varepsilon_a) + \frac{\deg a}{q-1}(\omega)$$

where $\varepsilon_a \in K^*$ is well-determined modulo F^* . The element $\chi(a) = (\varepsilon_a)^{q-1}$ is then uniquely determined by a , and the assignment $a \mapsto \chi(a)$ gives a "Hecke character" of K of conductor 1.

When $m = p^n$ is the power of an irreducible polynomial p , we can refine this construction slightly. The divisor (p) of k is totally ramified in K ; let $\mathfrak{p}$ denote its unique prime factor.

PROPOSITION 3.2. - If $(a, \mathfrak{p}) = 1$ then $\chi(a) \equiv 1 \pmod{\mathfrak{p}}$.

The proof of (3.2) is not difficult. As a consequence, we see that we may specify ε_a uniquely, for divisors a which are prime to $\mathfrak{p}$, by insisting that $\varepsilon_a \equiv 1 \pmod{\mathfrak{p}}$. The assignment $a \mapsto \varepsilon_a$ then gives a "Hecke character" of K of conductor $\mathfrak{p}$.

BIBLIOGRAPHY

- [1] CARLITZ L., A class of polynomials, Trans. Amer. Math. Soc. 43 (1938), 167-182.
- [2] GALOVICH S. and ROSEN M., The class number of cyclotomic fields, to appear in J. Number Theory.
- [3] HAYES D., Explicit class field theory for rational function fields, Trans. Amer. Math. Soc. 189 (1974), 77-91.

(texte reçu le 28 novembre 1980)

--:--:--

Benedict H. GROSS
Department of Mathematics
Princeton University
Princeton, New Jersey 08540

TRANSCENDANCE ET FONCTIONS ELLIPTIQUES

par

Eric REYSSAT

-:-:-:-

1. - Introduction

Trois grandes méthodes de transcendance sont actuellement en pleine expansion. L'une, initiée par Mahler et reprise récemment par exemple dans les travaux de van der Poorten et Loxton, étudie certaines séries vérifiant des équations fonctionnelles. Une autre consiste à étudier des fonctions vérifiant des systèmes d'équations différentielles et des conditions arithmétiques sur les coefficients de Taylor. Cette méthode a été développée par Siegel et considérablement renforcée par les travaux de Shidlovski ; elle permet de montrer la transcendance (et l'indépendance algébrique) de valeurs de fonctions hypergéométriques comme la fonction exponentielle et les fonctions de Bessel. Enfin la méthode de Gel'fond et Schneider, étendue par Baker, permet de travailler sur des fonctions vérifiant un théorème d'addition algébrique et des équations différentielles - ces deux propriétés n'étant pas toujours simultanément indispensables. Elle permet d'étudier par exemple les propriétés arithmétiques de fonctions exponentielles, elliptiques ou abéliennes.

Nous nous limiterons dans cet exposé à étudier quelques résultats sur les fonctions elliptiques obtenus par cette dernière méthode.

Nous donnons pour commencer un petit aperçu des résultats sur les fonctions elliptiques que la méthode de Gel'fond-Schneider et ses prolongements ont permis de démontrer récemment.

a) Du point de vue strictement de la transcendance, un progrès a été marqué par la découverte par Waldschmidt de nouveaux nombres transcendants, liés à la fonction σ de Weierstrass (cf. théorème 2).

b) Une généralisation de la notion de transcendance est celle d'indépendance linéaire sur le corps $\bar{\mathbb{Q}}$ des nombres algébriques. Cette voie a également connu de grands progrès récents. Citons le résultat de Laurent [L] sur la transcendance des périodes non nulles de formes différentielles elliptiques définies sur $\bar{\mathbb{Q}}$ et à résidus rationnels ; la démonstration utilise la méthode de Baker. Un autre résultat très important a été démontré par Bertrand et Masser [B-M] : si $u_1, \dots, u_n$ sont des points algébriques d'une fonction $\wp$ linéairement indépendants sur $\mathbb{Q}$, et si $\wp$ n'a pas de multiplication complexe, alors les nombres $1, u_1, \dots, u_n$ sont linéairement indépendants sur $\bar{\mathbb{Q}}$ (le cas où $\wp$ admet une multiplication complexe a été traité par Masser en 1974).

c) Le point de vue quantitatif de la transcendance est celui des mesures de transcendance. L'étude systématique des nombres transcendants fournis par les théorèmes de Schneider (cf. §.3), et celui de Waldschmidt cité plus haut, nous a permis d'obtenir de nombreuses mesures, parfois très précises et proches des meilleures possibles (voir au §.4, les exemples des nombres $\frac{\pi}{w}$ et $\wp(1)$).

d) Après la transcendance vient l'indépendance algébrique de plusieurs nombres, domaine qui a également connu des développements récents. Citons par exemple les travaux de Wüstholz [Wü], ceux de Choodnovsky sur un analogue elliptique partiel du théorème de Lindemann-Weierstrass (cf [3]), et les résultats liés à la fonction σ de Weierstrass que nous avons récemment obtenus et que nous discutons au §.5 (cf. [R]).

e) Enfin les mesures d'indépendance algébrique, bien qu'encore rares dans le domaine des fonctions elliptiques, existent maintenant sous des formes très précises grâce aux travaux de Choodnovsky (cf. [C1] et [C2]).

Il ne peut être question d'exposer ici tous ces résultats, et nous renvoyons pour cela à la bibliographie. On se limitera ici, après un bref rappel sur les fonctions elliptiques (§.2), à exposer les idées de la démonstration des théorèmes de transcendance de Schneider (§.3), afin de découvrir les problèmes qui se posent dans les démonstrations de mesures de transcendance (§.4) et d'indépendance algébrique (§.5).

2. - Rappels sur les fonctions elliptiques

Soit L un réseau de $\mathbb{C}$. Une fonction f est dite elliptique par rapport à L si elle est méromorphe sur $\mathbb{C}$ et admet tout élément de L pour période. Une fonction θ est dite fonction thêta par rapport à L si elle est entière et "pas trop loin d'être périodique" :

$$\theta(z+w) = e^{L_w(z)} \theta(z) \quad w \in L,$$

où L_w est une fonction affine de z . Remarquons qu'une telle fonction définit une fonction elliptique f par la formule

$$f(z) = \frac{d}{dz} \frac{\theta'}{\theta}(z) = \frac{d^2}{dz^2} \log \theta(z).$$

Weierstrass a construit un exemple fonction thêta non triviale (i.e. définissant une fonction elliptique non constante) ; il s'agit de la fonction σ , canoniquement associé au réseau L , et définie par

$$\sigma(z) = z \prod_{L \setminus \{0\}} \left(1 - \frac{z}{w}\right) \exp\left(\frac{z}{w} + \frac{z^2}{2w^2}\right).$$

On définit les fonctions ζ et $\wp$ de Weierstrass par les formules :

$$\zeta = \sigma'/\sigma \quad \text{et} \quad \wp = -\zeta'.$$

La fonction $\wp$ est alors elliptique, la fonction ζ est quasi-périodique :

$$\zeta(z+w) = \zeta(z) + \eta$$

où η est une constante dépendant de ω . La fonction σ vérifie la relation

$$\sigma(z+\omega) = \pm e^{\eta(z+\frac{\omega}{2})} \sigma(z).$$

Notons enfin dès maintenant une propriété fondamentale de la fonction $\wp$, à savoir son équation différentielle qu'on peut écrire sous la forme :

$$\wp'^2(z) = 4\wp^3(z) - g_2\wp(z) - g_3,$$

où g_2 et g_3 sont des constantes dépendant uniquement du réseau L .

3. - Quelques résultats de transcendance

L'équation différentielle de la fonction $\wp$ servira dans les démonstrations de transcendance à exprimer toutes les dérivées de $\wp$ en fonction de $\wp$ et $\wp'$ uniquement. Pour avoir des formules algébriques, on est amené à supposer que les invariants g_2 et g_3 sont des nombres algébriques ; c'est ce que nous ferons dans toute la suite.

Le travail de transcendance le plus important sur les fonctions elliptiques a été publié par Schneider en 1937. Trois théorèmes sur les fonctions elliptiques y sont démontrés ; voici l'un d'eux :

THÉORÈME 1. - Soient a, b deux nombres algébriques non tous deux nuls, et u un nombre complexe non pôle de $\wp$. Alors l'un des deux nombres $au + b\zeta(u)$ et $\wp(u)$ est transcendant.

Les deux autres théorèmes concernent le cas où la fonction $az + b\zeta(z)$ est remplacée par une fonction exponentielle ou une autre fonction elliptique.

On déduit du théorème 1 le fait que si ω est une période non nulle de $\wp$ et η la quasi-période de ζ associée, alors les trois nombres $1, \omega, \eta$ sont linéairement indépendants sur $\overline{\mathbb{Q}}$. En particulier ω, η et ω/η sont transcendants.

Schéma de démonstration du théorème 1

On se limitera au cas où $a = 1$, $b = 0$. On suppose donc par l'absurde que u et $\wp(u)$ sont algébriques. On commence par construire une fonction auxiliaire $F(z) = P(z, \wp(z))$, où P est un polynôme non nul à coefficients $P_{i,j}$ entiers, de sorte que F ait de nombreux zéros : $F^{(k)}(mu) = 0$ pour $k < K$, $m < M$. Cette construction est simplement la résolution d'un système linéaire :

$$\sum_{i,j} P_{i,j} S_{i,j,m,k} = 0.$$

Les coefficients $S_{i,j,m,k}$ sont les dérivées $k^{\text{ième}}$ au point mu de monômes $z^i \wp(z)^j$. On utilise alors l'équation différentielle de $\wp$, ainsi que son théorème de multiplication :

$$\wp(mu) = R_m(\wp(u))$$

où R_m est une fraction rationnelle.

Ces propriétés montrent que $S_{i,j,m,k}$ est une fraction rationnelle $S_{i,j,m,k}(u, \wp(u), \wp'(u), g_2, g_3)$. C'est en particulier un nombre algébrique. On se ramène au cas où $S_{i,j,m,k} \in \mathbb{Z}$ par conjugaison et multiplication par un dénominateur (que l'on doit estimer en fonction de K et M). On en déduit l'existence d'une solution $(P_{i,j})$ "pas trop grande".

Une fois cette construction algébrique achevée, on utilise les propriétés analytiques de la fonction F . Elle n'est pas nulle puisque les fonctions z et $\wp(z)$ sont algébriquement indépendantes. On peut donc trouver des entiers k_0 et m_0 tels que $\gamma = F^{(k_0)}(m_0 u) \neq 0$. On choisit ces nombres minimaux en ce sens que $k_0 \leq K_0$, $m_0 \leq M_0$ et $F^{(k)}(mu) = 0$ pour $k < K_0$ et $m < M_0$. Le lemme de Schwarz (essentiellement la formule de Jensen) dit qu'une fonction analytique ayant beaucoup de zéros doit être très petite sur un grand disque, ainsi que ses dérivées. On en déduit que le nombre γ est très petit, par exemple :

$$0 \neq |\gamma| < 2^{-K_0 M_0}.$$

Pour obtenir la contradiction cherchée, il ne reste plus qu'à utiliser les propriétés algébriques de γ : en le multipliant par ses conjugués puis par un dénominateur (qu'il faut estimer en fonction de K_0 et M_0), on obtient un entier rationnel non nul de valeur absolue < 1 , ce qui prouve le théorème.

Les propriétés de $\wp$ utilisées dans cette démonstration sont essentiellement les suivantes : le fait que z et $\wp(z)$ sont algébriquement indépendantes, l'équation différentielle et le théorème de multiplication, et la croissance de $\wp$ (utilisée dans l'application de la formule de Jensen). L'étude de ces propriétés a permis à Schneider, puis à Lang d'établir un théorème général de transcendance, contenant en particulier les trois résultats de Schneider sur les fonctions elliptiques. Le problème se pose de savoir si les trois théorèmes de Schneider sont les seules conséquences concernant les fonctions elliptiques du théorème de Schneider-Lang. L'emploi de la fonction σ est par exemple exclu puisque (à cause de la forme de ses dérivées) on ne pourrait que montrer la transcendance de l'un des nombres $\sigma(u)$, $\zeta(u)$, $\wp(u)$, ce qui est inclus dans le théorème 1. Mais Waldschmidt a pu appliquer le théorème de Schneider-Lang à de nouvelles fonctions, exhibées par Serre en lien avec l'étude de la paramétrisation d'extensions de courbes elliptiques. Ces fonctions dépendent de deux paramètres β et u (où $u \notin L$) et sont définies par la formule

$$f_{\beta, u}(z) = \frac{\sigma(z-u)}{\sigma(z) \sigma(u)} e^{(\zeta(u) + \beta) z}.$$

Cette fonction vérifie l'équation différentielle :

$$f'(z) = f(z) \left\{ \beta + \frac{1}{2} \frac{\wp'(z) + \wp'(u)}{\wp(z) - \wp(u)} \right\}$$

dans laquelle la fonction ζ n'intervient plus. Elle vérifie également un théorème d'addition (donc de multiplication).

L'application du théorème de Schneider-Lang à cette fonction a ainsi permis à Waldschmidt de montrer le résultat suivant (cf. [Wa]) :

THÉOREME 2. - Si $\beta, u, v \in \mathbb{C}$ sont tels que $\beta, \wp(u), \wp(v)$ soient algébriques, u sans torsion (i.e. $u \notin \mathbb{Q}.L$) et $v-u$ non pôle de $\wp$, alors le nombre $f_{\beta, u}(v)$ est transcendant. En particulier, $\sigma(u) e^{-\frac{1}{2}u\zeta(u)}$ est transcendant.

La fonction $f_{\beta, u}$ est multiplicativement quasi-périodique :

$$f_{\beta, u}(z+\omega) = e^{\omega \zeta(u) - \eta u + \beta \omega} f_{\beta, u}(z) \quad \text{pour } \omega \in L.$$

De même que le théorème 1 entraîne la transcendance de η , le théorème 2 permet de montrer la transcendance du nombre $e^{\omega \zeta(u) - \eta u + \beta \omega}$.

4. - Mesures de transcendance

Le problème est ici de rendre quantitatifs les résultats de transcendance. Ainsi, si $P(u)$ est algébrique et que P est un polynôme non nul de $\mathbb{Z}[X]$, le théorème 1 dit que $P(u)$ n'est pas nul ; on cherche alors à minorer le nombre $|P(u)|$. Les minoration cherchées dépendront soit du degré d et de la hauteur H (= maximum des valeurs absolues des coefficients) du polynôme P , soit simplement de sa taille $t(P) = d + \log H$, ce qui est évidemment moins précis mais souvent suffisant pour les applications. On dira ainsi qu'un nombre complexe θ a un type de transcendance $\leq \tau$ (réel ≥ 1) si pour tout polynôme non nul $P \in \mathbb{Z}[X]$, on a $|P(\theta)| > c^{-t(P)^\tau}$ où c ne dépend que de θ et τ . On peut enfin remarquer qu'il est équivalent de minorer les nombres $|P(\theta)|$ ou de minorer les nombres $|\theta - \alpha|$ lorsque α est algébrique (la minoration dépendant du degré et de la hauteur -ou de la taille- de α , c'est-à-dire de son polynôme minimal) ; les minoration de $|P(\theta)|$ et de $|\theta - \alpha|$ sont d'ailleurs essentiellement les mêmes.

Quelles minoration peut-on attendre ? On déduit facilement du principe des tiroirs que si θ est transcendant on ne peut espérer mieux que des minoration du type

$$|P(\theta)| > H^{-cd} \quad \text{ou} \quad |P(\theta)| > c^{-t(P)^2}$$

où c ne dépend que de θ ; il existe en effet une infinité de polynômes P vérifiant les inégalités inverses. En particulier, un nombre transcendant ne peut avoir un type de transcendance < 2 . On peut montrer réciproquement que presque tout nombre complexe (pour la mesure de Lebesgue) a un type de transcendance ≤ 2 et donc égal à 2. Mais on ne sait exhiber aucun nombre concret ayant cette propriété !

La meilleure mesure de transcendance connue concerne le nombre π . On peut l'écrire :

$$|\pi - \alpha| > c^{-d(\log H + d \log d) \log(d+1)}.$$

En particulier, la minoration est la meilleure possible en H lorsque d est fixé (c'est de la forme H^{-c}), et π a un type de transcendance inférieur à $2+\varepsilon$ pour tout $\varepsilon > 0$.

Les premières mesures de transcendance de nombres liés aux fonctions elliptiques ont été démontrées par Fel'dman en 1951. Elles concernaient les périodes et les points algébriques de $\mathcal{P}$ (i. e. les nombres u tels que $\mathcal{P}(u) \in \bar{\mathbb{Q}}$). Par exemple

$$|\omega - \alpha| > c^{-d^4(d(\log d)^5 + \log H(\log \log H)^4)} \quad \text{pour } H \geq 16.$$

Contrairement à la mesure précédente, ce n'est pas de la forme H^{-c} lorsque le degré est fixé, et donne $5+\varepsilon$ comme borne pour le type de transcendance.

D'autres mesures de transcendance ont été démontrées encore par Fel'dman (ne donnant pas toujours un type de transcendance fini), puis par Masser. Nous avons ensuite entrepris une étude systématique des nombres dont la transcendance se déduit des théorèmes de Schneider, et plus récemment du théorème 2 de Waldschmidt. Ces nombres ont en particulier un type de transcendance fini (≤ 6). Deux d'entre eux sont particulièrement intéressants : d'abord le nombre π/ω où ω est une période non nulle de $\mathcal{P}$; il admet pour mesure

$$\left| \frac{\pi}{\omega} - \alpha \right| > c^{-(\log H + d \log d)^2};$$

le résultat est assez loin du meilleur possible en H lorsque le degré est fixé. Par contre on en déduit que $\frac{\pi}{\omega}$ a un type de transcendance $\leq 2+\varepsilon$ pour tout $\varepsilon > 0$. C'est le seul nombre autre que π pour lequel on connaisse un type de transcendance < 3 . Enfin, le nombre $\mathcal{P}(1)$ admet pour mesure

$$|\mathcal{P}(1) - \alpha| > c^{-d^3(d + \log H)};$$

cette minoration est de la forme H^{-c} lorsque d est fixé. Mais elle ne donne que $\tau \leq 4$ comme majoration du type de transcendance.

Méthode de démonstration de mesures de transcendance

Supposons par exemple que $\wp(u)$ est algébrique, et cherchons à montrer une mesure de transcendance pour u . Soit donc α un nombre algébrique, et supposons par l'absurde que

$$|u - \alpha| < \varepsilon = \varepsilon(d, H)$$

où ε est une fonction très petite du degré et de la hauteur de α .

On reprend essentiellement la démonstration de transcendance esquissée au §. 3 : on construit une fonction $F(z) = P(z, \wp(z))$ avec $0 \neq P \in \mathbb{Z}[X, Y]$ de sorte que pour $k < K$, $m < K$, le nombre

$$F^{(k)}(mu) = \sum P_{i,j} S_{i,j,m,k}(u, \wp(u), \wp'(u), g_2, g_3)$$

soit très petit (on ne peut plus demander qu'il soit nul puisque les coefficients du système ne sont plus supposés algébriques). Pour cela, on résout le système

$$\sum P_{i,j} S_{i,j,m,k}(\alpha, \wp(u), \wp'(u), g_2, g_3) = 0 \quad k < K, m < M$$

dont les coefficients sont cette fois algébriques, en procédant comme au §. 3.

Ainsi $|F^{(k)}(mu)| < \varepsilon$ à un terme d'erreur près. Les propriétés analytiques de F permettent de trouver comme au §. 3 des entiers k_0 et m_0 tels que

$$0 \neq \left| \sum P_{i,j} S_{i,j,m_0,k_0}(\alpha, \wp(u), \wp'(u), g_2, g_3) \right| < \sqrt{\varepsilon}$$

à un terme d'erreur près ; on utilise pour cela le fait que ce nombre est proche de $|F^{(k_0)}(m_0 u)|$. On a ainsi trouvé un nombre algébrique non nul et très petit.

L'argument donné au §. 3. permet bien d'en déduire une contradiction à condition que les conjugués et le dénominateur de ce nombre ne soient pas trop grands devant $1/\sqrt{\varepsilon}$. Or, les majorations que l'on peut obtenir pour ces conjugués dépendent de k_0 et m_0 , alors que $\varepsilon = \varepsilon(d, H)$ n'en dépend pas (contrairement au cas de la démonstration de transcendance). Il est donc nécessaire de majorer k_0 et m_0 en fonction des paramètres K et M (qui eux dépendent du ε), ce qui revient à majorer le nombre de zéros d'une fonction de la forme $P(z, \wp(z))$ en fonction du degré du polynôme P . Plusieurs méthodes permettent de donner de telles majorations (appelées "lemmes de zéros").

Des lemmes de zéros adaptés à chaque cas ont été démontrés pour obtenir les mesures de transcendance citées plus haut. Il existe maintenant des lemmes de zéros plus généraux (dus à Brownawell et Masser) permettant de démontrer un analogue quantitatif du théorème de Schneider-Lang. D'autres formes de lemmes de zéros très généraux sont actuellement démontrées par Masser et Wüstholz, et ont une importance capitale en théorie des nombres transcendants.

Nous retrouverons au paragraphe suivant l'utilité des lemmes de zéros.

5. - Indépendance algébrique

Les premiers résultats d'indépendance algébrique en lien avec les fonctions elliptiques sont dus à Choodnovsky, qui a démontré l'indépendance algébrique des deux nombres $\frac{\omega}{\pi}$ et $\frac{\omega}{\eta}$ où ω est une période non nulle de $\wp$, et η la quasi-période de ζ associée. On en déduit dans un cas particulier que les deux nombres π et $\Gamma(1/4)$ sont algébriquement indépendants.

L'idée des démonstrations d'indépendance algébrique est la suivante : on cherche à démontrer l'indépendance de deux nombres a et b (par exemple $\frac{\omega}{\pi}$ et $\frac{\omega}{\eta}$). On utilise des fonctions f_1 et f_2 (éventuellement $f_3, \dots$) qui prennent en des points x_m ainsi que leurs dérivées des valeurs dans une extension algébrique finie fixe $\mathcal{K}$ de $\mathbb{Q}(a, b)$ (par exemple $f_1(z) = \wp(z)$, $f_2(z) = \zeta(z) - \frac{\eta}{\omega} z$, $x_m = (2m+1)\frac{\omega}{2}$). On suppose par l'absurde que $\mathbb{Q}(a, b)$ (et donc $\mathcal{K}$) a un degré de transcendance < 2 , ce qui permet d'écrire $\mathcal{K} = \mathbb{Q}(x, y)$ où y est algébrique sur $\mathbb{Q}(x)$. Comme au §. 3, on commence par construire une fonction $F(z) = P(f_1(z), f_2(z))$, où P est cette fois un polynôme à coefficients dans $\mathbb{Z}[x]$, de sorte que F ait beaucoup de zéros : $F^{(k)}(x_m) = 0$ pour $k < K$ et $m < M$. On en déduit comme au §. 3 des entiers k_0 et m_0 tels que $|F^{(k_0)}(x_{m_0})|$ soit non nul et très petit. En prenant la norme de cet élément sur $\mathbb{Q}(x)$ puis en multipliant par un dénominateur, on en déduit l'existence d'un polynôme Q dans $\mathbb{Z}[X]$ tel que $Q(x)$ soit non nul et très petit, par exemple

$$(1) \quad 0 \neq |Q(x)| < e^{-t(Q)\kappa}$$

où $t(Q)$ est la taille du polynôme Q , et κ un nombre réel (en pratique on a souvent $2 \leq \kappa \leq 4$). Dans le cas d'une démonstration de transcendance, on a $x = 1$

et donc $Q(x) \in \mathbb{Z}$ ce qui fournit la contradiction. Dans le problème qui nous occupe, si x est algébrique, la norme de $Q(x)$ sur $\mathbb{Q}$ nous fournit encore un entier non nul et de valeur absolue < 1 , d'où une contradiction. Mais en général, x est un nombre transcendant. Il y a alors deux méthodes permettant parfois d'achever la démonstration :

a) Si on sait que x a un type de transcendance $< \kappa$ (cf. §.4), l'inégalité (1) nous fournit aussitôt une contradiction. C'est par exemple le cas si $\kappa = 2,5$ et que $x = \frac{\omega}{\pi}$ d'après le §.4.

b) Si on ne connaît rien sur x , la seule inégalité (1) ne peut fournir de contradiction ; on montre en effet facilement que pour toute fonction φ , on peut construire un nombre transcendant x vérifiant $0 \neq |Q(x)| < e^{-\varphi(t(Q))}$ pour une infinité de polynômes Q .

Cependant, Gel'fond a montré que de tels polynômes Q sont assez rares (i. e. leur taille doit croître vite). De manière précise, on peut montrer que si x est nombre complexe transcendant, il n'existe pas de suite infinie $(Q_N)_{N > N_0}$ de polynômes de $\mathbb{Z}[X]$ vérifiant

$$(2) \quad t(Q_N) \leq N \quad \text{et} \quad \log |Q_N(x)| < -4N^2.$$

Pour obtenir une contradiction, il suffit donc de reprendre, pour chaque entier N assez grand, la construction d'une fonction auxiliaire $F_N(z)$ qui permet de construire comme plus haut un polynôme Q_N vérifiant (1). Pour en déduire que Q_N vérifie (2), il faut savoir majorer sa taille en fonction de N , ce qui revient encore une fois à majorer les entiers k_0 et m_0 en fonction de M et K : on utilise ici aussi un "lemme de zéros" (cf. §.4).

L'intérêt de ce critère de Gel'fond est qu'il suffit d'obtenir une majoration du type (1) avec n'importe quel $\kappa > 2$, alors qu'on sait rarement majorer le type de transcendance de x par un nombre proche de 2 (et parfois on ne sait pas si ce type est fini). L'inconvénient est qu'il demande un bon lemme de zéros ; de plus, il ne se généralise pas simplement au cas de plusieurs nombres, contrairement à la méthode a) : ainsi pour prouver que trois nombres sont algébriquement indépendants, on construit par l'absurde un polynôme Q tel que

$0 \neq |Q(x, y)| < e^{-t(Q)^\kappa}$ où cette fois x et y sont deux nombres algébriquement indépendants. Si on sait par ailleurs que le couple (x, y) a un type d'indépendance algébrique (défini comme le type de transcendance) strictement inférieur à κ , on obtient ainsi une contradiction.

Nous donnons maintenant deux exemples d'énoncés d'indépendance algébrique que nous avons récemment obtenus par ces méthodes. Les démonstrations utilisent une fonction de la forme $f_{\beta, u}$, où β est choisi de sorte que $f_{\beta, u}$ admette une période ω dans le réseau L . Il est en effet très intéressant dans les démonstrations d'indépendance algébrique de travailler avec des fonctions $f_1, f_2, \dots$ qui ont une période commune, car les zéros que l'on construit pour la fonction $F = P(f_1, f_2, \dots)$ en fourniront une quantité d'autres par périodicité. C'est pourquoi, pour $\omega \in L \setminus \{0\}$, on définit la fonction

$$g_{u, \omega}(z) = f_{\beta, u}(z) \quad \text{où} \quad \beta = u \frac{\eta}{\omega} - \zeta(u).$$

En utilisant les fonctions $\wp(z)$ et $g_{u, \omega}(z)$, et le critère de Gel'fond, on obtient le résultat suivant :

THÉORÈME 3. - Soient u, v deux nombres complexes sans torsion (i.e. $u, v \notin \mathbb{Q}.L$), distincts modulo L , et tels que $\wp(u)$ et $\wp(v)$ soient algébriques. Alors deux des trois nombres

$$\zeta(u) - \frac{\eta}{\omega} u, \quad e^{i\pi u/\omega}, \quad g_{u, \omega}(v)$$

sont algébriquement indépendants.

On déduit en particulier le corollaire suivant d'une variante de ce théorème :

COROLLAIRE. - Soit $\wp$ la fonction de Weierstrass vérifiant l'équation différentielle $\wp'^2(z) = 4(\wp^3(z) - \wp(z))$. Si l'on pose $t = \Gamma(1/4)^2 / 2\sqrt{\pi}$, alors les deux nombres

$$e^{i\pi\sqrt{2}} \quad \text{et} \quad \wp(t) + i(\zeta(t) - \frac{2\pi}{t})$$

sont algébriquement indépendants.

Les deux fonctions $\wp(z)$ et $g_{u, \omega}(z)$ utilisées plus haut admettent ω pour période. On peut leur adjoindre les deux fonctions $e^{2i\pi z/\omega}$ et $\zeta(z) - \frac{\eta}{\omega} z$ qui ont la même propriété. En utilisant un résultat de Choodnovsky disant que le

couple $(\frac{\omega}{\pi}, \frac{\omega}{\eta})$ a un type d'indépendance algébrique $\leq 3+\varepsilon$, on obtient le résultat suivant :

THÉORÈME 4. - Sous les hypothèses du théorème 3, notons $\tau = \omega'/\omega$ où ω' est une période de $\wp$ linéairement indépendante de ω . Alors trois au moins des six nombres

$$\frac{\omega}{\pi}, \frac{\omega}{\eta}, e^{i\pi\tau}, e^{i\pi u/\omega}, \zeta(u) - \frac{\eta}{\omega} u, g_{u,\omega}(v)$$

sont algébriquement indépendants.

-:-:-:-

BIBLIOGRAPHIE

- [B-M] D. BERTRAND and D. MASSER, Linear forms in elliptic integrals, Inventiones math. 58 (1980), 283-288.
- [C1] G. V. CHOUDNOVSKY, Algebraic independence of values of exponential and elliptic functions, Proc. I. C. M., Helsinki (1978)
- [C2] G. V. CHOUDNOVSKY, Algebraic grounds for the proof of algebraic independence, Part I : elementary algebra ; Pub. Math. Univ. P. et M. Curie (Paris VI), n° 25 (1979).
- [C3] G. V. CHOUDNOVSKY, Algebraic independence of the values of elliptic function at algebraic points, Inventiones Math. 61 (1980), 267-290.
- [L] M. LAURENT, Transcendance de périodes d'intégrales elliptiques, J. für die reine und angew. Math. 316 (1980), 122-139.
- [R] E. REYSSAT, Propriétés d'indépendance algébrique de nombres liés aux fonctions de Weierstrass, Acta Arith. (à paraître).
- [Wa] M. WALDSCHMIDT, Nombres transcendants et fonctions sigma de Weierstrass, C.R. Math. Rep. Acad. Sci. Canada 1 (1979), 111-114.

- [Wu] G. WÜSTHOLZ, Algebraische Unabhängigkeit von Werten von Funktionen, die gewissen Differentialgleichungen genügen, J. für die reine und angew. Math. 127 (1980), 102-119.

(texte reçu le 17 février 1981)

-:-:-:-

Eric REYSSAT
Université P. et M. Curie (Paris VI)
Mathématiques, Tour 45-46
4, place Jussieu
F 75230 PARIS CEDEX 05

THÉORIE ADDITIVE ET GÉOMÉTRIE DES NOMBRES

par

Jean-Marc DESHOUILERS

(présentation d'un travail effectué en commun avec F. DRESS)

-:-:-:-

Soit $\mathcal{Q}$ une suite strictement croissante d'entiers positifs et $r(N)$ le nombre de manières d'écrire l'entier N comme somme de deux éléments de $\mathcal{Q}$;
la majoration triviale

$$r(N) \leq A(N) \quad (:= \text{Card} \{ a \in \mathcal{Q} \ ; \ a \leq N \})$$

n'est pas susceptible d'être améliorée en général (choisir $\mathcal{Q} = \{ 1, 2, 3, \dots, N \}$).
Le problème que nous considérons est l'obtention de majorations plus fines, sous certaines hypothèses de régularité sur la suite $\mathcal{Q}$.

Aux Journées de Théorie des Nombres d'Orsay de 1980, nous avons présenté la majoration

$$r(N) \leq 4 (A(N))^{2/3} ,$$

valable dès que la suite des différences premières de la suite $\mathcal{Q}$ est strictement croissante, et nous avons également montré par un argument géométrique que

l'exposant $2/3$ est le meilleur possible. Nous voulons souligner ici l'équivalence entre l'étude du nombre de représentations et le dénombrement de points entiers sur des courbes.

Par commodité, nous nous placerons dans le cadre suivant ; pour un entier $P \geq 2$, on notera $\mathcal{B}^P$ la classe des fonctions de classe $\mathcal{C}^P$ de $\mathbb{R}^+$ dans $\mathbb{R}^+$ telles que $a(0) = 0$, $a(1) = 1$ et $a^{(p)} > 0$ pour $1 \leq p < P+1$. Une telle fonction a étant choisie, on remarque que pour tout réel t , le nombre de solutions en entiers positifs m et n de l'équation

$$t = a(m) + a(n)$$

est fini ; nous noterons désormais $r_a(t)$, ou $r(t)$ ce nombre de solutions. On remarque également que la fonction a est inversible et on note A son inverse. Dans le cas où $a(n)$ est entier pour n entier, le lecteur pourra considérer la suite $\mathcal{A} = \{a(1), \dots, a(N), \dots\}$ et vérifier que pour N entier les symboles $r(N)$ et $A(N)$ conservent leur signification.

Le résultat principal est celui-ci

THÉORÈME. - Pour tout nombre réel $\alpha \in [0, 1]$, on a les implications

(i) $\Rightarrow$ (ii) $\Rightarrow$ (iii), avec

$$(i) \quad \forall a \in \mathcal{B}^P : r(t) \ll (A(t))^\alpha$$

$$(ii) \quad \forall f \in \mathcal{B}^P : \# \{n \leq x, f(n) \in \mathbb{N}\} \ll (L_f(x))^\alpha, \text{ où } L_f(x) \text{ désigne la} \\ \text{longueur du graphe de l'application } f|_{[0, x]}, \text{ (c'est-à-dire} \\ L_f(x) = \int_0^x \sqrt{1+f'^2(t)} dt),$$

$$(iii) \quad \forall a \in \mathcal{B}^P : (\forall p \in [1, P] : (-1)^{p-1} A^{(p)} > 0) \Rightarrow r(t) \ll (A(t))^\alpha.$$

Remarques et corollaires

Dans le cas $P=2$, les conditions (i) et (iii) sont équivalentes ; on trouve ainsi l'équivalence de (i) et (ii) ; il semble que van der Corput ait été le premier à démontrer que (ii) est valide avec $\alpha = 2/3$; Jarnik a démontré que ce résultat est le meilleur possible.

. Néanmoins, dans le cas $P = 2$, on peut démontrer directement par un argument "fareysien" que les assertions (i) et (iii) sont valides avec la majoration $r^{3/2}(t) \leq ((\frac{\sqrt{3}}{\pi}) + \epsilon) A(t)$ dès que $A(t)$ est assez grand (en fonction de $\epsilon > 0$) et que la constante indiquée est optimale.

. On notera que pour tout nombre réel $c > 1$, la fonction $a(x) = x^c$ est non seulement dans la classe $\mathcal{B}^{[c+1]}$, mais est également telle que $(-1)^{p-1} A^{(p)} > 0$ pour $p = 1, 2, \dots, [c+1]$.

. Dans le cas $P = 3$, H.P.F. Swinnerton-Dyer a démontré que (ii) est valide en prenant pour α tout nombre réel supérieur à $3/5$, d'où la validité de (iii) pour $P \geq 3$ et $\alpha > 3/5$.

. Comme il est aisé de le constater, pour $\alpha < \frac{1}{2}$, aucune des relations (i), (ii), (iii) n'est valide pour aucune valeur de P .

. La démonstration du théorème est effective, en ce sens que la démonstration de l'implication (i) $\Rightarrow$ (ii) permet de faire dépendre la constante impliquée dans (ii) explicitement de celle qui est impliquée dans (i), et de même pour l'implication (ii) $\Rightarrow$ (iii). Quoiqu'il en soit, la constante obtenue aussi dans (iii) est supérieure à celle dont on est parti en (i).

(texte reçu le 17 décembre 1981)

-:-:-:-

Jean-Marc DESHOUILERS
U.E.R. de Mathématiques
et d'Informatique
Université de Bordeaux I
F 33405 TALENCE CEDEX

SUR LES AUTOMORPHISMES D'EXTENSIONS TRANSCENDANTES
DE CORPS VALUÉS

par

Michel MATIGNON et Marc REVERSAT

-:-:-

§. 1. - Introduction

Ce travail est consacré à l'étude des automorphismes continus d'extensions transcendentes de corps valués non archimédiens.

Les premiers résultats dans cette voie furent ceux de Tate ([2]), Sen ([7]) et Ax ([1]) :

THÉORÈME. - Soient K un corps complet pour une valeur absolue non archimédienne et $\hat{K}$ un complété d'une clôture algébrique $\bar{K}$ de K . Alors, le sous-corps de $\hat{K}$ des invariants par le groupe $\text{Aut}(\bar{K}/K)$ des K -automorphismes de $\bar{K}$ (qui opère par continuité sur $\hat{K}$) est l'adhérence de la clôture radicielle de K .

Lors d'un travail sur les équations différentielles p -adiques, Dwork et Robba ([2]) ont été amenés, pour des questions de rationalité, à prouver le résultat suivant (en caractéristique zéro, mais la généralisation à toute caractéristique est immédiate) :

THÉORÈME ([2], th. 8). - Soit L un corps algébriquement clos, maximallement complet pour une valeur absolue non archimédienne, soit K un sous-corps fermé de L . Alors, le sous-corps de L des éléments invariants par le groupe $\text{Aut}_{\text{cont}}(L/K)$ des K -automorphismes continus de L est l'adhérence de la clôture radicielle de K .

Ce dernier résultat est donc analogue à celui de Tate, Sen et Ax. C'est ce qui a conduit Dwork et Robba à la question suivante :

PROBLÈME (Dwork-Robba, [2]). - Soient L un corps algébriquement clos et complet pour une valeur absolue non archimédienne, K un sous-corps fermé de L . Le sous-corps de L des invariants par le groupe $\text{Aut}_{\text{cont}}(L/K)$ est-il l'adhérence de la clôture radicielle de K ?

A ce problème, qui est le point de départ de notre travail, nous donnons une réponse négative (§. 4.2 et exemple suivant le théorème 4) qui apparaît comme une conséquence naturelle d'une étude précise des automorphismes continus d'une extension transcendante pure de degré 1.

Plus précisément, soient K un corps complet pour une valeur absolue non archimédienne, $\hat{K}(X)$ une extension transcendante d'un complété d'une clôture algébrique de K ; la valeur absolue de $\hat{K}$ admet un prolongement (non-unique) à $\hat{K}(X)$. Nous étudions ici le groupe $\text{Aut}_{\text{cont}}(\hat{K}(X)/K)$ des K -automorphismes continus du corps $\hat{K}(X)$ (complété d'une clôture algébrique de $K(X)$).

Lorsque l'extension $\hat{K}(X)/\hat{K}$ n'est pas immédiate, il est aisé de vérifier que tout élément de $\text{Aut}(\hat{K}/K)$ se prolonge en un K -automorphisme continu de $\hat{K}(X)$, ainsi la réponse au problème est positive dans cette situation (§. 3). En revanche, l'étude est beaucoup plus difficile lorsque l'extension $\hat{K}(X)/\hat{K}$ est immédiate. Notre résultat principal (théorème 2) donne une condition nécessaire et suffisante pour qu'un élément de

$\text{Aut}(\bar{K}/K)$ se prolonge en un élément de $\text{Aut}_{\text{cont}}(\hat{K}(\bar{X})/K)$. Ce critère s'avère être très utilisable, en particulier, lorsque K est un corps local de caractéristique résiduelle nulle il nous permet de construire les premiers exemples qui répondent négativement au problème (§.4.2).

On définit la notion d'ordre de transcendance fini ou infini pour un automorphisme (§.4.4) : soit σ un élément de $\text{Aut}_{\text{cont}}(\hat{K}(\bar{X})/K)$, on dit que σ est d'ordre de transcendance fini s'il existe un entier $n > 0$ tel que :

$$|\sigma^n(X) - X| \leq \text{distance de } X \text{ à } \bar{K},$$

sinon on dit que σ est d'ordre de transcendance infini. On montre (théorème 4) que si σ est d'ordre de transcendance infini, alors $\mathbb{Z}_p$ est facteur direct de $\text{Gal}(\bar{K}/\bar{K}^{<\sigma>})$ (p est la caractéristique résiduelle de K et $\bar{K}^{<\sigma>}$ est le sous-corps de $\bar{K}$ des éléments invariants par σ).

Nous donnons aussi quelques propriétés supplémentaires concernant les automorphismes continus de $\hat{K}(\bar{X})$ qui laissent $\hat{K}$ invariant. Soit δ un élément de $\hat{K}(\bar{X})$, alors, si la valeur absolue de δ est suffisamment petite ($|\delta| \leq \text{distance de } X \text{ à } \bar{K}$), l'application entre $\hat{K}(X)$ et $\hat{K}(X+\delta)$, qui à une fraction rationnelle $f(X)$ associe $f(X+\delta)$, est un isomorphisme isométrique de corps valués. Elle se prolonge en un isomorphisme isométrique entre $\hat{K}(\bar{X})$ et $\hat{K}(\bar{X}+\delta)$, donc en un $\hat{K}$ -endomorphisme continu de $\hat{K}(\bar{X})$ (en fait, tous les $\hat{K}$ -endomorphismes continus de $\hat{K}(\bar{X})$ sont de cette forme). Si la caractéristique résiduelle de K est nulle, cet endomorphisme est toujours un isomorphisme. Par contre, si la caractéristique résiduelle de K est non nulle, nous construisons explicitement de tels endomorphismes non surjectifs (c'est-à-dire que nous donnons (théorème 6) une construction d'éléments Y de $\hat{K}(\bar{X})$ tels que $\hat{K} \subsetneq \hat{K}(\bar{Y}) \subsetneq \hat{K}(\bar{X})$). Autrement dit, l'orbite de X par $\text{Aut}_{\text{cont}}(\hat{K}(\bar{X})/\hat{K})$ est la boule circonscrite de $\hat{K}(\bar{X})$ de centre X et de rayon la distance de X à $\bar{K}$ si et seulement si la caractéristique résiduelle de K est nulle (théorème 7).

La rédaction de cet exposé ne contient pas de démonstration. Celles-ci figurent dans un article à paraître.

Notations

Si E est un corps valué non archimédien, on note $|\cdot|$ la valeur absolue ; $\hat{E}$ désigne le complété de E pour cette valeur absolue ; $|E^\times|$ désigne le groupe des valeurs du groupe multiplicatif $E^\times$ de E ; $\bar{E}$ désigne une clôture algébrique de E . Si H est un groupe d'automorphismes de E , E^H désigne le sous-corps de E formé des éléments invariants sous l'action de H . Si p est la caractéristique de E on note $E^{p^{-\infty}}$ la clôture radicielle de E . Soient $K \subset E$ deux corps, on note $\text{Aut}(E/K)$ le groupe des K -automorphismes de E , si de plus E est valué, on note $\text{Aut}_{\text{cont}}(E/K)$ le groupe des K -automorphismes continus de E .

Convention

Si E est un corps de caractéristique p on fait la convention que $p^0 = 1$ même si p est nul.

§.2. - Classification des extensions transcendentes de degré 1 sur un corps valué complet algébriquement clos

Soit K un corps valué ultramétrique complet et algébriquement clos. Soit $K(X)$ une extension transcendante de K . Il existe trois extensions de la valeur absolue de K à $K(X)$ ([6]).

i) L'extension $K(X)$ de K est sans ramification mais il y a extension du corps résiduel.

Quitte à faire un changement linéaire sur X la valeur absolue est donnée par la norme de Gauss :

$$\left| \sum_{i=0}^d a_i X^i \right| = \max_{0 \leq i \leq d} |a_i|$$

où a_i est un élément de K .

ii) L'extension $K(X)$ de K est inerte mais il y a extension du groupe des valeurs.

Quitte à faire un changement linéaire sur X , la valeur absolue est la norme des séries de Laurent sur une circonférence de rayon $r \notin |K^\times|$. Alors :

$$\widehat{K}(X) = \left\{ \sum_{n \in \mathbb{Z}} a_n X^n, a_n \in K, \lim_{|n| \rightarrow \infty} |a_n| r^n = 0 \right\}$$

et

$$\left| \sum_{n \in \mathbb{Z}} a_n X^n \right| = \max_n |a_n| r^n.$$

iii) L'extension $K(X)$ de K est immédiate (i.e., elle est inerte et non ramifiée).

Alors il existe une suite $(\omega_n)_{n \in \mathbb{N}}$ d'éléments de K telle que la suite $(|\omega_{n+1} - \omega_n|)_{n \in \mathbb{N}}$ tende en décroissant vers un réel r strictement positif. Si de plus $B(\omega_n, r_n^+)$ désigne la boule circonferenciée de K de centre ω_n et de rayon $r_n = |\omega_{n+1} - \omega_n|$, alors :

$$\bigcap_n B(\omega_n, r_n^+) = \emptyset.$$

La valeur absolue est ainsi définie :

Soit $P(X) \in K[X]$, alors :

$$|P(X)| = \lim_n |P(\omega_n)|.$$

Alors $\widehat{K}(X)$ est le corps des fonctions K -analytiques sur la boule circonferenciée de centre X et de rayon r .

Désormais, Ω désigne un corps valué ultramétrique maximalement complet et algébriquement clos, K un sous-corps de Ω , et X un élément de Ω n'appartenant pas à $\widehat{K}$.

§. 3. - Corps des invariants par les automorphismes continus

Le théorème suivant montre que les éléments de $\widehat{K(X)}$ invariants par $\text{Aut}_{\text{cont}}(\widehat{K(X)}/K)$ sont dans $\widehat{K}$.

THÉORÈME 1 ([10]). - Soient K un corps valué complet, $\widehat{K}(X)$ une extension valuée transcendante de $\widehat{K}$, G le groupe des K -automorphismes continus de $\widehat{K}(X)$, G' la restriction de G à $\widehat{K}$. Alors

$$(\widehat{K}(X))^G = (\widehat{K}^{G'})^{\wedge}.$$

Ce théorème est une conséquence immédiate du théorème de Tate-Sen-Ax, que nous avons rappelé dans l'introduction, et de la proposition suivante :

PROPOSITION 1. - Les hypothèses sont celles du théorème 1. Soit F un corps fermé tel que $K \subset F \subset \widehat{K}(X)$. Alors $F \subset \widehat{K}$ ou bien $\widehat{K}(X)$ est de degré fini sur F .

Pour dénombrer cette proposition on utilise la théorie des fonctions analytiques sur un corps valué ultramétrique.

Remarque. - Cette proposition est l'analogue du résultat suivant dans le cas non valué. Soient $K(X)$ une extension transcendante pure d'un corps K et F un corps, $K \subset F \subset K(X)$, alors $F = K$ ou bien l'extension $K(X)$ de F est finie. Le théorème de Lüroth nous dit même que $F = K(Y)$ où $Y \in K(X)$. Par contre sous les hypothèses de la proposition 1 et si $F \not\subset \widehat{K}$ nous ne savons pas s'il existe $Y \in \widehat{K}(X)$ tel que $F = \widehat{K}(Y)$.

COROLLAIRE 1. - Les hypothèses sont celles du théorème 1, on suppose de plus que K est algébriquement clos. Alors :

$$(\widehat{K}(X))^G = K.$$

La proposition suivante explicite le cas non immédiat.

PROPOSITION 2. - Les hypothèses sont celles du théorème 1, on suppose de plus que l'extension $\widehat{K}(X)$: n'est pas immédiate. Alors :

$$\text{Aut}_{\text{cont}}(\widehat{K}(X)/K) \big|_{\widehat{K}} = \text{Aut}(\widehat{K}/K)$$

et donc : (si p désigne la caractéristique de K)

$$(\widehat{K}(X))^G = (K^{p^{-\infty}})^{\wedge}.$$

Ce résultat est analogue aux théorèmes de Tate-Sen-Ax ([8], [7], [1]) et Dwork-Robba ([2]), mais la démonstration utilise le théorème de Tate-Sen-Ax.

§. 4. - Prolongement des automorphismes de $\bar{K}$ à $\hat{\bar{K}}(\bar{X})$

Nous supposons désormais que l'extension $\hat{\bar{K}}(\bar{X})$ de $\hat{\bar{K}}$ est immédiate.

On note $r = \inf_{x \in \bar{K}} |X-x|$.

4.1. - Le théorème fondamental

Nous pouvons énoncer le théorème fondamental de ce travail ; il donne une condition nécessaire et suffisante pour qu'un K -automorphisme de $\bar{K}$ se prolonge en un K -automorphisme continu de $\hat{\bar{K}}(\bar{X})$. La démonstration utilise des résultats de Kaplansky sur les corps valués (cf. [6], chap. 7, p. 220).

THÉORÈME 2 ([10]). - Soient K un corps valué complet de caractéristique résiduelle p positive ou nulle, $\hat{\bar{K}}(\bar{X})$ une extension transcendante valuée immédiate de $\hat{\bar{K}}$, σ un K -automorphisme de $\bar{K}$. Les assertions suivantes sont équivalentes :

(i) L'automorphisme σ se prolonge en un K -automorphisme continu de $\hat{\bar{K}}(\bar{X})$,

(ii) Il existe un entier $s \geq 0$ et $a_0, \dots, a_s, b_0, \dots, b_s, c, w \in \bar{K}$ possédant les propriétés suivantes :

$$\begin{aligned} |X-w|^{p^s} |p| &\leq r^{p^s} \\ \max_{0 \leq k \leq s} (|a_k| r^{p^k}, |b_k| r^{p^k}) &\leq r^{p^s}, \\ |a_s| &= |b_s| = 1, \end{aligned}$$

pour tout $x \in \bar{K}$ on a :

$$|P(\sigma(x-w)) - Q(x-w) + c| \leq |X-x|^{p^s}$$

où

$$P(Z) = \sum_{k=0}^s a_k Z^{p^k}$$

et

$$Q(Z) = \sum_{k=0}^s b_k Z^{p^k}.$$

Dans le cas où $r \notin |\bar{K}^*|$ et dans le cas où $p=0$ (alors $(\bar{K}(X))^\wedge$ est algébriquement clos puisque une extension algébrique finie immédiate d'un corps valué est de degré une puissance de la caractéristique résiduelle) le théorème 2 s'exprime plus simplement :

COROLLAIRE. - Les hypothèses sont celles du théorème 2. On suppose de plus que $p=0$ ou bien que $r \notin |\bar{K}^*|$. Soit $\sigma \in \text{Aut}(\bar{K}/K)$. Les assertions suivantes sont équivalentes :

- i) L'automorphisme σ se prolonge en un K -automorphisme continu de $\hat{\bar{K}(X)}$,
- ii) Il existe deux éléments de $\bar{K}$, b et c , tels que :

$$|b| = 1$$

et que pour tout $x \in \bar{K}$:

$$|\sigma(x) + bx + c| \leq |X - x|.$$

Ce corollaire permet d'étudier le cas très simple des séries formelles en égale caractéristique nulle.

4.2. - Application aux corps de séries formelles

On suppose que $K = k((T))$, $|T| < 1$, le corps de séries formelles où k est de caractéristique nulle et algébriquement clos.

L'analogue du théorème de Puiseux montre que $\hat{\bar{K}} = k((T^{1/n}))_{n \in \mathbb{N}^*}$.

Soit $\Omega = \Omega(k, \mathbb{Q})$ le corps des séries formelles $z : z = \sum_{r \in \mathbb{Q}} \alpha_r T^r$, à coefficients α_r dans k et à support bien ordonné (on rappelle que $\text{support}(z) = \{r \in \mathbb{Q}, \alpha_r \neq 0\}$). Alors Ω est un corps maximalement complet ([6]) et algébriquement clos.

Exemples. - (conséquences immédiates du corollaire)

1. - Soient $S = \{-\frac{1}{n}, n \in \mathbb{N}^*\}$, $X = \sum_{r \in S} T^r$ et $G = \text{Aut}_{\text{cont}}(\hat{\bar{K}(X)}/K)$. Alors

$$(\hat{\bar{K}(X)})^G = \hat{\bar{K}} \neq K.$$

2. - Soient p un nombre premier, $S = \{-\frac{1}{p^n}, n \in \mathbb{N}\}$, $X = \sum_{r \in S} T^r$ et $G = \text{Aut}_{\text{cont}}(\widehat{\overline{K(X)}}/K)$. Alors :

$$\widehat{\overline{K(X)}}^G = K((T^{p^{-n}})) \neq K.$$

3. - Soient $S = \{-\frac{1}{p}, p \text{ premier}\}$, $X = \sum_{r \in S} T^r$ et $G = \text{Aut}_{\text{cont}}(\widehat{\overline{K(X)}}/K)$. Alors :

$$\widehat{\overline{K(X)}}^G = K.$$

Plus généralement on montre :

PROPOSITION 3. - Soient $K = k((T))$, k algébriquement clos de caractéristique nulle et H un sous-groupe de $\text{Aut}(\overline{K}/K)$. Alors il existe X un élément de Ω n'appartenant pas à $\widehat{\overline{K}}$ tel que :

$$(\widehat{\overline{K(X)}})^G = (\overline{K^H})^\wedge$$

où

$$G = \text{Aut}_{\text{cont}}(\widehat{\overline{K(X)}}/K).$$

4. 3. - Anneaux des polynômes de Ore

On suppose que $r \in |\overline{K}^\times|$, où K est un corps valué complet de caractéristique résiduelle p .

On désigne par $\mathcal{Q}_r$ l'ensemble des polynômes $\sum_{i=1}^p a_i Z^i$ de $\overline{K}[Z]$ tels que :

- i) $a_{p^t} \neq 0$.
- ii) $\max_{1 \leq i \leq p^t} |a_i| r^i \leq r^{p^t}$.

iii) Si i n'est pas une puissance de p

$$|a_i| r^i < r^{p^t}.$$

On désigne par $\mathcal{Q}_r^\circ$ le sous-ensemble de $\mathcal{Q}_r$ formé des polynômes $\sum_{1 \leq i \leq p^t} a_i Z^i$ de $\overline{K}[Z]$ tels que :

- i) $a_{p^t} \neq 0$
- ii) $\max_{1 \leq i \leq p^t} |a_i| r^i < r^{p^t}$.

Soit φ l'application de $\mathcal{Q}_r$ dans $\mathcal{Q}_1$ définie par :

$$\varphi(P(Z)) = \frac{1}{\rho^{\deg P}} P(\rho Z)$$

où $\rho \in \bar{K}$ et $|\rho| = r$.

Sur $\mathcal{Q}_1$ on définit une relation d'équivalence par :

$$P \in \mathcal{Q}_1, Q \in \mathcal{Q}_1, P \equiv Q \Leftrightarrow P - Q \in \mathcal{Q}_1^\circ.$$

Soit k le corps résiduel de K , on vérifie que $\mathcal{Q}_1/\mathcal{Q}_1^\circ$ est un sous-anneau de $\bar{k}[Z]$ pour les lois d'addition et de composition des polynômes, de plus si $P(Z) \in \mathcal{Q}_1/\mathcal{Q}_1^\circ$ alors $P(Z) = \sum a_h Z^{ph}$ où $a_h \in \bar{k}$; i.e. $\mathcal{Q}_1/\mathcal{Q}_1^\circ$ est l'anneau des polynômes additifs de $\bar{k}[Z]$. La structure de cet anneau a été étudiée par Ore [5], c'est un anneau non commutatif, euclidien à gauche et à droite.

La bijection φ entre $\mathcal{Q}_1$ et $\mathcal{Q}_r$ définit par transport de structure une relation d'équivalence, on note $\mathcal{Q}_r/\mathcal{Q}_r^\circ$ le quotient muni des opérations transportées. Si $P \in \mathcal{Q}_r$ on note $\bar{P}$ son image dans $\mathcal{Q}_r/\mathcal{Q}_r^\circ$. Le quotient $\mathcal{Q}_r/\mathcal{Q}_r^\circ$ est ainsi muni d'une structure d'anneau euclidien non commutatif.

PROPOSITION 4. - Les hypothèses sont celles du théorème 2. Soit $\sigma \in \text{Aut}(\bar{K}/K)$ qui se prolonge à $\text{Aut}_{\text{cont}}(\widehat{K(X)}/K)$. Alors les polynômes P et $Q \in \mathcal{Q}_r$ définis au théorème 2 peuvent être choisis tels que $\bar{P}$ et $\bar{Q}$ soient premiers entre eux à gauche dans $\mathcal{Q}_r/\mathcal{Q}_r^\circ$.

C'est une conséquence immédiate du fait que l'ensemble des polynômes $\bar{P}$ où P vérifie ii) du théorème 2, est un idéal à gauche de $\mathcal{Q}_r/\mathcal{Q}_r^\circ$.

On montre aussi, quitte à faire une homotétie sur X , qu'on peut se ramener en plus à des polynômes unitaires :

PROPOSITION 5. - Les hypothèses sont celles du théorème 2. Soit $\sigma \in \text{Aut}(\bar{K}/K)$ qui se prolonge à $\text{Aut}_{\text{cont}}(\widehat{K(X)}/K)$. Il existe $\alpha \in \bar{K}^\times$ tel que les polynômes P et Q associés à $Y = \alpha X$ dans le théorème 2 soient unitaires et tels que $\bar{P}$ et $\bar{Q}$ soient premiers entre eux à gauche dans $\mathcal{Q}_{|\alpha|r}/\mathcal{Q}_{|\alpha|r}^\circ$. Alors $\bar{P}$ et $\bar{Q}$ sont uniques.

Remarque. - Dans certain cas on ne peut choisir $\alpha \in \bar{K}$ tel que $|\alpha|_r = 1$.

Par exemple, si $K = k((T))$, $X = \sum_{n \geq 0} T^{-(1/3 \cdot 2^{2n})}$ et $\sigma \in \text{Aut}(K/K)$ tel que $\sigma(T^{1/p}) = T^{1/p}$ pour tout nombre premier p différent de 3 et $\sigma(T^{1/3}) = j T^{1/3}$ où j est une racine cubique de l'unité différente de 1. Alors σ se prolonge et

$$|\sigma(X) - j X| \leq 1.$$

Il n'existe pas dans $\hat{\bar{K}}$ d'éléments α de module 1 tel que $\sigma(\alpha) = j \alpha$.

4.4. - Ordre de transcendance d'un automorphisme de $\hat{\bar{K}}(X)$

PROPOSITION 6 ([10]). - Soient K un corps valué complet, $\hat{\bar{K}}(X)$ une extension transcendante valuée immédiate de $\hat{\bar{K}}$. Soit $\sigma \in \text{Aut}_{\text{cont}}(\hat{\bar{K}}(X)/K)$. Les propriétés suivantes sont équivalentes :

i) Il existe $n \in \mathbb{N}^*$ tel que :

$$|\sigma^n(X) - X| \leq r_X$$

$$\text{où } r_X = \inf_{x \in \bar{K}} |X - x|.$$

ii) Pour tout Y de $\hat{\bar{K}}(X)$ non dans $\hat{\bar{K}}$ il existe $n_Y \in \mathbb{N}^*$ tel que :

$$|\sigma^{n_Y}(Y) - Y| \leq r_Y$$

$$\text{où } r_Y = \inf_{x \in \bar{K}} |Y - x|.$$

La démonstration utilise les techniques employées dans la démonstration du théorème 2.

DÉFINITION. - On dira qu'un élément $\sigma \in \text{Aut}_{\text{cont}}(\hat{\bar{K}}(X)/K)$ est d'ordre de transcendance fini si il vérifie l'une des propriétés équivalentes de la proposition 6.

On dira que son ordre de transcendance est infini dans le cas contraire.

THÉORÈME 3 ([10]). - Soient K un corps valué complet, $\hat{K}(X)$ une extension transcendante valuée immédiate de $\hat{K}$, σ un K -automorphisme continu de $\hat{K}(X)$. Soient P et Q les deux polynômes unitaires de $\mathcal{O}_{|a|_r}$ définis par la proposition 5. Les assertions suivantes sont équivalentes :

- i) L'automorphisme σ est d'ordre de transcendance fini,
- ii) Il existe un polynôme $T \in \mathcal{O}_{r'}$, où $r' = r^{d^\circ P}$, tel que

$$\overline{T \circ P} = \overline{\sigma(T \circ Q)}$$

($\circ$ désigne la composition des polynômes et si $R(Z) = \sum \alpha_n Z^n \in \bar{K}[Z]$, on pose $\sigma R(Z) = \sum \sigma(\alpha_n) Z^n$).

La démonstration utilise essentiellement la structure euclidienne de l'anneau $\mathcal{O}_r / \mathcal{O}_r^\circ$.

THÉORÈME 4 ([10]). - Soient K un corps valué complet de caractéristique résiduelle p non nulle, $\hat{K}(X)$ une extension transcendante valuée immédiate de $\hat{K}$, σ un K -automorphisme continu de $\hat{K}(X)$, et $\langle \sigma \rangle$ le groupe topologique engendré par la restriction de σ à $\bar{K}$. Alors si σ est d'ordre de transcendance infini, $\mathbb{Z}_p$ est facteur direct de $\text{Aut}(\bar{K} / \bar{K}^{\langle \sigma \rangle})$.

Remarque. - Ce théorème permet de construire des extensions transcendentes immédiates $\hat{K}(X)$ de $\hat{K}$ d'inégale caractéristique ou d'égale caractéristique positive telles que le corps des invariants de $\hat{K}(X)$ par $\text{Aut}_{\text{cont}}(\hat{K}(X)/K)$ soit différent de $(K^{p^{-\infty}})^\wedge$.

Soit $\sigma \in \text{Aut}(\bar{\mathbb{Q}}_p / \mathbb{Q}_p)$ tel que le groupe $\langle \sigma \rangle$ engendré par σ soit isomorphe à $\mathbb{Z}_q$, $q \neq p$, tel que $\bar{\mathbb{Q}}_p^{\langle \sigma \rangle}$ contienne les racines q^n èmes de l'unité pour tout $n \in \mathbb{N}$. Alors la théorie de Kummer montre que l'extension $\bar{\mathbb{Q}}_p$ de $\bar{\mathbb{Q}}_p^{\langle \sigma \rangle}$ est de la forme :

$$\bar{\mathbb{Q}}_p = \bar{\mathbb{Q}}_p^{\langle \sigma \rangle} = \bar{\mathbb{Q}}_p^{\langle \sigma \rangle} (\sqrt[q]{e}) = \dots = \bar{\mathbb{Q}}_p^{\langle \sigma \rangle} (\sqrt[q^n]{e}) = \bar{\mathbb{Q}}_p$$

où $|e| > 1$.

Soit $\omega_n = \sum_{k \leq n} e^{q^{-k}}$. La suite ω_n est pseudo-convergente. Soit $X \in \Omega$, une clôture maximale complète de $\mathbb{Q}_p$, tel que pour tout $n \in \mathbb{N}$, $|X - \omega_n| \leq |\omega_n - \omega_{n+1}|$. Puisque $|\sigma^k(\omega_n) - \omega_n| = |\omega_n|$ ou 0, on voit facilement que $X \notin \hat{\mathbb{Q}}_p$ et donc X définit une extension immédiate $\hat{\mathbb{Q}}_p(X)$ de $\hat{\mathbb{Q}}_p$. Supposons alors que σ se prolonge en un $\mathbb{Q}_p$ -automorphisme continu de $\overline{\mathbb{Q}_p(X)}$. Il est alors facile de voir que σ est d'ordre de transcendance infini et le théorème 4 affirme que $\mathbb{Z}_p$ est facteur direct de $\mathbb{Z}_q$ ce qui est absurde. Par conséquent :

$$\overline{\hat{\mathbb{Q}}_p(X)}^G = \hat{\mathbb{Q}}_p \neq \hat{\mathbb{Q}}_p^{<\sigma>}$$

où $G = \text{Aut}_{\text{cont}}(\overline{\hat{\mathbb{Q}}_p(X)} / \hat{\mathbb{Q}}_p^{<\sigma>})$.

THÉOREME 5 ([10]). - Soient K un corps valué complet de caractéristique résiduelle p non nulle, r un élément du groupe des valeurs de $K^\times$, P et Q deux polynômes de $\mathcal{O}_r$ unitaires, de même degré d et tels que $\bar{P}$ et $\bar{Q}$ soient premiers entre eux à gauche dans $\mathcal{O}_r / \mathcal{O}_r^\circ$, et σ un K -automorphisme de $\bar{K}$.

a) Soit $T \in \mathcal{O}_{r,d}$ tel que $\overline{T \cdot P} = \sigma(\overline{T \cdot Q})$. Alors les assertions suivantes sont équivalentes :

i) Il existe $X \in \Omega$, $X \notin \hat{K}$, tel que l'extension valuée transcendante $\hat{K}(X)$ de $\hat{K}$ vérifie les propriétés suivantes :

1. L'extension $\hat{K}(X)$ de $\hat{K}$ est immédiate, $r = \inf_{x \in \hat{K}} |X - x|$,
2. L'automorphisme σ se prolonge en un K -automorphisme de $\hat{K}(X)$,

et $|p| |X|^d < r^d$

$$|P(\tilde{\sigma}(X)) - Q(X)| \leq r^d.$$

ii) Il existe $Y \in \Omega$, $Y \notin \hat{K}$ tel que l'extension valuée transcendante $\hat{K}(Y)$ de $\hat{K}$ soit immédiate, tel que σ se prolonge en un K -automorphisme $\tilde{\sigma}$ de $\hat{K}(Y)$ et que

$$|\tilde{\sigma}(Y) - Y| \leq r_Y$$

où $r_Y = \inf_{x \in \hat{K}} |Y - x|$.

b) Pour tout $T \in \mathcal{O}_{r^d}$, $\overline{T \cdot P} \neq {}^\sigma \overline{(T \cdot Q)}$. Alors les assertions suivantes sont équivalentes :

i) Il existe $X \in \Omega$, $X \notin \hat{K}$, tel que l'extension valuée transcendante $\hat{K}(X)$ de $\hat{K}$ vérifie les propriétés suivantes :

1. L'extension $\hat{K}(X)$ de $\hat{K}$ est immédiate, $r = \inf_{x \in \hat{K}} |X - x|$,
2. L'automorphisme σ se prolonge en un K -automorphisme $\tilde{\sigma}$ de $\hat{K}(X)$,

$$|p| |X|^d < r^d$$

et

$$|P(\tilde{\sigma}(X)) - Q(X)| \leq r^d.$$

ii) Le groupe $\mathbb{Z}_p$ est facteur direct de $\text{Aut}(\hat{K}/\hat{K}^{<\sigma>})$.

Remarque. - Dans b) pour construire X vérifiant i), on utilise le théorème 90 de Hilbert additif adapté aux corps valués. On utilise aussi le fait que la différence $\mathcal{D}_{\hat{K}/\hat{K}^{<\sigma>}}$ de l'extension infinie $\hat{K}$ de $\hat{K}^{<\sigma>}$ est de valeur absolue 1.

§.5. - Prolongements de l'automorphisme identité de $\hat{K}$ à $\hat{K}(X)$

Nous démontrons d'abord un théorème de structure des corps fermés F algébriquement clos entre K et $\hat{K}(X)$.

THÉORÈME 6 ([10]). - Soient K un corps valué complet et $\hat{K}(X)$ une extension valuée transcendante de $\hat{K}$. Alors si :

a) La caractéristique résiduelle de K est nulle, les seuls corps F fermés et algébriquement clos tels que $K \subset F \subset \hat{K}(X)$, sont $\hat{K}$ et $\hat{K}(X)$,

b) La caractéristique résiduelle de K est non nulle, il y a une infinité de corps F fermés et algébriquement clos tels que : $K \subset F \subset \hat{K}(X)$.

Pour démontrer a), on utilise suivant une idée de M. van der Put, les modules universels des différentielles continues [9] ; cette démonstration ne donne aucun renseignement dans le cas b) puisque les modules différentiels considérés sont nuls. Pour démontrer b), nous utilisons la notion de différentielle dans les extensions infinies de corps valués, notion introduite par J. Fresnel et B. de Mathan [3] et développée dans [4]. On construit explicitement des éléments Y de $\widehat{K(X)}$ tels que :

$$\widehat{K} \not\subset \widehat{K(Y)} \not\subset \widehat{K(X)}.$$

Remarque. - Comme corollaire de ce théorème, on déduit que si $K = \mathbb{F}_p$, le complété de la clôture algébrique du corps local $\mathbb{F}_p((X))$ contient une infinité de corps algébriquement clos et complets.

On en déduit le théorème suivant :

THÉORÈME 7 ([10]). - Soient K un corps valué complet et $\widehat{K(X)}$ une extension valuée transcendante de $\widehat{K}$.

a) Si la caractéristique résiduelle de K est nulle, l'orbite de X par $\text{Aut}_{\text{cont}}(\widehat{K(X)}/\widehat{K})$, est la boule circonferenciée de $\widehat{K(X)}$ de centre X et de rayon $r = \inf_{x \in \widehat{K}} |X-x|$;

b) Si la caractéristique résiduelle de K est non nulle, l'orbite de X par $\text{Aut}_{\text{cont}}(\widehat{K(X)}/\widehat{K})$ est dense mais non égale à la boule circonferenciée de $\widehat{K(X)}$ de centre X et de rayon $r = \inf_{x \in \widehat{K}} |X-x|$.

-:-:-:-

BIBLIOGRAPHIE

- [1] J. AX, Zeros of polynomials over local fields, the Galois action, J. Algebra, 15 (1970), 417-428.
- [2] B. DWORK and Ph. ROBBA, On ordinary linear p-adic differential equations, Trans. Amer. Math. Soc., 231 (1977), 1-46.

- [3] J. FRESNEL et B. de MATHAN, Algèbres L^1 p -adiques, Bull. Soc. Math. France, n° 106 (1978), 225-260.
- [4] J. FRESNEL et M. MATIGNON, Produit tensoriel topologique de corps valués, à paraître.
- [5] O. ORE, On a special class of polynomials, Trans. Amer. Math. Soc. 35 (1933), 559-584 (errata, ibid., 36 (1934), 275).
- [6] O. SCHILLING, The theory of valuations, Math. Surveys IV, New-York, 1950.
- [7] S. SEN, On automorphisms of local fields, Ann. of Math., 90 (1969), 33-40.
- [8] J. TATE, p -divisible groups, Proc. Conf. Local Fields, Driebergen, Springer (1967), 158-183.
- [9] M. van der PUT, Continuous derivations of valued fields, Bull. Soc. Math. France, n° 101 (1973), 71-112.
- [10] M. MATIGNON et M. REVERSAT, Sur les automorphismes d'extensions transcendentes des corps valués, à paraître.

(texte reçu le 5 octobre 1981)

--:--:--

M. MATIGNON et M. REVERSAT
 U.E.R. de Mathématiques et
 d'Informatique
 Université de Bordeaux I
 F 33405 TALENCE CEDEX

GROUPES DISCRETS DE QUATERNIONS

par

Marius van der PUT

-:-:-:-

Un corps de quaternions D sur $\mathbb{Q}$ qui est défini positif fournit pour un nombre premier p , non ramifié dans D , des sous-groupes discrets de $\mathrm{PGL}(2, \mathbb{Q}_p)$. Dans le paragraphe 2, on développe ces groupes et les courbes de Mumford qui s'en déduisent. Pour un corps de quaternions indéfini D sur $\mathbb{Q}$ on obtient des sous-groupes discrets de $\mathrm{PGL}(2, \mathbb{R})$ ainsi que des courbes complètes sur $\mathbb{R}$. Le lien entre ces deux familles de courbes est le contenu d'un théorème remarquable de Čerednik. Dans les paragraphes 3 et 4 l'auteur a écrit ce qu'il a pu comprendre des travaux de Čerednik et Drinfeld sur le sujet. Je remercie M. M. Rapoport pour ses indications concernant les travaux de Čerednik et Drinfeld.

§ 1.1. - Groupe de quaternions réels et surfaces abéliennes

Une algèbre de quaternions D sur $\mathbb{Q}$ est un espace vectoriel de dimension 4 sur $\mathbb{Q}$. La multiplication bilinéaire de D est donnée pour une base convenable $\{e_0, e_1, e_2, e_3\}$ par les formules

- (i) $e_0 = 1$ est l'élément neutre de D ;
- (ii) $e_1^2 = a$, $e_2^2 = b$ où $a, b \in \mathbb{Z}$ et $ab \neq 0$;
- (iii) $e_i e_j = \text{signe}(i, j, k) e_k$ pour toute permutation (i, j, k) de $(1, 2, 3)$.

Nous supposons que D est un corps non commutatif. Cette propriété est équivalente à : l'équation $x_0^2 - x_1^2 a - x_2^2 b = 0$ n'a que la solution triviale $(0, 0, 0)$ dans $\mathbb{Q}^3$. Soit v une place de $\mathbb{Q}$ et soit $\mathbb{Q}_v$ le complété de $\mathbb{Q}$ par rapport à v (donc $\mathbb{Q}_v = \mathbb{R}$ ou $\mathbb{Q}_p$). L'algèbre $D \otimes \mathbb{Q}_v$ est un corps non commutatif ou bien isomorphe à $M(2, \mathbb{Q}_v)$, l'algèbre des matrices de rang 2 sur $\mathbb{Q}_v$. Dans le premier cas on dit que D est ramifiée en v . Les résultats suivants sont très classiques ([1]) :

- (a) D est ramifiée en v si et seulement si le symbole de Hilbert $(a, b)_v$ a valeur -1 .
- (b) L'ensemble S des places ramifiées de D est fini et son cardinal est pair.
- (c) Pour chaque ensemble fini V de places de $\mathbb{Q}$, de cardinal pair, il existe une algèbre de quaternions unique telle que $S = V$.

Un ordre de D est un sous-anneau de D qui est un $\mathbb{Z}$ -module libre de rang 4. Chaque ordre de D est contenu dans un ordre maximal (pour l'inclusion). Fixons un ordre maximal M de D . L'algèbre des adèles D_A de D est le produit restreint $\prod^* D \otimes \mathbb{Q}_v$ par rapport aux sous-groupes ouverts, compacts $M \otimes \mathbb{Z}_v$ de $D \otimes \mathbb{Q}_v$ pour $v \neq \infty$. La définition de D_A ne dépend pas du choix de M . On désigne par D^1 et D_A^1 les éléments de D et D_A de norme réduite 1. Le théorème d'approximation forte ([15], th. 4, p. 74) affirme que :

- (d) D^1 est un sous-groupe discret de D_A^1 et D_A^1 / D^1 est compact.

En particulier, si D est une algèbre de quaternions indéfinie sur $\mathbb{Q}$, i.e. ∞ n'est pas ramifiée, alors $M^1 = M \cap D^1$ est un sous-groupe discret de $(D \otimes \mathbb{R})^1 \cong \mathrm{Sl}(2, \mathbb{R})$ à quotient compact. Nous fixons maintenant un isomorphisme $f : D \otimes \mathbb{R} \xrightarrow{\sim} M(2, \mathbb{R})$. Pour un entier $n \geq 1$ on note par $\Gamma(D, n)$ le sous-groupe discret $\{f(d) \mid d \in M^1 \text{ et } d \equiv \mathrm{id} \text{ modulo } n\}$ de $\mathrm{Sl}(2, \mathbb{R})$. Le groupe $\Gamma(D, n)$ agit sur le demi-plan de Poincaré $\mathcal{K} = \{z \in \mathbb{C} \mid \mathrm{im}(z) > 0\}$ comme groupe discontinu. La partie (a) du théorème suivant est bien connue ([12], ch. 1). Nous suivons [11], p. 128-138, pour la partie (b).

(1.1) THÉORÈME

- (a) $\mathcal{K}/\Gamma(D, n)$ est une courbe non singulière et complète,
- (b) $\mathcal{K}/\Gamma(D, n)$ est la variété de modules des surfaces abéliennes A sur $\mathbb{C}$ munies de
 - (i) une application $M \rightarrow \mathrm{End}(A)$ (multiplications complexes),
 - (ii) un isomorphisme $\frac{1}{n}M/M \xrightarrow{\sim} A[n] = \{x \in A \mid nx = 0\}$ (structure de niveau n).

Démonstration. - $\mathcal{K}/\Gamma(D, n)$ est certainement une surface de Riemann. Sa compacité se déduit aisément de la compacité de $\Gamma(D, n) \backslash \mathrm{Sl}(2, \mathbb{R})$. A un élément z de $\mathcal{K}$ on associe $\Lambda(z) = \{f(m) \begin{pmatrix} z \\ 1 \end{pmatrix} \in \mathbb{C}^2 \mid m \in M\}$ où f est l'isomorphisme fixé $D \otimes \mathbb{R} \xrightarrow{\sim} M(2, \mathbb{R})$ et où $M(2, \mathbb{R})$ agit sur $\mathbb{C}^2$ de façon naturelle, c'est-à-dire :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = \begin{pmatrix} az_1 + bz_2 \\ cz_1 + dz_2 \end{pmatrix}.$$

Un calcul immédiat montre que $\Lambda(z)$ est un réseau de $\mathbb{C}^2$. Le tore complexe $A = \mathbb{C}^2/\Lambda(z)$ possède un homomorphisme $M \rightarrow \mathrm{End}(A)$ donné par $m \mapsto f(m)$ et A possède une structure de niveau n donnée par :

$$f : \frac{1}{n}M/M \xrightarrow{\sim} \frac{1}{n}\Lambda(z)/\Lambda(z) = A[n] \subset A.$$

Il faut maintenant vérifier que A est une surface abélienne. D'après [9] p. 35, il faut montrer l'existence d'une forme hermitienne définie positive H sur $\mathbb{C}^2$ telle que les valeurs de $\mathrm{im} H$ sur $\Lambda(z) \times \Lambda(z)$ sont des entiers.

Dans D on définit la conjugaison $z \mapsto \bar{z}$ par la formule :

$$x_0 + x_1 e_1 + x_2 e_2 + x_3 e_3 = x_0 - x_1 e_1 - x_2 e_2 - x_3 e_3 .$$

La norme réduite et la trace réduite sont données par $N(z) = z \bar{z}$ et $\text{tr}(z) = z + \bar{z}$.

Ces opérations sont prolongées par linéarité à $D \otimes \mathbb{R}$. Soit ρ un élément de D tel que $-\rho^2$ est rationnel et positif. (Les possibilités pour $-\rho^2$ se déduisent de [14], th. 3.8, p. 78). Comme l'application $D \otimes \mathbb{R} \rightarrow \mathbb{C}^2$ qui envoie sur $f(d) \begin{pmatrix} z \\ 1 \end{pmatrix}$ est bijective on peut définir la forme E sur $\mathbb{C}^2$ par la formule

$$E(f(d_1) \begin{pmatrix} z \\ 1 \end{pmatrix}, f(d_2) \begin{pmatrix} z \\ 1 \end{pmatrix}) = c \text{tr}(\rho d_1 \bar{d}_2)$$

où $c \neq 0$ est un entier tel que $E(\Lambda(z), \Lambda(z)) \subseteq \mathbb{Z}$. On vérifie aisément que E est bilinéaire et antisymétrique. En outre on a $E(ix, iy) = E(x, y)$. En effet, il existe un élément $\mu \in D \otimes \mathbb{R}$ avec $f(\mu) \begin{pmatrix} z \\ 1 \end{pmatrix} = i \begin{pmatrix} z \\ 1 \end{pmatrix}$. L'élément μ satisfait $\mu^2 = -1$ et $\bar{\mu} = -\mu$. Alors :

$$E(f(d_1) i \begin{pmatrix} z \\ 1 \end{pmatrix}, f(d_2) i \begin{pmatrix} z \\ 1 \end{pmatrix}) = c \text{tr}(\rho d_1 \mu \overline{d_2 \mu}) = c \text{tr}(\rho d_1 \bar{d}_2).$$

Pour H on prend la forme hermitienne $H(x, y) = E(ix, y) + i E(x, y)$. Il faut maintenant vérifier que $H(x, x) > 0$ pour $x \neq 0$. On a $H(x, x) = c \text{tr}(\rho d \mu \bar{d})$ et $\mu = \lambda \gamma \rho \gamma^{-1}$ pour un $\lambda \in \mathbb{R}$, $\lambda > 0$, et $\gamma \in D \otimes \mathbb{R}$. Donc $H(x, x)$ est égale à $c N(\gamma) \text{tr}(d \gamma \rho \overline{d \gamma} \rho^{-1})$. On choisit c tel que $c N(\gamma) > 0$ et on considère sur D l'involution $*$: $d \mapsto \rho \bar{d} \rho^{-1}$. Un calcul explicite montre que $\text{tr}(d d^*) > 0$ pour chaque $d \in D$, $d \neq 0$. Cela montre que $H(x, x) > 0$ pour $x \neq 0$.

Soit maintenant A une surface abélienne sur $\mathbb{C}$ munie d'un homomorphisme $M \rightarrow \text{End}(A)$. On représente A comme $\mathbb{C}^2 / \Lambda$. L'homomorphisme se prolonge à un homomorphisme $D \otimes \mathbb{R} \rightarrow M(2, \mathbb{C})$. Après un changement de base de $\mathbb{C}^2$ on peut supposer que cette application n'est autre que :

$$D \otimes \mathbb{R} \xrightarrow[\sim]{f} M(2, \mathbb{R}) \subset M(2, \mathbb{C}).$$

On constate que le réseau Λ est un M -sous-module de $\Lambda \otimes \mathbb{Q} \simeq M \otimes \mathbb{Q} = D$.

D'après un théorème d'Eichler une algèbre de quaternions indéfinie a les propriétés :

(i) tous les ordres maximaux sont conjugués ;

(ii) chaque ordre maximal est un anneau principal à gauche.

On en déduit que Λ est engendré comme M -module par un seul élément $\begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$. Les nombres complexes z_1, z_2 sont indépendants sur $\mathbb{R}$ parce que $f(D \otimes \mathbb{R}) \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = \mathbb{C}^2$. Quitte à multiplier le réseau Λ par une constante, on peut supposer que Λ est engendré par $\begin{pmatrix} z \\ 1 \end{pmatrix}$ où $z = \pm z_1/z_2$ et $z \in \mathcal{K}$.

Nous avons donc vérifié que A est la surface algébrique correspondante au point z de $\mathcal{K}$. Un calcul immédiat montre que $\mathbb{C}^2/\Lambda(z_1)$ et $\mathbb{C}^2/\Lambda(z_2)$ avec leurs structures (i) et (ii) sont isomorphes si et seulement s'il existe un $\gamma \in \Gamma(D, n)$ avec $\gamma(z_2) = z_1$. Soit $\alpha \xrightarrow{\pi} S$ une famille analytique de surfaces abéliennes munies des structures (i) et (ii).

On peut montrer que l'application $g : S \rightarrow \mathcal{K}/\Gamma(D, n)$ donnée par $g(s) = z$ modulo $\Gamma(D, n)$ si $\pi^{-1}(s) \cong \mathbb{C}^2/\Lambda(z)$ pour les structures (i) et (ii), est analytique. Cela montre que $\mathcal{K}/\Gamma(D, n)$ est la variété grossière de modules. Pour $n \geq 3$ on peut montrer en plus que $\mathcal{K}/\Gamma(D, n)$ possède une famille universelle de surfaces abéliennes ayant (i) et (ii) (comparer avec (4.1)).

§. 2. - Groupes de quaternions p -adiques et courbes de Mumford

$\mathbb{C}_p$ désigne le complété de la clôture algébrique de $\mathbb{Q}_p$. Le groupe $\mathrm{PGL}(2, \mathbb{Q}_p) = \mathrm{GL}(2, \mathbb{Q}_p)/\mathbb{Q}_p^*$ agit de façon naturelle sur la droite projective $\mathbb{P}^1(\mathbb{C}_p)$. Ce qui nous intéresse ce sont les sous-groupes discrets Γ de $\mathrm{PGL}(2, \mathbb{Q}_p)$ et leur action sur $\mathbb{P}^1(\mathbb{C}_p)$. D'abord quelques résultats généraux (comparez aussi [10], p. 113, 114).

(2.1) PROPOSITION. - Soit Γ un sous-groupe discret de $\mathrm{PGL}(2, \mathbb{Q}_p)$. Les conditions suivantes sont équivalentes :

- (1) $\Gamma \backslash \mathrm{PGL}(2, \mathbb{Q}_p)$ est compact ;
- (2) $\Gamma \backslash T$ est fini où T désigne l'arbre de Bruhat-Tits de $\mathrm{PGL}(2, \mathbb{Q}_p)$
- (3) Γ est engendré par un nombre fini d'éléments et $\mathbb{P}^1(\mathbb{Q}_p)$ est l'ensemble des points limites de Γ .

Démonstration. - L'arbre de Bruhat-Tits T de $\mathrm{PGL}(2, \mathbb{Q}_p)$ est défini par :

- (i) les sommets de T sont les classes d'équivalence $[M]$ des $\mathbb{Z}_p$ -sous-modules M , libre de rang 2, de $\mathbb{Q}_p^2$. La relation d'équivalence est donnée par $M \sim M'$ si $M = \lambda M'$ pour un $\lambda \in \mathbb{Q}_p^*$.
- (ii) $\{[M], [M']\}$ est une arête de T s'il existe $M_1 \in [M], M_2 \in [M']$ tels que $M_1 \subset M_2$ et $M_2/M_1 \cong \mathbb{Z}_p$.

On sait que T est un arbre et que chaque sommet de T est lié avec $(p+1)$ autres sommets de T . Les demi-droites (ou plutôt leurs classes d'équivalence) sont en relation biunivoque avec les points de $\mathbb{P}^1(\mathbb{Q}_p)$. Le groupe $\mathrm{PGL}(2, \mathbb{Q}_p)$ agit sur T par la formule $\gamma[M] = [\gamma M]$. Soit $M_o = \mathbb{Z}_p^2 \subset \mathbb{Q}_p^2$. Alors le stabilisateur de $[M_o]$ est égale au sous-groupe ouvert et compact $\mathrm{PGL}(2, \mathbb{Z}_p)$ de $\mathrm{PGL}(2, \mathbb{Q}_p)$. Comme l'action de $\mathrm{PGL}(2, \mathbb{Q}_p)$ sur T est transitive, on a un isomorphisme :

$$\mathrm{PGL}(2, \mathbb{Q}_p) / \mathrm{PGL}(2, \mathbb{Z}_p) \xrightarrow{\sim} T.$$

Donc $\Gamma \backslash \mathrm{PGL}(2, \mathbb{Q}_p)$ est compact si et seulement si

$$\Gamma \backslash T = \Gamma \backslash \mathrm{PGL}(2, \mathbb{Q}_p) / \mathrm{PGL}(2, \mathbb{Z}_p) \text{ est fini.}$$

Cela montre l'équivalence de (1) et (2).

Un point p de $\mathbb{P}^1(\mathbb{Q}_p)$ est un point limite s'il existe une suite (γ_n) d'éléments distincts de Γ et un point q de $\mathbb{P}^1(\mathbb{Q}_p)$ tel que $\lim \gamma_n(q) = p$. Supposons maintenant que $\Gamma \backslash T$ est fini. Soit L une demi-droite de T . Il existe $[M]$ et une suite infinie (γ_n) de Γ tel que les $[\gamma_n M]$ sont des sommets de L . On peut remplacer (γ_n) par une sous-suite et on peut choisir des représentants $\tilde{\gamma}_n \in \mathrm{GL}(2, \mathbb{Q}_p)$ de γ_n tel que $\lim \tilde{\gamma}_n = A \in \mathrm{M}(2, \mathbb{Q}_p)$, $A \neq 0$ et $\det A = 0$. Le point $p = A(\mathbb{Q}_p^2)$ de $\mathbb{P}^1(\mathbb{Q}_p)$ est un point limite. Un calcul facile montre que p correspond à la demi-droite L . Ce qui montre que $\mathbb{P}^1(\mathbb{Q}_p)$ est l'ensemble des points limites de Γ . Finalement, dans [6], p. 20, lemma (3.2.2) on a démontré qu'un groupe discret Γ avec points limites $\mathbb{P}^1(\mathbb{Q}_p)$ satisfait : $\Gamma \backslash T$ est fini si et seulement si Γ est engendré par un nombre fini d'éléments. Nous remarquons que la proposition reste valable si on remplace $\mathbb{Q}_p$ par un corps local quelconque.

(2.2) Nous rappelons un résultat de [6], p. 19 : Si le groupe discret Γ est engendré par un nombre fini d'éléments, alors Γ possède un sous-groupe distingué Γ_0 , d'indice fini dans Γ , tel que Γ_0 est un groupe libre.

Nous appliquons les résultats précédents à une algèbre de quaternions D sur $\mathbb{Q}$ telle que ∞ est ramifié et p est non ramifié. Soit M un ordre maximal de D . Alors $\Lambda = (M \otimes \mathbb{Z}[\frac{1}{p}])^* / \{ \pm p^n \cdot \text{id} \mid n \in \mathbb{Z} \}$ est un sous-groupe discret de $(D \otimes \mathbb{Q}_p)^* / \mathbb{Q}_p^* \cong \text{PGL}(2, \mathbb{Q}_p)$ et le quotient $\Lambda \backslash \text{PGL}(2, \mathbb{Q}_p)$ est compact. Cela résulte de la propriété (d) du §.1. Le groupe Λ possède des sous-groupes de congruence $\Lambda(n) = \Lambda(0, n)$ pour chaque entier $n \geq 1$ tel que $p \nmid n$. La proposition (2.1) et les résultats généraux de [6] montrent la proposition suivante :

(2.3) PROPOSITION. - $X = \mathbb{C}_p - \mathbb{Q}_p / \Lambda(D, n)$ est une courbe non singulière et complète. La réduction stable de cette courbe n'a que des composantes irréductibles de genre 0 (on dit, dans ce cas, que X est une courbe de Mumford).

(2.4) Dans [6], chap. IX, on a fait un calcul explicite des groupes $\Lambda(D, n)$ et des réductions stables pour le cas où D est l'algèbre de Hamilton. Cela veut dire que D est donnée par $(a, b) = (-1, -1)$. L'ordre maximal M de D est le $\mathbb{Z}$ -module engendré par $\frac{1}{2}(e_0 + e_1 + e_2 + e_3)$, e_1, e_2, e_3 . L'algèbre D est ramifiée en 2 et ∞ . Soit $p \neq 2$. Pour $p \equiv 1 \pmod{4}$ le corps $\mathbb{Q}_p$ contient un élément i avec $i^2 = -1$. L'isomorphisme $D \otimes \mathbb{Q}_p \xrightarrow{\sim} M(2, \mathbb{Q}_p)$ peut être donné par la formule usuelle

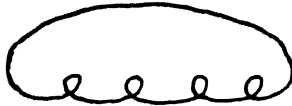
$$a_0 + a_1 e_1 + a_2 e_2 + a_3 e_3 \longmapsto \begin{pmatrix} a_0 + i a_1 & a_2 + i a_3 \\ -a_2 + i a_3 & a_0 - i a_1 \end{pmatrix}.$$

Pour $p \equiv 3 \pmod{4}$ le corps $\mathbb{Q}_p$ contient des éléments α et β tels que $\alpha^2 + \beta^2 = -1$. L'isomorphisme $D \otimes \mathbb{Q}_p \xrightarrow{\sim} M(2, \mathbb{Q}_p)$ peut être donné par les formules :

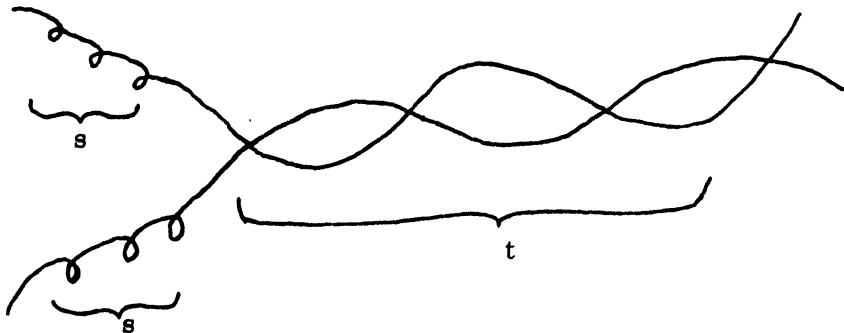
$$e_0 \longmapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} ; \quad e_1 \longmapsto \begin{pmatrix} \alpha & \beta \\ \beta & -\alpha \end{pmatrix} ; \quad e_2 \longmapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Le groupe Λ n'est pas libre. Grâce au fait que M est un anneau euclidien pour la norme on peut faire un calcul explicite des générateurs et des relations de Λ . En particulier, on essaie de trouver un sous-groupe libre de Λ , d'indice fini dans Λ .

(2.5) PROPOSITION ([6], ch. IX). - (a) Pour $p \equiv 1 \pmod{4}$ ou $p \equiv 7 \pmod{8}$ le sous-groupe $\Lambda(2)$ est libre de rang $\frac{p+1}{2}$ et $\Lambda/\Lambda(2) \cong A_4$. La réduction stable de la courbe $\mathbb{C}_p - \mathbb{Q}_p/\Lambda(2)$ est une courbe rationnelle sur $\mathbb{F}_p$ avec $\frac{p+1}{2}$ points doubles ordinaires



(b) Si $p \equiv 3 \pmod{8}$ le sous-groupe $\Lambda(2)$ n'est pas libre. Il existe un sous-
groupe $\Lambda^*(2)$ de $\Lambda(2)$ d'indice 2 qui est libre de rang p . La réduction stable
X de la courbe $\mathbb{C}_p - \mathbb{Q}_p/\Lambda^*(2)$ est



C'est-à-dire X a deux composantes irréductibles X_1, X_2 . Chaque X_i a s points doubles ordinaires et les composantes se rencontrent normalement en t points. En plus $t = \frac{1}{2}$ (le nombre de représentations de p comme somme de
trois carrés) et $2s + t = p + 1$.

(2.6) Remarque. - Ce qui manque dans le cas p -adique c'est le lien de $\mathbb{C}_p - \mathbb{Q}_p/\Lambda(D, n)$ avec une famille de surfaces abéliennes. Dans les deux paragraphes suivants on étudie le lien entre les deux familles de courbes des paragraphes 1 et 2.

§. 3. - Le théorème de Čerednik

Soit D une algèbre de quaternions sur $\mathbb{Q}$. On suppose que ∞ est ramifiée et on écrit l'ensemble S des places ramifiées de D comme $S = T \cup \{\infty\}$ avec $\infty \notin T$. Soit p un nombre premier, $p \notin S$ et soit $\hat{D}$ l'algèbre de quaternions sur $\mathbb{Q}$ ramifiée en $T \cup \{p\}$. Alors

(3.1) THÉORÈME (Čerednik [2], [3]). - Les courbes $\mathbb{C}_p - \mathbb{Q}_p / \Lambda^1(D, n)$ et $\mathcal{K} / \Gamma(\hat{D}, n)$ sont isomorphes.

Idée de la démonstration

Comme les deux courbes sont définies sur des corps différents, il faut préciser l'énoncé. Le théorème veut dire que les deux courbes ont un corps de définition commun K , extension finie de $\mathbb{Q}$, et que ces deux courbes sur K sont isomorphes. Le groupe $\Lambda^1(D, n)$ est le sous-groupe de $\Lambda(D, n)$ qui correspond aux éléments de norme 1. D'après (d) du §. 1, le sous-groupe D^1 de $(D \otimes \mathbb{Q}_p)^1 \times \prod_{\ell \neq p}^* (D \otimes \mathbb{Q}_\ell)^1$ est discret et est à quotient compact.

Posons $E = \prod_{\ell \neq p}^* (D \otimes \mathbb{Q}_\ell)^1$, i. e. le produit restreint des groupes $(D \otimes \mathbb{Q}_\ell)^1$.

C'est un groupe localement compact tel que les sous-groupes U , ouverts et compacts, forment une base des voisinages de 1 dans E . Pour un tel U on écrit $D_U^1 = D^1 \cap ((D \otimes \mathbb{Q}_p)^1 \times U)$. Le groupe D_U^1 est discret et à quotient compact dans $(D \otimes \mathbb{Q}_p)^1 \simeq \mathrm{SL}(2, \mathbb{Q}_p)$. On associe à U la courbe $S_U = \mathbb{C}_p - \mathbb{Q}_p / D_U^1$ sur $\mathbb{C}_p$ et son corps de fonctions rationnelles L_U . Le corps $L = \varinjlim U L_U$ (qui correspond à une tour $\varinjlim S_U$ de courbes) admet une action naturelle du groupe E . C'est-à-dire, il existe un homomorphisme continu $E \rightarrow \mathrm{Aut}(L / \mathbb{C}_p)$ tel que $L^U = L_U$ pour chaque sous-groupe ouvert et compact U de E .

Le corps $\mathbb{C}_p = L^E$ est appelé le corps des constantes de L . Čerednik montre que L , avec son action de E , peut être défini sur $\bar{\mathbb{Q}} =$ la clôture algébrique de $\mathbb{Q}$. Cela veut dire qu'il existe un sous-corps L' de L invariant par E tel que $(L')^E = \bar{\mathbb{Q}}$ et $L' \otimes_{\bar{\mathbb{Q}}} \mathbb{C}_p = L$. Le corps $L'' = L' \otimes_{\bar{\mathbb{Q}}} \mathbb{C}$ possède les propriétés :

- (α) il existe un homomorphisme injectif et continu $E \rightarrow \text{Aut}(L''/\mathbb{C})$.
- (β) il existe un sous-groupe ouvert et compact U de E tel que $(L'')^U$ est le corps des fonctions rationnelles d'une courbe X_U sur $\mathbb{C}$ de genre > 1 .
- (γ) pour chaque sous-groupe ouvert et compact V de U l'application naturelle $X_V \rightarrow X_U$ est non ramifiée.

Un théorème d'Ihara [7] dit que chaque (L'', E) avec les propriétés (α), (β) et (γ) peut être construit à partir d'un sous-groupe Γ de $Sl(2, \mathbb{R}) \times E$ ayant les propriétés : Γ est discret et est à quotient compact ; les projections de Γ dans $Sl(2, \mathbb{R})$ et E sont injectives.

Pour un Γ donné, on fait la construction d'une tour de courbes comme avant. Pour un sous-groupe ouvert et compact U de E on pose $\Gamma_U = \Gamma \cap (Sl(2, \mathbb{R}) \times U)$ et $X_U = \mathbb{K}/\Gamma_U$ et M_U = le corps des fonctions rationnelles de X_U . Le corps $M = \varinjlim M_U$ possède une action naturelle de E . Le théorème d'Ihara dit que $(L'', E) \cong (M, E)$ pour un Γ convenable.

L'algèbre des quaternions $\hat{D}$ donne un sous-groupe $\hat{D}^1$ de $(\hat{D} \otimes \mathbb{R})^1 \times \prod_{\ell \neq p}^* (\hat{D} \otimes \mathbb{Q}_\ell)^1 \cong Sl(2, \mathbb{R}) \times E$ du type considéré. La démonstration de Čerednik se termine par identifier $\hat{D}^1$ et Γ .

Remarque. - La démonstration de Čerednik est assez longue et compliquée. Un outil essentiel me paraît être le théorème d'Ihara. Je n'ai pas pu consulter [7] pour avoir une idée de sa démonstration.

§. 4. - La courbe modulaire attachée à une algèbre de quaternions sur $\mathbb{Q}$

Nous présentons ici la méthode de V. Drinfeld [5] pour obtenir les résultats de Čerednik. Soit D un corps de quaternions sur $\mathbb{Q}$ non ramifié en ∞ . On désigne par M un ordre maximal de D .

(4.1) THÉORÈME. - Soit $n \geq 3$. Il existe un schéma projectif S_n sur $\mathbb{Z}[\frac{1}{n}]$ qui est le schéma de modules des surfaces abéliennes (ou plutôt des familles de surfaces abéliennes paramétrisées par des $\mathbb{Z}[\frac{1}{n}]$ -schéma) A avec les structures supplémentaires :

- (1) un homomorphisme $M \rightarrow \text{End}(A)$
- (2) un isomorphisme $\frac{1}{n}M/M \xrightarrow{\sim} A[n]$ (= les points d'ordre n de A)
- (3) si A est définie sur un corps de caractéristique p où $p \nmid n$ et D est ramifié en p , alors l'action de M sur l'espace tangent $T_{A,0}$ est spéciale.

Remarques. - 1°) La partie (3) veut dire que $T_{A,0} \otimes \overline{\mathbb{F}}_p$ possède une base e_1, e_2 telle que l'action de $M \otimes \mathbb{Z}_p$ sur $T_{A,0} \otimes \overline{\mathbb{F}}_q$ restreint au sous-anneau $\mathcal{O}$ de $M \otimes \mathbb{Z}_p$, non ramifié et de rang 2 sur $\mathbb{Z}_p$, a la forme matricielle $m \in \mathcal{O} \mapsto \begin{pmatrix} \chi_1(m) & 0 \\ 0 & \chi_2(m) \end{pmatrix}$ où $\chi_1, \chi_2 : \mathcal{O} \rightarrow \overline{\mathbb{F}}_q$ sont les deux homomorphismes d'anneaux possibles.

2°) Soit ρ un élément de D avec $-\rho^2 = 1$ le produit des nombres premiers p qui sont ramifiés dans D . (L'existence de ρ se déduit de [14], th. 3.8, p. 78). L'application $X \mapsto X^* = \rho X \rho^{-1}$ est une involution de D telle que $\text{tr}(X X^*)$ est définie positive. Drinfeld montre d'abord à l'aide de (1) et (3) que A possède une polarisation principale unique telle que l'involution de Rosatti qui y correspond est $X \mapsto X^*$. On peut donc ajouter aux structures supplémentaires de A la polarisation principale correspondante à $X \mapsto X^*$. D'après des théorèmes de Mumford [8] il existe un schéma de modules S_n qui est quasi-projectif.

3°) Soit A une surface abélienne définie sur un corps K complet par rapport à une valuation discrète. On suppose A munie d'un homomorphisme $M \rightarrow \text{End}(A)$. Il existe une extension finie L de K telle que le modèle de Néron $\mathcal{A}$ de $A \otimes_K L$ a réduction stable. Soit $\bar{L}$ le corps résiduel de L . Il existe alors une suite exacte $1 \rightarrow (\bar{L}^*)^i \rightarrow \mathcal{A} \otimes \bar{L} \rightarrow B \rightarrow 1$ où $i \in \{0, 1, 2\}$ et où B est une variété abélienne sur $\bar{L}$. L'action de M sur A induit un homomorphisme $M \rightarrow \text{End}((\bar{L}^*)^i)$. Le groupe $\text{End}((\bar{L}^*)^i)$ est égal à : 0 pour $i=0$, $\mathbb{Z}$ pour $i=1$ et à $M(2, \mathbb{Z})$ pour $i=2$. Comme $M \otimes \mathbb{Q} = D$ est un corps de quaternions, les possibilités $i=1$ ou 2 sont exclues. Cela entraîne que A sur K a potentiellement bonne réduction. On sait que cela implique que S_n est projectif.

4°) On appelle S_n la courbe modulaire attachée à un corps de quaternions sur $\mathbb{Q}$. C'est l'analogue de la courbe modulaire usuelle qui correspond à $M(2, \mathbb{Q})$.

(4.2) THÉORÈME. - Soit $\hat{S}_n$ le complété de S_n par rapport à (p) où p est un nombre premier avec $p \nmid n$ et D est ramifiée en p . Le schéma formel $\hat{S}_n$ sur $\mathbb{Z}_p$ est isomorphe à une réunion finie de schémas formels de la forme $\Gamma \backslash \Omega$ où Γ est un sous-groupe discret de $\mathrm{PGL}(2, \mathbb{Q}_p)$ associé à $\hat{D}$ et n et où Ω est le schéma formel sur $\mathbb{Z}_p$ associé à l'espace analytique $\mathbb{C}_p - \mathbb{Q}_p$.

(4.3) Remarques. - 1°) La courbe sur $\mathbb{Q}_p$ qui correspond à $\hat{S}_n$ est $S_n \times_{\mathbb{Z}[1/n]} \mathbb{Q}_p$. Le théorème dit que chaque composante de celui-ci est isomorphe à $\mathbb{C}_p - \mathbb{Q}_p / \Gamma$ (où je pense que $\Gamma = \Lambda^1(\hat{D}, n)$).

D'autre part, chaque composante de $S_n \times_{\mathbb{Z}[1/n]} \mathbb{C}$ est isomorphe à $\mathcal{K} / \Gamma(D, n)$ parce que ces deux courbes paramétrisent les surfaces abéliennes A sur $\mathbb{C}$ munies des structures supplémentaires $M \longrightarrow \mathrm{End}(A)$ et $\frac{1}{n}M/M \xrightarrow{\sim} A[n]$.

La courbe $S_n \times_{\mathbb{Z}[1/n]} \mathbb{Q}$ est probablement connexe et son corps de définition K est une extension abélienne de $\mathbb{Q}$ (voir [12]). Cela explique que $S_n \times_{\mathbb{Z}[1/n]} \mathbb{Q}_p$ et $S_n \times_{\mathbb{Z}[1/n]} \mathbb{C}$ peuvent avoir plusieurs composantes connexes (qui sont conjuguées). Je note que V. Drinfeld ne donne pas explicitement la structure du groupe Γ dans le théorème (4.2), mais on peut deviner que $\Gamma = \Lambda^1(\hat{D}, n)$. Cela entraîne le théorème (3.1) :

$$\mathcal{K} / \Gamma(D, n) \cong \mathbb{C}_p - \mathbb{Q}_p / \Lambda^1(\hat{D}, n).$$

2°) Je n'ai pas réussi à comprendre (ou plutôt à reconstruire) la démonstration de (4.2). Néanmoins je termine le paragraphe en établissant la raison de l'apparition de $\hat{D}$ dans ce théorème.

3°) M. M. Rapoport m'a communiqué qu'il a calculé la fonction zêta de Hasse de la courbe S_n en utilisant pour le facteur local en p le théorème (4.2) ; (voir aussi la remarque [4], p. 155).

(4.4) Supposons encore que D soit un corps de quaternions indéfini sur $\mathbb{Q}$ et que D soit ramifié en p . Pour $n \geq 3$ tel que $p \nmid n$, on a d'après (4.1) une famille universelle $\mathcal{C} \rightarrow S_n$ de surfaces abéliennes munies des structures (1), (2) et (3). Soit s un point de S_n de caractéristique p . La surface abélienne $A = \mathcal{C} \times \mathbf{k}(s)$ est définie sur un corps fini de caractéristique p . En plus il existe un homomorphisme $M \rightarrow \text{End}(A)$. Le module de Tate $T_p = \varprojlim A[p^m]$ est un $M \otimes \mathbb{Z}_p$ -module. Son rang, comme $\mathbb{Z}_p$ -module, est $<4>$ et alors l'espace vectoriel à gauche $T_p \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ sur le corps $D \otimes \mathbb{Q}_p$ est réduit à 0. Donc aussi $T_p = 0$ et A est supersingulière (i.e. $p : A \rightarrow A$ est purement inséparable). D'après un théorème de Tate [13], $A \otimes \mathbb{F}_p$ est isogène à un produit de deux courbes elliptiques supersingulières. Un autre théorème de Tate [9], appendix I, permet de calculer $\text{End}(A) \otimes \mathbb{Q}$ et $\text{End}_M(A) \otimes \mathbb{Q}$. La dernière algèbre s'identifie à $\hat{D}$.

-:-:-:-

BIBLIOGRAPHIE

- [1] A. BLANCHARD, Les corps non commutatifs, collection Sup, 1972.
- [2] I. V. ČEREDNIK, Towers of algebraic curves uniformized by discrete subgroups of $\text{PGL}_2(k_w) \rtimes E$, Math. Sb 99 (141) (1976), 187-215.
- [3] I. V. ČEREDNIK, Uniformization of algebraic curves by discrete arithmetic subgroups of $\text{PGL}_2(k_w)$ with compact quotients, Math. Sb 100 (142) (1976), 55-78.
- [4] P. DELIGNE et M. RAPOPORT, Les schémas de modules de courbes elliptiques, Modular Functions II, Lect. Notes, Math. 349 (1973).
- [5] V. G. DRINFELD, Coverings of p-adic symmetric regions, Funct. Analysis and its appl. vol. 10 (1976), n° 2, 107-115.
- [6] L. GERRITZEN and M. van der PUT, Schottky groups and Mumford curves, Lect. Notes, Math. 817 (1980).
- [7] Y. IHARA, On congruence monodromy problems, Lect. Notes, vol. 2, Dept of Math., Univ. of Tokyo, Tokyo, 1969.
- [8] D. MUMFORD, Geometric Invariant Theory, Ergebnisse der Math. Band 34 (1965).
- [9] D. MUMFORD, Abelian varieties, Oxford University Press, 1974.

- [10] J.-P. SERRE, Arbres, amalgames, Sl_2 . Astérisque 46 (1977).
- [11] G. SHIMURA, On the theory of automorphic functions, Ann. of Math. (2) 70 (1959), 101-144.
- [12] G. SHIMURA, Introduction to the arithmetic theory of automorphic functions, I. Shoten and Princeton Univ. Press (1971).
- [13] J. TATE, Endomorphisms of abelian varieties over finite fields, Inv. Math. 2 (1966), 134.
- [14] M.-F. VIGNÉRAS, Arithmétique des algèbres de quaternions, Lect. Notes, Math. 800 (1980).
- [15] A. WEIL, Basic Number Theory, Grundlehren, Band 144 (1967).

(texte reçu le 16 juin 1981)

-:-:-:-

Marius van der PUT
 Rijksuniversiteit Groningen
 Mathematisch Instituut
 Postbus 800, 9700 av Gronigen
 GRONIGEN

HYPERGEOMETRIC FUNCTIONS AS p -ADIC ANALYTIC FUNCTIONS

by

B. DWORK

---:---:---

The object of this talk is to indicate how a Frobenius structure may be assigned to the system

$$(1)_{a,b,c} = (1) \quad \frac{d}{d\lambda} (u_1, u_2) = (u_1, u_2) \begin{pmatrix} -\frac{c}{\lambda} & \frac{a-c}{\lambda-1} \\ \frac{c-b}{\lambda} & \frac{c-a-b}{\lambda-1} \end{pmatrix}$$

Let a, b, c be elements of $\mathbb{Q} \cap \mathbb{Z}_p$ lying in the interval $(0, 1)$ (except that c may be 1). We assume that the least common multiple of the denominators of a, b, c is strictly less than p .

Let Ω be an algebraically closed field complete under a non-archimedean valuation extending that of $\mathbb{Q}_p$. For each $\lambda \neq 0, 1, \infty$ in Ω we put

$$\Gamma_0 = \text{Min} \left(1, \frac{1}{|\lambda|} \right)$$

$$\Gamma_1 = \text{Min} \left(1, |\lambda - 1| / |\lambda| \right)$$

$$\Gamma_{1/\lambda} = \text{Min} \left(1, |\lambda - 1| \right)$$

$$\Gamma_\infty = \text{Min} \left(1, |\lambda| \right).$$

We define L_λ to be the space of analytic elements on a region of the form

$$\{ x \mid |x| > \Gamma_0 - \varepsilon, |x-1| > \Gamma_1 - \varepsilon, |1-x\lambda| > \Gamma_{1/\lambda} - \varepsilon, \left| \frac{1}{x} \right| > \Gamma_\infty - \varepsilon \}$$

where $0 < \varepsilon < \text{Min}(\Gamma_0, \Gamma_1, \Gamma_{1/\lambda}, \Gamma_\infty)$ and ε is not fixed but is free to vary for different elements of L_λ .

$$\text{Let } f = x^{b-1} (1-x)^{c-b} (1-\lambda x)^{-a}.$$

$$\text{We define } D_f = \frac{1}{x f} \circ x \frac{d}{dx} \circ x f \text{ and set } W_f (= W_{f, \lambda}) = L_\lambda / D_f L_\lambda.$$

This is a space of dimension two and $1, \frac{1}{1-x}$ represent a basis of this space.

The Cartier operator in characteristic p may be lifted to characteristic zero in the following way.

Let (a', b', c') be subject to the same conditions as (a, b, c) above and related by the condition that

$$\left. \begin{aligned} \mu_a &= p a' - a \\ \mu_b &= p b' - b \\ \mu_c &= p c' - c \end{aligned} \right\} \text{all lie in } \mathbb{N} \text{ in the interval } [0, p-1].$$

$$\text{Put } h(x, \lambda) = x^{b'-1} (1-x)^{c'-b'} (1-\lambda x)^{-a'}$$

$$G(x, \lambda) = \frac{x f(x, \lambda)}{x^p h(x^p, \lambda^p)}.$$

Subject to the condition $\lambda \neq 0, 1, |\lambda - 1| > |p|^{1/p-1}$, we define a mapping

$\alpha_{f, h}$ of $W_{f, \lambda}$ onto W_{h, λ^p} by

$$\xi \longmapsto \psi(\xi \cdot G(x, \lambda))$$

where

$$(\psi \xi)(x) = \frac{1}{p} \sum \xi(z^p)$$

the sum being over all z such that $z^p = x$.

The matrix of $\alpha_{f,h}$ (relative to the bases represented by $1, \frac{1}{1-x}$ in each space) is analytic as function of λ in the region

$$\{\lambda \mid \lambda \neq 0, \infty, |\lambda-1| > |p|^{1/p-1}\}$$

and furthermore the matrix has at most poles at $0, \infty$ and the coefficients are bounded by 1 in the region

$$R_0 = \{\lambda \mid |\lambda| = 1 = |\lambda-1|\}.$$

A dual theory is constructed by means of the direct sums of function analytic on the four disks

$$\{x \mid |x| < \Gamma_0\}, \{x \mid |x-1| < \Gamma_1\}, \{x \mid |1-x\lambda| < \Gamma_1/\lambda\},$$

$\{x \mid |\frac{1}{x}| < \Gamma_\infty\}$, and if $K_{f,\lambda}$ represents in this theory the space dual to $W_{f,\lambda}$ then there exists a commutative diagram, (except for a factor of p)

$$\begin{array}{ccc} K_{f,\lambda} & \xrightarrow{\quad} & W_{(1/f),\lambda} \\ \uparrow \alpha_{f,h}^* & & \uparrow \alpha_{(1/f), (1/h)}^{-1} \\ K_{h,\lambda^p} & \xrightarrow{\quad} & W_{(1/h),\lambda^p} \end{array}$$

where the horizontal maps are suitable rational maps (i. e. their matrices are rational functions of λ). This diagram gives the symplectic structure. By means of it we establish that relative to the bases represented by $1, \frac{1}{1-x}$, the matrix of $\alpha_{f,h}$ has the following form

1	$\mu_c < \text{Min}(\mu_a, \mu_b)$	$\begin{pmatrix} a_1 & p a_3 \\ a_2 & p a_4 \end{pmatrix}$
2	$\mu_c > \text{Max}(\mu_a, \mu_b)$	$\begin{pmatrix} p a_1 & a_3 \\ p a_2 & a_4 \end{pmatrix}$
3	$\mu_b < \mu_c < \mu_a$	$\begin{pmatrix} a_1 & a_3 \\ a_2 & a_4 \end{pmatrix}$
4	$\mu_a < \mu_c < \mu_b$	$p \begin{pmatrix} a_1 & a_3 \\ a_2 & a_4 \end{pmatrix}$

where in all cases the function a_i ($i=1,2,3,4$) is bounded by 1 on R_0 ,

$$\left| \det \begin{pmatrix} a_1 & a_3 \\ a_2 & a_4 \end{pmatrix} \right| = 1 \text{ on } R_0.$$

In case 1 (resp. case 2), the reductions mod p of a_1, a_2 (resp. a_3, a_4) are non-trivial polynomials of degree strictly less than p . We have no need for a more explicit representation of the a_i .

We now indicate the relation between $\alpha_{f,h}$ and the differential equation (1). Let $\beta \in \Omega$. Then for

$$|\lambda - \beta| < |\beta| \min(1, |\beta - 1|),$$

there exists a natural map $T_{\beta, \lambda, f}$ of $K_{f, \beta}$ onto $K_{f, \lambda}$ whose matrix relative to the dual bases $1^*, (\frac{1}{1-x})^*$ is a solution matrix of (1) at β which reduces to the identity at $\lambda = \beta$. Furthermore we have the commutative diagram:

$$\begin{array}{ccc} K_{f, \beta} & \xrightarrow{T_{\beta, \lambda, f}} & K_{f, \lambda} \\ \uparrow \alpha_{f, h, \beta}^* & & \uparrow \alpha_{f, h, \lambda}^* \\ K_{h, \beta^p} & \xrightarrow{T_{\beta^p, \lambda^p, h}} & K_{h, \lambda^p} \end{array}$$

Let $C_f(\beta, \lambda)$ be the solution matrix of (1) at β satisfying $C_f(\beta, \beta) = I$. Likewise let $C_h(\beta, \lambda)$ be the solution matrix of (1) $_{a', b', c'}$ at β which reduces to identity at $\beta = \lambda$, then (with $\alpha = \begin{pmatrix} a_1 & a_2 \\ p a_3 & p a_4 \end{pmatrix}$ in case 1, etc)

$$(2) \quad C_h(\beta^p, \lambda^p) \alpha(\lambda) = \alpha(\beta) C_f(\beta, \lambda).$$

We deduce from this, letting $\beta^{p^\ell} = \beta$, a semilinear mapping

$$(u_1, u_2) \longmapsto (u_1, u_2)^\sigma (\lambda^p) \alpha(\lambda)$$

of solutions of (1) $_{a', b', c'}$ at β defined over $\mathbb{Q}_p(\beta)$ onto solutions of (1) $_{a, b, c}$ at β , the symbol $(u_1, u_2)^\sigma (\lambda^p)$ being explained by

$$\sum a_j (\lambda - \beta)^j \longmapsto \sum a_j^\sigma (\lambda^p - \beta^\sigma)^j$$

where σ is the Frobenius automorphism of $\mathbb{Q}_p(\beta)$ over $\mathbb{Q}_p$.

To indicate the consequences of this structure, let us restrict our attention to the case in which $(a', b', c') = (a, b, c)$.

Then in case 3, case 4, $\beta \neq 0, 1, \infty$, $\beta^p = \beta$, the solutions of (1) at β converge and are bounded in $D(\beta, 1^-)$. In case 1 (which we will now discuss, there being a similar theory for case 2), there are two possibilities

Ordinary Case. - $|a_1(\beta)| = 1$. Then there is a unique solution at β convergent on $D(\beta, 1^-)$. The second solution is unbounded on $D(\beta, 1^-)$ and grows like $\log \lambda/\beta$ as $|\lambda - \beta| \rightarrow 1$.

Super singular Case. - $|a_1(\beta)| < 1$. Then all solutions are unbounded on $D(\beta, 1^-)$ and grow like $\sqrt{\log \lambda/\beta}$ as $|\lambda - \beta| \rightarrow 1$.

Furthermore in the ordinary case, by the theory of semilinear mappings there exists a solution matrix Y defined over Ω_0 the maximal unramified extension of $\mathbb{Q}_p$ such that

$$Y^\sigma(\lambda^p) \alpha(\lambda) = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} Y(\lambda).$$

Writing

$$Y(\lambda) = \begin{pmatrix} u_1 & u_2 \\ v_1 & v_2 \end{pmatrix}$$

we normalize Y by the condition $|u_1(\beta)| = 1$, $|\det Y(\beta)| = 1$. We then show that

$$Y = \begin{pmatrix} 1 & 1 \\ \tau & 0 \end{pmatrix} \begin{pmatrix} u & 0 \\ 0 & \hat{u} \end{pmatrix} \begin{pmatrix} 1 & \eta \\ 0 & 1 \end{pmatrix}$$

where u assume only unit values on $D(\beta, 1^-)$,

η is an analytic element on $R_f = \{\lambda \mid |a_1(\lambda)| = 1\}$

$$\frac{u(\lambda)}{u^\sigma(\lambda^p)} = a_1(\lambda) + p a_3(\lambda) \eta(\lambda^p)$$

$$\tau^\sigma(\lambda^p) - p \tau(\lambda) = p a_3(\lambda) \frac{\omega(\lambda^p)}{u(\lambda) u^\sigma(\lambda^p)}$$

$$\omega = \det Y.$$

The relations show that while u is only defined on $D(\beta, 1^-)$, the ratio $u(\lambda)/u^\sigma(\lambda^P)$ is an analytic element on R_f . It also follows that τ is unbounded.

For further information we refer the reader to the Princeton Ph D Thesis of Mark Heiligman and also to the Lecture Notes of our course at Strasbourg in the winter of 1980. A discussion of the canonical lifting, i. e. of the solution of the equation

$$\tau^\sigma(\lambda^P + z) = p \tau(\lambda)$$

was given in a D.P.P. talk on Dec. 1, 1980.

(texte reçu le 13 janvier 1981)

-:-:-:-

B. DWORK
 Maths Department Fine Hall
 Princeton University
 PRINCETON N.J 08540
 U.S.A

SUR LE THÉORÈME DE FUKASAWA-GEL'FOND

par

François GRAMAIN

-:-:-:-

1. - Introduction

En 1915, G. Pólya [P], montrait qu'une fonction entière f telle que $f(\mathbb{N}) \subset \mathbb{Z}$, et de type exponentiel $< \log 2$ (id est telle que $\limsup_{r \rightarrow +\infty} (\log |f|_r / r) < \log 2$, où $|f|_r = \sup \{ |f(z)| ; |z| \leq r \}$ et $\log$ désigne le logarithme népérien) est un polynôme, ce résultat étant le meilleur possible, comme le montre la fonction $f(z) = 2^z$. L'étude des fonctions entières telles que $f(\mathbb{N}) \subset \mathbb{Z}$ ou $f(\mathbb{Z}) \subset \mathbb{Z}$ est maintenant très complète, en particulier grâce à Ch. Pisot (on trouvera une bibliographie importante dans [Gra 1], [Gra 2] et [Wa]). Les fonctions entières f telles que $f(\mathbb{Z}[i]) \subset \mathbb{Z}[i]$ furent étudiées en premier par S. Fukasawa en 1926 [F], et, en 1929, A. Gel'fond [G] améliorant le résultat de Fukasawa montrait que :

Il existe un réel $\alpha > 0$ tel que, si f est une fonction entière vérifiant $\limsup_{r \rightarrow +\infty} (\log |f|_r / r^2) < \alpha$ et $f(\mathbb{Z}[i]) \subset \mathbb{Z}[i]$, alors f est un polynôme.

En 1929, Gel'fond trouvait pour α une valeur $< 10^{-45}$. Il faut attendre 1979 et L. Gruman [Gru] pour améliorer cette constante, et obtenir $\alpha = 0,0396\dots$. En 1980, D. Masser [M] publie une note aux C.R.A.S. dans laquelle il donne la meilleure constante α_0 que puisse fournir la méthode des séries d'interpolation, utilisée par Gel'fond (voir [Gra 3] pour une démonstration complète des résultats de [M]). On peut vérifier (voir [Gra-We]) que α_0 est voisin de $1/2e$. De plus, D. Masser montre qu'on ne peut avoir $\alpha > \pi/2e$, en construisant une fonction entière (non polynômiale) de type $\pi/2e$ d'ordre 2 telle que $f(\mathbb{Z}[i]) \subset \mathbb{Z}[i]$.

Les démonstrations de ces résultats utilisent des propriétés arithmétiques de $\mathbb{Z}[i]$ de plus en plus fines, en particulier sur les premiers de $\mathbb{Z}[i]$. En fait, une méthode "de transcendance", la méthode de Schneider, permet d'obtenir la meilleure constante α possible (dans le théorème de Gel'fond), dans des cas plus généraux que celui de $\mathbb{Z}[i]$.

THÉORÈME. - Soit K le corps quadratique imaginaire de discriminant $-\Delta$, et $a = \sqrt{\Delta}/2$ l'aire d'un parallélogramme fondamental du réseau $\mathcal{O}_K$ des entiers de K .

(i) Si f est une fonction entière vérifiant $f(\mathcal{O}_K) \subset \mathcal{O}_K$ et

$$\limsup_{r \rightarrow +\infty} \frac{\log |f|_r}{r^2} < \frac{\pi}{2ea},$$

alors f est un polynôme.

(ii) Il existe une fonction entière f telle que $f(\mathcal{O}_K) \subset \mathcal{O}_K$ et

$$\limsup_{r \rightarrow +\infty} \frac{\log |f|_r}{r^2} = \frac{\pi}{2ea}.$$

On trouvera la démonstration complète de ce théorème dans [Gra 4]. Nous donnerons ici la preuve du résultat suivant, un peu plus fort que la partie (i) du théorème :

PROPOSITION. - Soit K le corps quadratique imaginaire de discriminant $-\Delta$, et $a = \sqrt{\Delta}/2$ l'aire d'un parallélogramme fondamental du réseau $\mathbb{O}_K$ des entiers de K . Il existe une constante $C > 0$ (ne dépendant que de K) telle que, si f est une fonction entière vérifiant $f(\mathbb{O}_K) \subset \mathbb{O}_K$, et, pour r assez grand

$$\log |f|_r \leq \frac{\pi}{2ea} r^2 - C r^{5/3} (\log r)^{1/3},$$

alors f est polynôme.

Au paragraphe 2 nous donnons les lemmes nécessaires à la preuve de la proposition qui fait l'objet du paragraphe 3.

2. - Quelques lemmes

Les lemmes 1 et 2 sont dus à D. Masser (le deuxième dans le cas particulier de $\mathbb{Z}[i]$). Le lemme 3 est un lemme de Schwarz pour les fonctions analytiques ayant de nombreux zéros dans un réseau, et il est, au terme correctif près, le meilleur possible. Le lemme 4, le plus original de ce travail, montre qu'une fonction entière vérifiant "deux équations aux différences finies dans deux directions différentes" est d'ordre ≤ 1 . Quant au lemme 5, il est dû à M. Waldschmidt [W2] et il repose sur l'utilisation de la méthode de Schneider.

LEMME 1. - Soit $z \in \mathbb{C}$ et $r \geq 0$. Si dw désigne l'élément d'aire de $\mathbb{R}^2 \simeq \mathbb{C}$, l'intégrale

$$I_r(z) = \iint_{D(0,r)} \log |z-t| dw(t)$$

existe. On a $I_0(z) = 0$, et, si $r > 0$,

$$I_r(z) = \begin{cases} \pi r^2 \log |z| & \text{si } |z| \geq r \\ \pi r^2 \log r - \frac{\pi}{2} (r^2 - |z|^2) & \text{si } |z| \leq r \end{cases}.$$

Démonstration. - La convergence de cette intégrale provient de ce que

$$\int_0^{2\pi} \int_0^x (\log \rho) \rho \, d\rho \, d\theta = 2\pi \int_0^x (\log \rho) \rho \, d\rho$$

existe. En effet, par intégration par parties, on a :

$$\int (\log \rho) \rho \, d\rho = \frac{1}{2} \rho^2 \log \rho - \frac{1}{2} \int \rho \, d\rho = \frac{1}{2} \rho^2 \log \rho - \frac{1}{4} \rho^2,$$

et $\rho^2 \log \rho \rightarrow 0$ quand $\rho \rightarrow +0$.

On a donc $I_r(z) = \int_0^r \varphi(\rho) \rho \, d\rho$, avec $\varphi(\rho) = \int_0^{2\pi} \log |f(\rho e^{i\theta})| \, d\theta$, où $f(t) = z - t$. Si $z = 0$ le résultat est immédiat ; et si $z \neq 0$, la formule de Jensen ([W1], 1.5.3) montre que, pour $\rho > 0$, on a $\varphi(\rho) = 2\pi \max(\log |z|, \log \rho)$. Le lemme en découle aussitôt.

c. q. f. d.

LEMME 2. - Soit $\{\zeta_j\}_{j \in \mathbb{N}} = \Lambda$ un réseau de $\mathbb{R}^2 \simeq \mathbb{C}$, où les ζ_j sont ordonnés de sorte que $|\zeta_j| \leq |\zeta_{j+1}|$ pour tout $j \in \mathbb{N}$. Soit a l'aire d'un parallélogramme fondamental de Λ . Il existe une constante C_1 (ne dépendant que de Λ) aisément calculable, telle que, si $z \in \mathbb{C}$ vérifie $|z| = \theta |\zeta_n|$, on ait, pour $n \geq 2$

$$\left| \log \left| \prod_{j=0}^{n-1} (z - \zeta_j) \right| - \frac{1}{2} n \log n - n w(\theta) \right| \leq C_1 \max(1, \theta) \sqrt{n} \log n,$$

où l'astérisque signifie qu'on omet dans le produit les facteurs de module < 1 , et où

$$w(\theta) = \begin{cases} \log \theta - \frac{1}{2} \log \frac{\pi}{a} & \text{si } \theta \geq 1 \\ \frac{\theta^2}{2} - \frac{1}{2} - \frac{1}{2} \log \frac{\pi}{a} & \text{si } \theta \leq 1. \end{cases}$$

Ce lemme résulte du fait qu'un réseau est bien réparti dans le plan, donc que $\log \left| \prod_{j=0}^{n-1} (z - \zeta_j) \right|$ est voisin de $\frac{1}{a} I_{|\zeta_n|}(z)$. On utilise aussi l'estimation classique $|\zeta_n| = \sqrt{\frac{an}{\pi}} + O(1)$.

LEMME 3. - Soit Λ un réseau de $\mathbb{R}^2 \simeq \mathbb{C}$, dont l'aire d'un parallélogramme fondamental est a . Il existe une constante C_2 (ne dépendant que de Λ) aisément calculable, ayant la propriété suivante : si ρ , R_1 et R_2 sont des

réels vérifiant $3 \leq \rho + 1 \leq R_1 \leq R_2$, et f une fonction holomorphe au voisinage de $\bar{D}(0, R_2)$, telle que $f(\Lambda \cap \bar{D}(0, \rho)) = \{0\}$, alors on a

$$\log |f|_{R_1} \leq \log |f|_{R_2} - \frac{\pi}{a} \rho^2 \log \frac{R_2}{R_1} + C_2 \frac{R_2^2}{R_1} \log \rho .$$

Démonstration. - Soit ζ l'élément courant de Λ . La fonction

$$g(z) = f(z) \prod_{|\zeta| \leq \rho} \frac{R_2^2 - z \bar{\zeta}}{R_2(z - \zeta)}$$

est holomorphe au voisinage de $\bar{D}(0, R_2)$, et, d'après les propriétés élémentaires des produits de Blaschke, on a $|g|_{R_2} = |f|_{R_2}$. D'autre part,

$$\frac{R_2^2 - z \bar{\zeta}}{R_2(z - \zeta)} = \frac{z}{R_2} \left(\frac{R_2^2}{z} - \bar{\zeta} \right) (z - \zeta)^{-1} ,$$

et le réseau des $\bar{\zeta}$ est symétrique de Λ par rapport à l'axe réel. Le nombre n des facteurs de Blaschke vérifie $|n - \pi \rho^2 / a| \leq C_3 \rho$, et on a $R_2^2 / R_1 \rho \geq R_1 / \rho > 1$, donc le lemme 2 montre que

$$|\log |g|_{R_1} - \log |f|_{R_1} - \frac{\pi}{a} \rho^2 (\log \frac{R_1}{R_2} + \log \frac{R_2^2}{R_1 \rho} - \log \frac{R_1}{\rho})| \leq C_2 \frac{R_2^2}{R_1} \log \rho .$$

Il suffit alors d'appliquer à g le principe du maximum ($|g|_{R_1} \leq |g|_{R_2}$) pour obtenir le lemme.

c. q. f. d.

LEMME 4. - Soit α et β deux nombres complexes linéairement indépendants sur $\mathbb{R}$, et $f : \mathbb{C} \rightarrow \mathbb{C}$ une fonction bornée sur tout compact vérifiant les deux équations fonctionnelles

$$\varphi(z) + \sum_{0 \leq n \leq N_1} P_n(z) f(z + \alpha n) = \psi(z) + \sum_{0 \leq n \leq N_2} Q_n(z) f(z + \beta n) = 0 ,$$

où les P_n (resp. Q_n) sont des éléments non tous nuls de $\mathbb{C}[z]$. Alors, si les fonctions φ et $\psi : \mathbb{C} \rightarrow \mathbb{C}$ sont bornées sur tout compact et vérifient

$$\limsup_{r \rightarrow +\infty} \frac{\log |\varphi|_r}{r \log r} < \tau , \text{ et } \limsup_{r \rightarrow +\infty} \frac{\log |\psi|_r}{r \log r} < \tau' , \text{ avec } \tau \text{ et } \tau' \geq 0 ,$$

la croissance de la fonction f est limitée par

$$\limsup_{r \rightarrow +\infty} \frac{\log |f|_r}{r \log r} \leq \frac{D+D'}{r_0} + \frac{r_1}{r_0} \max(\tau, \tau'),$$

où D (resp. D') est le maximum des degrés des polynômes P_n (resp. Q_n) ;
 r_0 le diamètre du plus grand disque contenu dans le parallélogramme de sommets
 $0, \alpha, \beta$ et $\alpha+\beta$; et r_1 le diamètre du plus petit disque contenant ce paral-
lélogramme.

Démonstration. - Tout $z \in \mathbb{C}$ a une écriture unique sous la forme

$z = c_\alpha(z)\alpha + c_\beta(z)\beta$, avec $c_\alpha(z)$ et $c_\beta(z)$ réels. On peut supposer, sans perte de généralité, que $P_0 P_{N_1} Q_0 Q_{N_2} \neq 0$. Soit M tel que le parallélogramme $\{\max(|c_\alpha(z)|, |c_\beta(z)|) \leq M\}$ contienne les zéros de $P_0 P_{N_1} Q_0 Q_{N_2}$, et soit $N = \max(N_1, N_2)$. Pour R réel positif, posons :

$$[f]_R = \sup \{ |f(z)| ; \max(|c_\alpha(z)|, |c_\beta(z)|) \leq R \}$$

et

$$\{f\}_R = \sup \{ |f(z)| ; |c_\alpha(z)| \leq R+1, |c_\beta(z)| \leq R \}.$$

On a noté, comme d'habitude

$$|f|_R = \sup \{ |f(z)| ; |z| \leq R \}.$$

Fixons un $R \geq M+N+1$ assez grand pour que $\log |\varphi|_r \leq \tau r \log r$, et $\log |\psi|_r \leq \tau' r \log r$, si $r \geq r_1(R+1)$.

Soit z tel que $R \leq c_\alpha(z + \alpha N_1) \leq R+1$, et $|c_\beta(z + \alpha N_1)| \leq R$. On a

$$f(z + \alpha N_1) = -\frac{\varphi(z)}{P_{N_1}(z)} - \sum_{n=0}^{N_1-1} \frac{P_n(z)}{P_{N_1}(z)} f(z + \alpha n),$$

donc il existe une constante C_4 ne dépendant que du réseau engendré par α et β et des polynômes P_n , telle que

$$|f(z + \alpha N_1)| \leq C_4 R^D [f]_R + e^{\tau r_1(R+1) \log(r_1(R+1))}.$$

De même, pour $-R-1 \leq c_\alpha(z) \leq -R$ et $|c_\beta(z)| \leq R$, on a

$$f(z) = -\frac{\varphi(z)}{P_o(z)} - \sum_{n=1}^{N_1} \frac{P_n(z)}{P_o(z)} f(z + \alpha n),$$

d'où l'existence de C_5 telle que

$$|f(z)| \leq C_5 R^D [f]_R + e^{\tau r_1(R+1) \log(r_1(R+1))}.$$

Cela montre que

$$\{f\}_R \leq C_6 R^D [f]_R + e^{\tau r_1(R+1) \log(r_1(R+1))}.$$

Une utilisation analogue de la deuxième équation fonctionnelle vérifiée par f montre que

$$[f]_{R+1} \leq C_7 R^{D'} \{f\}_R + e^{\tau' r_1(R+1) \log(r_1(R+1))}.$$

On a donc

$$[f]_{R+1} \leq C_8 R^{D+D'} [f]_R + e^{r_1(\max(\tau, \tau') + \varepsilon) R \log R}$$

pour tout $\varepsilon > 0$, dès que $R > R_o(\varepsilon)$.

Par itération, si K est un entier positif, et si on a choisi $C_8 > 1$, on a

$$[f]_{R+K} \leq C_8^K (R+K)^{K(D+D')} ([f]_R + e^{r_1(\max(\tau, \tau') + \varepsilon)(R+K) \log(R+K)}) .$$

Mais, si ρ est un réel positif, on a $|f|_{r_o \rho} \leq [f]_\rho$, d'où :

$$\log |f|_{r_o(R+K)} \leq K(D+D') \log(R+K) + r_1(\max(\tau, \tau') + \varepsilon) (R+K) \log(R+K) + O(K),$$

et on en déduit immédiatement le lemme en faisant tendre K vers l'infini.

c. q. f. d.

LEMME 5. - Soit K un corps quadratique imaginaire, et $\mathcal{O}_K$ l'anneau des entiers de K . Il existe une constante $C_9 > 0$ (ne dépendant que de K), telle que, si f est une fonction entière vérifiant $f(\mathcal{O}_K) \subset \mathcal{O}_K$ et

$$\limsup_{r \rightarrow +\infty} \frac{\log |f|_r}{r^2} < C_9,$$

alors f est un polynôme.

C'est un cas particulier du théorème 2 de [W2]. En fait, on n'a pas besoin d'un résultat aussi précis, et le théorème 2.2.1 de [W1], qui est un raffinement du théorème de Schneider-Lang, suffit pour conclure, au paragraphe suivant.

3. - La preuve de la proposition.

Soit donc f une fonction entière vérifiant $f(\mathcal{O}_K) \subset \mathcal{O}_K$ et

$$\log |f|_r \leq \frac{\pi}{2ea} r^2 - Cr^{5/3} (\log r)^{1/3},$$

pour r assez grand. Soit $\alpha \neq 0$ un entier de K , et H un entier suffisamment grand. Nous allons construire une fonction

$$f(z) = \sum_{0 \leq \lambda_1 \leq L_1} \sum_{0 \leq \lambda_2 \leq L_2} a(\lambda) z^{\lambda_1} f(z + \alpha \lambda_2),$$

avec $L_1 = H^{5/3} (\log H)^{-2/3}$ et $L_2 = H^{2/3} (\log H)^{1/3}$, et où $a(\lambda) = a(\lambda_1, \lambda_2) \in \mathbb{Z}$ pour $\lambda_1 \in \{0, 1, \dots, [L_1]\}$ et $\lambda_2 \in \{0, 1, \dots, [L_2]\}$, telle que $F(\zeta) = 0$ pour tout $\zeta \in \mathcal{O}_K \cap \bar{D}(0, H)$. Pour cela, il suffit de résoudre un système linéaire homogène en les $a(\lambda)$, de $\frac{\pi H^2}{2ea} + O(H)$ équations à $([L_1] + 1)([L_2] + 1) \geq H^{7/3} (\log H)^{-1/3}$ inconnues, dont les coefficients sont des entiers de K dont le logarithme du module est majoré par $\frac{\pi}{2ea} H^2 + O(H^{5/3} (\log H)^{1/3})$. Le lemme de Siegel ([W1], lemme 1.3.1) montre qu'il existe une solution non triviale $a(\lambda) \in \mathbb{Z}$, vérifiant

$$\log \max_{ea} |a(\lambda)| \leq \frac{\pi^2}{2} H^{5/3} (\log H)^{1/3} (1 + O(H^{-1/3} (\log H)^{1/3})).$$

On veut montrer que F est identiquement nulle. Comme $F(0) = 0$, le théorème de Liouville montre qu'il suffit de prouver que F est bornée. On va faire la démonstration par récurrence suivante : Supposant que $F(\mathcal{O}_K \cap \bar{D}(0, N)) = \{0\}$ on va montrer que $|F|_{N+1} < 1$. Comme $F(\mathcal{O}_K) \subset \mathcal{O}_K$, il en résultera que $F(\mathcal{O}_K \cap \bar{D}(0, N+1)) = \{0\}$.

Par construction, l'hypothèse de récurrence est vérifiée pour $N = H$. Supposons donc $N \geq H$ et $F(\zeta) = 0$ pour tout $\zeta \in \mathcal{O}_K \cap \bar{D}(0, N)$. Le lemme 3, appliqué à F , avec $\rho = N$, $R_1 = N+1$ et $R_2 = \sqrt{e}(N+1)$ fournit

$$\log |F|_{N+1} \leq \log |F|_{\sqrt{e}(N+1)} - \frac{\pi}{2a} N^2 + O(N \log N),$$

d'où :

$$\begin{aligned} \log |F|_{N+1} &\leq \frac{\pi^2}{2ea} H^{5/3} (\log H)^{1/3} + H^{5/3} (\log H)^{-2/3} \log N + \frac{\pi |\alpha|}{\sqrt{e} a} H^{2/3} (\log H)^{1/3} N \\ &\quad - C e^{5/6} N^{5/3} (\log N)^{1/3} + O(N^{5/3}). \end{aligned}$$

Compte tenu de la forme du second membre de cette inégalité, pour obtenir $\log |F|_{N+1} < 0$, il suffit de vérifier que $\log |F|_{H+1} < 0$, et cette dernière inégalité est réalisée, pour H assez grand, si

$$C e^{5/6} > \frac{\pi}{ea} + 1 + \frac{\pi |\alpha|}{\sqrt{e} a}.$$

On a ainsi montré que, sous cette condition sur C , la fonction F est identiquement nulle. Si nous faisons cette construction pour deux valeurs $\mathbb{R}$ -linéairement indépendantes de $\alpha \in \mathcal{O}_K$, nous voyons que f vérifie les hypothèses du lemme 4 (avec $\varphi = \psi = 0$), donc que, d'après le lemme 5, f est un polynôme.

BIBLIOGRAPHIE

- [F] S. FUKASAWA, Über ganzwertige ganze Funktionen, Tôhoku Math. J., t. 27 (1926), 41-52.
- [G] A. GEL'FOND, Sur les propriétés arithmétiques des fonctions entières, Tôhoku Math. J., t. 30 (1929), 280-285.
- [Gra 1] F. GRAMAIN, Fonctions entières arithmétiques, Séminaire Delange-Pisot-Poitou (théorie des nombres), 19e année (1977-78), n° 8, 14 p.
- [Gra 2] F. GRAMAIN, Fonctions entières arithmétiques, Séminaire P. Lelong-H. Skoda (analyse) 17e année (1976-77), Lecture Notes in Math. n° 694 Berlin-Heidelberg-New York : Springer 1978.
- [Gra 3] F. GRAMAIN, Sur le théorème de Fukasawa-Gel'fond-Gruman-Masser, Séminaire Delange-Pisot-Poitou (théorie des nombres), 22e année (1980-81), Birkhäuser Verlag (à paraître).
- [Gra 4] F. GRAMAIN, Sur le théorème de Fukasawa-Gel'fond, Inventiones Mathematicae (à paraître).
- [Gra-We] F. GRAMAIN et M. WEBER (à paraître).
- [Gru] L. GRUMAN, Propriétés arithmétiques des fonctions entières, Bull. Soc. Math. France, t. 108 (1980), 421-440.
- [M] D. MASSER, Sur les fonctions entières à valeurs entières, C.R.A.S. Paris, t. 291, série A (1980), 1-4.
- [P] G. PÓLYA, Über ganzwertige ganze Funktionen, Rend. Circ. Math. Palermo, t. 40 (1915), 1-16.
- [W 1] M. WALDSCHMIDT, Nombres transcendants, Lecture Notes in Math. n° 402, Berlin-Heidelberg-New York : Springer 1974.
- [W 2] M. WALDSCHMIDT, Pólya's theorem by Schneider's method, Acta Math. Acad. Scient. Hungaricae, t. 31 (1978), 21-25.
- [Wa] R. WALLISSER, Aperçu sur les fonctions entières arithmétiques, in Problemes diophantiens, fasc. 3 (1981). Publications Mathématiques de l'Université P. et M. Curie.

(texte reçu le 10 mars 1980)

-:-:-:-

François GRAMAIN
 Université de Paris VI
 U. E. R. de Mathématiques
 4, place Jussieu - Tour 45-46, 5e ét.
 F 75230 PARIS CEDEX 05

PADÉ-APPROXIMATIONS IN NUMBER THEORY

by

F. BEUKERS

-:-:-:-

Introduction

In 1873, Hermite [H], was the first to construct explicit simultaneous Padé-approximations to the system of functions $1, e^z, e^{2z}, \dots, e^{nz}$ and discovered the transcendence of e . Since that year there have been several other applications of Padé-approximations in number theory. Very recently there has been an upsurge of interest in the use of Padé-approximations in irrationality and transcendence proofs, stimulated by Apéry's remarkable irrationality proof for $\zeta(3)$. In this exposition we give a rough overview of these various applications.

We first define the term Padé-approximation, which we shall abbreviate as P.A. in what follows. Let $f_1, f_2, \dots, f_k$ be a system of functions analytic around $z=0$ and suppose $f_1(0) \neq 0$. We distinguish two kinds of P.A.'s (see K. Mahler [Ma], H. Jager [J]).

Type I : polynomials $P_1(z), \dots, P_k(z)$ of degree $n_1, \dots, n_k$ such that

$$P_1(z) f_1(z) + \dots + P_k(z) f_k(z) = O(z^{N+k+1})$$

where $N = \sum n_i$.

Type II : polynomials $P_1(z), \dots, P_k(z)$ of degree $N-n_1, \dots, N-n_k$ with $\sum n_i = N$, such that

$$P_i(z) f_j(z) + P_j(z) f_i(z) = O(z^{N+1}) \quad i, j = 1, \dots, k.$$

Notice that if $k = 2$ then both types coincide, and the rational functions $-P_1(z)/P_2(z)$, constitute the so-called Padé-table of the function $f_1(z)/f_2(z)$.

Various applications

One of the first to apply P.A.'s in number theory was A. Thue, although he does not refer to them as such. For an account of this see C. L. Siegel [Si 3]. In 1937, Siegel [Si 1] used P.A.'s to the function $(1-z)^{1/n}$ to study the diophantine equation

$$(1) \quad ax^n - by^n = c \quad (a, b, c, n \in \mathbb{Z}, n \geq 3)$$

in the unknown positive rational integers x, y . He showed,

THEOREM 1. - If $|ab| > \lambda_n |c|^{2\frac{n-1}{n-2}}$ (where λ_n is an explicit constant) then equation (1) has at most one solution.

By elaborating Siegel's method one can show that if $n \geq 5$ and $c = 1$, equation (1) has at most 2 solutions, see [D]. Very recently J. Evertse showed that if c is a prime power then there are at most $2n+6$ solutions (unpublished yet).

By examining Siegel's method and applying an ingenious trick on the coefficients of the P.A.'s of $(1-z)^{1/3}$ A. Baker [Ba 1] was able to show,

THEOREM 2. - For any $\frac{p}{q} \in \mathbb{Q}$ we have

$$\left| \frac{p}{q} - \sqrt[3]{2} \right| > \frac{10^{-6}}{2.955 q}.$$

This was the first example of an explicit bound for the approximation of an algebraic number by rationals which is better than the trivial Lionville-estimate (which would be $\left| \frac{p}{q} - \sqrt[3]{2} \right| > 10^{-1} q^{-3}$). It seems extremely hard to find non-trivial lower bounds for other algebraic numbers beside the ones mentioned in Baker's paper.

In 1977 the author [Be 1], using P.A.'s to $\sqrt{1-z}$ obtained

THEOREM 3. - For any $x, r \in \mathbb{N}$ we have

$$\left| \frac{x}{2^r} - \sqrt{2} \right| > \frac{2^{-43.9}}{2^{1.8r}}.$$

Multiplication of this inequality with $2^{2r}(\sqrt{2} + x \cdot 2^{-r})$ yields

$$\left| x^2 - 2^{2r+1} \right| > 2^{0.2r} 2^{-43.4}$$

from which we easily derive

COROLLARY. - Let $D \in \mathbb{Z}$ and let $x, n \in \mathbb{N}$ be a solution of the diophantine equation $x^2 + D = 2^n$. Then $n < 435 + 10 \log |D| / \log 2$.

As a consequence we see that for given $D \in \mathbb{Z}$ the diophantine equation $x^2 + D = 2^n$ can be solved in finitely many steps. Moreover, after some technical considerations it is possible to show that $x^2 + D = 2^n$ has at most four solutions, unless $D = 7$ in which case the solutions read $(x, n) = (1, 3) (3, 4) (5, 5) (11, 7) (181, 15)$.

By using P.A.'s to the function $\sum_{r=0}^{2m} \binom{3m}{m+r} (-z)^r$ the author [Be 4] showed in 1980,

THEOREM 4. - For all $k > 5000$ we have

$$\|(\frac{3}{2})^k\| > 2^{-0.9k}$$

where $\|x\|$ denotes $\min_{m \in \mathbb{Z}} |x-m|$.

It is a well-known fact that if $\|(3/2)^k\| > (3/4)^k$ for some $k \geq 5$ then $g(k) = 2^k + [(3/2)^k] - 2$ for this value of k , where $g(k)$ denotes the number $\min\{s \mid a = n_1^k + \dots + n_s^k \text{ for all } a \in \mathbb{N}\}$ in Waring's problem. Unfortunately Theorem 4 does not give the required lower bound. It seems very hard however to obtain anything better than the trivial lower bound 2^{-k} .

Irrationality results. - In attempts to interpret and generalise Apéry's irrationality proof several people began to reappraise the older methods that existed in irrationality and transcendence theory and added many new and interesting results. In this way E. Bombieri in 1979-80 continued Siegel's [Si2] and Galoschkin's [G] work on G-functions and obtained some strong theorems, of which we mention one

COROLLARY. - Let $L_r(z)$ be the r th polylogarithm defined by

$$L_r(z) = \frac{z}{1^r} + \frac{z^2}{2^r} + \frac{z^3}{3^r} + \dots$$

Then, for any $\varepsilon > 0$ and any $d \in \mathbb{N}$ there exists an explicit constant $c = c(k, d, \varepsilon)$ such that for $q > c|p|^{1+\varepsilon}$ the numbers $L_1(p/q), L_2(p/q), \dots, L_k(p/q)$ ($p/q \in \mathbb{Q}$) do not satisfy an algebraic relation of degree d with coefficients in $\mathbb{Q}$.

In another direction, G. V. Chudnovsky and others have constructed explicit P.A.'s to functions or systems of functions to obtain irrationality results. In particular Chudnovsky [C2] succeeded in finding a very wide class of explicit type I and II approximations of generalised hypergeometric functions. To quote a few results,

- 1) $\Gamma(\frac{1}{4})^4/\pi^2$ is irrational [C 2]
- 2) $L_2(\frac{1}{q}) \notin \mathbb{Q}$ for all $q \in \mathbb{Z}$, $q \geq 14$ [C 1, 2]
- 3) If $q > (ek)^{\frac{1}{2}} |p|^{k+1}$ then $1, L, (p/q), \dots, L_k(p/q)$ [C 2]
are $\mathbb{Q}$ -linear independent
- 4) $|\frac{\pi}{\sqrt{3}} - \frac{p}{q}| > \frac{1}{q^{8.31}}$ and $|\log 2 - \frac{p}{q}| > \frac{1}{q^{4.63}}$ [C 1]
for q sufficiently large
- 5) $|\pi - \frac{p}{q}| > \frac{1}{q^{19.89}}$ for q sufficiently large. [C 1]

Unfortunately, Chudnovsky's papers referred to are difficult to read if the reader does not fill in the detailed computations by himself. For a more detailed account of results 4) one may consult [A-R 1, 2] or [Ba 2] for a weaker version of this result. A proof of result 3) can be found in [N] although there is a mistake on the last page which yields an exponent 2 for $|p|$ instead of the correct $k+1$. For a weaker form of 5) see [M1]. Finally, the author [Be 3] proves irrationality of some classical constants by using a simple trick involving Legendre-polynomials.

$\zeta(3)$ Again

Despite the interest in P.A.'s that Apéry's discovery of $\zeta(3) \notin \mathbb{Q}$ has aroused, it is still not clear from which P.A.'s one might obtain irrationality of $\zeta(3)$. However, it becomes possible if we extend the idea of P.A. a little.

They by now traditional way to prove $\zeta(3) \notin \mathbb{Q}$ can be sketched as follows. Define

$$a_n = \sum_{k=0}^n \binom{n}{k}^2 \binom{n+k}{k}^2.$$

Then there exist numbers $b_n \in [1, \dots, n]^{-3} \mathbb{Z}$ such that

$$(2) \quad 0 < |a_n \zeta(3) - b_n| < 3(\sqrt{2}-1)^{4n}.$$

If $\zeta(3)$ were rational, say p/q , then $|a_n \zeta(3) - b_n| \geq q^{-1} [1, \dots, n]^{-3}$ contradicting the upper bound in (2) for n sufficiently large. For full details, see [R], [P] or [Be 2].

We will now show how the numbers a_n and b_n can be derived from Padé-type approximations. We look for polynomials $A_n(z)$, $B_n(z)$, $C_n(z)$, $D_n(z)$ of degree n such that

$$(3) \quad \begin{aligned} A_n(z) L_2(z) + B_n(z) L_1(z) + C_n(z) &= 0(z^{2n+1}) \\ 2A_n(z) L_3(z) + B_n(z) L_2(z) + D_n(z) &= 0(z^{2n+1}) \end{aligned}$$

and $B_n(1) = 0$. The four polynomials have $4(n+1)$ coefficients and the system (3) together with $B_n(1) = 0$ gives $2(2n+1)+1 = 4n+3$ linear conditions, so that A_n , B_n , C_n , D_n really exist. Write

$$A_n(z) = \sum_{r=0}^n \alpha_r z^r \quad \text{and} \quad B_n(z) = \sum_{r=0}^n \beta_r z^r.$$

Since degree $C_n, D_n \leq n$, the Taylor coefficient of z^m ($n+1 \leq m \leq 2n$) in $A_n L_2 + B_n L_1$, $2A_n L_3 + B_n L_2$ respectively must be zero, i.e.

$$(4) \quad \begin{aligned} \sum_{r=0}^n \frac{\alpha_r}{(m-r)^2} + \frac{\beta_r}{m-r} &= 0 \\ \sum_{r=0}^n \frac{2\alpha_r}{(m-r)^3} + \frac{\beta_r}{(m-r)^2} &= 0. \end{aligned} \quad m = n+1, \dots, 2n$$

Furthermore, $B_n(1) = 0$ implies $\sum \beta_r = 0$. This system of linear equations for α_r and β_r is easy to solve. Consider the rational function

$$R_n(t) = \sum_{r=0}^n \frac{\alpha_r}{(t-r)^2} + \frac{\beta_r}{t-r} = \frac{Q_n(t)}{t^2(t-1)^2 \dots (t-n)^2}.$$

The conditions (4) now imply that $R_n(t)$ and its derivative are zero for $t = n+1, n+2, \dots, 2n$. This implies that $Q_n(t)$ is a multiple of $(t-n-1)^2(t-n-2)^2 \dots (t-2n)^2$. If we put $Q_n(t)$ equal to this product, then degree $Q_n(t) = 2n$, whereas the denominator has degree $2n+2$. This automatically implies $\sum \beta_r = 0$. Therefore, the coefficients α_r, β_r can be obtained from the partial fraction expansion of

$$\frac{(t-n-1)^2 (t-n-2)^2 \dots (t-2n)^2}{t^2 (t-1)^2 \dots (t-n)^2}.$$

In particular, it is easy to see that

$$\alpha_r = \binom{n}{r}^2 \binom{2n-r}{n}^2.$$

Substitute $z=1$ in (3) and use $B_n(1)=0$. Then the second line yields

$$(5) \quad 2A_n(1) \zeta(3) + D_n(1) = \text{remainder}$$

where

$$A_n(1) = \sum_{r=0}^n \binom{n}{r}^2 \binom{2n-r}{n}^2 = \sum_{k=0}^n \binom{n}{k}^2 \binom{n+k}{k}^2 = a_n.$$

Thus we have recovered the number a_n from (3). It is now a matter of computation to show that approximation (5) is actually the same as (1).

--:--:--

REFERENCES

- [A-R 1] ALLADI K., ROBINSON M., On certain irrational values of the logarithm, Lecture Notes in Math. 751, 1-9.
- [A-R 2] ALLADI K., ROBINSON M., Legendre polynomials and irrationality, J. reine und angewandte Math. 318 (1980), 137-155.
- [A] APÉRY R., Irrationalité de $\zeta(2)$ et $\zeta(3)$, Journées arithmétiques de Luminy, Astérisque n° 61 (1979), 11-13.
- [Ba 1] BAKER A., Rational approximations to $\sqrt[3]{2}$ and other algebraic numbers, Quart. J. Math. 15 (1964), 376-383.
- [Ba 2] BAKER A., Approximations to the logarithm of certain rational numbers, Acta Arith. 10 (1964), 315-323.
- [Be 1] BEUKERS F., The generalised Ramanujan-Nagell equation, Thesis, University of Leiden (1979), also to appear in Acta Arith.
- [Be 2] BEUKERS F., A note on the irrationality of $\zeta(2)$ and $\zeta(3)$, Bull. London Math. Soc. 11 (1979), 268-272.

- [Be 3] BEUKERS F., Legendre polynomials in irrationality proofs, Bull. Australian Math. Soc. 22 (1980), 431-438.
- [Be 4] BEUKERS F., Fractional parts of powers of rationals, Math. Proc. Cambridge Phil. Soc. (1981).
- [C1] CHUDNOVSKY G.V., Acad. Sc. Paris, 288 (1979), 607-609, 965-967, 1001-1003.
- [C2] CHUDNOVSKY G.V., Padé-approximations to the generalised hypergeometric functions I, J. Math. pures et appl. 58 (1979), 445-476.
- [D] DOMAR Y., On the diophantine equation $|Ax^n - By^n| = 1$, $n \geq 5$, Math. Scand. 2 (1965), 29-32.
- [G] GALOČKIN A.I., Estimates form below of polynomials in the values of analytic functions of a certain class, Math. USSR Sbornik 24 (1974), 385-407.
- [G] GALOČKIN A.I., Lower bounds of linear forms in the values of certain G-functions (Russian), Math. Zametki 18 (1975), 541-552.
- [H] HERMITE C., Sur la fonction exponentielle, Oeuvres III, 150-181.
- [J] JAGER H., A multidimensional generalisation of the Padé table, Thesis, University of Amsterdam (1964).
- [Ma] MAHLER K., Application of some formulae by Hermite to the approximation of exponentials and logarithms, Math. Ann. 168 (1976), 200-227.
- [Mi] MIGNOTTE M., Approximations rationnelles du nombre π , Sém. Delange-Pisot-Poitou, 14e année 1972-73, n° 12.
- [N] NIKISIN E.M., On irrationality of the values of the function $F(x, s)$, Math. USSR Sbornik 37 (1980), 381-388.
- [P] POORTEN A. J. van der, A proof that Euler missed... Apéry's proof of the irrationality of $\zeta(3)$, Math. Intelligencer 1 (1978), 195-203.
- [R] REYSSAT E., Irrationalité de $\zeta(3)$ selon Apéry, Sém. Delange-Pisot-Poitou, 20e année, 1978-79, n° 6.
- [Si 1] SIEGEL C. L., Die Gleichung $ax^n - by^n = c$, Math. Ann. 114 (1937), 57-68.

- [Si 2] SIEGEL C. L. , Gesammelte Abh. I, 239-241.
- [Si 3] SIEGEL C. L. , Einige Erläuterungen zu Thues Untersuchungen über
Annäherungswerte algebraischer Zahlen und diophantische
Gleichungen, Nachrichten Akad. Wiss. Göttingen 8 (1970),
169-195.

(texte reçu le 9 mars 1981)

-:-:-:-

F. BEUKERS
Mathematisch Institut der
Rijksuniversiteit te Leiden
Wassenaarseweg 80 - Postbus 9512
2333 AL LEIDEN
(Pays Bas)

SUR LA DENSITÉ DIVISORIELLE D'UNE SUITE D'ENTRIERS

par

Gérald TENENBAUM

-:-:-:-

Nous reproduisons ici l'introduction et la bibliographie de l'article portant le même titre, à paraître au "Journal of Number Theory".

Introduction

Soit n un nombre entier et $\tau(n)$ le nombre de ses diviseurs ; pour toute suite d'entiers strictement croissante $\mathcal{Q}$, on désigne par $\tau(n, \mathcal{Q})$ le nombre des diviseurs de n qui appartiennent à $\mathcal{Q}$.

Dans [7], Hall introduit la définition suivante :

DÉFINITION 1 (Hall) . - On dit qu'une suite d'entiers $\mathcal{Q}$ possède une densité divisorielle z , et l'on note $D\mathcal{Q} = z$, s'il existe une suite d'entiers $\mathcal{P}$ de densité asymptotique 1 telle que l'on ait

$$\tau(n, \mathcal{Q}) \sim z \tau(n)$$

lorsque n tend vers l'infini en restant dans $\mathcal{P}$.

Contrairement à ce que laisserait supposer la relation asymptotique

$$\sum_{n < x} \tau(n, \mathcal{Q}) \sim x \sum_{\substack{d < x \\ d \in \mathcal{Q}}} \frac{1}{d},$$

qui a lieu dès que la série $\sum_{d \in \mathcal{Q}} \frac{1}{d}$ diverge, les notions de densités divisorielle et logarithmique sont assez dépendantes : Hall construit, pour tout couple (z, w) de $[0, 1]^2$ une suite $\mathcal{Q}$ satisfaisant à $D\mathcal{Q} = z$ et $\delta\mathcal{Q} = w$ (ici et dans la suite, δ désigne la densité logarithmique). Il prouve cependant le résultat suivant, conjecturé par Erdős, qui établit l'existence d'un lien entre les deux densités pour une suite constituée par des blocs suffisamment longs d'entiers consécutifs.

THÉORÈME A (Hall [7]). - Soit $\{b_j\}$ une suite de nombres réels satisfaisant à $b_{j+1} \geq c b_j$ pour tout j , avec $c > 1$, et soit $\mathcal{Q}$ la suite d'entiers définie par

$$\mathcal{Q} = \{d : \exists j : b_{2j} \leq d < b_{2j+1}\}.$$

Alors, si $\delta\mathcal{Q} = z$, on a aussi $D\mathcal{Q} = z$.

La notion de densité divisorielle est également liée à celle d'équirépartition modulo 1 sur les diviseurs.

DÉFINITION 2 (Hall [6]). - Pour toute fonction arithmétique réelle f , on pose

$$\Delta(n; f) := \sup_{0 \leq u < v \leq 1} \left| \frac{1}{\tau(n)} \text{card} \{d : d|n, f(d) \in [u, v[\pmod{1}\} - (v-u) \right|.$$

On dit que f est équirépartie (mod 1) sur les diviseurs s'il existe une suite d'entiers $\mathcal{J}$ de densité asymptotique 1 telle que l'on ait :

$$(1) \quad \lim_{\substack{n \rightarrow \infty \\ n \in \mathcal{J}}} \Delta(n; f) = 0.$$

Considérons, pour z dans $[0, 1]$, la suite

$$\mathcal{Q}(z; f) := \{d : f(d) < z \pmod{1}\}.$$

Il est clair que (1) implique

$$(2) \quad D\mathcal{Q}(z; f) = z;$$

réciroquement, si (2) a lieu pour tout z de $[0, 1]$ alors f est équirépartie (mod 1) sur les diviseurs (Hall [8]).

La méthode naturelle pour établir des résultats du type (1) consiste à majorer les sommes de Weyl

$$\sigma_v(n, f) := \sum_{d|n} e(v f(d)),$$

où $v \in \mathbb{Z} \setminus \{0\}$ et où $e(x) := e^{2i\pi x}$, et à appliquer l'inégalité d'Erdős-Turán.

Lorsque f est additive, les sommes de Weyl sont multiplicatives et cela représente un atout précieux dans la conduite des calculs. La fonction $f(d) = \log d$ a été étudiée dans [2], [4] et [5] ; elle est équirépartie et l'on a pour tout $\lambda < \frac{\log \pi}{\log 2} - 1 = 0,651\dots$ et presque tout entier n

$$\Delta(n; \log) \leq \tau(n)^{-\lambda}.$$

Le cas des fonctions f non additives est plus délicat. On peut utiliser le théorème A pour montrer par exemple que $(\log d)^\alpha$ et $(\log \log d)^\beta$ sont équiréparties respectivement pour $0 < \alpha < 1$ et $\beta > 1$ (cf. [7]). La restriction concernant β est nécessaire mais Hall a conjecturé qu'il suffit de supposer $\alpha > 0$ (cf. [6]). Dans [8], il a montré que l'on peut prendre $0 < \alpha < 1 + \log 2$.

Nous avons cherché une condition nécessaire et suffisante simple pour $DQ = z$ s'exprimant sous forme de propriétés de moyennes. Bien entendu, le critère obtenu permet également de prouver des résultats d'équirépartition.

THÉORÈME 1. - Soit Q une suite d'entiers de fonction caractéristique χ . Alors $DQ = z$ si, et seulement si, on a pour x infini

$$(3) \quad \sum_{k < x} \left| \sum_{\substack{n < x \\ n \equiv 0 \pmod{k}}} \frac{\chi(n) - z}{4^{\Omega(n)} n} \right| = o(\sqrt{\log x})$$

où $\Omega(n)$ désigne le nombre des facteurs premiers d'un entier n , comptés avec leur ordre de multiplicité.

Remarques. - (i) Ce résultat permet de vérifier directement certaines propriétés connues, comme le fait que les progressions arithmétiques distinctes de $\mathbb{N}$ ou la suite des entiers sans facteur carré ne possèdent pas de densité divisorielle ou encore que, si $\psi(n) \rightarrow \infty$, la suite des entiers n satisfaisant à

$$(4) \quad \left| \Omega(n) - \frac{1}{2} \log \log n \right| \leq \psi(n) \sqrt{\log \log n}$$

est de densité divisorielle unité (cf. [3], [7]). Pour ce dernier point il suffit de constater que $DQ = 1$ si et seulement si

$$\sum_{n < x} \frac{\chi(n) \tau(n)}{4^{\Omega(n)} n} \sim \sum_{n < x} \frac{\tau(n)}{4^{\Omega(n)} n}$$

et la conclusion découle du fait classique que la somme de droite est dominée par les entiers n satisfaisant à (4).

(ii) On peut aussi donner une nouvelle démonstration du theorem 2 de [8].

Soit f une fonction multiplicative satisfaisant à

(a) $f(p) = 1 + O(p^{-\sigma})$, où σ est un réel positif fixé, uniformément pour tout nombre premier p ,

(b) $0 \leq f(p)^\nu \leq \theta_1 \theta_2^\nu$, où θ_1 et θ_2 sont deux réels positifs, $\theta_2 < 2$, uniformément pour tout nombre premier p et tout entier non négatif ν .

Alors la condition (3) implique

$$\sum_{n < x} \frac{f(n) \chi(n)}{n \tau(n)} = (z + o(1)) \sum_{n < x} \frac{f(n)}{n \tau(n)}.$$

En effet, si l'on définit une fonction multiplicative g par l'identité

$$\sum_{d|n} g(d) = \frac{f(n) 4^{\Omega(n)}}{\tau(n)}.$$

on constate facilement que g satisfait (a) et que, pour tout nombre premier p et tout entier non négatif ν , on a

$$g(p)^\nu \leq \theta_1 (4\theta_2)^\nu.$$

De plus,

$$\begin{aligned} S(x) &:= \sum_{n < x} \frac{(\chi(n) - z) f(n)}{n \tau(n)} = \sum_{n < x} \frac{\chi(n) - z}{4^{\Omega(n)}_n} \sum_{k|n} g(k) \\ &= \sum_{k < x} g(k) \sum_{\substack{n < x \\ n \equiv 0 \pmod{k}}} \frac{\chi(n) - z}{4^{\Omega(n)}_n} = \sum_{k < x} g(k) A_k(x), \quad \text{disons.} \end{aligned}$$

Maintenant, si r est un réel > 1 tel que $(4\theta_2)^r < 8$ et si $s = \frac{r}{r-1}$, l'inégalité de Hölder implique

$$|S(x)| \leq \left\{ \sum_{k < x} |g(k)|^r |A_k(x)| \right\}^{1/r} \left\{ \sum_{k < x} |A_k(x)| \right\}^{1/s};$$

l'inégalité (3) implique que le second facteur est $o((\log x)^{1/2s})$ et l'estimation triviale $|A_k(x)| \ll ((\log x)^{1/4} / 4^{\Omega(k)}_k)$, valable uniformément pour $k < x$, permet de majorer le second par

$$(\log x)^{1/4r} \left\{ \sum_{k < x} \frac{|g(k)|^r}{4^{\Omega(k)}_k} \right\}^{1/r} \ll (\log x)^{1/4r} \left\{ \prod_{p < x} \sum_{\nu=0}^{\infty} \frac{|g(p)^\nu|^r}{(4p)^\nu} \right\}^{1/r} \ll (\log x)^{1/2r}$$

d'où la conclusion souhaitée.

L'emploi du théorème 1 permet de généraliser le théorème A de la manière suivante :

THÉORÈME 2. - Soit $\{b_j\}$ une suite croissante de nombres réels satisfaisant pour x infini à

$$(5) \quad \text{card} \{j : b_j < x\} \ll (\log x)^\alpha ;$$

où α est une constante positive, et soit $\mathcal{Q}$ la suite d'entiers définie par

$$\mathcal{Q} = \{d : \exists j : b_{2j} \leq d < b_{2j+1}\} .$$

Alors, si $\delta \mathcal{Q} = z$, on a aussi $D\mathcal{Q} = z$.

COROLLAIRE 1. - Soit f une fonction dérivable réelle, définie sur $\mathbb{R}^+$. Si $f'(x) \rightarrow 0$ et si la suite $\{f(n) : n = 1, 2, \dots\}$ est équirépartie (mod 1), alors la fonction $f((\log d)^\alpha)$ est, pour tout réel positif α , équirépartie (mod 1) sur les diviseurs.

COROLLAIRE 2. - Soit g une fonction dérivable réelle, définie sur $\mathbb{R}^+$. Si $|x g'(x) \log x| \rightarrow +\infty$ et s'il existe un réel $\alpha > -1$ tel que la fonction $x g'(x) (\log x)^{-\alpha}$ soit monotone et tende vers 0 à l'infini, alors g est équirépartie (mod 1) sur les diviseurs.

L'un ou l'autre de ces corollaires implique l'équirépartition de $(\log d)^\alpha$ pour tout $\alpha > 0$.

Le théorème suivant donne un critère d'équirépartition (mod 1) sur les diviseurs qui est l'analogue du critère de Weyl dans le cadre de l'équirépartition classique.

THÉORÈME 3. - Une condition nécessaire et suffisante pour que f soit équirépartie (mod 1) sur les diviseurs est que l'on ait, pour tout entier non nul ν et x infini,

$$(6) \quad \sum_{k < x} \left| \sum_{\substack{n < x \\ n \equiv 0 \pmod{k}}} \frac{e(\nu f(n))}{4^{\Omega(n)} n} \right| = o(\sqrt{\log x}) .$$

Je tiens à remercier ici Richard R. Hall qui m'a éclairé, au cours de nombreuses et amicales discussions, sur les notions nouvelles qui sont à la base de ce travail.

BIBLIOGRAPHIE

- [1] H. DELANGE, Sur des formules de Atle Selberg, Acta Arithm. 19 (1971), 105-146.
- [2] P. ERDÖS and R.R. HALL, Some distribution problems concerning the divisors of integers, Acta Arithm. 26 (1974), 175-188.
- [3] P. ERDÖS et G. TENENBAUM, Sur la structure de la suite des diviseurs d'un entier, Ann. Inst. Fourier, 31, 1 (1981), 17-37.
- [4] R.R. HALL, The divisors of integers I, Acta Arithm. 26 (1974), 41-46.
- [5] R.R. HALL, Sums of imaginary powers of the divisors of integers, J. London Math. Soc. (2), 9 (1975), 571-580.
- [6] R.R. HALL, The distribution of $f(d) \pmod{1}$, Acta Arithm. 31 (1976), 91-97.
- [7] R.R. HALL, A new definition of the density of an integer sequence, J. Austral. Math. Soc. (series A) 26 (1978), 487-500.
- [8] R.R. HALL, The divisor density of integer sequences, J. London Math. Soc., à paraître.
- [9] G. RAUZY, Propriétés statistiques de suites arithmétiques, P.U.F., Collection SUP, (1976).
- [10] A. SELBERG, Note on a paper by L. G. Sathe, J. Indian Math. Soc. (N.S.) 18 (1954), 83-87.
- [11] D. V. WIDDER, The Laplace Transform, Princeton University Press (1946).

(texte reçu le 11 mai 1981)

---:---

Gérald TENENBAUM
 U. E. R. de Mathématiques
 et d'Informatique
 Université de Bordeaux I
 F 33405 TALENCE CEDEX

REPRÉSENTATIONS DES CORPS DE NOMBRES
ET THÉORIE DE BAKER

par

Daniel BERTRAND

-:-:-:-

§ 1. - Introduction

Le présent exposé reprend, en la précisant, une méthode élaborée en collaboration avec D. Masser (voir [3]) pour l'étude des combinaisons linéaires à coefficients dans $\overline{\mathbb{Q}}$ de certains nombres transcendants (on a désigné par $\overline{\mathbb{Q}}$ la clôture algébrique de $\mathbb{Q}$ dans $\mathbb{C}$). Cette méthode repose sur le critère de transcendance suivant, dont on trouvera une discussion dans [4], chap. 5 et 7.

THÉORÈME 1 (Schneider-Lang). - On désigne par K un corps de nombres, par n et ℓ deux entiers ≥ 1 , par $f_1, \dots, f_\ell$ des fonctions méromorphes sur $\mathbb{C}^n$, d'ordre fini, et par Γ un sous-groupe de $\mathbb{C}^n$ engendrant $\mathbb{C}^n$ sur $\mathbb{C}$. On suppose que l'algèbre $K[f_1, \dots, f_\ell]$ est stable sous les dérivations $\partial/\partial z_1, \dots, \partial/\partial z_n$, et que son degré de transcendance sur K est $\geq n+1$. Alors, les fonctions $f_1, \dots, f_\ell$ ne peuvent prendre simultanément des valeurs dans K en tous les points de Γ .

Comme il est bien connu, cet énoncé, appliqué au cas $n=1$, contient les théorèmes de Hermite-Lindemann et de Gel'fond-Schneider sur les valeurs de la fonction exponentielle. La méthode évoquée plus haut permet, pour des choix convenables de n , d'en déduire une nouvelle démonstration des résultats qualitatifs de la théorie de Baker sur les formes linéaires de logarithmes (voir [1], chap. 2). En voici, dans le cas $n=2$, une illustration, tirée de l'exposé de D. Masser au Colloque de Durham de 1979, et qui concerne le problème de Siegel sur la transcendance du nombre

$$I = \int_0^1 \frac{dt}{1+t^3} = \frac{1}{3\sqrt{-3}} (\sqrt{-3} \operatorname{Log} 2 + i\pi) .$$

Considérons le corps $K = \mathbb{Q}(\sqrt{-3}, I)$, et soit Γ le sous-groupe de $\mathbb{C}^2$ engendré par les vecteurs $(i\pi, \operatorname{Log} 2)$ et $(-3 \operatorname{Log} 2, i\pi)$. Leur déterminant $3(\operatorname{Log} 2)^2 - \pi^2$ étant non nul, Γ engendre $\mathbb{C}^2$ sur $\mathbb{C}$. Or les fonctions $\exp(z_1)$, $\exp(z_2)$, $z_1 + \sqrt{-3} z_2$ vérifient les hypothèses du théorème 1, et prennent sur Γ des valeurs dans K . Donc K ne peut être un corps de nombres.

On reconnaît dans Γ l'orbite du point $(i\pi, \operatorname{Log} 2)$ sous l'action de $\mathbb{Z}[\sqrt{-3}]$ induite par la représentation régulière du corps quadratique $F = \mathbb{Q}(\sqrt{-3})$ sur $\mathbb{C}^2$. C'est cet aspect de la méthode que nous allons préciser.

§.2. - Endomorphismes de groupes algébriques

Le théorème de Schneider-Lang est bien adapté à l'étude des sous-groupes analytiques de groupes algébriques commutatifs, définis sur $\bar{\mathbb{Q}}$ (voir [4], chap. 3, 5, 6). Soient G un tel groupe algébrique, TG l'espace tangent à l'origine de G , et $e_G : TG(\mathbb{C}) \longrightarrow G(\mathbb{C})$ l'application exponentielle sur le

groupe des points complexes de G . Notons $\mathcal{M}_G$ l'ensemble des éléments de $TG(\mathbb{C})$ dont l'image par e_G appartient à $G(\overline{\mathbb{Q}})$, et soit W un sous-espace de TG , défini sur $\overline{\mathbb{Q}}$. Le théorème 1 admet dans ces conditions le corollaire suivant (voir [4]) : si $W(\mathbb{C})$ est engendré sur $\mathbb{C}$ par des éléments de $\mathcal{M}_G$, l'image de $W(\mathbb{C})$ par e_G est un sous-groupe algébrique de $G(\mathbb{C})$. En effet, le théorème 5.2.1. de [4] entraîne alors que la clôture de Zariski G_1 de $e_G(W(\mathbb{C}))$ dans $G(\mathbb{C})$ a une dimension $\leq \dim W$. Comme la différentielle de e_G à l'origine est l'identité, $\dim G_1$ est donc égale à $\dim W$, l'espace tangent TG_1 coïncide avec W , et il en est de même de $G_1(\mathbb{C})$ et de $e_G(W(\mathbb{C}))$.

Cet énoncé peut être amélioré sous certaines hypothèses sur l'anneau d'endomorphismes $\text{End } G$ de G . On fixe pour la suite un corps de nombres F . On dira qu'une représentation linéaire de l'algèbre semi-simple F n'a pas de multiplicité si sa décomposition en représentations irréductibles ne contient pas la représentation nulle, et ne fait pas apparaître deux fois le même plongement de F dans $\overline{\mathbb{Q}}$.

On suppose désormais que le groupe algébrique G est de type (F) , c'est-à-dire qu'il existe un homomorphisme injectif j de F dans $\text{End}_0 G = \overline{\mathbb{Q}} \otimes \text{End } G$. La composition de j par l'injection canonique de $\text{End}_0 G$ dans $\text{End}(TG)$ fournit une représentation χ de F sur TG . Soit alors W un sous-espace de TG défini sur $\overline{\mathbb{Q}}$ et stable sous l'action de $\chi(F)$, de sorte que χ induit une représentation χ_W de F sur W . Dans ces conditions, on peut énoncer :

THÉORÈME 2. - Soit D un élément de $\mathcal{M}_G \cap W(\mathbb{C})$. Si χ_W n'a pas de multiplicité, D appartient à un sous-espace $W'(\mathbb{C})$ de $W(\mathbb{C})$, défini sur $\overline{\mathbb{Q}}$, dont l'image par e_G est un sous-groupe algébrique de G , de type (F) .

Démonstration. - Soit Γ l'orbite de D sous l'action de $\chi(F \cap j^{-1}(\text{End } G))$. Le sous-espace W' de W engendré sur $\mathbb{C}$ par Γ répond à la question. En effet, d'après l'hypothèse faite sur χ_W , W' est défini par l'annulation de formes linéaires à coefficients dans la clôture galoisienne de F , qui sont propres pour l'action de ${}^t\chi(F)$ (écrire D dans une base de W diagonalisant l'action de F). Donc W' est défini sur $\overline{\mathbb{Q}}$, et est de plus stable sous l'action de $\chi(F)$. En particulier, $e_G(W'(\mathbb{C}))$ a pour clôture de Zariski dans $G(\mathbb{C})$ un groupe algébrique

de type (F). Par ailleurs, la relation $e_G(d(\alpha)D) = \alpha(e_G(D))$, valable pour tout élément α de $\text{End } G$, montre que Γ est contenu dans $\mathcal{M}_G$. Le corollaire au théorème 1 cité plus haut permet de conclure.

Le théorème 2 ramène un problème de transcendance à l'étude des sous-groupes algébriques de type (F) de G . Lorsque le groupe algébrique G est (F)-irréductible, c'est-à-dire qu'il ne contient pas de sous-groupes algébriques propres de type (F), il admet en particulier le corollaire suivant : si W est distinct de TG , l'intersection de $W(\mathbb{C})$ avec $\mathcal{M}_G$ est réduite à $\{0\}$; par exemple, si χ elle-même n'a pas de multiplicité, tout élément non nul de $\mathcal{M}_G$ engendre le $\chi(F) \otimes \mathbb{C}$ -module $TG(\mathbb{C})$.

§.3. - Applications

Des choix convenables du groupe algébrique G permettent de déduire du théorème 2 les énoncés de transcendance de la théorie de Baker et de les généraliser. Soit ainsi G la puissance n -ième du groupe multiplicatif $\mathbb{G}_m$ (resp. d'une courbe elliptique E , définie sur $\overline{\mathbb{Q}}$). Pour toute extension F de $\mathbb{Q}$ (resp. du corps $k = \mathbb{Q} \otimes \text{End } E$) de degré n , le groupe algébrique G est de type (F), et est même (F)-irréductible (dans le cas d'une courbe elliptique à multiplications complexes, cela se voit par exemple en notant qu'un corps de nombres de degré $2n$ ne peut agir sur une variété abélienne de dimension $< n$). Soit $\{\alpha_1, \dots, \alpha_n\}$ la base duale de la base de F sur $\mathbb{Q}$ (resp. sur k) associée à une représentation de F sur TG . On déduit du corollaire au théorème 2 que pour tout n -uplet $\{\ell_1, \dots, \ell_n\}$ de logarithmes non tous nuls de nombres algébriques (resp. de valeurs non toutes nulles d'intégrales elliptiques de 1ère espèce prises entre des points de $E(\overline{\mathbb{Q}})$), le nombre $\alpha_1 \ell_1 + \dots + \alpha_n \ell_n$ est non nul. L'indépendance linéaire sur $\overline{\mathbb{Q}}$ de logarithmes de nombres algébriques, linéairement indépendants sur $\mathbb{Q}$, en découle (pour le cas elliptique, voir D. Bertrand et D. Masser, Invent. Math., 58 (1980), pp. 283-288).

Voici pour conclure une liste d'applications du théorème 2 à d'autres groupes algébriques G :

- produit de $\mathbb{G}_m^n$ par le groupe additif $\mathbb{G}_a$: on obtient le théorème de Baker ([1], Th. 2.1) sur la transcendance de combinaisons linéaires à coefficients dans $\overline{\mathbb{Q}}$ de logarithmes de nombres algébriques ;
- extension d'une variété abélienne à multiplications réelles par $\mathbb{G}_a$: on en déduit la transcendance de combinaisons linéaires à coefficients dans $\overline{\mathbb{Q}}$ d'intégrales abéliennes de 1ère ou de 2ème espèce (voir [3], th. 2, et, dans un cadre plus général, D. Bertrand, Séminaire Delange-Pisot-Poitou, 1979-80) ;
- carré d'une extension par $\mathbb{G}_a$ d'une variété abélienne de type CM : on obtient la transcendance de combinaisons linéaires à coefficients dans $\overline{\mathbb{Q}}$ d'intégrales abéliennes de 1ère et de 2ème espèce (voir M. Laurent, C.R.A.S. 290 (1980), pp. 397-399 pour le cas elliptique, et [3], th. 3, dans le cas général) ;
- carré d'une variété abélienne de type C.M. , moyennant certaines hypothèses sur le groupe des automorphismes du corps de multiplications complexes : ce cas a été étudié par M. Laurent, qui en déduit de nouveaux résultats de transcendance sur les quotients de valeurs de la fonction B d'Euler ;
- produit de deux courbes elliptiques à multiplications complexes par des corps $\mathbb{Q}(\sqrt{-d})$, $\mathbb{Q}(\sqrt{-d'})$ distincts : si u_1, u_2 (resp. u'_1, u'_2) désignent des "points algébriques" des fonctions elliptiques de Weierstrass correspondantes, non tous deux nuls, on obtient la transcendance du nombre complexe $(u_1 + \sqrt{-d'} u_2) / (u'_1 + \sqrt{-d} u'_2)$ (on fait ici agir $\mathbb{Q}(\sqrt{-d}, \sqrt{-d'})$ sur G^2) ;
- extension d'une courbe elliptique à multiplications complexes par $\mathbb{G}_m^2$: ce cas fournit la transcendance de certains nombres liés aux fonctions sigma de Weierstrass (voir D. Bertrand et M. Laurent, C.R.A.S., 1981, à paraître).

Nous renvoyons à [2] pour un exposé plus complet de ce type de résultats. Signalons enfin un problème ouvert : démontrer par la méthode précédente les énoncés quantitatifs de la théorie de Baker (voir [1], chap. 3), et les généraliser aux autres situations considérées ici.

RÉFÉRENCES

- [1] A. BAKER, Transcendental Number Theory, Cambridge U. P., 1975.
- [2] D. BERTRAND, Endomorphismes de groupes algébriques ; applications arithmétiques, en préparation.
- [3] D. BERTRAND et D. MASSER, Formes linéaires d'intégrales abéliennes, C.R.A.S. Paris, 290 (1980), 725-727.
- [4] M. WALDSCHMIDT, Nombres transcendants et groupes algébriques, Astérisque n° 69-70, 1979.

(texte reçu le 20 mai 1981)

-:-:-:-

Daniel BERTRAND
Université de Nice,
Mathématiques
Parc Valrose
F 06034 NICE CEDEX

K-THÉORIE ET CORPS CYCLOTOMIQUES

par

Christophe SOULÉ

-:-:-:-

Soit A un anneau unitaire. D. Quillen [7], [9], a associé à A une suite de groupes abéliens $K_n A$, $n \geq 0$. Dans cet exposé on montre comment, si A est l'anneau des entiers d'un corps de nombres F , les groupes $K_n A$ sont reliés à l'arithmétique des extensions cyclotomiques de F .

1. - Preliminaires

1.1. - La K-théorie de Quillen

Le groupe $K_0(A)$ a été introduit par A. Grothendieck [4]. Pour $n \geq 1$, Quillen considère le groupe $GL_m(A)$ des matrices $m \times m$ à coefficients dans A inversibles. On plonge $GL_m(A)$ dans $GL_{m+1}(A)$ par

$$g \longmapsto \begin{pmatrix} g & 0 \\ 0 & 1 \end{pmatrix},$$

et l'on note $GL(A)$ le groupe de matrices infinies $GL(A) = \varinjlim_m GL_m(A)$.

Une définition de $K_n(A)$ est alors la suivante :

$$K_n(A) = \pi_n(BGL^+(A)),$$

où $BGL^+(A)$ est un espace topologique obtenu en attachant deux cellules (en dimension deux et trois) à l'espace classifiant du groupe $GL(A)$, de façon à obtenir un H-espace dont l'homologie est la même que celle de $GL(A)$ (pour la définition exacte, voir [7]).

On ne sait pas calculer $K_n(A)$ en général. Si A est l'anneau des entiers dans un corps de nombres F , ce que nous supposons désormais, $K_n(A)$ est de type fini et A. Borel [1] a calculé son rang. De plus, $K_1(A) = A^*$ et $K_0(A) = \mathbb{Z} \oplus Cl(A)$, où $Cl(A)$ est le groupe des classes d'idéaux de A [8].

1.2. - Module d'Iwasawa

Soit p un nombre premier impair. On pose :

$$F_n = F(\sqrt[p]{1}) \text{ (dans une clôture algébrique fixée de } F),$$

$$A_n = \text{éléments de } F_n \text{ entiers en dehors de } p,$$

$$F_\infty = \bigcup_n F_n,$$

$$G_\infty = \text{Gal}(F_\infty/F),$$

$$M_\infty = \text{plus grande } p\text{-extension abélienne de } F_\infty \text{ non ramifiée en dehors de } p,$$

$$X = \text{Gal}(M_\infty/F_\infty),$$

$$\mathbb{Z}_p = \text{entiers } p\text{-adiques},$$

$$\mathbb{Z}_p(1) = \varprojlim_n \mu_{p^n}, \text{ le module de Tate.}$$

Si M est un G_∞ -module on pose :

$$M(i) = X \otimes \mathbb{Z}_p(1)^{\otimes i}$$

$$M_{G_\infty} = \text{groupe des coinvariants de } M \text{ sous } G_\infty.$$

Si Ω est un $\mathbb{Z}_p$ -module de type fini, on note :

$t\Omega$ le dual de Pontryagin de sa partie de torsion,

$\# \Omega$ l'ordre de $t\Omega$,

et $t\Omega = \text{Hom}(\Omega, \mathbb{Z}_p)$.

2. - Conjecture principale et K-théorie

2.1. - THÉORÈME 1. ([10], [3]) - Pour tout entier $i \geq 2$, il existe des morphismes

$$\text{ch}_{i,1} : K_{2i-1}(A) \otimes \mathbb{Z}_p \longrightarrow \mathbb{Z}_p^{(i)}_{G_\infty} \oplus t X(i)_{G_\infty}$$

$$\text{ch}_{i,2} : K_{2i-2}(A) \otimes \mathbb{Z}_p \longrightarrow t X(i)_{G_\infty}$$

dont le noyau et le conoyau sont finis. De plus $\text{ch}_{i,2}$ est surjectif, et l'image de $\text{ch}_{i,1}$ contient $\mathbb{Z}_p^{(i)}_{G_\infty}$.

On pense que $\text{ch}_{i,1}$ et $\text{ch}_{i,2}$ sont des isomorphismes. Ceci a été prouvé par Tate pour $\text{ch}_{2,2}$.

2.2. - Notons $\zeta_F(s)$, $s \in \mathbb{C}$, la fonction zêta de F . Si F est totalement réel et i pair, Siegel a montré que $\zeta_F(1-i)$ est un nombre rationnel.

La conjecture principale des corps cyclotomiques implique que la partie p-primaire de $\zeta_F(1-i)$ est

$$|\zeta_F(1-i)|_p = \frac{\# X(i)_{G_\infty}}{\# \mathbb{Z}_p^{(i)}_{G_\infty}}.$$

Cette conjecture est démontrée si $F \subset \mathbb{Q}(\sqrt[p]{1})$ (Mazur et Wiles, à paraître). On obtient ainsi des éléments non triviaux dans la K-théorie de A .

Exemple. - Si $F = \mathbb{Q}$, on a $\zeta_F(1-i) = b_i/2i$, où les nombres de Bernoulli b_i sont définis par la formule

$$x/e^x - 1 = \sum_i b_i x^i/i!.$$

2.3. - Si $F/\mathbb{Q}$ n'est pas abélien, le théorème 1 fournit, à l'inverse, quelques informations nouvelles sur le module X . Ainsi, quand F est totalement réel et i pair, le groupe $X(i)_{G_\infty}$ est fini, et nul pour presque tout p .

3. - Régulateurs p-adiques

Soit E la limite projective pour les applications normes des groupes d'unités A_n^* . Le théorème 1, joint aux résultats de Borel [1] et Iwasawa [5], montre que si $i \geq 2$ on a :

$$K_{2i-1}(A) \otimes \mathbb{Q}_p \simeq E(i-1)_{G_\infty} \otimes \mathbb{Q}_p.$$

En particulier, si F est abélien sur $\mathbb{Q}$, les tours d'unités cyclotomiques fournissent des éléments explicites de $K_{2i-1}(A) \otimes \mathbb{Q}_p$.

Soit $\hat{A}_p$ le produit des complétés de A aux places divisant p . Si ω désigne le caractère de $\text{Gal}(F(\mu_p):F)$ obtenu par action sur les racines p -ièmes de l'unité, et Φ l'ensemble des caractères de $F/\mathbb{Q}$, on désigne par

$$L_p(F, \omega^{1-i}, s) := \prod_{\chi \in \Phi} L_p(\chi \omega^{1-i}, s), \quad s \in \mathbb{Z}_p,$$

la fonction L p-adique du caractère ω^{1-i} , $i \in \mathbb{N}$, [6].

THÉORÈME 2. ([11]) - Soit $F/\mathbb{Q}$ abélien et totalement réel. Si i est impair, $i \geq 3$, et si le nombre $L_p(F, \omega^{1-i}, i)$ est non nul, alors le morphisme

$$K_{2i-1}(A) \otimes \mathbb{Q}_p \longrightarrow K_{2i-1}(\hat{A}_p) \otimes \mathbb{Q}_p$$

est injectif.

Si $i=1$ le résultat analogue classique est la formule de Leopoldt pour le résidu en $s=1$. La non nullité de ce résidu montre que les unités globales (i. e. $K_1(A)$) ont une image de rang maximum dans les unités locales.

4. - Théorèmes de Stickelberger

Soient $\zeta = e^{2\pi i/f}$, $A = \mathbb{Z}[\zeta]$ et $G = \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. Si $a \wedge f = 1$ on pose $\sigma_a \zeta = \zeta^a$, $\sigma_a \in G$. Pour tout entier i on définit

$$w_i = \begin{cases} 2 & \text{si } i \text{ est impair} \\ \text{dén. } b_i/2i & \text{si } i \text{ est pair.} \end{cases}$$

Enfin, on note $B_i(x)$ le i -ème polynôme de Bernoulli ($B_i(0) = b_i$).

Si b est un entier premier à f on définit :

$$\theta_{b,i} = w_i(b^i - \sigma_b) \sum_{\substack{a \wedge f = 1 \\ 0 < a < f}} \frac{f^{i-1}}{i} B_i\left(\frac{a}{f}\right) \sigma_a^{-1}$$

dans l'algèbre de groupe $\mathbb{Q}[G]$.

Un théorème classique de Stickelberger affirme que $\theta_{b,1} \cdot \text{Cl}(A) = 0$.

Coates et Sinnott [2] ont montré que $\theta_{b,i} \in \mathbb{Z}[G]$ et que $\theta_{b,i} \cdot X(i)_{G_\infty} = 0$ quand p ne divise pas b . Ils conjecturent que $\theta_{b,i} \cdot K_{2i-2}(A) = 0$.

Récemment, j'ai pu montré l'analogie de cette conjecture où l'on remplace A par une courbe sur un corps fini [12]. Les outils essentiels sont la structure de λ -anneau sur $\bigoplus_n K_n(A)$ et la preuve par Tate et Deligne de la conjecture de Stark pour les corps de fonctions.

-:-:-:-

BIBLIOGRAPHIE

- [1] A. BOREL, Stable real cohomology of arithmetic groups, Ann. Scient. Ec. Norm. Sup. 4e série, 7 (1974), 235-272.
- [2] J. COATES, W. SINNOTT, An analogue of Stickelberger's Theorem for the higher K-groups, Inventiones math. 24, 149-161 (1974).
- [3] W. DWYER, E. FRIEDLANDER, Etale K-theory and Arithmetic, à paraître.
- [4] A. GROTHENDIECK, SGA VI, Théorème de Riemann-Roch.

15-06

- [5] K. IWASAWA, On $\mathbb{Z}_\ell$ -extensions of algebraic number fields, Ann. of Math. 98 (1973), 246-326.
- [6] K. IWASAWA, Lectures on p-adic L-functions, Annals of Math. Studies, n° 74.
- [7] J.-L. LODAY, K-théorie et représentations de groupes, Ann. Scient. Ec. Norm. Sup., 4e série, 9 (1976), 309-377.
- [8] J. MILNOR, Introduction to Algebraic K-theory, Annals of Math. Studies, n° 72.
- [9] D. QUILLEN, Algebraic K-theory I, Springer Lecture Notes in Math. n° 341 (1973), 85.
- [10] Ch. SOULÉ, K-théorie des anneaux d'entiers de corps de nombres et cohomologie étale, Inv. Math. 55 (1979), 251-295.
- [11] Ch. SOULÉ, On higher p-adic regulators, dans les Comptes Rendus de la conférence d'Evanston 1980, à paraître aux Springer Lecture Notes.
- [12] Ch. SOULÉ, K-théorie et correspondances algébriques, Note aux Comptes Rendus Acad. Sc. 16.2.1981.

(texte reçu le 6 mars 1981)

-:-:-:-

Christophe SOULÉ
Université de Paris VII
U.E.R. d'Algèbre et Géométrie
Tour 45-55, 5e ét.
2, place Jussieu
F 75221 PARIS CEDEX 05

ACCÉLÉRATION DE LA CONVERGENCE
DE CERTAINES RÉCURRENCES LINÉAIRES

par

Henri COHEN

-:-:-:-

Le but de mon exposé était de généraliser la "méthode d'Apéry" exposée très en détail dans [1] à des récurrences d'ordre supérieur à 2, et de montrer quels résultats arithmétiques on peut en déduire. Exemple typique :

THEOREME. - Il existe $C > 0$ telle que pour tout $a, b, c \in \mathbb{Z}$ avec
 $(a, b) \neq (0, 0)$ on ait :

$$|a \operatorname{Log}^2 2 + b \operatorname{Log} 2 + c| \geq \frac{C}{H^{286,819}}$$

où $H = \sup(|a|, |b|)$.

La méthode et quelques applications sont données en détail dans [2].

Depuis mon exposé, j'ai obtenu d'autres résultats en collaboration avec G. Rhin. Par exemple nous savons maintenant faire marcher la méthode d'Apéry pour $\zeta(4)$. La récurrence diagonale obtenue est la suivante :

$$u_{n+1} = 3(45n^4 + 90n^3 + 72n^2 + 27n + 4) u_n + \frac{3n^8(9n^2 - 1)}{4n^2 - 1} u_{n-1}.$$

La convergence est exponentielle et $u_n/(n!)^4$ possède de bonnes propriétés arithmétiques, mais malheureusement pas tout à fait assez bonnes pour conclure à l'irrationalité de $\zeta(4)$ (qui bien sûr est déjà connue, mais là n'est pas la question).

Nous savons également faire marcher la méthode pour obtenir des approximations simultanées à $\zeta(2)$ et $\zeta(3)$ en utilisant la formule habituelle pour $\zeta(2)$

et la formule
$$\zeta(3) = \sum_{r=1}^{\infty} \frac{1}{r^2} \sum_{k=1}^{r-1} \frac{1}{k}.$$

Les convergences sont exponentielles et on a de bonnes propriétés arithmétiques, mais à nouveau insuffisantes pour conclure à l'indépendance linéaire de 1, $\zeta(2)$, $\zeta(3)$.

-:-:-:-

RÉFÉRENCES

- [1] Ch. BATUT, M. OLIVIER, Sur l'accélération de la convergence de certaines fractions continues, Séminaire de Théorie des Nombres de Bordeaux, 1979-1980, n° 23 (25 pages).
- [2] H. COHEN, Accélération de la convergence de certaines récurrences linéaires, Séminaire de Théorie des Nombres de Grenoble, 6 et 13 novembre 1980 (47 pages).

(texte reçu le 13 mai 1981)

-:-:-:-

Henri COHEN
Laboratoire de Mathématiques Pures
Institut Fourier dépendant de
l'Université Scientifique et Médicale
de Grenoble associé au C.N.R.S.
B.P. 116
F 38402 St MARTIN D'HÈRES

SUBSTITUTIONS ALÉATOIRES ITÉRÉES

par

Jacques PEYRIÈRE

--:--:--

Pour étudier simultanément plusieurs constructions de B. Mandelbrot ([3] à [6]) nous avons introduit [9] ce que nous avons appelé les systèmes de Mandelbrot (M-systèmes). Ils définissent un nouveau type de processus de naissance. Dans le cas ici traité, ces processus sont des chaînes de Markov dont les états successifs sont des mots : on passe d'un mot au suivant en remplaçant au hasard chacune de ses lettres par un mot. On autorise, en outre, une certaine dépendance entre les substitutions de lettres voisines. Le résultat démontré ici concerne l'estimation asymptotique, presque sûre et en moyenne quadratique, du nombre d'occurrences d'un mot déterminé dans le $n^{\text{ième}}$ terme de la suite. Dans [9] on étudie des M-systèmes plus généraux qui engendrent des graphes colorés au lieu de mots.

1. - Les M-systèmes

Soit A un ensemble fini que nous appellerons alphabet. L'ensemble des mots non vides formés avec A est noté A^+ .

On considère une partie $\mathcal{L}$ de A^+ , stable par passage aux sous-mots et l'on se donne un système $(\Omega_w, p_w)_{w \in \mathcal{L}}$ d'espaces probabilisés dénombrables, projectif dans le sens suivant : si w' est un sous-mot de w , on se donne aussi une application $r_{w',w}$ (dépendant non seulement de w et w' mais aussi de la position de w' dans w) telle que l'image de p_w par $r_{w',w}$ soit $p_{w'}$. On suppose aussi que l'on a $r_{w'',w'} \circ r_{w',w} = r_{w'',w}$ chaque fois que w'' est un sous-mot de w' , lui-même sous-mot de w . Enfin, pour chaque lettre a , on se donne une application g_a de Ω_a dans $\mathcal{L}$.

Si $w = a_1 a_2 \dots a_v$ est un mot appartenant à $\mathcal{L}$, on définit une application g_w de Ω_w dans A^+ ainsi : $g_w(w)$ est la concaténation des mots $\{g_{a_j} \circ r_{a_j,w}^{(w)}\}_{1 \leq j \leq v}$.

Nous supposons que les données précédentes sont telles que, pour tout w , l'image de g_w soit contenu dans $\mathcal{L}$. Dans ces conditions, on dira que l'on a défini un M-système.

Un M-système définit une probabilité de transition Q sur $\mathcal{L} \times \mathcal{L}$:
 $Q(w, w') = p_w(g_w^{-1}(w'))$. La chaîne de Markov stationnaire ayant Q pour probabilité de transition sera notée $\{X_n\}_{n \geq 0}$. La probabilité sur les trajectoires issues de X_0 sera notée $\mathbb{P}_{X_0}$ et l'espérance correspondante $\mathbb{E}_{X_0}$.

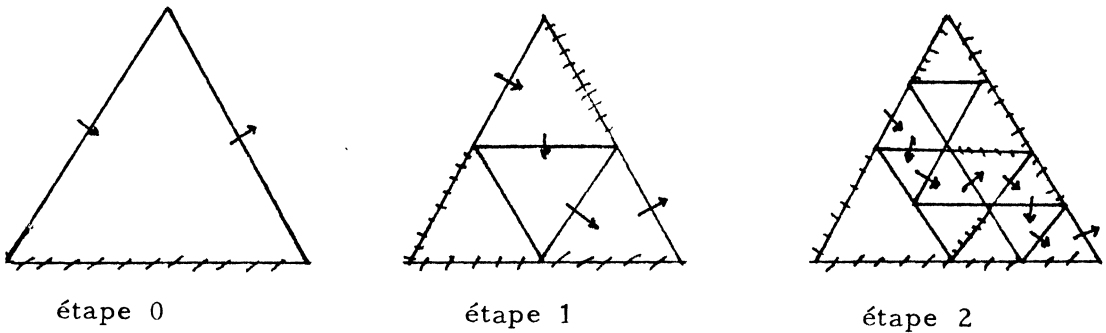
2. - Exemples

1) Une substitution $\sigma : A \longrightarrow A^+$ définit un M-système : pour tout mot w , Ω_w est réduit à un seul élément et $g_a = \sigma(a)$.

2) Donnons-nous, pour chaque a dans A , un espace probabilisé dénombrable (Ω_a, p_a) . A chaque mot $w = a_1 a_2 \dots a_v$, on associe l'espace probabilisé $(\Omega_w, p_w) = \prod_{1 \leq j \leq v} (\Omega_{a_j}, p_{a_j})$. Les applications $r_{w',w}$ sont les projections. On obtient ainsi un système projectif. Dans ces conditions, les substitutions de deux lettres distinctes d'un même mot sont indépendantes.

3) Voici une des constructions de B. Mandelbrot ayant motivé l'introduction des M-systèmes. On part d'un triangle T_0 dont on distingue deux des côtés, l'un est le côté d'entrée, l'autre celui de sortie. On sélectionne au hasard et indépendamment une moitié de chacun de ces côtés. Pour joindre, en passant par l'intérieur de T_0 , les deux moitiés sélectionnées, on est amené à traverser un ou trois des quatre triangles homothétiques de T_0 dans le rapport $1/2$ et qui le pavent. Chacun des triangles traversés est naturellement muni de côtés d'entrée et de sortie. On remplace T_0 par le ou les triangles traversés et l'on répète l'opération précédente indéfiniment, étant entendu que l'on sélectionne la même moitié d'un segment qu'il soit considéré comme côté de sortie d'un triangle ou côté d'entrée d'un autre. A part cela, tous les choix sont indépendants et faits selon la même loi. Il s'agit d'un processus de naissance : un triangle en engendre un ou trois ; de plus deux triangles voisins interagissent. Nous ne détaillons pas de M-système le décrivant (on peut en utiliser un qui agisse sur un alphabet à deux lettres).

Voici une figure qui illustre la construction précédente.



Dans [9] on trouve plus de détails et d'autres exemples. Enfin nous rencontrerons d'autres M-systèmes dans les démonstrations qui suivent.

3. - Résultats

Considérons un M -système. Nous noterons E_w l'espérance associée à p_w . Nous ferons les hypothèses suivantes :

H.1. - Pour tout a dans A , $E_a(|g_a|^2)$ est fini ($|w|$ désigne la longueur du mot w).

H.2. - Il existe un entier ℓ , positif ou nul, tel que, quel que soit le mot w , concaténation des mots $\{w_j\}_{1 \leq j \leq 2n-1}$ tels que la longueur de chacun des w_{2j} soit supérieure ou égale à ℓ , les variables $\{r_{w_{2j-1}, w}\}_{1 \leq j \leq n}$ définies sur (Ω_w, p_w) soient indépendantes.

Si w est un mot, $L(w)$ désigne le vecteur de $\mathbb{R}^A$ dont la composante correspondant à a est le nombre de fois que a figure dans w . On note M la matrice, indexée par $A \times A$, dont la colonne correspondant à a est $E_a(L \circ g_a)$. On adopte la terminologie de [10] en ce qui concerne les matrices à coefficients positifs.

Avec ces notations on a $E_w(L \circ g_w) = M L(w)$, d'où :

$$\mathbb{E}_{X_0} (L \circ X_{n+1}) \parallel X_n) = M L(X_n).$$

H.3. - On suppose que l'on a une partition $A = A_1 \cup A_2$ telle que la décomposition correspondante de M en blocs soit de la forme $\begin{pmatrix} S & T \\ O & U \end{pmatrix}$. On suppose en outre que la matrice S est primitive (c'est-à-dire, pour un k convenable, aucun coefficient de S^k n'est nul) et que sa valeur propre de Perron-Frobenius ρ est strictement supérieure à 1 et aux modules des valeurs propres de U .

On désigne par ξ le vecteur propre de M , associé à ρ , dont la somme $|\xi|$ des composantes est égale à 1.

THÉORÈME 1. - Sous les hypothèses H.1, H.2 et H.3, pour tout a dans A_1 , il existe une variable aléatoire Z telle que $\rho^{-n} L(X_n)$ tende $\mathbb{P}_a$ -presque sûrement et en moyenne quadratique vers $Z\xi$. De plus la variable aléatoire Z est $\mathbb{P}_a$ -presque sûrement non nulle.

Désignons par B_k l'ensemble des mots de longueur k qui peuvent apparaître avec une probabilité non nulle dans la descendance d'une lettre de A_1 . Si w est un mot, $L^{(k)}(w)$ désigne le vecteur de $\mathbb{R}^{B_k}$ dont la composante correspondant à w' est le nombre de fois que w' figure dans w . On note M_k la matrice indexée par $B_k \times B_k$ dont le terme correspondant à (w', w) est l'espérance par rapport à p_w du nombre de mots égaux à w' qui figurent dans $g_w(\cdot)$ et dont la première lettre est engendrée par la première lettre de w .

THÉORÈME 2. - Sous les hypothèses H.1, H.2 et H.3, pour tout k , M_k a ρ pour valeur propre simple et si ξ_k désigne le vecteur propre associé tel que $|\xi_k| = 1$, alors, pour tout a dans A_1 , $\rho^{-n} L^{(k)}(X_n)$ converge $\mathbb{P}_a$ -presque sûrement et en moyenne quadratique vers $Z \xi_k$.

La démonstration de la première assertion du théorème 1 fait l'objet des paragraphes 2 et 5, celle du théorème 2 est faite au paragraphe 6. L'assertion $\mathbb{P}_a(Z=0)=0$ n'est pas démontrée ici.

Ces résultats sont à rapprocher de certains obtenus dans le cas déterministe [1].

4. - Changement d'alphabet

Nous avons déjà défini B_k . Notons B'_k l'ensemble des mots de k lettres qui apparaissent avec une probabilité non nulle à la fin de l'un des mots engendrés par une quelconque lettre de A_1 . On pose $A^{(k)} = B_k \cup (\bigcup_{1 \leq j < k} B'_j)$ et $A^{(1)} = A$.

A chaque mot $X = x_1 x_2 \dots x_\nu$ construit sur l'alphabet A , on associe un mot $\rho_k(X)$ construit sur l'alphabet $A^{(k)}$ par le procédé suivant :

si $|X| < k$, alors $\rho_k(X) = X$,
et si $|X| \geq k$, alors

$$\rho_k(X) = (x_1 x_2 \dots x_k) (x_2 x_3 \dots x_{k+1}) \dots (x_{\nu-k+1} x_{\nu-k+2} \dots x_\nu) (x_{\nu-k+2} x_{\nu-k+3} \dots x_\nu)$$

($\rho_k(X)$ est constitué de $\nu-k+1$ éléments de B_k suivis d'un de B'_{k-1}).

Nous allons définir un M -système, opérant sur $A^{(k)}$, qui soit essentiellement équivalent au M -système de départ. On note $\mathcal{L}_k$ l'ensemble des sous-mots des mots $\{\rho_k(X)\}_{X \in \mathcal{L}}$. A chaque $\rho_k(X)$ on associe l'espace probabilisé (Ω_X, p_X) et au mot $W = (x_1 x_2 \dots x_k)(x_2 x_3 \dots x_{k+1}) \dots (x_\nu x_{\nu+1} \dots x_{\nu+k-1})$ appartenant à $\mathcal{L}_k$ on associe l'espace probabilisé (Ω_w, p_w) où $w = x_1 x_2 \dots x_\nu x_{\nu+1} \dots x_{\nu+k-1}$. Les applications $r_{W', W}$ sont des applications $r_{w', w}$ pour des w' et w convenablement choisis dans $\mathcal{L}$. Définissons maintenant les applications de génération $g_\alpha^{(k)}$ pour α dans $A^{(k)}$. Si α appartient à B_k , $g_\alpha^{(k)}(\cdot)$ est le mot obtenu en ne gardant dans $\rho_k(g_\alpha^{(k)}(\cdot))$ que les éléments de B_k dont la première lettre est engendrée par la première lettre de α . Si α appartient à $\bigcup_{1 \leq j < k} B'_j$, alors on pose $g_\alpha^{(k)} = \rho_k \circ g_\alpha$.

Nous venons, comme annoncé, de définir un M -système opérant sur $A^{(k)}$ et $\{\rho_k(X_n)\}_{n \geq 0}$ est une chaîne de Markov stationnaire dont la probabilité de transition est celle que définit ce M -système. Observons que, l'hypothèse H.2 étant satisfaite pour le M -système du départ, elle l'est aussi pour le nouveau en remplaçant ℓ par $\ell+k-1$.

Notons M_k la matrice associée à ce M -système. A la partition $A^{(k)} = B_k \cup (\bigcup_{1 \leq j < k} B'_j)$ correspond une décomposition de $\tilde{M}_k$ en blocs $\tilde{M}_k = \begin{pmatrix} M_k & M'_k \\ 0 & M''_k \end{pmatrix}$. La matrice M''_k est stochastique par rapport à ses colonnes. La matrice M_k s'obtient en remplaçant chacun des éléments $m_{a,b}$ de la matrice M par une matrice dont la somme des éléments de chaque colonne est $m_{a,b}$. On en déduit que les valeurs propres de $\tilde{M}_k$ sont en module inférieures à ρ .

Notons P_k le projecteur de $\mathbb{R}^{A^{(k)}}$ sur $\mathbb{R}^{B_k}$ parallèlement à $\mathbb{R}^{A^{(k)}} \setminus B_k$. Si W appartient à $\mathcal{L}_k$, notons $L^k(W)$ le vecteur de $\mathbb{R}^{A^{(k)}}$ décrivant la composition de W . On a, si X appartient à $\mathcal{L}$, $L^{(k)}(X) = P_k L^k(\rho_k(X))$.

5. - Estimation des moments d'ordre 2

Si $w = x_1 x_2 \dots x_v$ appartient à $\mathcal{L}$, on pose, si $v > 1$,

$$V_w = E_w(L \circ g_{x_1} \circ r_{x_1, w} \otimes L \circ g_{x_v} \circ r_{x_v, w} + L \circ g_{x_v} \circ r_{x_v, w} \otimes L \circ g_{x_1} \circ r_{x_1, w}) \\ - E_{x_1}(L \circ g_{x_1}) \otimes E_{x_v}(L \circ g_{x_v}) - E_{x_v}(L \circ g_{x_v}) \otimes E_{x_1}(L \circ g_{x_1})$$

et, si a appartient à A ,

$$V_a = E_a(L \circ g_a \otimes L \circ g_a) - E(L \circ g_a) \otimes E(L \circ g_a).$$

Si w a une longueur strictement supérieure à ℓ , l'hypothèse H.2 entraîne que V_w est nul.

On a :

$$E_X(L \circ g_X \otimes L \circ g_X) = M \otimes M L(X) \otimes L(X) + \sum_{1 \leq k \leq \ell} \sum_{w \in B_k} V_w L_w^{(k)}(X),$$

ce que nous écrirons de la façon suivante :

$$E_X(L \circ g_X \otimes L \circ g_X) = M \otimes M L(X) \otimes L(X) + \sum_{1 \leq k \leq \ell} V^k \cdot L^{(k)}(X).$$

On obtient

$$\mathbb{E}_{X_0}(L(X_n) \otimes L(X_n)) = M^n \otimes M^n L(X_0) \otimes L(X_0) + \sum_{1 \leq k \leq \ell} \sum_{0 \leq j < n} (M \otimes M)^{n-j-1} V^k \cdot P_k \tilde{M}_k^j L^k(\rho(X_0))$$

$$(\text{on a, en effet, } \mathbb{E}_{X_0} L^k(\rho_k(X_n)) = \tilde{M}_k^n L^k(\rho_k(X_0)))$$

d'où, puisque l'on a $\rho^{-n} M^n = M' + O(\alpha^n)$ où α appartient à $]0, 1[$ et M' est un projecteur sur $M \xi$,

$$\rho^{-2n} \mathbb{E}_{X_0}(L(X_n) \otimes L(X_n)) = M' \otimes M' [L(X_0) \otimes L(X_0) + \rho^{-2} \sum_{1 \leq k \leq \ell} V^k \cdot P_k (I - \rho^{-2} M_k)^{-1} L^k(X_0)] \\ + O(\alpha^n).$$

La démonstration de la première assertion du théorème 1 se termine alors comme celle de Harris [2] relative aux processus de Galton-Watson à plusieurs types. On peut trouver une démonstration de la seconde assertion dans [7] ou [9].

6. - Etude spectrale des mots engendrés (théorème 2)

Le théorème 2 résulte de l'application du théorème 1 aux M-systèmes construits au paragraphe 4. On a simplement à démontrer qu'une certaine matrice S_k est primitive : $A_1^{(k)}$ est constitué des éléments de B_k dont la première lettre appartient à A_1 , $A_2^{(k)}$ est constitué des autres éléments de $A^{(k)}$, la décomposition correspondante de $\tilde{M}_k$ étant $\tilde{M}_k = \begin{pmatrix} S_k & T_k \\ O & U_k \end{pmatrix}$.

Soit ν le plus petit entier tel que tout α de $A_1^{(k)}$ apparaisse avec une $\mathbb{P}_{X_0}$ -probabilité non nulle dans l'un des termes de la suite $\{X_j\}_{1 \leq j \leq \nu}$ pour un X_0 appartenant à A_1 . Il est clair que, pour chaque α appartenant à $A_1^{(k)}$ il existe une lettre a dans A_1 telle que α figure, avec une $\mathbb{P}_a$ -probabilité non nulle, comme sous-mot de X_ν . Observons que, si a_0 est un élément de A_1 , quel que soit N , il existe τ tel que, avec une $\mathbb{P}_{a_0}$ -probabilité non nulle, X_τ contienne plus de N fois chaque lettre de A_1 (toutes les composantes de ξ indexées par A_1 sont en effet non nulles). On choisit N assez grand et l'on prend l'espérance de $L^k(\rho_k(X_{\tau+\nu}))$ par rapport à $\mathbb{P}_{a_0}$, ce qui montre que la matrice $S_k^{\tau+\nu}$ possède une colonne dont tous les éléments sont non nuls et donc que la matrice S_k est primitive.

-:-:-:-

BIBLIOGRAPHIE

- [1] COQUET J., KAMAE T. et MENDÈS FRANCE M., Sur la mesure spectrale de certaines suites arithmétiques, Bull. Soc. Math. France 105 (1977), 369-384.
- [2] HARRIS T.E., Some mathematical models for branching processes, Second Berkeley Symposium on Mathematical Statistics and Probability, Univ. Calif. Press, 1951.
- [3] MANDELBROT B., Fractals : Form, Chance and Dimension, Freeman and C°, 1977
- [4] MANDELBROT B., Les objets fractals, La Recherche 9, 85, 1-13.

- [5] MANDELBROT B., Colliers aléatoires et une alternative aux promenades au hasard sans boucle : les cordonnets discrets et fractals, C.R.A.S. 286 (1978), 933-936.
- [6] MANDELBROT B., Fractal limits of random beadsets and geometric imbedding of birth processes, To appear
- [7] PEYRIÈRE J., Mandelbrot random beadsets and birth processes with interaction, IBM Research report R C-7417.
- [8] PEYRIÈRE J., Processus de naissance avec interaction des voisins, C.R.A.S. 289 (1979), 223-224 et 557.
- [9] PEYRIÈRE J., Processus de naissance avec interaction des voisins, évolution de graphes, Ann. Inst. Fourier 31 (1981).
- [10] SENETA E., Non-négative matrices, J. Wiley (1973).

(texte reçu le 27 mai 1981)

-:-:-:-

Jacques PEYRIÈRE
 Université de Paris-Sud
 Centre d'Orsay
 Mathématiques - bât. 425
 F 91405 ORSAY CEDEX

ESTIMATING $\liminf (p_{n+r} - p_n) / \log p_n$

by

Martin HUXLEY

-:-:-:-

Hardy and Littlewood conjectured that the number of solutions of $p' - p = n$, $p' \leq N$ in primes p , p' is

$$\frac{N}{\log^2 N} H(n)$$

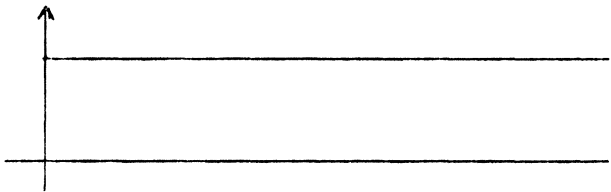
to within a factor $(1 + o(1))$. For simplicity of exposition factors $(1 + o(1))$ will be omitted from formulae. Here $H(n)$ is an arithmetic function

$$H(n) = (1 + (-1)^n) \prod_{p > 2} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{\substack{p | n \\ p > 2}} \frac{p-1}{p-2}.$$

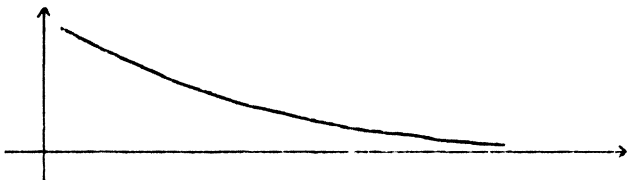
Equivalently, the conjecture is that

$$Z(2n) = \sum_{\substack{p' - p = 2n \\ p > N, p' \leq 2N}} \log p \cdot \log p' \sim 2NH(2n).$$

This corresponds to a distribution histogram for $(p'-p)/\log p$ which is constant



since $H(n)$ has mean value unity. This conjecture goes back to Hardy and Littlewood. Erdős proposed that $(p_{r+1} - p_r)/\log p_r$ should have the distribution histogram of e^{-x} .



Very little has been proved ; we cannot show that

$$E_r = \liminf_{n \rightarrow \infty} \frac{p_{n+r} - p_n}{\log p_n}$$

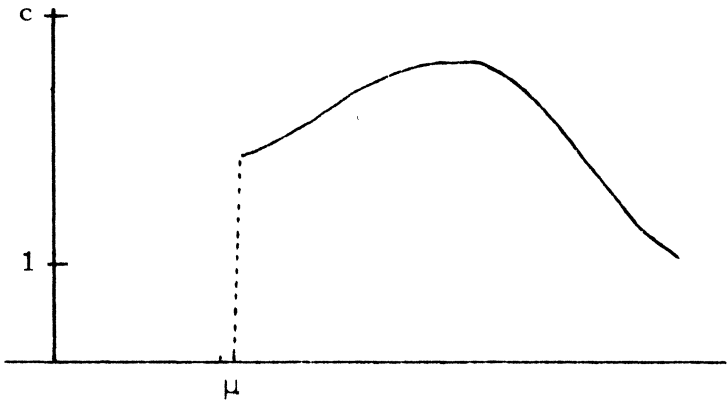
is zero, even for $r = 1$.

The direct attack rests on three inequalities. From the Brun sieve we get the first inequality

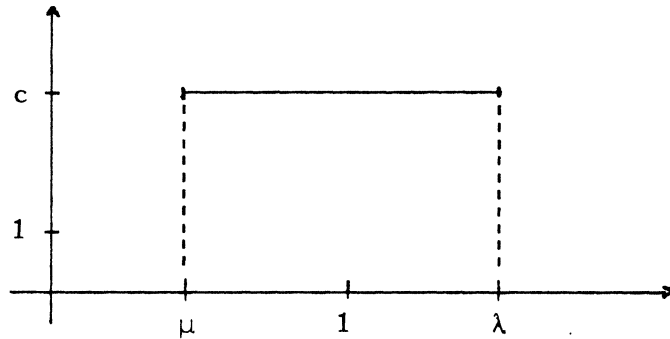
$$Z(2n) \leq 2 c N H(2n) .$$

Thus the distribution histogram is bounded.

Now suppose that $\frac{p_{n+1} - p_n}{\log p_n} \geq \mu$ for $N \leq p_n < p_{n+1} < 2N$. The distribution histogram is



a distribution of total mass 1 with centre of mass at 1 on a suitable scale, since the mean of $p_{n+1} - p_n$ is $\log N \sim \log p_n$. The worst case is



The conditions give $\lambda + \mu = 2$, $\lambda - \mu = 1/c$, so

$$\mu = 1 - 1/2c.$$

This is Erdős's bound $E_1 \leq 1 - 1/2c$.

Bombieri's theorem with the linear sieve [1] gives $c = 4$. Chen [2] has obtained $c = 3.917\dots$.

The second approach is that of Hardy and Littlewood. If

$$S(\alpha) = \sum_{N \leq p < 2N} \log p \cdot e(p\alpha),$$

then

$$Z(2n) = \int_0^1 S(\alpha) \bar{S}(\alpha) e(2n\alpha) d\alpha.$$

The major arcs contribution is

$$\int_M S(\alpha) \bar{S}(\alpha) e(2n\alpha) d\alpha = 2NH(2n)$$

exactly as conjectured (if one neglects the error term in the prime number theorem). But there is no good enough estimate on the minor arcs, and in fact

$$\int_0^1 S(\alpha) \bar{S}(\alpha) d\alpha = N \log N$$

$$\int_M S(\alpha) \bar{S}(\alpha) d\alpha = N \log Q,$$

where the major arcs are defined by the Farey dissection of order Q .

$Q < N^{\frac{1}{2}}$ is necessary if the major arcs have length $1/\varepsilon N$, so half the support of $|S(\alpha)|^2$ is on the minor arcs.

The way forward is to take weights $t(n)$ and let

$$T(\alpha) = \sum t(n) e(2n\alpha)$$

such that $T(\alpha) \geq 0$. Then

$$\int_0^1 \geq \int_M$$

$$\sum t(n) Z(2n) \geq \sum t(n) 2NH(2n) ,$$

an inequality in the right direction. Unfortunately there must be a term $t(0)$ with a weight on $n = 0$. Using Bombieri's theorem Q can be close to $N^{\frac{1}{2}}$, and one gets

$$\sum_{n > 0} t(n) Z(2n) \geq N T(0) - \frac{1}{4} t(0) N \log N .$$

The right hand side is positive when

$$T(0) > \frac{1}{4} t(0) \log N ,$$

so that the support of $t(n)$ is of order $\log N$ in length, and one cannot hope to get a smaller order of magnitude for $p_{n+1} - p_n$. Let us choose the best weights.

$T(\alpha)$ is a sum of squares, but if $T(\alpha) = T_1(\alpha) + T_2(\alpha)$, and both T_1 and T_2 are non-negative, the inequality given by $T(\alpha)$ is a consequence of those given by $T_1(\alpha)$ and by $T_2(\alpha)$. So we may suppose

$$T(\alpha) = |U(\alpha)|^2 = U(\alpha) \overline{U(\alpha)}$$

(since we want real coefficients). Let

$$U(\alpha) = \sum_{-k}^k u(n) e(2n\alpha) ,$$

then

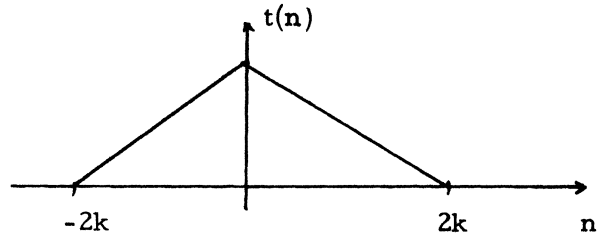
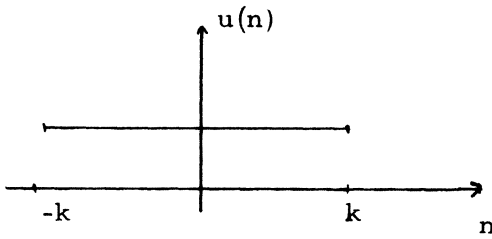
$$T(0) = |U(0)|^2 = \left| \sum u(n) \right|^2 ,$$

$$t(0) = \sum |u(r)|^2$$

and

$$T(0) \leq (2k+1) \sum |u(n)|^2 = (2k+1) t(0) ,$$

equality when $u(n)$ is constant.



The right hand side is positive when

$$2k > \frac{1}{4} \log N ,$$

so $Z(2n) > 0$ for some $2n \sim 4k \sim \frac{1}{2} \log N$, and $E_1 \leq \frac{1}{2}$.

To deal with $p_{n+r} - p_n$ we may put

$$S^{(i)}(\alpha) = \sum_{\substack{N \leq p_j < 2N \\ j \equiv i \pmod{r}}} \log p \cdot e(p\alpha)$$

$$Z_r(2n) = \sum_{\substack{p_j - p_i = 2n \\ j \equiv i \pmod{r}}} \log p_i \cdot \log p_j .$$

We use [3] Bombieri's theorem on

$$\int_M^r \sum_{i=1}^r |S^{(i)}(\alpha)|^2 d\alpha = \int \sum_i |\text{main} + \text{error terms}|^2 d\alpha .$$

The main term is tractable ; the squared error term is positive. In the cross-product term, we may sum over i to obtain a sum over all primes, and then apply Bombieri's theorem. This gives

$$r \sum t(n) Z_r(2n) \geq N T(0) - \frac{1}{2} (r - \frac{1}{2}) t(0) N \log N ,$$

giving $E_r \leq r - \frac{1}{2}$ in the same way.

Suppose now that $Z(2n) = 0$ for $n < h$, but $2k > h$

$$\begin{aligned} \sum_{n=1}^{2k} t(n) Z(2n) &= \sum_h^{2k} t(n) Z(2n) \\ &< \sum_h^{2k} 2c H(2n) t(n) N = N \sum_h^{2k} 2c t(n) . \end{aligned}$$

Hence we have

$$T(0) < 2c \sum_h^{2k} t(n) + \frac{1}{4} (t_0) \log N .$$

The right hand side is a quadratic form in $u(n)$, which is minimum when

$$\sum_{h \leq |m-n| \leq 2k} u(n) + \frac{\ell}{4c} u(m) = 2\rho U(0) \quad (\ell = \log N)$$

for some constant ρ . This gives the weights as simultaneous equations. Differencing eliminates ρ

$$u(m+1-h) - u(m+h) = - \frac{\ell}{2A} \{u(m+1) - u(m)\} .$$

Changing to a continuous variable by

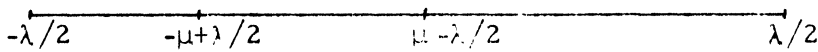
$$m = \frac{1}{2} x \ell , \quad 2k = \frac{1}{2} \lambda \ell , \quad h = \frac{1}{2} \mu \ell$$

we have

$$\begin{aligned} f(x) &= 0 \quad \text{for } |x| \geq \lambda/2 , \\ f'(x) &= 2c \{ f(x+\mu) - f(x-\mu) \} , \end{aligned}$$

where $u(n)$ is supposed to be a piecewise differentiable function of x .

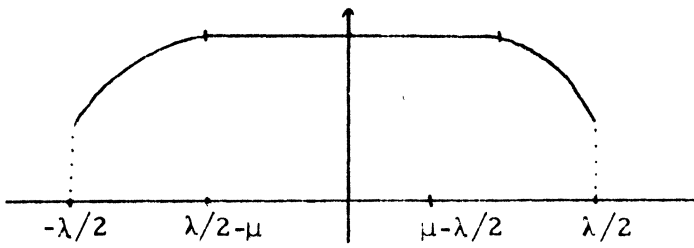
There are three pieces



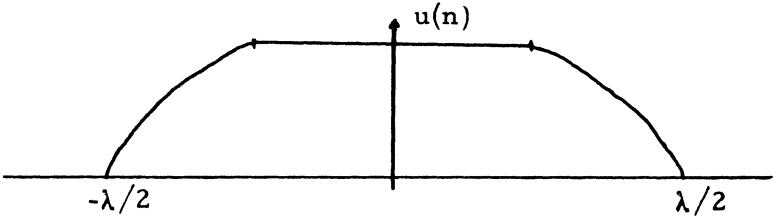
On the middle range $f'(x) = 0$, on the right, if we assume symmetry

$$f'(x) = -2c f(\mu-x) .$$

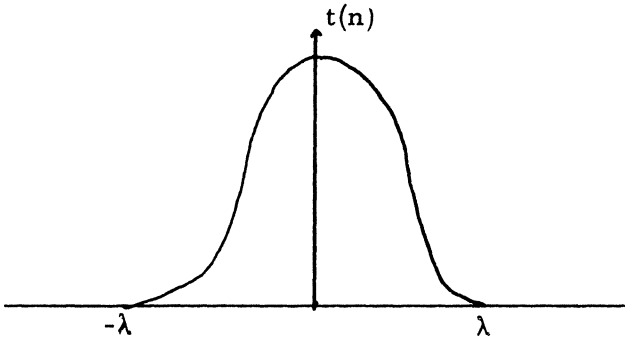
The solution of this functional equation is a cosine



or, if we choose λ optimally



This corresponds to weights $t(n)$



Hence even if the distribution of $(p_{n+1} - p_n) / \log p_n$ is as bad as it can be, we get a bound, which turns out to be

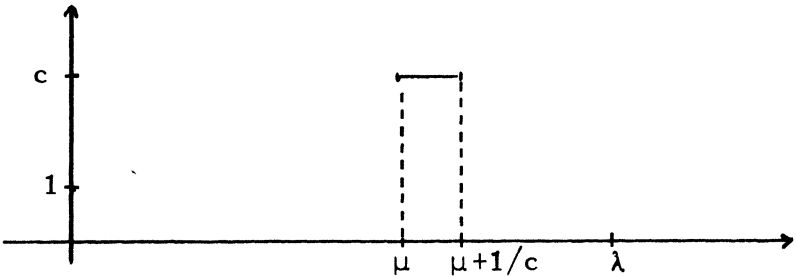
$$E_1 \leq \frac{1}{4} + \frac{\pi}{16}$$

and similarly

$$E_r \leq \frac{2r-1}{4r} \left\{ 2r-1 + \frac{\pi}{4} \right\} .$$

The λ, μ idea is from [1], the choice of weights is mine [4].

Now for E_r it so happens that μ and λ are more than $1/c$ apart, so the worst possible distribution is height c between $x = \mu$ and $x = \mu + 1/c$, 0 elsewhere.



Hence we have

$$\sum_1^{2k} t(n) Z_r(2n) \leq \sum_h^j t(n) 2c N H(2n) \leq 2c \sum_h^j t(n) N$$

where $j = \frac{1}{2} \nu \ell$, and we take $\nu = \mu + 1/c$. This gives a quadratic form as before, and leads to a functional equation

$$\frac{f'(x)}{2c} = f(x+\mu) - f(x+\nu) - f(x-\mu) + f(x-\nu) .$$

The formula must change at $\mu - \lambda/2$, $\nu = \lambda/2$, $\nu - \lambda/2 - \mu$, ... in fact, at a set of points which are generated by those translations by μ or ν lying within the interval $[-\lambda/2, \lambda/2]$. If this set is infinite, the method fails. If it is finite, the solutions contain linear combinations of sines and cosines. It's very complicated, and keeps Dr Siebert calculating for weeks.

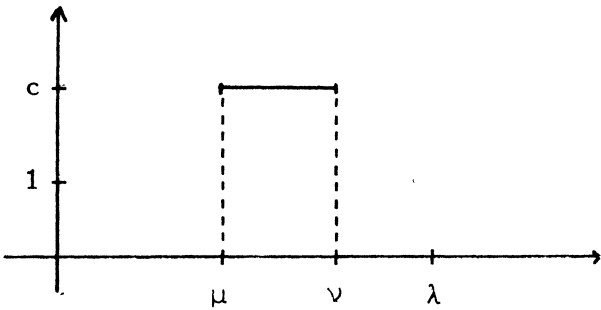
We can enlist a third inequality by considering instead of $U(\alpha)$ a function $W(\alpha)$ with $w(-n) = -w(n)$, and for $T(\alpha)$ consider $V(\alpha) = |W(\alpha)|^2$, so that

$$V(n) = \sum_{a-b=n} w(a) w(b) = - \sum_{a+b=n} w(a) w(b) .$$

The circle method result now reads

$$- \sum_1^{2k} v(n) Z(2n) \leq N V(0) + \frac{1}{4} v(0) N \log N \leq \frac{1}{4} v(0) N \ell ,$$

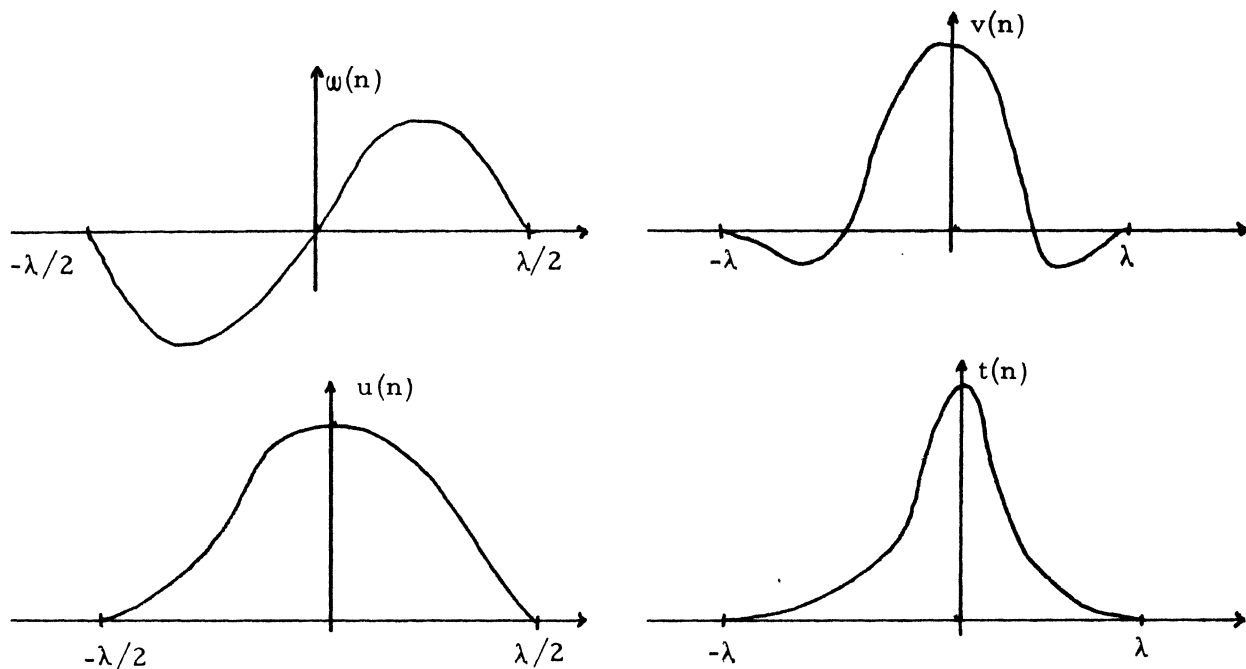
Since $W(0) = 0$. There are now two sets of weights $u(n)$, $w(n)$, and the third inequality is an upper bound again. Again if the worst distribution histogram is this,



fixing λ and $W(\alpha)$ gives an inequality between μ and ν . Choosing $U(\alpha)$ gives another inequality between μ and ν , and so a bound for μ when we eliminate ν . Next one varies λ , the weights $w(n)$ and the weights $u(n)$,

checking whether the distribution histogram given is really the worst case.

In the end I found the optimum choice [5] by accident. It is a "singular solution" with $\lambda = \mu + \nu$ and no change of formula at $x = \frac{1}{2} \lambda - \mu (= \nu - \frac{1}{2} \lambda)$.



$w(n)$ is a sine, $u(n)$ is $1+\cosine$. This method gives

$$E_r \leq \frac{2r-1}{16r} \left\{ 4r + (4r-1) \frac{\theta_r}{\sin \theta_r} \right\}, \quad E_1 \leq 0.4425 \dots,$$

where θ_r satisfies $\theta + \sin \theta = \pi/4r$. All previous bounds are improved, but only slightly. These numbers are with $c = 4$, substituting Chen's 3.9 changes the fourth decimal place.

A curiosity is the use of the circle method with an integrand $V(\alpha)$ which vanishes at the centres of major arcs.

-:-:-:-

REFERENCES

- [1] BOMBIERI E. and DAVENPORT H. , Small differences between prime numbers, Proc. Royal Soc. A. 293 (1966), 1-18.
- [2] CHEN J.-R. , On the Goldbach's problem and the sieve methods, Sci. Sin. XXI (1978), 701-739.
- [3] HUXLEY M.N. , On the differences of primes in arithmetical progressions, Acta Arith. 15 (1969), 367-392.
- [4] HUXLEY M.N. , Small differences between consecutive primes, Mathematika 20 (1973), 229-232.
- [5] HUXLEY M.N. , Small differences between consecutive primes II, Mathematika 24 (1977), 142-152.

(texte reçu le 25 juin 1981)

--:--:--

Martin HUXLEY
University College
CARDIFF CFI IXL

EXTENSIONS WITH IDENTICAL WILD RAMIFICATION

by

S. M. J. WILSON

--:--:--

Let R be a Dedekind ring with field of quotient F and let $\mathfrak{O}$ be an R -order in an algebra A . We denote by $G_{\oplus}(\mathfrak{O})$ the Grothendick group of all $\mathfrak{O}$ -lattices (finitely generated R -torsion-free $\mathfrak{O}$ -modules) with respect to direct sum.

For the purpose of this paper, Martinet's conjecture may be restated as

THEOREM 0 (Fröhlich). - If N is an algebraic number field, $\Gamma \leq \text{Gal}(N)$ and N/N^{Γ} is not wildly ramified then $[\mathfrak{O}_N] = [\text{free}]$ in $G_{\oplus}(\mathbb{Z}\Gamma)$.
(Here $\mathfrak{O}_N = \text{int}(N)$ is considered as a $\mathbb{Z}\Gamma$ -module.)

Some years ago I made a suggestion (which I might now call a conjecture...) that this result might generalize as follows :

CONJECTURE. - If N and N' are algebraic number fields with monomorphisms, $\Gamma \longrightarrow \text{Gal}(N)$ and $\Gamma \longrightarrow \text{Gal}(N')$ and if $\mathfrak{O}_N$ is locally isomorphic to $\mathfrak{O}_{N'}$ as a $\mathbb{Z}\Gamma$ -module then $[\mathfrak{O}_N] = [\mathfrak{O}_{N'}]$ in $G_{\oplus}(\mathbb{Z}\Gamma)$.

(The condition that $\mathfrak{O}_N \cong_{\text{locally}} \mathfrak{O}_{N'}$ is certainly necessary.)

Some recent work of Queyruet [Q1] and [Q2] has led me to take my conjecture more seriously and this has resulted in the

THEOREM 1. - The conjecture is true if there is a bijection $p \longmapsto \alpha(p)$ between the primes of N^{Γ} , wildly ramified in N and those of N'^{Γ} wildly ramified in N' , such that N_p and $N'_{\alpha(p)}$ are isomorphic as Γ -algebras.

I. - Relative groups and K_1

With $\mathfrak{O}$ and A as above we have a relative group $G_{\oplus, \text{rel}}(\mathfrak{O})$, fitting into the following exact sequence (see [B]).

$$G_1(\mathfrak{O}) \xrightarrow{(\otimes F)} G_1(A) \xrightarrow{d} G_{\oplus, \text{rel}}(\mathfrak{O}) \xrightarrow{\delta} G_{\oplus}(\mathfrak{O}) \xrightarrow{(\otimes F)} G_{\oplus}(A) \dots \quad (1)$$

We recall that the relative group is generated by triples (M, N, α) where M and N are $\mathfrak{O}$ -lattices and α is an A -isomorphism $\alpha : M \otimes_R F \longrightarrow N \otimes_R F$, that $d : (V, \alpha) \longmapsto (M, N, \alpha)$ where M is any full $\mathfrak{O}$ -lattice in the A -module V and that $\delta : (M, N, \alpha) \longrightarrow [M] - [N]$.

(1) is natural with respect to extension of $\mathfrak{O}$.

If $\mathfrak{p}$ is a maximal ideal of R we write $M_{\mathfrak{p}}$ for the $\mathfrak{p}$ -adic completion of an R -module M . Then localizations induce a map

$$G_{\mathfrak{O}, \text{rel}}(\mathfrak{O}) \longrightarrow \bigsqcup_{\mathfrak{p}} G_{\mathfrak{O}, \text{rel}}(\mathfrak{O}_{\mathfrak{p}}) \quad (2)$$

which is an isomorphism (see e. g. [Q1]). We shall regard these two groups as identified by this map.

Although much of what follows is true more generally we make the following assumptions which lead directly to the case in question. First, let $\bar{\mathfrak{Q}}$ be an algebraic closure of $\mathfrak{Q}$. We assume that $F \subseteq \bar{\mathfrak{Q}}$, $|F : \mathfrak{Q}| < \infty$ and $R = \text{int}(F)$.

We put $\Omega_F = \text{Gal}(\bar{\mathbb{Q}}/F)$, $\bar{A} = A \otimes_F \bar{\mathbb{Q}}$ and $R_A = K_o(A)$. Then we have the "det" maps of Fröhlich :

$$\det : G_1(A) \xrightarrow{\sim} \text{Hom}_{\Omega_F}^+(R_{\bar{A}}, \bar{\mathbb{Q}}^*) \quad (3)$$

$$\det : G_1(A_p) \xrightarrow{\sim} \text{Hom}_{\Omega_F}(R_{\bar{A}}, (\bar{\mathbb{Q}}_p^*) \quad (4)$$

for any maximal ideal p of R . (Here the "+" restricts to those maps f such that, for every embedding $i : \mathbb{Q} \rightarrow \mathbb{C}$ such that $i(F) \leq \mathbb{R}$ and every simple A -module V such that $\text{End}_{A \otimes_{i(F)} \mathbb{R}}(V \otimes_{\mathbb{Q}} \mathbb{C}) \cong H$, if $([V]) > 0$.)

Also (cf. [W]), writing $\bar{\mathbb{Z}} = \text{int}(\bar{\mathbb{Q}})$,

$$\det(G_1(\mathfrak{O})) = \text{Hom}_{\Omega_K}^+(R_{\bar{A}}, \bar{\mathbb{Z}}^*) \quad (5)$$

$$\det(G_1(\mathfrak{O}_p)) = \text{Hom}_{\Omega_K}(R_{\bar{A}}, (\bar{\mathbb{Z}}_p^*) \quad (6)$$

Examining the local components ((2)) we see that $G_{\oplus, \text{rel}}(\mathfrak{O})$ is torsion free so that if K/F is finite ($K \subset \bar{\mathbb{Q}}$) the extension map

$$G_{\oplus, \text{rel}}(\mathfrak{O}) \longrightarrow G_{\oplus, \text{rel}}(\mathfrak{O} \otimes_{\mathbb{Q}} \mathbb{Q}_K)$$

is injective (since the composite with the restriction map is multiplication by $[K : F]$). Hence putting

$$\bar{G}_{\oplus, \text{rel}}(\mathfrak{O})_F = \varinjlim_{\substack{\bar{\mathbb{Q}} \supset K \supset F \\ |K:F| < \infty}} G_{\oplus, \text{rel}}(\mathfrak{O} \otimes_{\mathbb{Q}} \mathbb{Q}_K)$$

we have, from (1) to (6), a commutative diagram with exact rows and injective columns :

$$\begin{array}{ccccccc} \text{Hom}_{\Omega_F}^+(R_{\bar{A}}, \bar{\mathbb{Z}}^*) & \hookrightarrow & \text{Hom}_{\Omega_F}^+(R_{\bar{A}}, \bar{\mathbb{Q}}^*) & \xrightarrow{d} & G_{\oplus, \text{rel}}(\mathfrak{O}) & \longrightarrow & G_{\oplus}(\mathfrak{O}) \\ \downarrow & & \downarrow & & \parallel & & \\ \text{Hom}_{\Omega_F}(R_{\bar{A}}, U_o(\bar{\mathbb{Q}})) & \hookrightarrow & \text{Hom}_{\Omega_F}(R_{\bar{A}}, J_o(\bar{\mathbb{Q}})) & \xrightarrow{\hat{d}} & G_{\oplus, \text{rel}}(\mathfrak{O}) & & \\ \downarrow & & \downarrow & & \uparrow & & \\ \text{Hom}(R_{\bar{A}}, U_o(\bar{\mathbb{Q}})) & \hookrightarrow & \text{Hom}(R_{\bar{A}}, J_o(\bar{\mathbb{Q}})) & \xrightarrow{\hat{d}} & \bar{G}_{\oplus, \text{rel}}(\mathfrak{O})_F & & \end{array} \quad (7)$$

where the $\hat{d}$ maps are formed from maps of the form $\det^{-1} \circ d$ using (2).

Here $U_o =$ finite unit ideles and $J_o =$ finite ideles.

If $f \in \text{Hom}(R_A, J_o(\mathbb{Q}))$ we write (f) for $\hat{a}(f)$.

Suppose $K \subseteq \mathbb{Q}$, $|K : \mathbb{Q}| = n < \infty$ we choose $\sigma_1, \dots, \sigma_n : \bar{\mathbb{Q}} \rightarrow \bar{\mathbb{Q}}$ extending the n embeddings of K in $\bar{\mathbb{Q}}$.

If Y is an Ω -group then we unite $\eta : Y \rightarrow Y$ by $y \mapsto \pi y^{\sigma_1}$. We note that

$\eta : G_{\oplus, \text{rel}}(\mathfrak{D}) \rightarrow G_{\oplus, \text{rel}}(\mathfrak{D})$ extends the restriction map :

$$G_{\oplus, \text{rel}}(\mathfrak{D} \otimes_{\mathbb{Z}} \mathfrak{D}_K) \rightarrow G_{\oplus}(\mathfrak{D}).$$

And that, in fact, η provides a morphism of diagrams from (7) with

$$\mathfrak{D} = \mathfrak{D} \otimes_{\mathbb{Z}} \mathfrak{D}_K, \quad R = \mathfrak{D}_K \quad \text{to (7) with } \mathfrak{D} = \mathfrak{D} \quad \text{and} \quad R = \mathbb{Z}. \quad (8)$$

II. - The resolvent

Take new N, Γ as in the statement of the theorem and put $K = N^{\Gamma}$. From now on $\mathfrak{D} = R\Gamma$ and $R_{\bar{A}} = R_{\Gamma}$ character group.

For the sake of clarity take a finite extension M of N normal over K ($M = N$ will do). We have an isomorphism of $M\Gamma$ -modules (Γ acting on N)

$$\begin{array}{ccc} \zeta : N \otimes_K M & \longrightarrow & M\Gamma \\ \text{by } n \otimes m & \longmapsto & \sum n^{\gamma} m^{\gamma}. \end{array}$$

Abusively we shall write $\zeta(n \otimes 1) = \zeta(n)$.

Put $r = (\mathfrak{D}_N \otimes_{\mathfrak{D}_K} \mathfrak{D}_M, \mathfrak{D}_M^{\Gamma}, \zeta) \in G_{\oplus}(K\Gamma)$. Choose $a \in N$ so that $aK\Gamma = N$. We see that

$$\begin{aligned} (\mathfrak{D}_N, a \mathfrak{D}_{K\Gamma}, 1) &= (\mathfrak{D}_N \otimes_{\mathfrak{D}_K} \mathfrak{D}_M, (a \otimes 1) \mathfrak{D}_M^{\Gamma}, 1) \\ &= (\mathfrak{D}_N \otimes_{\mathfrak{D}_K} \mathfrak{D}_M, \zeta(a \otimes 1) \mathfrak{D}_M^{\Gamma}, \zeta) \\ &= r + (\det \zeta(a)) \dots \end{aligned} \quad (9)$$

For each maximal ideal $\mathfrak{p}$ of $\mathfrak{D}_K$ put

$$r_{\mathfrak{p}} = \text{component of } r \text{ at } \mathfrak{p} \quad (= r \otimes_{\mathfrak{D}_K}^{\mathfrak{p}}, \text{ cf. (2)}).$$

If p is tame in N we choose $a_p \in N_p$ such that $a_p \mathfrak{O}_{K_p}^\Gamma = \mathfrak{O}_{N_p}$ and we rapidly obtain, as in (9)

$$r_p = (\det \zeta(a_p)). \quad (10)$$

In any case we have, for an integer prime p

$$(\eta(r))_p = \sum_{p \mid p} \eta(r_p). \quad (11)$$

Note that $r_p^{\sigma_i}$ is independent of the choice of σ_i so that $\eta(r_p)$ is independent of the choice of $\{\sigma_i\}$.

III. - Galois Gauss sums

From [Q] and [F. T.] we know that for the Galois group Γ of N we have local and global Gauss sums τ_p , for each p of $\mathfrak{O}_K$, and τ with the following properties

$$\begin{aligned} \tau, \tau_p &\in \text{Hom}(R_\Gamma, \overline{\mathfrak{O}}^\times), \quad \tau_p \text{ depending only on } \Gamma \text{ and } N_p \\ \tau &= \prod_p \tau_p \end{aligned} \quad (12)$$

$$(\tau_p(\chi), q) = 1 \quad \text{if } q \in \mathbb{Z} \setminus p. \quad (13)$$

$$\eta(\det \zeta(a))/\tau \in \text{Hom}_\Omega(R_\Gamma, \overline{\mathfrak{O}}^\times) \quad (14)$$

(where $\Omega = \Omega_{\mathfrak{O}}$).

There is a map $y \in \text{Hom}_\Omega(R_\Gamma, \overline{\mathbb{Z}}^\times)$ such that

$$\begin{aligned} y \eta(\det \zeta(a))/\tau &\text{ lies in } \text{Hom}_\Omega^+(R_\Gamma, \overline{\mathfrak{O}}^\times) \\ \text{and so is equal to } \det(\lambda) &\text{ for some } \lambda \in G_1(\mathfrak{O}, \Gamma) \end{aligned} \quad (15)$$

and finally if p is a prime of K , tame in N then

$$\eta(\det \zeta(a_p)) \tau_p^{-1} \in \text{Hom}(R_\Gamma, (\overline{\mathbb{Z}})_p^*)$$

so by (6)

$$(\eta(\det \zeta(a_p))) = (\tau_p)$$

and by (10)

$$\eta r_p = (\tau_p). \quad (16)$$

IV. - The proof of Theorem 1

Let p be an integer prime. Then the component of $\eta(r)$ at p can be expressed as follows

$$(\eta(r))_p = \sum_{p|p} \eta(r_p) \quad \text{by (11)}$$

$$= \sum_{\substack{p|p \\ p \text{ tame}}} (\tau_p) + \sum_{\substack{p|p \\ p \text{ wild}}} \eta(r_p) \quad \text{by (16)}$$

$$= (\tau_p) + \sum_{\substack{p|p \\ p \text{ wild}}} (\eta(r_p) - (\tau_p)) \quad \text{by (12) and (13)}$$

We now assemble a new set of data for N' corresponding to that we have for N , distinguishing the new objects with a " ' " .

$$\begin{aligned} \text{Then } (\eta(r))_p - (\eta'(r'))_p &= \\ &= (\tau)_p - (\tau')_p + \sum_{\substack{p|p \\ p \text{ wild}}} (\eta(r_p) - \eta'(r'_{\alpha(p)}) + \tau'_{\alpha(p)} - \tau_p) \\ &= (\tau)_p - (\tau')_p \dots \end{aligned} \quad (17)$$

The wild sum vanishes as the extensions are identical at the wild primes and moreover $\eta(r_p)$ does not depend on the choice of the $\{\sigma_i\}$ and τ_p depends only on Γ and N_p .

Hence in $\bar{G}_{\oplus}(\mathbb{Z}\Gamma)$

$$\begin{aligned} &(\mathfrak{D}_N, a \mathfrak{D}_K \Gamma, 1) - (\mathfrak{D}_{N'}, a' \mathfrak{D}_{K'} \Gamma, 1) \\ &= \eta(r) - \eta'(r') + \eta(\det \zeta(a)) - \eta'(\det \zeta'(a')) \quad \text{by (9)} \\ &= (\tau) - \eta(\det \zeta(a)) - (y) - ((\tau') - \eta'(\det \zeta'(a')) - (y')) \quad \text{by (17)} \\ &\quad \text{(using the 2nd row of (7) to insert the (y)'s)} \\ &= \det(\lambda) - \det(\lambda') \in d(G_1(\mathfrak{D}\Gamma)) . \end{aligned}$$

Hence from (1) $[\mathfrak{D}_N] - [\mathfrak{D}_{N'}] = [a \mathfrak{D}_K \Gamma] - [a' \mathfrak{D}_{K'} \Gamma] = 0$ in $G_{\oplus}(\mathbb{Z}\Gamma)$.

REFERENCES

- [B] H. BASS, Algebraic K-theory, Benjamin.
- [F. T.] A. FRÖHLICH and M. J. TAYLOR, The arithmetic theory of Galois Gauss sums for tame characters, Phil. Trans. Royal Society London, 298 (141-181)
- [Q1] J. QUEYRUT, S-groupes des classes d'un ordre arithmétique, to appear in J. Alg.
- [Q2] J. QUEYRUT, Structure galoisienne des anneaux d'entiers d'extension sauvagement ramifiés, I, Annales Institut Fourier, fasc. 3, tome 31 (1981).
- [Wi] S. M. J. WILSON, Reduced norms in the K-theory of orders, J. Alg. 46 (1977), 1-11.

(texte reçu le 9 juillet 1981)

-:-:-:-

S. M. J. WILSON
 University of Durham
 Department of Mathematics
 Science Laboratories
 South Road
 G.-B. DURHAM DH1 3LE

THÉORIE D'IWASAWA DES TOURS MÉTABELIENNES

par

Jean-François JAULENT

-:-:-:-

Résumé

Soient ℓ un nombre premier impair, et K un corps abélien imaginaire de degré d , dont le groupe de Galois $\Delta = \text{Gal}(K/\mathbb{Q})$ est annulé par $(\ell-1)$.

Nous étudions les $\frac{d}{2} \mathbb{Z}_{\ell}$ -extensions N de K , galoisiennes mais non abéliennes sur $\mathbb{Q}$, qui sont associées aux caractères ℓ -adiques impairs χ du groupe Δ ; et nous considérons leurs ℓ -groupes de classes respectifs comme modules sur l'algèbre à produit croisé $\Theta = \mathbb{Z}_{\ell}[[\theta]] \circ [\Delta]$ du groupe de Galois Δ sur l'anneau d'Iwasawa $\mathbb{Z}_{\ell}[[\theta]]$, pour l'action de Δ sur θ définie par le caractère χ .

Nous montrons que tout Θ -module noethérien est pseudo-isomorphe à un Θ -module élémentaire, ce qui nous permet d'attacher aux ℓ -groupes de classes d'idéaux d'une telle tour d'extensions, des invariants λ_{φ} , μ_{φ} et ν_{φ} indexés par les caractères ℓ -adiques de Δ . L'étude des invariants ν_{φ} relève de la théorie des genres.

1. - Position du problème

Soient ℓ un nombre premier impair, et K un corps abélien imaginaire de degré d étranger avec ℓ , de groupe de Galois Δ . Nous supposons que l'exposant de Δ divise $(\ell - 1)$, ce qui apporte une simplification technique (les représentations de Δ étant réalisables sur $\mathbb{Q}_\ell$) mais cette restriction n'est pas indispensable au développement des considérations qui suivent.

D'après l'exactitude de la conjecture de Leopoldt pour les corps abéliens, le groupe de Galois $\text{Gal}(\check{K}/K)$ de la composée $\check{K}$ de toutes les $\mathbb{Z}_\ell$ -extensions de K est un $\mathbb{Z}_\ell$ -module libre de rang $\frac{d}{2} + 1$. Plus précisément, le résultat de Brumer [1], joint au résultat classique de Herbrand sur les unités, permet d'affirmer que la somme des deux représentations de Δ données respectivement par $\text{Gal}(\check{K}/K)$ et par le tensorisé $\mathbb{Z}_\ell \otimes_{\mathbb{Z}} U_K$ du groupe $U_K = E_K / \mu_K$ des unités de K modulo son sous-groupe de torsion, est égale à la représentation régulière ; ce qui s'écrit :

$$\text{Gal}(\check{K}/K) \oplus (\mathbb{Z}_\ell \otimes_{\mathbb{Z}} U_K) = \mathbb{Z}_\ell[\Delta].$$

En particulier, parmi les $\mathbb{Z}_\ell$ -extensions N de K , il en est exactement $\frac{d}{2} + 1$ qui sont galoisiennes sur $\mathbb{Q}$: ce sont la $\mathbb{Z}_\ell$ -extension cyclotomique, qui est abélienne sur $\mathbb{Q}$; et les $\frac{d}{2}$ $\mathbb{Z}_\ell$ -extensions non abéliennes indexées par les caractères ℓ -adiques χ de Δ qui prennent la valeur -1 sur la conjugaison complexe, lesquelles sont métabeliennes sur $\mathbb{Q}$. Pour chacune d'elles en effet, le groupe de Galois $\text{Gal}(N/\mathbb{Q})$ s'écrit comme produit semi-direct du groupe $\text{Gal}(N/K) \simeq \mathbb{Z}_\ell$ et de Δ , l'action de Δ sur $\mathbb{Z}_\ell$ étant définie par le caractère χ de Δ , conformément à l'identité :

$$\tau \eta \tau^{-1} = \eta^{\chi(\tau)}, \quad \text{pour tous } \eta \text{ de } \mathbb{Z}_\ell \text{ et } \tau \text{ de } \Delta.$$

Par exemple, si K est quadratique imaginaire, l'unique $\mathbb{Z}_\ell$ -extension de K qui est galoisienne mais non abélienne sur $\mathbb{Q}$ est la prodiédrale, étudiée dans [2].

Considérons donc une $\mathbb{Z}_\ell$ -extension N de K , métabelienne sur $\mathbb{Q}$, de caractère χ d'ordre n divisant d ; notons G son groupe de Galois, $\Gamma = \text{Gal}(N/K)$ le sous-groupe dérivé, isomorphe à $\mathbb{Z}_\ell$, puis Δ un relèvement de $\text{Gal}(N/\mathbb{Q})$ dans G et $H = \text{Ker } \chi$ le centre de G . Le quotient G/H

est en particulier un groupe métacyclique de centre trivial qui s'identifie au produit semi-direct de Γ par $T = \Delta/H$ pour l'action fidèle de T sur Γ définie par le caractère χ .

Faisons choix d'un générateur topologique γ de Γ et posons $\delta = \gamma - 1$. La théorie d'Iwasawa (cf. [3] et [8]) étudie le groupe de Galois $\mathbb{H}$ de la ℓ -extension $\hat{N}$ abélienne maximale non ramifiée sur N comme module sur l'algèbre formelle $\Lambda = \mathbb{Z}_\ell[[\delta]]$. Or, ici, le corps N étant supposé galoisien sur $\mathbb{Q}$, il en est de même de son extension $\hat{N}$ de sorte que le groupe $\mathbb{H}$ est aussi un $\mathbb{Z}_\ell[\Delta]$ -module. Pour tenir compte de ces deux structures, il est alors naturel d'introduire la résolvante :

$$\theta = \frac{1}{n} \sum_{\tau \in T} \chi(\tau^{-1}) (\gamma^{\chi(\tau)} - 1).$$

Il vient en effet :

LEMME. - La résolvante θ est un générateur de l'algèbre d'Iwasawa $\Lambda = \mathbb{Z}_\ell[[\delta]]$.

(i) Plus précisément, on a $\theta \equiv \delta \pmod{\delta^2}$ et donc $\Lambda = \mathbb{Z}_\ell[[\theta]]$.

(ii) Pour tout τ de Δ , on a $\tau \theta \tau^{-1} = \chi(\tau) \theta$.

Démonstration. - Pour toute racine n ième de l'unité r dans $\mathbb{Z}_\ell$, nous avons, par la formule du binôme :

$$\gamma^r - 1 = (1 + \delta)^r - 1 = \sum_{k \geq 1} \binom{r}{k} \delta^k.$$

Il suit :

$$\theta = \frac{1}{n} \sum_{\tau \in T} \chi(\tau^{-1}) (\gamma^{\chi(\tau)} - 1) = \delta + \sum_{k \geq 2} \left[\frac{1}{n} \sum_{\tau \in T} \chi(\tau^{-1}) \binom{\chi(\tau)}{k} \right] \delta^k$$

ce qui établit (i). L'assertion (ii) est immédiate.

Considérons par conséquent l'algèbre de groupe $\Theta = \mathbb{Z}_\ell[[\theta]] \cdot [\Delta]$ à coefficients dans l'anneau local complet $\mathbb{Z}_\ell[[\theta]]$, tordue par la relation :

$$\tau \theta \tau^{-1} = \chi(\tau) \theta, \text{ pour tout } \tau \text{ de } \Delta.$$

Les idempotents centraux $e_\Phi = \frac{1}{d} \sum_{\tau \in H} \Phi(\tau^{-1}) \tau$, attachés aux induits des caractères irréductibles du centre de G , donnent lieu à un isomorphisme d'algèbres :

$$\Theta = \mathbb{Z}_\ell[[\theta]] \cdot [\Delta] = \bigoplus_{\Phi \in H^*} \mathbb{Z}_\ell[[\theta]] \cdot [T] e_\Phi.$$

Le premier problème qui se pose est donc d'étudier l'algèbre à produit croisé $\Sigma = \mathbb{Z}_\ell[[\theta]] \cdot [T]$ du groupe cyclique T sur l'anneau d'Iwasawa $\Lambda = \mathbb{Z}_\ell[[\theta]]$.

2. - Description des Σ -modules projectifs de type fini

Rappelons que l'anneau d'Iwasawa $\Lambda = \mathbb{Z}_\ell[[\theta]]$ est un anneau local régulier complet de dimension 2, donc, en particulier, factoriel. Et l'algèbre Σ est une algèbre noethérienne de dimension n^2 sur son centre $C = \mathbb{Z}_\ell[[\theta^n]]$, qui admet $\Lambda = \mathbb{Z}_\ell[[\theta]]$ comme sous-algèbre commutative maximale. En effet, si $\tilde{C} = \mathbb{Q}_\ell((\theta^n))$ désigne le corps des fractions de C , le tensorisé $\tilde{\Sigma} = \tilde{C} \otimes_C \Sigma$ est une algèbre simple centrale sur $\mathbb{Q}_\ell((\theta^n))$, qui contient $\mathbb{Q}_\ell((\theta))$ comme sous-corps commutatif maximal.

Pour étudier les Σ -modules projectifs de type fini, introduisons les idempotents $e_\varphi = \frac{1}{n} \sum_{\tau \in T} \varphi(\tau^{-1}) \tau$, associés aux caractères ℓ -adiques irréductibles φ de T . Nous avons :

PROPOSITION 1. - Tout Σ -module projectif de type fini est somme directe essentiellement unique de Σ -modules projectifs indécomposables de type fini.
Plus précisément :

- (i) La décomposition de l'algèbre Σ est donnée par : $\Sigma = \bigoplus_{\varphi \in T^*} e_\varphi$.
- (ii) Il existe n classes d'isomorphie de Σ -modules noethériens projectifs et indécomposables ; elles sont représentées par les n modules Λe_φ .

Démonstration. - Le fait que tout Σ -module noethérien M s'écrive de façon essentiellement unique comme somme directe d'indécomposables résulte directement du théorème de Krull-Schmidt. Bien entendu, si M est projectif, il en est de même de ses facteurs directs.

(i) La décomposition directe de Σ est immédiate. Il suffit donc de vérifier que les modules Λe_φ sont indécomposables. Et cela résulte de ce que, si I est un Σ -module projectif noethérien et indécomposable, le tensorisé $\Omega_\ell(\theta^n) \otimes_C I$ est somme directe d'exemplaires de $\Omega_\ell(\theta)$.

(ii) D'après ce qui précède, il reste à montrer que deux modules Λe_φ et Λe_ψ associés à des caractères distincts, ne sont pas Σ -isomorphes. Or cela est clair, puisque si λe_ψ était l'image de e_φ dans un tel isomorphisme, λ serait inversible dans Λ , contrairement à l'identité $e_\psi \lambda e_\psi = 0$, qui entraîne $\lambda(0) = 0$.

SCOLIE. - Les Σ -modules noethériens qui sont Σ -projectifs sont exactement ceux qui sont C -projectifs.

Démonstration. - Le résultat sera acquis si nous montrons que tout Σ -module noethérien C -projectif M est facteur direct de son tensorisé $M_\Sigma = \Sigma \otimes_C M$.

Or, la suite exacte naturelle :

$$0 \longrightarrow \text{Ker } p \longrightarrow M_\Sigma \xrightleftharpoons[q]{p} M \longrightarrow 0, \text{ définie par } p(\sigma \otimes m) = \sigma m,$$

est scindée par l'application $q|_m \mapsto \sum_{\tau \in T} \tau^{-1} \otimes \tau m$.

PROPOSITION 2. - Tout idéal projectif de l'algèbre Σ s'écrit comme somme directe indécomposable d'idéaux principaux $\Lambda e_\varphi \lambda_\varphi$ avec $\lambda_\varphi \in \Lambda$.

En particulier, les idéaux de l'algèbre Λ qui sont des Σ -modules projectifs sont exactement les idéaux principaux ambiges, c'est-à-dire les idéaux $\ell^\mu \theta^\nu P(\theta^n) \Lambda$, où $P(\theta^n)$ est un polynôme distingué dans $\mathbb{Z}_\ell[\theta^n]$, de valuation nulle.

Démonstration. - D'après la proposition 1, tout idéal projectif I de l'algèbre Σ s'écrit comme somme directe d'idéaux indécomposables principaux $I_\varphi = \Lambda \alpha_\varphi$, avec $I_\varphi \simeq \Lambda e_\varphi$. Maintenant, pour chaque idéal I_φ , nous avons $e_\psi \alpha_\varphi \in I_\varphi$ pour tout caractère ψ , c'est-à-dire $e_\psi \alpha_\varphi = \varepsilon_\varphi(\psi) \alpha_\varphi$ avec $\varepsilon_\varphi(\psi) \in \Lambda$; puis, par orthogonalité des idempotents, $\varepsilon_\varphi(\psi) = 0$ pour tous les caractères, sauf un. Autrement dit, nous pouvons écrire $\alpha_\varphi = e_\varphi \lambda_\varphi$ avec $\lambda_\varphi \in \Lambda$; ce qui conduit à la décomposition annoncée.

D'autre part, si I est un idéal principal de Λ , le théorème de préparation de Weierstrass nous assure l'existence d'un unique générateur de I de la forme $\iota^\mu \theta^\nu Q(\theta)$ où $Q(\theta)$ est un polynôme distingué de valuation nulle. Cela étant, l'idéal I n'est un Σ -module que s'il est invariant par le groupe $T = \text{Gal}(\Lambda / C)$; autrement dit, lorsqu'à tout τ de T correspond une unité $u(\tau)$ de $\mathbb{Z}_\ell$ donnée par $u(\tau) \iota^\mu \theta^\nu Q(\theta) = \iota^\mu \chi^\nu(\tau) \theta^\nu Q(\chi(\tau) \theta)$. Egalant les termes constants, nous obtenons $u(\tau) = \chi^\nu(\tau)$; puis $Q(\chi(\tau) \theta) = Q(\theta)$, c'est-à-dire finalement $Q(\theta) = P(\theta^n)$, pour un polynôme distingué P de valuation nulle.

Notons qu'il vient $I e_\varphi = \Lambda e_{\varphi \chi^\nu} \iota^\mu \theta^\nu P(\theta^n)$, pour tout caractère φ , conformément à la première partie de la proposition.

COROLLAIRE. - Le groupe des idéaux Σ -projectifs de l'algèbre Λ est le groupe abélien libre engendré par les idéaux $\iota \Lambda$ et $\theta \Lambda$, et les idéaux $P(\theta^n) \Lambda$ associés aux polynômes distingués irréductibles de valuation nulle de l'algèbre $\mathbb{Z}_\ell[\theta^n]$.

3. - Classification des Σ -modules noethériens

Intéressons-nous maintenant aux Σ -modules noethériens sans hypothèse de projectivité. Un tel module M est en particulier un Λ -module de type fini, donc pseudo-isomorphe comme tel à une somme directe finie de quotients de Λ par des puissances d'idéaux premiers principaux.

Ceci nous amène à poser :

DÉFINITION. - Par Σ -module élémentaire, nous entendons toute somme directe finie d'exemplaires des n Σ -modules projectifs Λe_φ et de leurs quotients respectifs $\Lambda e_\varphi / \theta^\nu \Lambda e_\varphi$, ainsi que des quotients $\Lambda e_1 / \iota^\mu \Lambda e_1$ et $\Lambda e_1 P^e(\theta^n) \Lambda e_1$ associés aux polynômes distingués $P(\theta^n)$ de $\mathbb{Z}_\ell[\theta^n]$ qui sont irréductibles et de valuation nulle.

Cela étant, le résultat fondamental est le suivant :

THÉORÈME 1. - Tout Σ -module noethérien est Σ -pseudo-isomorphe à un unique Σ -module élémentaire.

Démonstration. - Commençons par établir l'existence d'une pseudo-décomposition. Considérons pour cela un Σ -module noethérien M ; faisons choix d'un système fini de générateurs de la forme $(e_{\varphi_i} m_i)_{i \in I}$, et écrivons M comme quotient d'un Σ -module projectif de type fini :

$$0 \longrightarrow R \longrightarrow \bigoplus_{i \in I} \Lambda e_{\varphi_i} m_i \longrightarrow M \longrightarrow 0.$$

Cela étant, le noyau R est Λ -engendré par un nombre fini de relateurs $(\sum_{i \in I} \lambda_{ij} e_{\varphi_i} m_i)_{j \in J}$; et comme nous avons pris soin de choisir des générateurs $e_{\varphi_i} m_i$ isotypiques, nous sommes assurés que les transformations admissibles sur les relateurs sont compatibles avec la Σ -structure. Autrement dit, à un Σ -pseudo-isomorphisme près, nous pouvons supposer que R est Λ -engendré par un système de relateurs de la forme $(\lambda_i e_{\varphi_i} m_i)_{i \in I'}$. Maintenant, d'après la proposition 2, les Λ -modules $\Lambda \lambda_i e_{\varphi_i} m_i$ ne sont des Σ -modules que si les λ_i engendrent autant d'idéaux principaux ambiges dans l'algèbre Λ . Ecrivant donc $\lambda_i \Lambda = \ell^{\mu_i} \theta^{\nu_i} \prod_{j \in J_i} P_{ij}^{e_{ij}} (\theta^n) \Lambda$ avec les $P_{ij}(\theta^n)$ distingués irréductibles dans $\mathbb{Z}_\ell[\theta^n]$ et de valuation nulle, nous obtenons :

$$M \sim \left\{ \bigoplus_{i \in I \setminus I'} \Lambda e_{\varphi_i} \right\} \oplus \left\{ \bigoplus_{i \in I'} (\Lambda e_{\varphi_i} / \ell^{\mu_i} \theta^{\nu_i} \prod_{j \in J_i} P_{ij}^{e_{ij}} (\theta^n) \Lambda e_{\varphi_i}) \right\} ;$$

puis finalement

$$M \sim \left\{ \bigoplus_{i \in I \setminus I'} \Lambda e_{\varphi_i} \right\} \oplus \left\{ \bigoplus_{i \in I'} [(\Lambda e_{\varphi_i} / \ell^{\mu_i} \Lambda e_{\varphi_i}) \oplus (\Lambda e_{\varphi_i} / \theta^{\nu_i} \Lambda e_{\varphi_i}) \oplus (\bigoplus_{j \in J_i} \Lambda e_{\varphi_i} / P_{ij}^{e_{ij}} (\theta^n) \Lambda e_{\varphi_i})] \right\} ;$$

de sorte que la pseudo-décomposition annoncée sera établie si nous montrons que deux modules $\Lambda e_{\varphi} / I e_{\varphi}$ avec $I = \ell^{\mu} \Lambda$ ou $I = P(\theta^n) \Lambda$ attachés à des caractères différents sont néanmoins pseudo-isomorphes. Or cela résulte de ce que, pour tout caractère φ , le quotient $(\theta \Lambda e_{\varphi} + I e_{\varphi}) / I e_{\varphi}$ est un sous-module d'indice fini de $\Lambda e_{\varphi} / I e_{\varphi}$, qui est isomorphe à $\theta \Lambda e_{\varphi} / \theta I e_{\varphi}$, c'est-à-dire à $\Lambda e_{\varphi \chi} / I e_{\varphi \chi}$.

Pour ce qui est de l'unicité, renvoyons à l'appendice pour une démonstration complète et contentons-nous de vérifier ici que les Σ -modules élémentaires indécomposables énumérés dans la définition sont bien deux à deux non pseudo-isomorphes : compte tenu du résultat classique sur les Λ -modules, il nous suffit de remarquer que s'il existait pour $\varphi \neq \psi$ un pseudo-isomorphisme f de Λe_φ dans Λe_ψ (ou de $\Lambda e_\varphi / \theta^\nu \Lambda e_\varphi$ dans $\Lambda e_\psi / \theta^\nu \Lambda e_\psi$) ce ne pourrait être que l'homothétie associée à un élément λ de Λ non multiple de θ ; ce qui contredirait l'identité $e_\psi \lambda e_\psi = e_\psi f(e_\varphi) = 0$.

4. - φ -composantes d'un Σ -module noethérien

Soit M un Σ -module noethérien. Nous disons qu'il est de torsion lorsque sa pseudo-décomposition élémentaire ne comporte aucun facteur projectif Λe_φ , c'est-à-dire lorsque M est Σ -pseudo-isomorphe à un module :

$$M \sim \left[\bigoplus_{\varphi \in T^*} \bigoplus_{i \in \mathcal{I}_\varphi} \Lambda e_\varphi / \theta^{\nu_i} \Lambda e_\varphi \right] \oplus \left[\bigoplus_{j \in \mathcal{J}} \Lambda e_1 / \iota^{\mu_j} \Lambda e_1 \right] \oplus \left[\bigoplus_{k \in \mathcal{K}} \Lambda e_1 / P_k^{\epsilon_k}(\theta^n) \Lambda e_1 \right].$$

L'unicité d'une telle écriture nous conduit à poser :

DÉFINITION. - Nous appelons polynôme caractéristique d'un Σ -module noethérien de torsion M , le produit $\chi_\Sigma(M) = \left[\prod_{\varphi \in T^*} \theta_\varphi^{\nu_\varphi} \right] \iota^\mu P(\theta^n)$ des dénominateurs intervenant dans sa pseudo-décomposition élémentaire. Nous disons que l'indice $\nu_\varphi = \sum_{i \in \mathcal{I}_\varphi} \nu_i$ représente la θ_φ -valuation de $\chi_\Sigma(M)$; et nous notons $\nu = \sum_{\varphi \in T^*} \nu_\varphi$ la valuation totale, $\lambda \equiv \nu \pmod{n}$ le degré de $\chi_\Sigma(M)$ et μ sa ι -valuation.

Bien entendu, le polynôme caractéristique $\chi_\Lambda(M)$ de M comme Λ -module s'obtient en identifiant à θ dans $\chi_\Sigma(M)$ les n indéterminées θ_φ . Et réciproquement il est immédiat d'écrire $\chi_\Sigma(M)$ à partir de $\chi_\Lambda(M)$ dès que sont connus les indices ν_φ .

Ceci nous amène à considérer les φ -composantes d'un Σ -module M .

Pour tout caractère φ dans T^* , le projecteur associé à l'idempotent e_φ est un C -endomorphisme de M , ce qui permet d'écrire M comme somme directe de n C -modules :

$$M = \bigoplus_{\varphi \in T^*} e_\varphi M.$$

Cela étant, puisque deux modules Σ -pseudo-isomorphes ont clairement des φ -composantes respectives C -pseudo-isomorphes, il suffit pour étudier celles-ci de se limiter au cas où M est un Σ -module élémentaire indécomposable.

Il vient alors :

PROPOSITION 3. - Soit M un Σ -module élémentaire indécomposable.

(i) Si M s'écrit $\Lambda e_1 / \ell^\mu \Lambda e_1$, ses φ -composantes sont toutes C -isomorphes à $C / \ell^\mu C$;

(ii) Si M s'écrit $\Lambda e_1 / P^e (\theta^n) \Lambda e_1$, ses φ -composantes sont toutes C -isomorphes à $C / P^e (\theta^n) C$;

(iii) Si M s'écrit $\Lambda e_\psi / \theta^\nu \Lambda e_\psi$, sa φ -composante est donnée par $e_\varphi M \simeq C / \theta^{n\pi} C$ avec $\pi = [(\nu - \sigma) / n]$, où $\sigma \in \{0, 1, \dots, n-1\}$ est défini par $\varphi \psi^{-1} = \chi^\sigma$.

Démonstration. - L'identité $\tau \theta^k e_1 = \chi^k(\tau) \theta^k e_1$ qui définit l'action de T sur Λe_1 nous donne immédiatement :

$$e_{\chi^\sigma} \Lambda e_1 = \theta^\sigma e_1 \Lambda e_1 = \theta^\sigma C e_1, \text{ pour } \sigma = 0, 1, \dots, n-1.$$

La proposition en résulte.

Il est d'ailleurs possible de comparer directement les φ -composantes d'un Σ -module M au moyen de la relation de décalage $e_{\varphi\chi} \theta = \theta e_\varphi$ donnée par l'opérateur θ . Il vient ainsi :

PROPOSITION 4. - Pour tout Σ -module M , l'opérateur θ donne lieu à une suite exacte de C -modules :

$$0 \longrightarrow e_\varphi \text{Ker } \theta \longrightarrow e_\varphi M \xrightarrow{\theta} e_{\varphi\chi} M \longrightarrow e_{\varphi\chi} \text{Coker } \theta \longrightarrow 0.$$

Les résultats de la proposition 3 peuvent donc s'interpréter à l'aide du tableau suivant :

M	$\Lambda e_1 / \ell^\mu \Lambda e_1$	$\Lambda e_1 / P^\theta(\theta^n) \Lambda e_1$	$\Lambda e_\varphi \theta^\nu \Lambda e_\varphi$
Ker θ	0	0	$\mathbb{Z}_\ell e_\varphi \chi^{\nu-1}$
Coker θ	pseudo-nul	pseudo-nul	$\mathbb{Z}_\ell e_\varphi$.

Pour tout naturel m , introduisons les éléments $\omega_m = \gamma^{\ell^m} - 1$ puis $\xi_m = \frac{\omega_m}{\omega_{m-1}}$, qui engendrent autant d'idéaux ambiges de l'algèbre Λ . Nous pouvons enfin énoncer :

THÉORÈME 2. - Soient M un Σ -module de torsion de type fini et V un sous- $\mathbb{Z}_\ell$ -module noethérien de M, tel que les quotients $M/\xi_m(\theta M + V)$ soient d'ordre fini ℓ^{e_m} pour tout m. Alors, pour tout caractère φ de T, l'ordre $\ell^{e_\varphi m}$ de la φ -composante du quotient $M/\xi_m(\theta M + V)$ est donné par la formule :

$$e_m^\varphi = \mu \frac{\ell^m - 1}{n} + \lambda_\varphi m + o_\varphi(m),$$

où μ et λ_φ sont indépendants de m , et $o_\varphi(m)$ constant pour m assez grand.

Démonstration. - Notons $\chi_\Sigma(M) = \left[\prod_{\varphi \in T^*}^{\nu} \theta_\varphi^\varphi \right] \ell^\mu P(\theta^n)$ le polynôme caractéristique de M et $\mathfrak{d}$ le degré de P. Nous savons, par la théorie d'Iwasawa (cf. [3] et [7]), que l'indice e_m est donné par la relation :

$$e_m = \mu \ell^m + \lambda m + o(m), \quad \text{avec } \lambda = \mathfrak{d}n + \nu.$$

Le théorème résulte alors des propositions 3 et 4 qui donnent immédiatement :

$$e_m = \mu \frac{\ell^m - 1}{n} + (\mathfrak{d} + \pi_\varphi) m + o_\varphi(m),$$

l'indice π_φ étant calculé comme dans la proposition 3 (iii).

5. - Application au ℓ -groupe des classes $\mathcal{H}$

Nous reprenons les notations de la première partie. En particulier, χ désigne un caractère ℓ -adique impair du groupe de Galois Δ d'un corps abélien imaginaire K de degré d , et N l'unique $\mathbb{Z}_\ell$ -extension de K , galoisienne sur $\mathbb{Q}$, qui lui est associée.

Nous notons Γ le groupe de Galois $\text{Gal}(N/K)$, isomorphe à $\mathbb{Z}_\ell$; et, pour tout naturel m , nous désignons par K_m le sous-corps de N , métabélien de degré $d\ell^m$ sur $\mathbb{Q}$, qui est fixé par Γ^{ℓ^m} , puis par $\hat{K}_m$ son ℓ -corps de classes de Hilbert, qui est galoisien sur $\mathbb{Q}$. Nous nous intéressons au groupe de Galois $\mathcal{H} = \text{Gal}(\hat{N}/N)$ de la ℓ -extension abélienne maximale non ramifiée $\hat{N}$ de N : le corps $\hat{N}$ est la réunion des $\hat{K}_m$, de sorte que par l'application de réciprocité du corps de classes, le groupe $\mathcal{H}$ s'identifie à la limite :

$$\mathcal{H} = \varprojlim \mathcal{H}_m,$$

du système projectif des ℓ -groupes de classes respectifs des corps K_m , pour les applications normes.

Le groupe $\mathcal{H}$ est ainsi un $\mathbb{Z}_\ell[[\Theta]] \rtimes [\Delta]$ -module noethérien de torsion, et c'est comme tel que nous nous proposons de l'étudier. Suivant l'usage, nous notons $\mathcal{H}$ multiplicativement, en faisant opérer exponentiellement les groupes de Galois. Cela étant pour tout idempotent central e_Φ de l'algèbre $\Theta = \mathbb{Z}_\ell[[\Theta]] \rtimes [\Delta]$, la Φ -composante $\mathcal{H}^{e_\Phi}$ du groupe $\mathcal{H}$ est un Σ -module à droite auquel nous pouvons appliquer les résultats de structure qui précèdent.

En particulier, reformulant le théorème 2, nous obtenons :

THÉORÈME 3. - Soient ℓ un nombre premier impair, K un corps abélien imaginaire dont le groupe de Galois Δ est annulé par $(\ell-1)$, puis χ un caractère ℓ -adique impair de Δ , et N l'unique $\mathbb{Z}_\ell$ -extension de K , galoisienne sur $\mathbb{Q}$, qui est associée à χ . Alors pour tout caractère ℓ -adique φ de Δ , il existe des entiers μ_φ , λ_φ et α_φ tels que, pour tout naturel m assez grand, l'ordre ℓ^{e_φ} de la φ -composante du ℓ -groupe des classes $\mathcal{H}_m$ du sous-corps K_m de N cyclique de degré ℓ^m sur K , soit donné par l'identité :

$$e_\varphi^m = \mu_\varphi \frac{\ell^m - 1}{n} + \lambda_\varphi m + \alpha_\varphi.$$

Dans cette formule, l'entier n est l'ordre du caractère χ et l'indice μ_φ ne dépend que de la restriction de φ au noyau $\text{Ker } \chi$.

Maintenant, une première approche de la Θ -structure du groupe $\mathcal{H}$ consiste à introduire le sous-groupe $\mathcal{H}_\ell$, limite projective des groupes $\mathcal{H}_\ell(K_m)$ engendrés par les classes des idéaux au-dessus de ℓ : Par l'isomorphisme de réciprocité du corps de classes, le quotient $\mathcal{H}' = \mathcal{H}/\mathcal{H}_\ell$ s'identifie, en effet, au groupe de Galois $\text{Gal}(\hat{N}'/N)$ de la ℓ -extension abélienne maximale non ramifiée de N , où les places au-dessus de ℓ se décomposent complètement. Et, d'autre part, si K_{m_0} est le corps de décomposition dans N/K des places au-dessus de ℓ , le groupe $\Gamma_\ell^{m_0}$ opère trivialement sur $\mathcal{H}_\ell$ de sorte que celui-ci est annulé par l'opérateur $w_{m_0} = \gamma_\ell^{m_0} - 1$. Autrement dit, dans la pseudo-décomposition du Θ -module $\mathcal{H}_\ell$, ne peuvent figurer au dénominateur que les idéaux $\xi_i \Lambda$, pour $i = 0, \dots, m_0$ (cf. [4], th. 9). Plus précisément, si D désigne le groupe de décomposition de ℓ dans K et $\Gamma_{m_0} = \Gamma/\Gamma_\ell^{m_0}$ le groupe de Galois $\text{Gal}(K_{m_0}/K)$, le tensorisé $\mathcal{D}_\ell(K_{m_0}) = \mathbb{Z}_\ell \otimes_{\mathbb{Z}} \mathcal{D}_\ell(K_{m_0})$, du sous-groupe d'idéaux de K_{m_0} engendré par les places au-dessus de ℓ , s'écrit comme Θ -module :

$$\mathcal{D}_\ell(K_{m_0}) = \mathbb{Z}_\ell[\Gamma_{m_0}] \cdot [D] \simeq \bigoplus_{\varphi(D) \neq 1} \Lambda e_\varphi / w_{m_0} \Lambda e_\varphi.$$

Et il vient donc, avec les notations du théorème 3 :

THÉORÈME 4. - Soient D le groupe de décomposition de ℓ dans K , et K_{m_0} son sous-corps de décomposition dans N/K . Le sous-groupe $\mathcal{H}_\ell$, engendré dans $\mathcal{H}$ par les places au-dessus de ℓ , est un Θ -module de torsion pseudo-isomorphe comme tel à un facteur direct de la somme :

$$\bigoplus_{\varphi(D) \neq 1} \bigoplus_{i=0}^{m_0} \Lambda e_\varphi / \xi_i \Lambda e_\varphi = \bigoplus_{\varphi(D) \neq 1} \left[(\Lambda e_\varphi / \theta \Lambda e_\varphi) \oplus \left(\bigoplus_{i=1}^{m_0} \Lambda e_\varphi / \xi_i \Lambda e_\varphi \right) \right].$$

COROLLAIRE. - Sous les hypothèses du théorème 3, il existe des entiers
 $\mu'_\varphi = \mu_\varphi$, λ'_φ et o'_φ tels que, pour tout naturel m assez grand, l'ordre ℓ^m
de la φ -composante du groupe de Galois $H'_m = \text{Gal}(\hat{K}'_m/K_m)$ de la ℓ -extension
abélienne maximale non ramifiée de K_m , où les places au-dessus de ℓ se
décomposent totalement, soit donné par l'identité :

$$e_m^{\ell, \varphi} = \mu'_\varphi \frac{\ell^m - 1}{n} + \lambda'_\varphi m + o'_\varphi.$$

Démonstration. - D'après le théorème 4, l'invariant μ_Ω attaché au sous-groupe
 H_Ω est nul ; de là l'égalité $\mu'_\varphi = \mu_\varphi$, pour tout caractère φ .

SCOLIE. - Pour tout idempotent central e_Φ de l'algèbre Θ , l'indice
 $\lambda_\Phi = \sum_{\varphi|\Phi} \lambda_\varphi$ vérifie la congruence :

$$\lambda_\Phi \equiv \nu_\Phi \pmod{n},$$

où ν_Φ désigne la valuation du polynôme caractéristique $\chi_\Lambda(H_\Phi^{e_\Phi})$.

Un résultat analogue vaut pour λ'_Φ .

C'est immédiat, d'après l'écriture du polynôme caractéristique ; ce qui généralise le résultat donné par R. Gillard dans le cas prodiédral (cf. [2]).

Bien entendu, contrairement à ce qui se passe pour μ , les indices λ_φ attachés à des caractères qui coïncident sur le noyau $\text{Ker } \chi$ ne sont pas, en général, égaux. Plus précisément, la suite exacte de la proposition 4, appliquée au groupe H , faisant apparaître le sous-groupe ambige Ω et le quotient des genres $\mathcal{G}$, la comparaison des indices λ_φ se ramène essentiellement à un problème de théorie des genres dans l'extension procyclique N/K (cf. [5]).

6. - Appendice

Nous complétons, dans ce qui suit, la démonstration du théorème 1, en établissant l'unicité dans la pseudo-décomposition d'un Σ -module.

Considérons donc un Σ -module noethérien M ; supposons le pseudo-isomorphe à deux Σ -modules élémentaires E et E' ; et faisons choix d'un multiple commun assez grand $\kappa \in \mathbb{Z}_\ell[\theta^n]$ des polynômes caractéristiques $\chi_\Lambda(E)$ et $\chi_\Lambda(E')$.

Cela étant, dans la suite exacte courte :

$$0 \longrightarrow \text{Ker } \kappa \longrightarrow M \xrightarrow{\kappa} \text{Im } \kappa \longrightarrow 0 ,$$

le noyau $N = \text{Ker } \kappa$ est alors pseudo-isomorphe aux sous-modules de Λ -torsion $T(E)$ et $T(E')$ et l'image $I = \text{Im } \kappa$ aux modules projectifs $E/T(E)$ et $E'/T(E')$.

a) Partie projective

Comme tout pseudo-isomorphisme arrivant dans un Σ -module projectif (et donc sans $\mathbb{Z}_\ell$ -torsion) contient dans son noyau les éléments d'ordre fini et ceux-là seulement, nous pouvons, quitte à remplacer κ par un multiple convenable, supposer que I s'injecte avec un conoyau fini dans $E/T(E)$ comme dans $E'/T(E')$. Ecrivons alors $E/T(E) = \bigoplus_{j \in J} \Lambda e_{\varphi_j}$. D'après ce qui précède, le quotient $I/\theta I$ est isomorphe à un sous-module d'indice fini de la somme directe $\bigoplus_{j \in J} \mathbb{Z}_\ell e_{\varphi_j}$. Le théorème de la base adaptée appliqué à l'anneau principal semi-local $\mathbb{Z}_\ell[T]$ nous donne l'isomorphisme $I/\theta I \simeq \bigoplus_{j \in J} \mathbb{Z}_\ell e_{\varphi_j}$; ce qui entraîne $E/T(E) \simeq E'/T(E')$ comme annoncé.

b) Partie de torsion

Notons $T(N)$ le sous-module fini engendré par les noyaux des pseudo-isomorphismes de N dans $T(E)$ et $T(E')$. Le quotient $N/T(N)$ s'injecte alors avec un conoyau fini dans $T(E)$ comme dans $T(E')$, et il est alors facile de construire un pseudo-isomorphisme injectif de $T(E)$ dans $T(E')$; par exemple, en remarquant que si $T(E)$ s'écrit :

$$T(E) = \left[\bigoplus_{j \in \mathcal{J}} \Lambda e_{\varphi_j} / \theta^{\nu_j} \Lambda e_{\varphi_j} \right] \oplus \left[\bigoplus_{k \in \mathcal{K}} \Lambda e_1 / \mathfrak{p}_k^k e_1 \right] ,$$

le sous-module d'indice fini :

$$T'(E) = \ell^h \left[\bigoplus_{j \in \mathcal{J}} \Lambda e_{\varphi_j} / \theta^{\nu_j} \Lambda e_{\varphi_j} \right] \oplus \theta^{nh} \left[\bigoplus_{k \in \mathcal{K}} \Lambda e_1 / \mathfrak{P}_k^k e_1 \right],$$

est isomorphe à $T(E)$, et contenu dans l'image de N pour h assez grand.

c) Localisation

Il reste donc à établir qu'un module de torsion élémentaire, qui s'injecte avec un conoyau fini dans un autre, lui est nécessairement identique. Or, pour toute suite exacte à conoyau fini :

$$0 \longrightarrow \bigoplus_{i \in \mathcal{J}} \Lambda e_{\varphi_i} / \mathfrak{P}_i^{\nu_i} e_{\varphi_i} \longrightarrow \bigoplus_{i \in \mathcal{J}'} \Lambda e_{\varphi_i} / \mathfrak{P}_i^{\nu_i} e_{\varphi_i},$$

la multiplication par un élément convenable de C , étranger à un $\mathfrak{P}_{i_0}$ donné, conduit à une suite exacte à conoyau fini :

$$0 \longrightarrow \bigoplus_{\substack{i \in \mathcal{J} \\ \mathfrak{P}_i = \mathfrak{P}_{i_0}}} \Lambda e_{\varphi_i} / \mathfrak{P}_{i_0}^{\nu_i} e_{\varphi_i} \longrightarrow \bigoplus_{\substack{i \in \mathcal{J}' \\ \mathfrak{P}_i = \mathfrak{P}_{i_0}}} \Lambda e_{\varphi_i} / \mathfrak{P}_{i_0}^{\nu_i} e_{\varphi_i}.$$

De plus, puisque le quotient $\Lambda / \mathfrak{P}_{i_0}$ est infini, le plus petit entier ν_0 tel que $\mathfrak{P}_{i_0}^{\nu_0}$ annule l'un, et donc l'autre, des termes de cette dernière suite, est la borne supérieure commune des indices ν_i lorsque i décrit $\mathcal{J}$ ou $\mathcal{J}'$, avec la restriction $\mathfrak{P}_i = \mathfrak{P}_{i_0}$.

La démonstration se poursuit alors par récurrence sur le nombre de termes dans chacune des sommes directes, en distinguant deux cas :

- si $\mathfrak{P}_{i_0}$ est l'idéal premier engendré par θ , il faut tenir compte de l'action de θ sur les idempotents e_{φ} . C'est ainsi que par action de l'opérateur θ^{ν_0-1} , nous obtenons la suite exacte à conoyau fini :

$$0 \longrightarrow \bigoplus_{\substack{i \in \mathcal{J} \\ \mathfrak{P}_i = \mathfrak{P}_{i_0} ; \nu_i = \nu_0}} \mathbb{Z}_{\ell} e_{\varphi_i} \chi^{\nu_0-1} \longrightarrow \bigoplus_{\substack{i \in \mathcal{J}' \\ \mathfrak{P}_i = \mathfrak{P}_{i_0} ; \nu_i = \nu_0}} \mathbb{Z}_{\ell} e_{\varphi_i} \chi^{\nu_0-1},$$

et les termes $\Lambda e_{\varphi_i} / \mathfrak{P}_i^{\nu_0} e_{\varphi_i}$ dans $T(E)$ et $T(E')$ sont associés aux mêmes caractères,

- sinon, la démonstration n'est rien plus que la démonstration classique.

BIBLIOGRAPHIE

- [1] A. BRUMER, On the units of algebraic number fields, Mathematika 14 (1967), 121-124.
- [2] R. GILLARD, Remarques sur certaines extensions prodiédrales de corps de nombres, C.R. Acad. Sc. Paris 282 (1976).
- [3] K. IWASAWA, On Γ -extensions of algebraic number fields, Bull. Amer. Math. Soc. 65 (1959), 183-226.
- [4] K. IWASAWA, On $\mathbb{Z}_\ell$ -extensions of algebraic number fields, Ann. of Math. 98 (1973), 243-326.
- [5] J.-F. JAULENT, Sur la théorie des genres dans une extension procyclique, métabélienne sur un sous-corps (à paraître).
- [6] S. LANG, Cyclotomic fiels (ch. 5), Springer-Verlag (1978).
- [7] B. ORIAT, Introduction à la théorie d'Iwasawa, Pub. Math. Fac. Sci. Besançon (1980-1981).
- [8] J.-P. SERRRE, Classes des corps cyclotomiques, d'après Iwasawa, Sémin. Bourbaki 174 (1958).

(texte reçu le 4 mai 1981)

--:--:--

Jean-François JAULENT
 E. R. A. n° 070 654
 Université de Franche Comté
 Faculté des Sciences
 Mathématiques
 F 25030 BESANÇON CEDEX

SÉRIES DE DIRICHLET

par

Pierrette CASSOU-NOGUÈS

-:-:-:-

La fonction zêta de Riemann est définie pour $\text{Re}(s) > 1$ par

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s}.$$

Cette série se prolonge à tout le plan complexe, en une fonction méromorphe ayant un seul pôle pour $s=1$ et pour tout entier $k > 0$

$$\zeta(1-k) = -\frac{b_k}{k}$$

où b_k est le k -ième nombre de Bernoulli. Donc, pour tout entier $k > 0$, $\zeta(1-k) \in \mathbb{Q}$.

Soit K un corps de nombres quelconque et $\zeta_K(\cdot)$ sa fonction zêta de Dedekind. Shintani a montré que l'on pouvait écrire $\zeta_K(\cdot)$ comme une somme finie de séries de la forme

$$\sum_{m \in \mathbb{N}^r} \prod_{i=1}^n L_i(m)^{-s}$$

$$L_i(X) = v_{1i} X_1 + \dots + v_{ri} X_r + a_i.$$

Il a montré [10] que ces séries se prolongeaient à tout le plan complexe en des fonctions méromorphes dont tous les pôles se trouvent sur la droite réelle et qui prennent des valeurs rationnelles sur les entiers négatifs ou nuls. Ceci lui permet de retrouver le fait que $\zeta_X(1-k) \in \mathbb{Q}$ pour tout entier $k > 0$ (Siegel [9], Klingen [7]).

Soit maintenant $P \in \mathbb{C}[X_1, \dots, X_r]$ tel que $\operatorname{Re}(P(t_1, \dots, t_r)) > 0$ pour tout $(t_1, \dots, t_r) \in \mathbb{R}_+^r(t_1, \dots, t_r) \neq (0, \dots, 0)$. Soit $Q \in \mathbb{C}[X_1, \dots, X_r]$; considérons

$$Z(P, Q)(s) = \sum_{n \in \mathbb{N}^{*r}} Q(n) P(n)^{-s}$$

Il existe $\sigma_0 > 0$ tel que cette série soit absolument convergente pour $\operatorname{Re}(s) > \sigma_0$ et Mellin [8] a montré qu'une telle série se prolonge à tout le plan complexe en une fonction méromorphe dont tous les pôles sont sur la droite réelle. Deux questions se posent alors

- Peut-on calculer les valeurs aux entiers négatifs ?
- Lorsque l'on peut les calculer, ces valeurs sont-elles dans le corps engendré sur $\mathbb{Q}$ par les coefficients de P et Q ?

On peut calculer les valeurs aux entiers négatifs de $Z(P, Q)(.)$ lorsque P satisfait la condition suivante que nous noterons "condition *". Ecrivons :

$$P(X_1, \dots, X_r) = P_\alpha(X_1, \dots, X_r) + P_{\alpha-1}(X_1, \dots, X_r) + \dots + P_0(X_1, \dots, X_r)$$

où $P_i(X_1, \dots, X_r)$ est un polynôme homogène de degré i .

Alors $\operatorname{Re}(P_\alpha(t_1, \dots, t_r)) > 0$ pour tout $(t_1, \dots, t_r) \in \mathbb{R}_+^r(t_1, \dots, t_r) \neq (0, \dots, 0)$.

On constate alors que les valeurs aux entiers négatifs n'appartiennent pas toujours au corps engendré par les coefficients du polynôme.

Exemple :

$$P(X_1, X_2) = X_1^4 + X_2^4 + X_1 X_2$$

$$Z(P, 1)(0) = \frac{\pi}{8}.$$

Le but de cet article est de lier la nature de ces valeurs à la géométrie de certaines hypersurfaces définies à partir de P .

Dans toute la suite, nous fixons P satisfaisant la condition $*$. Nous supposons en outre P homogène. On note K le corps engendré sur $\mathbb{Q}$ par les coefficients de P et les racines α -ièmes de l'unité. On étudie pour tout polynôme $Q \in K[X_1, \dots, X_r]$

$$Z(P, Q)(\cdot).$$

Cette série se prolonge en une fonction holomorphe sur $\mathbb{C}$ sauf aux points $s = k/\alpha$ où $k \in \mathbb{Z}$ tel que $k \leq \deg Q + r$ et $-s \notin \mathbb{N}$, où elle peut avoir des pôles simples.

On convient de noter

$$Z(P, Q)\left(\frac{k}{\alpha}\right)$$

pour désigner soit le résidu de $Z(P, Q)(\cdot)$ si cette fonction a effectivement un pôle pour $s = \frac{k}{\alpha}$, soit la valeur au point $s = \frac{k}{\alpha}$ lorsque $-s \in \mathbb{N}$.

On définit δ le K -espace vectoriel engendré par les $Z(P, Q)(\frac{k}{\alpha})$ lorsque Q parcourt $K[X_1, \dots, X_r]$ et lorsque $k \in \mathbb{Z}$, $k \leq \frac{\deg Q + r}{\alpha}$ (on trouve donc ici, les valeurs aux entiers négatifs ou nuls et les pôles pour s entier $0 \leq s \leq \frac{\deg Q + r}{\alpha}$).

On obtient le résultat suivant :

THÉORÈME 1. - δ est de dimension inférieure ou égale à α^{r-1} et un système de générateurs est donné par

$$Z(P, X_1^{v_1-1} \dots X_r^{v_r-1}) \left(\frac{\sum_{i=1}^r v_i}{\alpha} \right)$$

où $(v_1, \dots, v_r)$ parcourt les r -uplets de $\mathbb{Z}$ tels que

$$\sum_{i=1}^r v_i \equiv 0(\alpha) \text{ et } 0 < v_i \leq \alpha.$$

Remarques

i) Les valeurs $Z(P, X_1^{v_1-1} \dots X_r^{v_r-1}) \left(\frac{\sum_{i=1}^r v_i}{\alpha} \right)$ sont en fait les résidus de $Z(P, X_1^{v_1-1} \dots X_r^{v_r-1})(\cdot)$ sur sa droite de convergence.

ii) On connaît des cas où la dimension de δ est strictement inférieure à α^{r-1} . Par exemple dans le cas où P est un produit de formes linéaires (séries de Shintani) elle est égale à 1.

Nous étudions ensuite la nature de ces générateurs.

Nous supposons maintenant que la variété projective V définie par l'annulation de P est non singulière et en position générale par rapport aux axes de coordonnées, ce qui signifie que les formes $X_i \frac{\partial P}{\partial X_i}$ n'ont pas de zéro commun différent de $(0, \dots, 0)$. On définit sur $K[X_1, \dots, X_r]$ $\mathcal{J}_A$ par

$$\mathcal{J}_A(X_i) = \begin{cases} 0 & \text{si } i \notin A \\ X_i & \text{si } i \in A \end{cases}.$$

Notons $P_A = \mathcal{J}_A(P)$ et V_A la variété définie par l'annulation de P_A .

THÉORÈME 2. - Les éléments de δ sont des combinaisons à coefficients dans K de π -fois des "périodes" sur les variétés V_A , de 1 et de π .

Remarques

i) On obtient des résultats analogues en considérant les résidus. On définit δ_i le K -espace vectoriel engendré par les

$$Z(P, Q) \binom{k}{\alpha} \quad k \in \mathbb{Z}, \quad k \leq \deg Q + r$$

avec $k \equiv i(\alpha)$, pour tout $0 < i < \alpha$.

ii) Si l'on considère

$$Z(P, Q, \xi)(s) = \sum^n Q(n) \xi^n P(n)^{-s}$$

où $\xi = (\xi_1, \dots, \xi_r) \in \mathbb{C}^r$ et $|\xi_i| \leq 1$, $\xi_i \neq 1$ pour tout $i \in \{1, \dots, r\}$, alors

$Z(P, Q, \xi)(.)$ a un prolongement holomorphe sur $\mathbb{C}$ et pour tout entier $k \geq 0$

$$Z(P, Q, \xi)(-k) \in K(\xi)$$

$K(\xi)$ étant le corps engendré sur K par les ξ_i .

I. - Préliminaires

Tous les résultats qui vont suivre reposent sur le théorème 0 qui donne une forme adéquate des résidus aux pôles et des valeurs aux entiers négatifs.

Notons J la forme $\mathbb{C}$ -linéaire définie sur $\mathbb{C}[X_1, \dots, X_r]$ par

$$J(X_1^{i_1} \dots X_r^{i_r}) = b_{i_1} \dots b_{i_r}.$$

THÉORÈME 0. - Soit un polynôme P satisfaisant l'hypothèse $*$. Pour tout polynôme $Q \in \mathbb{C}[X_1, \dots, X_r]$ et tout entier $k \in \mathbb{Z}$, $k \leq \deg Q + r$, il existe un polynôme $S_{k,Q} \in \mathbb{C}[X_1, \dots, X_r]$ tel que

$$\lim_{s \rightarrow k/\alpha} (s - \frac{k}{\alpha}) \Gamma(s) Z(P, Q)(s) = J(S_{k,Q})$$

On a des formules explicites.

Notons

$$P(X_1, \dots, X_r, Y) = P_\alpha(X_1, \dots, X_r) + Y P_{\alpha-1}(X_1, \dots, X_r) + \dots + Y^\alpha P_0(X_1, \dots, X_r)$$

où P_i est le polynôme homogène de degré i tel que

$$P(X_1, \dots, X_r) = P_\alpha(X_1, \dots, X_r) + P_{\alpha-1}(X_1, \dots, X_r) + \dots + P_0(X_1, \dots, X_r).$$

On peut toujours supposer que Q est un polynôme homogène. Pour tout $(x_1, \dots, x_r, t) \in \mathbb{R}^{r+1}$

$$S(x_1, \dots, x_r, t) = \int_{x_1 t}^{\infty} \dots \int_{x_r t}^{\infty} Q(t_1, \dots, t_r) e^{-t^2(t_1, \dots, t_r, t)} dt_1 \dots dt_r.$$

Alors $S_{k,Q}$ est le polynôme associé à la fonction polynôme

$$S_{k,Q}(x_1, \dots, x_r) = \frac{1}{(\deg Q + r - k)!} \left(\frac{d}{dt} \right)^{\deg Q + r - k} S(x_1, \dots, x_r, t) \Big|_{t=0}.$$

On peut montrer que le polynôme $S_{k,Q}$ défini par le théorème 0, vérifie

$$\frac{\partial^r}{\partial X_1 \dots \partial X_r} S_{k,Q} = Q P^{k'} \quad \text{si } k = -k'\alpha$$

$$\frac{\partial^r}{\partial X_1 \dots \partial X_r} S_{k,Q} = 0 \quad \text{sinon.}$$

Nous supposons dans tout ce qui suit que P est homogène.

II. - Etude de la dimension

Notons $S = \{1, \dots, r\}$.

Pour tout $A \subset S$, on définit

$\mathcal{L}_A$ le K -espace vectoriel engendré par les monômes

$$\prod_{i \in A} X_i^{v_i} \quad \text{tels que } \sum v_i \equiv 0 (\alpha) \quad \text{et } v_i \geq 0$$

$\mathcal{L}_A^A$ le sous-espace vectoriel de $\mathcal{L}_A$ engendré par les monômes qui satisfont en outre $v_i > 0$. On écrit $\mathcal{L}$ pour $\mathcal{L}_S$ et $\mathcal{L}^S$ pour $\mathcal{L}_S^S$; $\mathcal{L}_\emptyset = K$.

Soit $\Delta_A = \{(x_i)_{i \in A} \mid 0 < x_i < \infty\}$.

Définissons φ_A l'application

$$\begin{aligned} \mathcal{L}_A^A &\longrightarrow \mathbb{C} \\ \omega &\longmapsto \int_{\Delta_A} \omega e^{-P_A(t)} \frac{dt}{t} \\ \varphi_\emptyset &= \text{Id}_K. \end{aligned}$$

Ces intégrales ont été étudiées par E. Stevenson [11].

PROPOSITION 3. - Pour tout polynôme $Q \in K[X_1, \dots, X_r]$, pour tout $k \in \mathbb{Z}$, $k \leq \frac{\deg Q + r}{\alpha}$

$$Z(P, Q)(k) \in \sum_{A \subset S} \varphi_A(\mathcal{L}_A^A).$$

Pour montrer cela on utilise le théorème 0. On a donc :

$$\mathcal{O} \subset \sum_{A \subset S} \varphi_A(\mathcal{L}_A^A) .$$

LEMME 4. -

$$\sum_{A \subset S} \varphi_A(\mathcal{L}_A^A) = \varphi_S(\mathcal{L}^S)$$

Preuve. -

$$\varphi_S(\mathcal{L}^S) \subset \sum_{A \subset S} \varphi_A(\mathcal{L}_A^A) .$$

Si $w \in \mathcal{L}_A^A$, pour tout $i \notin A$, $w t_i \frac{\partial P}{\partial t_i} \in \mathcal{L}_{AU\{i\}}^{AU\{i\}}$ et

$$\int_{\Delta_A} w e^{-P_A(t)} \frac{dt}{t} = \int_{\Delta_{AU\{i\}}} w t_i \frac{\partial P}{\partial t_i} e^{-P_{AU\{i\}}(t)} \frac{dt_i}{t_i} \frac{dt}{t} .$$

On peut donc étudier $\mathcal{O}$ par l'intermédiaire de $\mathcal{L}^S$. Dwork [3] a étudié des quotients de cet espace.

Notons D_j les opérateurs sur $\mathcal{L}^S$

$$D_j = \exp(P(X)) \circ X_j \frac{\partial}{\partial X_j} \circ \exp(-P(X)) .$$

$$D_j Q = X_j \frac{\partial Q}{\partial X_j} - Q X_j \frac{\partial P}{\partial X_j} .$$

LEMME 5. - Il existe un homomorphisme surjectif φ_S qui rend le diagramme suivant commutatif

$$\begin{array}{ccc} \mathcal{L}^S & \xrightarrow{\quad} & \varphi_S(\mathcal{L}^S) \\ \downarrow & \nearrow \varphi_S & \\ \mathcal{L}^S / \sum D_j \mathcal{L}^S & & \end{array}$$

Preuve. - Soit $\omega_1 = X_j \frac{\partial \omega}{\partial X_j} - \omega X_j \frac{\partial P}{\partial X_j}$ $\omega \in \mathcal{L}^S$

$$\begin{aligned} \int_{\Delta_S} \omega_1 e^{-P(t)} \frac{dt}{t} &= \int_0^\infty \int_{\Delta_{S-\{j\}}} t_j \frac{\partial \omega}{\partial t_j} e^{-P(t)} \frac{dt_j}{t_j} \frac{dt}{t} \\ &\quad - \int_0^\infty \int_{\Delta_{S-\{j\}}} \omega t_j \frac{\partial P}{\partial t_j} e^{-P(t)} \frac{dt_j}{t_j} \frac{dt}{t} \\ &= \int_0^\infty \int_{\Delta_{S-\{j\}}} \frac{\partial \omega}{\partial t_j} e^{-P(t)} dt_j \frac{dt}{t} \\ &\quad + [\omega e^{-P(t)}]_{t_j=0}^{t_j=\infty} \int_0^\infty \int_{\Delta_{S-\{j\}}} \frac{\partial \omega}{\partial t_j} e^{-P(t)} dt_j \frac{dt}{t} = 0 . \end{aligned}$$

Dwork [3] a montré que $\mathcal{L}^S / \sum D_j \mathcal{L}^S$ est un K-espace vectoriel de dimension inférieure ou égale à α^{r-1} dont un système de générateurs est donné par

$$\prod_{i=1}^r X_i^{v_i} , \quad \sum_{i=1}^r v_i \equiv 0 \pmod{\alpha} \quad 0 < v_i \leq \alpha .$$

Donc $\varphi_S(\mathcal{L}^S)$ est de dimension inférieure ou égale à α^{r-1} et un système de générateurs est donné par

$$\int_{\Delta_S} t^v e^{-P(t)} \frac{dt}{t} , \quad \sum_{i=1}^r v_i \equiv 0 \pmod{\alpha} , \quad 0 < v_i \leq \alpha .$$

Donc $\mathcal{B} \subset \varphi_S(\mathcal{L}^S)$ est de dimension inférieure ou égale à α^{r-1} . De plus

$$\int_{\Delta_S} t^v e^{-P(t)} \frac{dt}{t} = Z(P, X^{v-1}) \left(\frac{\sum_{i=1}^r v_i}{\alpha} \right) .$$

Donc $\mathcal{B} = \varphi_S(\mathcal{L}^S)$ et le théorème 1 est montré.

III. - Identification avec les périodes

On suppose maintenant que la variété projective V définie par l'annulation de P est non singulière et en position générale par rapport aux axes de coordonnées (ceci signifie que les formes $X_i \frac{\partial P}{\partial X_i}$ n'ont pas de zéro commun).

Notons μ_α le groupe des racines α -ièmes de l'unité.

Si Q est un polynôme homogène tel que $\deg Q + r \equiv 0(\alpha)$, on définit pour tout $\zeta \in \mu_\alpha^r$

$$Z_\zeta(P, Q)(s) = \sum'_{n \in \mathbb{N}^r} \zeta_1^{n_1} \dots \zeta_r^{n_r} Q(\zeta_1^{n_1}, \dots, \zeta_r^{n_r}) P(\zeta_1^{n_1}, \dots, \zeta_r^{n_r})^{-s}.$$

On remarque que si $\zeta = (\zeta, \dots, \zeta)$, alors

$$Z_\zeta(P, Q)(s) = Z(P, Q)(s) \quad \text{pour tout } s \in \mathbb{C}.$$

Notons $\bar{\mu}_\alpha^r$ le quotient de μ_α^r par la diagonale.

Nous allons considérer maintenant les vecteurs

$$\left(Z_\zeta(P, X^{v-1}) \left(\frac{\sum_{i=1}^r v_i}{\alpha} \right) \right)_{\zeta \in \bar{\mu}_\alpha^r}.$$

Notons $\Delta_S(\zeta)$ l'image de Δ_S par l'application

$$\begin{aligned} \mathbb{R}^r &\longrightarrow \mathbb{C}^r \\ (x_i)_{i \in S} &\longrightarrow (\zeta_i x_i)_{i \in S}. \end{aligned}$$

Il est facile de voir que

$$Z_\zeta(P, X^{v-1}) \left(\frac{\sum_{i=1}^r v_i}{\alpha} \right) = \int_{\Delta_S(\zeta)} t^v e^{-P(t)} \frac{dt}{t}.$$

Définissons maintenant l'application

$$\begin{aligned} \psi_S : \mathbb{C}^S &\longrightarrow \mathbb{C}^{\alpha^{r-1}} \\ \omega &\longmapsto \left(\int_{\Delta_S(\zeta)} \omega e^{-P(t)} \frac{dt}{t} \right)_{\zeta \in \bar{\mu}_\alpha^r}. \end{aligned}$$

THÉORÈME 6. - Le K -espace vectoriel $\psi_S(\mathcal{L}^S)$ est de dimension α^{r-1} et une base est donnée par

$$\left(Z_{\zeta}(P, X^{v-1}) \left(\frac{\sum_{i=1}^r v_i}{\alpha} \right) \right)_{\zeta \in \bar{\mu}_{\alpha}^r}$$

où $(v_1, \dots, v_r)$ parcourt un système de r -uple d'entiers tels que $\sum v_i \equiv 0(\alpha)$ et $0 < v_i \leq \alpha$.

Preuve. - Pour montrer le théorème nous allons montrer qu'il existe un isomorphisme $\bar{\psi}_S$ qui rend le diagramme suivant commutatif

$$\begin{array}{ccc} \mathcal{L}^S & \xrightarrow{\psi_S} & \psi_S(\mathcal{L}^S) \\ \downarrow & & \nearrow \bar{\psi}_S \\ \mathcal{L}^S / \sum_{j=1}^r D_j \mathcal{L}^S & & \end{array}$$

Dwork [3] a montré que dans le cas où V est non singulière et en position générale $\mathcal{L}^S / \sum_{j=1}^r D_j \mathcal{L}^S$ est de dimension α^{r-1} et que le système de générateurs donné précédemment est une base. $\bar{\psi}_S$ existe et est surjective pour les mêmes raisons que $\bar{\psi}_S$. Pour montrer l'injection nous allons montrer que la matrice

$$\mathfrak{z} = \left(Z_{\zeta}(P, X^{v-1}) \left(\frac{\sum_{i=1}^r v_i}{\alpha} \right) \right)_{\zeta \in \bar{\mu}_{\alpha}^r} \Big|_{\sum v_i \equiv 0(\alpha)} \quad 0 < v_i \leq \alpha$$

est inversible.

Nous utilisons maintenant la théorie de la déformation introduite par Dwork pour étudier les fonctions zêta des hypersurfaces [5].

On définit $P_{\lambda}(X_1, \dots, X_r) = \sum_{i=1}^r a_i X_i^{\alpha} + \lambda R(X_1, \dots, X_r)$.

On a $P_0(X_1, \dots, X_r) = \sum_{i=1}^r a_i X_i^{\alpha}$ polynôme de Fermat et

$$P_1(X_1, \dots, X_r) = P(X_1, \dots, X_r).$$

On suppose que λ appartient à un domaine $\mathcal{D}$ du plan complexe qui contient 0 et 1 tel que la variété V_λ soit non singulière et en position générale. Alors $\mathcal{L}^S / \sum D_{j,\lambda} \mathcal{L}^S$ est encore de dimension α^{r-1} et admet la même base X^v , $\sum_{i=1}^r v_i \equiv 0 (\alpha)$, $0 < v_i \leq \alpha$

$$\mathfrak{X}_\lambda = \left(Z_\zeta (P_\lambda, X^{v-1}) \left(\frac{\sum_{i=1}^r v_i}{\alpha} \right) \right)_v \Big|_{\zeta \in \bar{\mu}_\alpha^r}.$$

On étudie l'équation différentielle en λ satisfaite par $\mathfrak{X}_\lambda$:

$$\frac{d}{d\lambda} \int_{\Delta_S(\zeta)} X^v e^{-P_\lambda(t)} \frac{dt}{t} = \int_{\Delta_S(\zeta)} \sigma_\lambda(t^v) e^{-P_\lambda(t)} \frac{dt}{t}$$

où σ_λ est l'opérateur défini sur $\mathcal{L}^S$ par

$$\sigma_\lambda = \exp P_\lambda \circ \frac{\partial}{\partial \lambda} \circ \exp(-P_\lambda).$$

L'opérateur σ_λ commute avec les opérateurs $D_{j,\lambda}$ et donc opère sur le quotient $\mathcal{L}^S / \sum D_{j,\lambda} \mathcal{L}^S$. Soit G_λ la matrice de σ_λ dans la base X^v . Alors G_λ est une matrice à coefficients rationnels en λ , et on peut supposer qu'elle est sans singularités dans $\mathcal{D}$. On a alors

$$\frac{\partial}{\partial \lambda} \mathfrak{X}_\lambda = G_\lambda \mathfrak{X}_\lambda$$

et donc $\frac{\partial}{\partial \lambda} \det \mathfrak{X}_\lambda = \text{trace } G_\lambda \cdot \det \mathfrak{X}_\lambda$.

Pour montrer que $\det \mathfrak{X}_\lambda \neq 0$ dans $\mathcal{D}$, il suffit de montrer que $\det \mathfrak{X}_0 \neq 0$.

On peut calculer $\mathfrak{X}_0$ et on trouve

$$\det \mathfrak{X}_0 = \prod_v \prod_j a_j \Gamma\left(\frac{v_j}{\alpha}\right) \Big| \zeta^{v_j} \Big|_v \Big|_{\zeta \in \bar{\mu}_\alpha^r}.$$

Le déterminant qui apparaît à droite est un déterminant de groupe ; il est non nul.

On a donc montré que

$$\psi_S(\mathcal{L}^S) \simeq \mathcal{L}^S / \sum_{j=1}^r D_j \mathcal{L}^S.$$

Pour tout $A \subset S$, notons $D_{i,A} = \mathfrak{T}_A \circ D_i$.

Définissons $W_A = \mathcal{L}_A^A / \sum_{i \in A} D_{i,A} \mathcal{L}_A^{A-\{i\}}$.

Dwork ([5]) a montré que

$$\mathcal{L}^S / \sum_{j=1}^r D_j \mathcal{L}^S \simeq \bigoplus_{A \subseteq S} W_A$$

et Katz ([6]) a montré qu'il existe un isomorphisme θ_A qui rend le diagramme suivant commutatif

$$\begin{array}{ccc} W_A & \xrightarrow{\theta_A} & \text{Prim}^{r_A-2}(V_A/K) \\ \mathcal{T}_A \circ \sigma_\lambda \downarrow & & \downarrow \frac{d}{d\lambda} \\ W_A & \xrightarrow{\theta_A} & \text{Prim}^{r_A-2}(V_A/K) \end{array}$$

où $\text{Prim}^{r_A-2}(V_A/K)$ désigne le sous-espace de $H_{\text{DR}}^{r_A-2}(V_A/K)$ des classes primitives (dans le sens de la théorie de Hodge).

Nous recherchons maintenant les sous-espaces de $\psi_S(\mathcal{L}^S)$ qui correspondent aux W_A .

On définit

$$\begin{aligned} \psi_A : \mathcal{L}_A^A &\longrightarrow \mathbb{C}^{\alpha^{r-1}} \\ \omega &\longmapsto \left(\int_{\Delta_A(\zeta)} \omega e^{-P_A(t)} \frac{dt}{t} \right)_{\zeta \in \bar{\mu}_\alpha^r} . \end{aligned}$$

Notons $\mathcal{M}_A = \psi_A(\mathcal{L}_A^A)$.

On peut montrer que :

$$W_A \simeq \mathcal{M}_A / \sum_{i \in A} \mathcal{M}_{A-\{i\}} = \bar{\mathcal{M}}_A$$

et que le diagramme suivant est commutatif

$$\begin{array}{ccccc} \bar{\mathcal{M}}_A & \xrightarrow{\bar{\psi}_A} & W_A & \xrightarrow{\theta_A} & \text{Prim}^{r_A-2}(V_A/K) \\ \frac{d}{d\lambda} \downarrow & & \downarrow \sigma_{\lambda,A} & & \downarrow \frac{d}{d\lambda} \\ \bar{\mathcal{M}}_A & \xrightarrow{\bar{\psi}_A} & W_A & \xrightarrow{\theta_A} & \text{Prim}^{r_A-2}(V_A/K) \end{array} .$$

Considérons la base de W_A

$$\prod_{j \in A} x_j^{v_j} \quad \text{où} \quad \sum_{j \in A} v_j \equiv 0 (\alpha) \quad \text{et} \quad 0 < v_j < \alpha.$$

On note (ω) son image dans $\text{Prim}^{r_A-2}(V_A/K)$.

Considérons une base de cycles (γ) et la matrice des périodes

$$P_\lambda = \left(\int_\gamma \omega \right)_{\substack{\omega \\ \gamma}}.$$

L'image dans $\overline{M}_A$ de la base de W_A nous donne la matrice

$$\rho_\lambda = \left(\int_{\Delta_A(\zeta)} t^v e^{-P_{\lambda,A}(t)} \frac{dt}{t} \right)_{\substack{v \mid \sum v_j \equiv 0 (\alpha) \\ \zeta \in \overline{\mu}_\alpha^r}} \quad 0 < v_j < \alpha$$

Les deux matrices vérifient la même équation différentielle. On en déduit donc que

$$P_\lambda^{-1} \rho_\lambda = P_0^{-1} \rho_0.$$

On peut remarquer que cette égalité ne dépend pas de la base de cycles choisis (si l'on change cette base on multiplie à gauche les deux membres par une même matrice), ni des $\zeta \in \overline{\mu}_\alpha^r$.

On peut faire des calculs effectifs de P_0 (Deligne [2]) et de ρ_0 (cf. $\mathfrak{X}_0$) et on montre que $\frac{1}{\pi} P_0^{-1} \rho_0$ est une matrice à coefficients dans K . Donc pour tout λ $P_\lambda^{-1} \rho_\lambda$ est une matrice à coefficients dans K .

Le théorème 2 est démontré.

-:-:-:-

BIBLIOGRAPHIE

- [1] P. CASSOU-NOGUÈS, Etude de certaines séries de Dirichlet associées à un polynôme (en préparation).
- [2] P. DELIGNE,

- [3] B. DWORK, On the Zeta function of a hypersurface, Publ. Math. I.H.E.S. (12) (1962), 5-85.
- [4] B. DWORK, On the Zeta function of a hypersurface II, Ann. of Maths 80 (1964), 227-299.
- [5] B. DWORK, A deformation theory for the Zeta function, Cong. Math. Stockholm (1962), 247-259.
- [6] N. KATZ, On the intersection matrix of a hypersurface, Ann. Scient. Ec. Norm. Sup. 4ème série, t. 2 (1969), 583-598.
- [7] H. KLINGEN, Über die Werte der Dedekindsche Zeta funktion, Math. Annalen 145 (1962), 265-272.
- [8] H. MELLIN, Eine formel für den Logarithmus transcenderter Funktionen von endlichen Geschlecht, Acta Soc. Scient. fennicae 29 (1900) n° 4.
- [9] C. L. SIEGEL, Über die Fourierschen Koeffizienten von Modulformen, Nachr. Akad. Wiss. Göttingen, Math. Phys. K 1, 3 (1970), 15-56.
- [10] T. SHINTANI, On evaluation of zeta functions of totally real algebraic number fields at non positive integers, J. of Fac. of Sc., Univ. of Tokyo, section 1, 23 (1976), 393-417.
- [11] E. STEVENSON, Integral representation of algebraic cohomology classes on hypersurfaces, Pacific Journal of Math. 71 (1977).

(texte reçu le 21 mai 1981)

--:--:--

Pierrette CASSOU-NOGUÈS
U.E.R. de Mathématiques
et d'Informatique
Université de Bordeaux I
F 33405 TALENCE CEDEX

APPLICATIONS POLYNOMIALES A JACOBIENNE CONSTANTE

par

Hyman BASS

--:--:--

1. - La conjecture jacobienne

Soit $F : \mathbb{C}^n \longrightarrow \mathbb{C}^n$ une application polynomiale. Ainsi $F(x) = (F_1(x), \dots, F_n(x))$ où chaque F_i est un élément de $\mathbb{C}^{[n]} = \mathbb{C}[X_1, \dots, X_n]$. La matrice jacobienne de F est

$$J(F) = (D_i F_j)_{1 \leq i, j \leq n} \quad (D_i = \frac{\partial}{\partial X_i}) .$$

Pour une application composée $G(F)$ on a $J(G(F)) = J(G)(F) \cdot J(F)$. Si F est inversible, d'inverse G , de sorte que $G_i(F) = X_i$ ($i = 1, \dots, n$), on trouve que $J(F)$ est inversible, ce qui revient à dire que $\det J(F) \in \mathbb{C}^\times$.

CONJECTURE JACOBIENNE. - Si $J(F)$ est inverisible, alors F est inversible.

Cette conjecture a été énoncée pour la première fois par O.H. Keller [K] en 1939. Elle reste un problème ouvert pour tout $n \geq 2$. (Son analogue en caractéristique $p > 0$ est fausse, comme le montre l'exemple $x \mapsto x + x^p$ pour $n = 1$.) Il y a une littérature assez ample, y compris plusieurs démonstrations fausses, consacrée à ce problème.

J'annonce ici quelques résultats partiels d'un travail en collaboration avec E.H. Connell et David Wright [BCW].

2. - Le théorème de réduction

Notons $GA_n(\mathbb{C})$ le groupe des automorphismes polynomiaux de $\mathbb{C}^n$, le "groupe affine de Cremona".

Soit $F = (F_1, \dots, F_n)$ un endomorphisme polynomial de $\mathbb{C}^n$. Pour tout $m \geq 0$ posons $F^{[m]} = (F_1, \dots, F_n, X_{n+1}, \dots, X_{n+m})$, qui est un endomorphisme polynomial de $\mathbb{C}^{n+m}$. On a $F \in GA_n(\mathbb{C}) \Leftrightarrow F^{[m]} \in GA_{n+m}(\mathbb{C})$, et $J(F^{[m]}) = \begin{pmatrix} J(F) & 0 \\ 0 & I_m \end{pmatrix}$.

THÉORÈME. - Supposons que $J(F)$ soit inversible. Il existe un entier $m \geq 0$, des éléments G, L de $GA_{n+m}(\mathbb{C})$, et un endomorphisme polynomial $\tilde{F}(T)$ de $\mathbb{C}[T]^{n+m}$, T étant une indéterminée, satisfaisant aux conditions suivantes :

(a) Pour $T = 1$, on a $\tilde{F}(1) = G \circ F^{[m]} \circ L$, de sorte que si $\tilde{F}$ est inversible alors F est inversible.

(b) Posons $r = n + m + 1$ et notons $\bar{F}$ l'endomorphisme polynomial de $\mathbb{C}^r$ correspondant à $\tilde{F}$. On a pour chaque $i = 1, \dots, r$, $\bar{F}_i = X_i - H_i$ où H_i est un polynôme cubique homogène et la matrice $J(H)$ est nilpotente.

COROLLAIRE. - Pour démontrer la conjecture jacobienne il suffit de la démontrer (pour tout n) pour des applications de la forme $F = X - H$ avec H cubique homogène et $J(H)$ nilpotente.

Remarque. - S. Wang [W] a démontré la conjecture jacobienne pour tout n et toute application polynomiale quadratique, même sur tout corps de caractéristique $\neq 2$.

3. - L'inverse formel

Notons $\mathbb{C}^{[[n]]}$ l'algèbre des séries formelles $\mathbb{C}[[X_1, \dots, X_n]]$. Un endomorphisme de $\mathbb{C}^{[[n]]}$ est donné par la suite $F = (F_1, \dots, F_n)$ des images F_i des X_i . On a $F_i(0) = 0$ ($i=1, \dots, n$), et F définit un automorphisme de $\mathbb{C}^{[[n]]}$ si et seulement si sa composante linéaire est inversible, ou également si et seulement si $J(F)(0)$ est inversible.

Supposons que $F_i = X_i - H_i$ où $H_i \in m^2$, m étant l'idéal maximal de $\mathbb{C}^{[[n]]}$ ($i=1, \dots, n$). Alors F est inversible. Nous présentons une formule de Abhyankar pour son inverse G .

Pour tout $U \in \mathbb{C}^{[[n]]}$ posons

$$\langle U, F \rangle = \sum_{p \in \mathbb{N}^n} D^{(p)}(U(F) \cdot j(F) \cdot H^p)$$

où

$$H^p = H_1^{p_1} \dots H_n^{p_n}$$

$$D^{(p)} = \frac{D_1^{p_1} \dots D_n^{p_n}}{p_1! \dots p_n!} \quad (D_i = \frac{\partial}{\partial X_i})$$

$$j(F) = \det J(F) = \det(D_i F_j) .$$

THÉORÈME (Abhyankar [A]). - $\langle U, F \rangle = U$.

COROLLAIRE. - Si $G_i(F) = X_i$ on a

$$G_i = \sum_{p \in \mathbb{N}^n} D^{(p)}(X_i j(F) \cdot H^p) .$$

4. - Le développement arboréal de l'inverse

Revenons à la conjecture jacobienne. D'après le théorème de réduction, il nous suffit de considérer une application polynomiale $F = (F_1, \dots, F_n)$ de la forme $F_i = X_i - H_i$ où H_i est cubique, homogène ($i=1, \dots, n$) et $J(H)$ est nilpotente. On a alors $j(F) = \det J(F) = 1$. Soit $G = (G_1, \dots, G_n)$ l'inverse formelle de F . La conjecture jacobienne équivaut à dire que les séries formelles G_i sont des polynômes.

D'après la formule d'Abhyankar pour les G_i on a

$$G_i = \sum_{d \geq 0} G_i^{(d)}$$

avec

$$G_i^{(d)} = \sum_{\substack{p \in \mathbb{N}^n \\ |p| = d}} D^{(p)} (X_i \cdot H^p).$$

Ici $|p|$ désigne $p_1 + \dots + p_n$, et on voit tout de suite que $G_i^{(d)}$ est un polynôme homogène de degré $2d+1$. Par conséquent, G_i est un polynôme $\Leftrightarrow G_i^{(d)} = 0$ pour tout $d \gg 0$.

THÉORÈME. - On a $G_i^{(0)} = X_i$, $G_i^{(1)} = H_i$, et, pour tout $d \geq 1$,

$$G_i^{(d)} = \sum_T \frac{1}{\alpha(T)} \sum_f P_{T,f}$$

où :

- T parcourt l'ensemble (des classes d'isomorphismes) des arbres "racinés" (i.e. munis d'un sommet distingué) à d sommets,

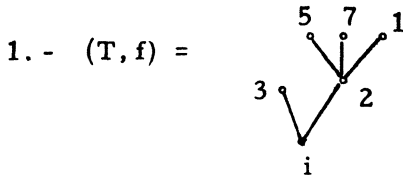
- $\alpha(T)$ désigne le nombre d'automorphismes de T ,

- f parcourt l'ensemble des applications de l'ensemble $V(T)$ des sommets de T dans $\{1, 2, \dots, n\}$ telle que f prend la valeur i en la racine de T

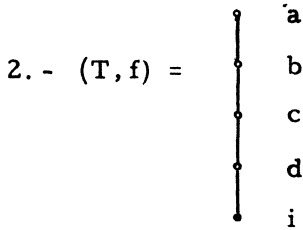
- on a $P_{T,f} = \prod_{v \in V(T)} D_{f(v_+)} H_{f(v)}$

où v_+ désigne l'ensemble des sommets juste au-dessus de v , et

$$D_{f(v_+)} = \prod_{w \in v_+} D_{f(w)}.$$

Exemples

$$P_{T,f} = (D_3 D_2 H_i) \cdot H_3 \cdot (D_5 D_7 D_1 H_2) \cdot H_5 \cdot H_7 \cdot H_1 \cdot$$



$$P_{T,f} = H_a (D_a H_b) (D_b H_c) (D_c H_d) (D_d H_i) \cdot$$

Ainsi

$$\sum_f P_{T,f} = \sum_{a=1}^n H_a J(H)_{a,i}^4$$

Rappelons que $J(H)$ est nilpotente. Ainsi si T est une droite, de longueur $d \gg 0$, on a $\sum P_{T,f} = 0$.

3. - Si T contient un sous-arbre de la forme  on a $P_{T,f} = 0$ quel que soit f , car si on dérive quatre fois, un polynôme cubique on trouve zéro.

On a : $J(H)^e = 0$ avec $e \leq n$.

CONJECTURE. - Il existe un entier $d(e)$ tel que, pour tout arbre raciné T , à $d \geq d(e)$ sommets, on a $\sum_f P_{T,f} = 0$.

Pour $e = 2$, on peut prendre $d(2) = 2$, en se servant de l'identité d'Euler. Pour $e = 3$, on a montré, par un calcul assez pénible, qu'il faut prendre $d(3) \geq 8$. Ce problème est en train d'être traité sur ordinateur par D. Grayson.

RÉFÉRENCES

- [A] S. ABHYANKAR, Lectures in algebraic geometry, notes by
Chris Christensen, Purdue Univ. (1974).
- [B C W] H. BASS, E.H. CONNELL, and D. WRIGHT, Polynomial maps with
constant jacobian : Reduction of degree, and formal expansion of the
inverse (to appear).
- [K] O.H. KELLER, Ganze CREMONA, Transformationen, monatschafte
für math. und Physik 47 (1939), 299-306,
- [W] S. WANG, A jacobian criterion for separability, J. Algebra, 65 (1980),
453-494.

(texte reçu le 10 juillet 1981)

--:--:--

Hyman BASS
Department of Mathematics
Columbia University
NEW YORK,
NEW YORK 100 27

BRUMER-STARK-STICKELBERGER

par

John TATE

--:--:--

§.1. - Définition et propriétés de $\theta_{S, K/k}$

Soit K/k une extension galoisienne finie abélienne de corps de nombres, soit $G = \text{Gal}(K/k)$ son groupe de Galois, et soit S un ensemble fini de places de k contenant les places archimédiennes et les places qui sont ramifiées dans K/k , et contenant au-moins deux places. Un caractère $\chi : G \rightarrow \mathbb{C}^*$ se prolonge par linéarité en un homomorphisme de l'algèbre $\mathbb{C}[G] = \sum_{\sigma \in G} \mathbb{C}\sigma$ dans $\mathbb{C}$, encore noté χ . On définit alors $\theta_{S, K/k}$, noté également $\theta_{S, G}$, ou même simplement θ , comme étant l'unique élément de $\mathbb{C}[G]$ tel que l'on ait, pour tous les caractères χ de G , l'égalité

$$\chi(\theta_{S, G}) = L_S(0, \chi^{-1}, K/k),$$

où $L_S(s, \chi, K/k)$ désigne la fonction L d'Artin privée de ses facteurs d'Euler relatifs aux places $p \in S$.

En d'autres termes, on a :

$$\theta_{S,G} = \sum_{\sigma \in G} \zeta_S(\sigma, 0) \sigma^{-1},$$

où $\zeta_S(\sigma, s)$ désigne la fonction zêta partielle construite avec les idéaux premiers non dans S , comme elle est définie par exemple dans [C].

Exemple. - Soit m un entier ≥ 2 , impair ou $\equiv 0 \pmod{4}$. Posons $\zeta = e^{2i\pi/m}$, et considérons la situation suivante : $k = \mathbb{Q}$, $K = \mathbb{Q}(\zeta)$, et S est l'ensemble de la place à l'infini de $\mathbb{Q}$ et des nombres premiers qui divisent m . Il existe un unique isomorphisme de $(\mathbb{Z}/m\mathbb{Z})^*$ sur G qui, à un entier a modulo m premier à m , associe l'automorphisme σ_a de K pour lequel $\zeta^{\sigma_a} = \zeta^a$, et l'on a alors :

$$\theta = \sum_{\substack{a=1 \\ (a,m)=1}}^m (1/2 - a/m) \sigma_a^{-1}.$$

En effet, la fonction zêta partielle associée à l'automorphisme σ_a de K est la fonction zêta de Hurwitz

$$\zeta(\sigma_a, s) = \sum_{\substack{n=1 \\ n \equiv a \pmod{m}}}^{\infty} n^{-s},$$

et il est bien connu (voir par exemple [W - W], §.13.21, p. 271) que l'on a

$$\zeta(\sigma_a, 0) = 1/2 - a/m.$$

Propriétés de $\theta_{S, K/k}$

$$1) \chi(\theta_S, K/k) = L_S(0, \chi^{-1}, K/k).$$

Cela est la définition même de θ .

2) Pour $p \notin S$, $\theta_{S \cup \{p\}, K/k} = (1 - \sigma_p^{-1}) \theta_{S, K/k}$, où $\sigma_p \in G$ désigne la substitution de Frobenius associée à l'idéal premier p .

Cela est une conséquence immédiate de la définition de θ .

3) Pour $v \in S$, on a $N_v \theta_{S, K/k} = 0$, où $N_v = \sum_{\sigma \in G_v} \sigma$ désigne la somme (dans $\mathbb{C}[G]$) des éléments du groupe de décomposition G_v de v .

Cela résulte du fait que, si $\chi(G_v) = \{1\}$, alors $L(0, \chi) = 0$ pour $\chi \neq 1$, et que l'on a également $L(0, 1) = \zeta_S(0) = 0$ grâce à l'hypothèse "card $S \geq 2$ ".

Donc, on a $\theta_S = 0$ chaque fois qu'une place de S se décompose complètement dans K .

En particulier, si θ est non nul, k est totalement réel et K est totalement imaginaire.

Comme dans l'exemple donné plus haut, on a :

4) $\theta_{S, K/k} \in \mathbb{Q}[G]$, i.e. les valeurs des fonctions zêta partielles en zéro sont rationnelles. Ce résultat, dû à Siegel ([S]), n'est pas facile. Il résulte également des formules de Shintani ([Sh]).

Soit $\mu = \mu_K$ le groupe des racines de l'unité de K , et soit $w = w(K)$ son ordre. Alors, on a :

5) $w \theta_{S, K/k} \in \mathbb{Z}[G]$.

Plus généralement, on a $\xi \theta_{S, K/k} \in \mathbb{Z}[G]$ pour tout élément $\xi \in \mathbb{Z}[G]$ qui annule le G -module monogène fini μ_K .

Ce résultat est dû à Deligne et Ribet ([D-R]) ; Pierrette Cassou-Noguès et Barsky en ont aussi donné indépendamment une démonstration basée sur les formules explicites de Shintani ([Sh]).

Donnons nous maintenant un corps K' intermédiaire entre k et K ($k \subset K' \subset K$), et posons $H = \text{Gal}(K/K')$ et $G' = \text{Gal}(K'/k)$

$$G' = G/H \left\{ \begin{array}{c} K \\ | \\ K' \\ | \\ k \end{array} \right\} G$$

6) L'homomorphisme d'algèbres $\mathbb{Q}[G] \rightarrow \mathbb{Q}[G']$ induit par l'homomorphisme naturel $G \rightarrow G'$ envoie $\theta_{S, G}$ sur $\theta_{S, G'}$.

Cela résulte immédiatement des définitions de $\theta_{S, G}$ et de $\theta_{S, G'}$.

Soit S' l'ensemble des places de K' au-dessus d'une place de S . Comme l'algèbre $\mathbb{Q}[G]$ est un $\mathbb{Q}[H]$ -module libre de rang $[G:H]$, on peut définir la norme

$$N_{\mathbb{Q}[G]/\mathbb{Q}[H]} : \mathbb{Q}[G] \longrightarrow \mathbb{Q}[H].$$

$$7) \theta_{S', H} = N_{\mathbb{Q}[G]/\mathbb{Q}[H]}(\theta_{S, G}).$$

Cela résulte de la formule d'induction des fonctions L d'Artin : pour tout caractère ψ de H , on a :

$$L(s, \psi, K/K') = L(s, \text{Ind}_H^G(\psi), K/k) = \prod_{\chi|_H = \psi} L(s, \chi, K/k).$$

§.2. - La conjecture de Brumer-Stark : propriétés générales

Notons K° l'ensemble des éléments de K^* vérifiant la condition $|\alpha|_v = 1$ pour toute place archimédienne v de K (groupe des "anti-unités" de K). Clairement, si $\alpha \in K^\circ$, la connaissance de l'idéal principal (α) détermine α au produit près par une racine de l'unité. Par ailleurs, notons $A_{K/k}$ l'ensemble des éléments ξ de $\mathbb{Z}[G]$ qui annulent le G -module μ_K (cf. §.1). La proposition suivante est inspirée par le lemme 6 de [St, IV] et a donc son origine dans le travail de Gilles Robert sur les unités elliptiques (Bull. Soc. Math. France, mémoire 36 (1973)).

PROPOSITION. - Soit α un idéal fractionnaire non nul de K . Les conditions suivantes sont équivalentes :

(I) Il existe $\alpha \in K^\circ$ tel que $\alpha^{w\theta} = (\alpha)$ et tel que $K(\alpha^{1/w})/k$ soit une extension abélienne de k .

(II) Il existe une extension L de K abélienne sur k et un élément $\beta \in L^\circ$ tel que $\alpha^\theta = (\beta)$ (où α^θ est défini par la formule $\alpha^\theta = (\alpha^{w\theta})^{1/w}$ dans une extension convenable de K).

(III) Pour presque tout idéal premier p de k , il existe $\alpha_p \in K^\circ$ tel que
 $\alpha_p \equiv 1 \pmod{p} O_K$ et que $a^{\frac{(\sigma - N_p)\theta}{p}}$ soit l'idéal principal de K engendré
par α_p .

(IV) Il existe une famille finie de générateurs $(a_i)_{i \in I}$ de $A_{K/k}$ et des
éléments $(\alpha_i)_{i \in I}$ de K° tels que $a^{a_i \theta} = (\alpha_i)$, et que $\alpha_i^j = \alpha_j^i$, $\forall i, j$.

Démonstration. - (Pour plus de détails, voir [T], ch. II, prop. 1.2.)

L'implication (I) $\Rightarrow$ (II) est immédiate (prendre $\beta = \alpha^{1/w}$ et $L = K(\beta)$).

Pour prouver (II) $\Rightarrow$ (III), on considère les idéaux p non ramifiés dans L/k et premiers à $w(L)$ et à $a^{m\theta}$ (où $m \neq 0$ est un entier tel que $m\theta \in \mathbb{Z}[G]$), et l'on prend $\alpha_p = \beta^{\frac{\sigma^L - N_p}{p}}$, où $\sigma_p^L \in \text{Gal}(L/K)$ est la substitution de Frobenius associée à p et à l'extension L/K (N_p est la norme absolue de l'idéal p ; on a $x^{\frac{\sigma_p^L}{p}} \equiv x^{N_p} \pmod{p}$ pour tout x entier dans L).

Pour montrer (III) $\Rightarrow$ (IV) on utilise le fait que les $\sigma_p - N_p$ engendrent l'idéal $A_{K/k}$ de $\mathbb{Z}[G]$, qui résulte lui-même, via le théorème de densité de Čebotarev, de ce que $w(K)$ est le P. G. C. D. des éléments $(N_p - 1)$ de $\mathbb{Z}$ et du fait que $\alpha_p^q = \alpha_q^p$ parce qu'ils engendrent le même idéal et sont congrus à 1 modulo $p O_K$. Il reste à prouver (IV) $\Rightarrow$ (I). Pour cela, on montre d'abord que, s'il existe des α_i comme dans (IV) pour un système de générateurs de $A_{K/k}$, alors de tels α_i existent pour tout autre système. Choisissons alors, pour tout $\sigma \in G$, un entier n_σ vérifiant l'égalité $\sigma \zeta = \zeta^{n_\sigma}$ pour tout $\zeta \in \mu_K$ (on peut écrire $\sigma = \sigma_p$ pour un p convenable et prendre $n_\sigma = N_p$).

On prend comme système de générateurs de $A_{K/k}$ w et les $(\sigma - n_\sigma)$ $\sigma \in G$. Il existe donc des éléments α et $\alpha_\sigma \in K^\circ$ tels que $a^{w\theta} = (\alpha)$ et $a^{(\sigma - n_\sigma)\theta} = (\alpha_\sigma)$. Soit alors $L = K(\alpha^{1/w})$ (cette définition ne dépend pas du choix de α). L'égalité $a^{\frac{\sigma - n_\sigma}{\sigma} w} = \alpha_\sigma^w$ montre que L/k est galoisienne, et que son groupe de Galois est une extension centrale de G . Les égalités $\alpha_\tau^{\sigma - n_\sigma} = \alpha_\sigma^{\tau - n_\tau}$ montrent que L/k est abélienne, C. Q. F. D.

Si, dans la conjecture principale de [St IV], on remplace la place archimédienne de k qui se décompose complètement dans K par une place non archimédienne $\mathfrak{p}$ qui se décompose complètement, soit $\mathfrak{p} = \prod_{i=1}^{[K:k]} \mathfrak{p}_i$ où les $\mathfrak{p}_i$ sont distincts, on obtient (voir [T], ch. IV, § 6 pour plus de détails), en tenant compte du fait que le groupe des classes d'idéaux de K est engendré par les idéaux premiers de K au-dessus des idéaux premiers de k complètement décomposés, l'énoncé suivant :

CONJECTURE (Brumer-Stark). - Chaque idéal α de K vérifie la propriété suivante :

Il existe un élément $\alpha \in K^\circ$ tel que $\alpha^{w\theta_{S,K/k}} = (\alpha)$ et tel que l'extension $K(\alpha^{1/w})/k$ est abélienne.

On reconnaît là l'énoncé (I) de la proposition ci-dessus.

La conjecture que l'élément $w\theta_{S,K/k} \in \mathbb{Z}[G]$ tue le groupe des classes d'idéaux de K a été énoncée par Brumer, et est discutée dans [C]. L'idée que l'on peut prendre $\alpha \in K^\circ$ et qu'alors $K(\alpha^{1/w})$ est une extension abélienne de k est due à Stark.

Notons $\mathfrak{I}_K$ le groupe des idéaux de K et $\mathfrak{I}_{S,K/k}^*$ le sous-groupe de $\mathfrak{I}_K$ formé des idéaux α qui vérifient les propriétés équivalentes (I), (II), (III), (IV) de la proposition ci-dessus pour $\theta = \theta_{S,K/k}$. La conjecture de Brumer-Stark est que l'on a l'égalité $\mathfrak{I}_{S,K/k}^* = \mathfrak{I}_K$.

Propriétés générales des groupes $\mathfrak{I}_{S,K/k}^*$

(0) $\mathfrak{I}_{S,K/k}^*$ est stable par G , et même plus généralement par tout automorphisme σ de K tel que $k^\sigma = k$ et $S^\sigma = S$.

Cela est immédiat.

(1) $\mathfrak{I}_{S,K/k}^*$ contient le groupe P_K des idéaux principaux de K .

Cela résulte de la propriété (IV) : pour $\alpha = (\gamma)$, $\gamma \in K^*$, on pose $\alpha_i = \gamma^{a_i \theta}$, ce qui a un sens grâce à la propriété 5) de θ , et l'on a alors $\alpha_i \in K^\circ$ grâce à la propriété 3) de θ .

Il résulte de cette propriété que la conjecture est une question de classes d'idéaux ; pour la vérifier, il suffit de montrer que des idéaux engendrant le groupe des classes vérifient les propriétés (I) à (IV) ; on peut, par exemple, utiliser les idéaux premiers de degré 1 de K .

(2) Soit $\mathfrak{p}$ un idéal premier de k non dans S . Alors,

$$\mathfrak{I}_{S \cup \{\mathfrak{p}\}, K/k}^* = \{a \in \mathfrak{I}_K \mid a^{\sigma_{\mathfrak{p}} - 1} \in \mathfrak{I}_{S, K/k}^*\}.$$

Ce groupe contient $\mathfrak{I}_{S, K/k}^*$. Donc, si la conjecture est vraie pour S , elle est vraie pour $S' = S \cup \{\mathfrak{p}\}$. En particulier, étant donné une extension K/k , si la conjecture est vraie pour l'ensemble S formé des places archimédiennes et des places non archimédiennes ramifiées dans K/k , elle est vraie quel que soit l'ensemble S choisi ; dans ce cas, on dit que la conjecture de Brumer-Stark est vraie pour K/k sans mentionner S .

(3) Revenons à la situation envisagée avant l'énoncé de la propriété 6) de θ .

Soit K' un corps intermédiaire entre k et K . Soit $f : \mathfrak{I}_{K'} \longrightarrow \mathfrak{I}_K$ l'homomorphisme évident d'extension des idéaux : $f(a') = a' \mathfrak{O}_K$. Alors,

$$\mathfrak{I}_{S, K'/k}^* = f^{-1}(\mathfrak{I}_{S, K/k}^*).$$

En effet, soit a' un idéal de K' . D'après la propriété 6) de θ , on a $f(a'^{\theta'}) = f(a')^{\theta}$ pour $\theta' = \theta_{S, K'/k}$ et $\theta = \theta_{S, K/k}$. D'après (II), on a l'équivalence $a' \in \mathfrak{I}_{S, K'/k}^* \Leftrightarrow f(a') \in \mathfrak{I}_{S, K/k}^*$. Ainsi, si la conjecture est vraie pour $(S, K/k)$, elle est vraie pour $(S, K'/k)$. Il faut toutefois noter que s'il existe un idéal premier $\mathfrak{p}$ de k ramifié dans K/k mais non dans K'/k , on ne peut pas affirmer que la conjecture pour l'extension K'/k est une conséquence de la conjecture pour l'extension K/k sans mentionner l'ensemble S .

(4) Considérons toujours un corps K' intermédiaire entre k et K ; soit $H = \text{Gal}(K/K')$, et soit S' l'ensemble des places de K' au-dessus d'une place de S . Notons $N : \mathbb{Z}[G] \longrightarrow \mathbb{Z}[H]$ la norme, de sorte que, d'après la propriété 7) de θ , l'on a $\theta' = N \theta$ pour $\theta = \theta_{S, K/k}$ et $\theta' = \theta_{S', K'/k}$.

Posons $A = A_{K/k}$ et $A' = A_{K/K'} = A \cap \mathbb{Z}[H]$, et soit NA l'idéal de $\mathbb{Z}[H]$ engendré par les Na , $a \in A$. On a trivialement $NA \subset A'$. Alors, l'égalité $NA = A'$ entraîne l'inclusion $\mathfrak{I}_{S, K/k}^* \subset \mathfrak{I}_{S', K/K'}^*$.

En particulier, si $NA = A'$ et si la conjecture est vraie pour le couple $(K/k, S)$, elle est vraie pour le couple $(K/K', S')$.

§.3. - Cas dans lesquels la conjecture est démontrée

(a) Corps de fonctions

Comme l'a remarqué B. Mazur, il y a une conjecture analogue à celle de Brumer-Stark dans le cas où k est un corps de fonctions algébriques d'une variable sur un corps fini. Cette conjecture a été démontrée par Deligne qui a prouvé l'analogue de la propriété (III) en utilisant ses 1-motifs, grâce au théorème fondamental de Weil qui exprime les fonctions L à l'aide du polynôme caractéristique de l'automorphisme de Frobenius opérant sur la jacobienne de K .

(b) $k = \mathbb{Q}$ (théorème de Stickelberger)

En utilisant le théorème de Kronecker-Weber et les propriétés (2) et (3), on se ramène tout de suite au cas où K est un corps cyclotomique. On prend $K = \mathbb{Q}(\zeta)$ ($\zeta = e^{2i\pi/m}$, $m \geq 3$, m impair ou $m \equiv 0 \pmod{4}$), et on prend S formé de la place à l'infini de $\mathbb{Q}$ et des diviseurs premiers de m . La propriété (1) montre qu'il suffit de prouver la propriété (II) pour les idéaux premiers $\mathfrak{p}$ premiers à m et de degré 1. Un tel idéal a une norme p congrue à 1 mod m . Soit $\chi_{\mathfrak{p}} : (O_K/\mathfrak{p})^* \longrightarrow \mu_p$ défini par $\chi_{\mathfrak{p}}(x \bmod \mathfrak{p}) \equiv \zeta^{(p-1)/m \bmod p}$ et soit :

$$g_{\mathfrak{p}} = \sum_{\nu=1}^{p-1} \chi_{\mathfrak{p}}(\nu) e^{2i\pi \nu/p}$$

la somme de Gauss correspondante.

Stickelberger a montré l'égalité

$$(g_{\mathfrak{p}}) = \mathfrak{p}^{\left(\frac{1}{2} \sum_{\sigma \in G} \sigma\right) + \theta},$$

où $\theta = \theta_{S, K/\mathbb{Q}} = \sum_{\substack{a=1 \\ (a, m)=1}}^m \left(\frac{1}{2} - \frac{a}{m}\right) \sigma_a^{-1}$, comme expliqué au §.1 (cf. [C], prop. 3.8).

Donc, $\mathfrak{p}$ vérifie la propriété (II) avec $L = \mathbb{Q}(e^{2i\pi/m p}, \sqrt{p})$ et $\mathfrak{p} = p^{-\frac{1}{2}} g_{\mathfrak{p}} \in L$.

(c) Extensions quadratiques

On considère une extension K/k quadratique ; on pose $G = \{1, \tau\}$. Pour tout $v \in S$, on a $G_v = \{1\}$ ou $G_v = \{1, \tau\}$. Mais si $G_v = \{1\}$ pour un $v \in S$, alors $\theta = 0$ (cf. la propriété 3) de θ). On peut donc supposer que l'on a $G_v = \{1, \tau\}$ pour tout $v \in S$.

Soit $Cl_{S,k}$ (resp. $Cl_{S,K}$) le groupe des classes d'idéaux de l'anneau $\mathcal{O}_{S,k}$ (resp. $\mathcal{O}_{S,K} = \mathcal{O}_{S,k} \mathcal{O}_K$) des S -entiers de k (resp. de K). Soit Coker (resp. Ker) le conoyau (resp. le noyau) de la flèche canonique $Cl_{S,k} \longrightarrow Cl_{S,K}$.

LEMME 1. - Si $G_v = G = \{1, \tau\}$ pour tout $v \in S$, alors :

$$\theta_{S,K/k} = \frac{2^{|S|-2} |\text{Coker}|}{w} (1-\tau).$$

Démonstration. - Parce que (dès le début) nous supposons $|S| \geq 2$, on a

$\zeta_{S,k}(0) = 0$. Donc $\theta_{S,K/k} = b(1-\tau)$, avec b tel que

$$\chi(\theta_{S,K/k}) = 2b = L_S(0, \chi),$$

χ désignant le caractère non-trivial de G . Mais dans le cas quadratique, on a

$$L_S(s, \chi) = \frac{\zeta_{S,K}(s)}{\zeta_{S,k}(s)}.$$

Rappelons que, d'après l'équation fonctionnelle de la fonction L combinée avec la formule du résidu de la fonction zêta au point 1, on a :

$$\zeta_{S,k}(s) \sim - \frac{h_{S,k} R_{S,k}}{w_k} s^{|S|-1}$$

pour $s \rightarrow 0$, où $h_{S,k} = |Cl_{S,k}|$, $R_{S,k}$ est le " S -régulateur" de K et $w_k = |\mu_k|$. En combinant ceci avec la même formule pour K au lieu de k , on trouve :

$$(*) \quad L_S(0, \chi) = \frac{h_{S,K} R_{S,K} w_k}{h_{S,k} R_{S,k} w_K}.$$

Soit (ϵ_i) une base du groupe $U_{S,k}$ des S -unités de $k \bmod \mu_K$, et soit $v_0 \in S$. Alors, par définition,

$$R_{S,k} = \pm \det_{i, v \in S - \{v_0\}} (\log \|\epsilon_i\|_v) > 0.$$

Pour chaque $v \in S$, soit v' la place de K au-dessus de S . Alors :

$$R_{S,K} = \pm (U_{S,K} : U_{S,k} \mu_K)^{-1} \det_{i,v \in S - \{v_0\}} (\log \|\varepsilon_i\|_{v'}) .$$

Mais il s'agit des valeurs absolues normées ; donc, $\|\varepsilon_i\|_{v'} = 2 \|\varepsilon_i\|_v$, et l'on en déduit que

$$\frac{R_{S,K}}{R_{S,k}} = \frac{2^{|S|-1}}{[U_{S,K} : U_{S,k} \mu_K]} = \frac{2^{|S|-1}}{[U_{S,K}^{\tau-1} : \mu_K^2]} .$$

Rappelons que K est totalement imaginaire et que k est totalement réel.

Donc τ est induit par la conjugaison complexe pour n'importe quel plongement

$K \subset \mathbb{C}$, de sorte que pour chaque racine de l'unité $\zeta \in \mu_K$, on a $\zeta^\tau = \zeta^{-1}$.

Donc $\mu_K^{\tau-1} = \mu_K^2$. D'autre part, τ agit trivialement sur $U_{S,K}/U_K$, donc un élément $\varepsilon \in U_{S,K}$ tel que $\varepsilon^{1+\tau} = 1$ est dans μ_K . Comme $\mu_K^{1+\tau} = \{1\}$, on voit que $H^1(G, U_{S,K}) = \mu_K / \mu_{S,K}^{\tau-1}$. Désignons simplement par H^1 l'ordre de ce dernier groupe. Alors

$$(**) \quad \frac{R_{S,K}}{R_{S,k}} = \frac{2^{|S|-1} H^1}{[\mu_K : \mu_K^2]} = 2^{|S|-2} H^1 .$$

LEMME 2. - Soit $\mathcal{G}$ un groupe fini d'automorphismes d'un anneau de Dedekind $\mathcal{O}$ tel que $\mathcal{O}$ est non ramifié sur $\mathcal{O}^{\mathcal{G}}$; alors il y a un isomorphisme

$$\text{Ker} (\text{Pic} (\mathcal{O}^{\mathcal{G}}) \longrightarrow \text{Pic}(\mathcal{O})) \approx H^1(\mathcal{G}, \mathcal{O}^*) .$$

En effet, si un idéal α de $\mathcal{O}^{\mathcal{G}}$ devient principal dans $\mathcal{O}$, disons $\alpha \mathcal{O} = (\alpha)$, alors, $\sigma \longrightarrow \alpha^\sigma / \alpha$ est un 1-cocycle de $\mathcal{G}$ dans $\mathcal{O}^*$, dont la classe dans $H^1(\mathcal{G}, \mathcal{O}^*)$ ne dépend que de la classe de α dans $\text{Pic}(\mathcal{O}^{\mathcal{G}})$. Si le cocycle est un cobord, on voit que α est principal. D'autre part, soit $\sigma \longmapsto \varepsilon_\sigma$ un 1-cocycle de $\mathcal{G}$ dans $\mathcal{O}^*$. Par le théorème 90 de Hilbert, il existe un α tel que $\varepsilon_\sigma = \alpha^{\sigma-1}$, donc $(\alpha)^{\sigma-1} = 1$; alors, l'idéal (α) est invariant par $\mathcal{G}$, et $\mathcal{O}/\mathcal{O}^{\mathcal{G}}$ étant non ramifié, alors $\alpha = \alpha \mathcal{O}$ pour un idéal α dans $\mathcal{O}^{\mathcal{G}}$, et le lemme 2 est démontré.

On a, avec les notations introduites avant l'énoncé du lemme 1 et au début de la démonstration du lemme 2,

$$\frac{\text{Coker}}{\text{Ker}} = \frac{h_{S,K}}{h_{S,k}}.$$

En combinant cette égalité avec le lemme 2, (*) et (**), on obtient

$$L(0, \chi) = 2^{|S|-2} |\text{Coker}| \frac{w_k}{w_K}.$$

On a $w_k = 2$ parce que k est totalement réel, donc $b = \frac{1}{2} L(0, \chi) = 2^{|S|-2} |\text{Coker}| w^{-1}$ où $w = w_K$ comme toujours. Le lemme est démontré.

Maintenant, la proposition suivante est à peu près évidente :

PROPOSITION. - Soit K/k une extension quadratique. Alors, la conjecture est vraie pour K/k , et même, plus précisément, dans les propriétés (I)-(IV), on peut remplacer θ par $\theta/2^{|S|-2}$.

Démonstration. - D'après le lemme, il nous faut montrer que, pour chaque α , il y a un $\alpha \in K$ tel que

$$\alpha |\text{Coker}| (1-\tau) = (\alpha)$$

et que $K(\alpha^{1/w})$ est abélienne sur k . Alors, par définition de "Coker", il y a un idéal $\mathfrak{c}$ de k et un $\gamma \in K^*$ tels que

$$\alpha |\text{Coker}| \mathfrak{D}_{S,K} = \gamma \mathfrak{c} \mathfrak{D}_{S,K}$$

donc :

$$\alpha |\text{Coker}| = \gamma \mathfrak{c} b,$$

où b est un idéal de K à support au-dessus de S . Mais pour un tel b nous avons $b^\tau = b$, parce que $G_v = G$ pour toute place finie $v \in S$. Donc $\alpha |\text{Coker}| (1-\tau) = (\gamma^{1-\tau})$, et $\gamma^{1-\tau} \in K^\circ$, parce que $G_v = G$ pour toute place archimédienne $v \in S$. Posons $\alpha = \gamma^{1-\tau}$. Alors, $\alpha^\tau = \alpha^{-1}$, ce qui implique que $L = K(\alpha^{1/w})$ est galoisienne sur k . Désignons encore par τ un automorphisme de L qui induit τ sur K , et par $\beta = \alpha^{1/w}$ un élément de L tel que $\beta^w = \alpha$. Alors $\alpha^{\tau+1} = 1 \Rightarrow \beta^{\tau+1} = \zeta \in \mu_K$, donc τ centralise $\text{Gal}(L/K)$, C.Q.F.D.

(d) Cas où G est engendré par les G_v pour des $v \in S$ tels que $|G_v| = 2$

D'après la proposition que nous venons de démontrer, la conjecture ne semble peut-être pas assez forte, parce que, au moins dans le cas quadratique, on a un $2^{|S|-2}$ de trop. Voici l'explication (voir lignes 24-34 à la page 199 de [Stark IV]) : Supposons d'abord simplement que $G_v = \{1, \tau_v\}$ est d'ordre 2 pour chaque v dans un certain sous-ensemble $S' \subset S$. Soient H le sous-groupe de G engendré par les produits $\tau_v \tau_{v'}$, pour $v, v' \in S'$, et H^+ le sous-groupe engendré par les τ_v , $v \in S'$. D'après la propriété 3) de θ , on a :

$$(1 + \tau_v) \theta = 0 \quad \text{pour } v \in S' \quad (\theta = \theta_{S, K/k}),$$

donc $\tau_v \theta = -\theta$, et $\tau_v \tau_{v'} \theta = \theta$; on a $\sigma \theta = \theta$ pour $\sigma \in H$. Ceci implique que, pour $K' = K^H$, $\theta' = \theta_{S, K'/k}$ et $G = \bigsqcup_{\rho} \rho H$, on a :

$$\theta = \sum_{\rho} a_{\rho} \rho \quad \sum_{\sigma \in H} \sigma \quad \text{et} \quad \theta' = \sum_{\rho} a_{\rho} \hat{\rho} |H|;$$

donc, pour un idéal α de K ,

$$\alpha^{\theta |H|} = (N_{K/K'}, \alpha)^{\theta'}.$$

Il s'ensuit que si la conjecture est vraie pour $(S, K'/k)$, avec θ' remplacé par $\theta' |H|^{-1}$ dans la propriété (II), alors la conjecture est vraie pour $(S, K/k)$.

Supposons maintenant que les τ_v pour $v \in S'$ engendrent G , c'est-à-dire que $G = H^+$. Alors K'/k est quadratique ($[K' : k] = [G : H] \leq 2$ parce que G est engendré par H et un τ_v quelconque; si $K' = k$, alors un produit d'un nombre impair de τ_v est égal à 1, donc $\theta = -\theta$, $\theta = 0$, et il n'y a rien à prouver).

D'après la proposition qui suit (c), combinée avec le paragraphe précédent, la conjecture sera prouvée pour K/k si nous pouvons montrer que $|H| \leq 2^{|S|-2}$, c'est-à-dire que $|G| \leq 2^{|S|-1}$. L'inégalité $|G| \leq 2^{|S'|}$ est évidente, G étant engendré par $|S'|$ éléments τ_v d'ordre 2. Donc c'est gagné si $S' \neq S$. Si $S' = S$, il nous faut montrer qu'il y a une relation entre les τ_v . Il y en a une ! Soit $-1 = (\dots, -1_v, \dots)$ l'idèle -1 de k . Pour chaque place v de k , soit $r_v : k_v^* \rightarrow G_v$ l'application d'Artin locale. On a $\prod_v r_v(-1_v) = 1$ par la loi de réciprocité. Pour $v \notin S$, $r_v(-1_v) = 1$, parce que $\bar{S}$ contient les

places ramifiées. Donc $\prod_{v \in S} r_v(-1_v) = 1$. Pour chaque $v \in S = S'$, on a $r_v(-1_v) = 1$ ou τ_v , mais pour v archimédien $r_v(-1_v) = \tau_v$, parce que $-1_v < 0$ n'est pas une norme de $K_v \approx \mathbb{C}$. Donc il y a une relation non-triviale entre les τ_v comme nous espérons, et la conjecture est vraie pour K/k .

(e) $K \supset k \supset k_0$ avec $\text{Gal}(K/k_0)$ non-abélien d'ordre 8,
 $G = \text{Gal}(K/k)$ d'ordre 4.

Sous cette hypothèse, avec K totalement imaginaire et k totalement réel, comme toujours, soit, pour chaque place réelle v de k , $G_v = \{1, \tau_v\}$ son groupe de décomposition. Si les τ_v ne sont pas tous égaux, ils engendrent G , et on gagne grâce à (d). Supposons donc $\tau = \tau_v$ pour tout v , et soit $G = \{1, \tau, \rho, \sigma\}$. Posons

$$\theta = \theta_{S, K/k} = b + c\tau + d\rho + e\sigma.$$

Comme $\tau\theta = -\theta$ on a $b = -c$, et $d = -e$. D'autre part, ρ et σ sont conjugués dans $G = \text{Gal}(K/k_0)$ (sinon ce groupe serait abélien, parce que τ , lui, est invariant par conjugaison), et il en résulte que $d = e$.

Conclusion : $\theta = \frac{a}{2}(1-\tau)$ pour un $a \in \mathbb{Q}$. Maintenant, soit $H = \{1, \tau\}$ et $K' = K^H$. Alors la norme de $\mathbb{Q}[G]$ à $\mathbb{Q}[H]$ de θ est $\theta^2 = (a^2/2)(1-\tau)$ parce que $\theta \in \mathbb{Q}[H]$. Par la propriété 7) des θ , on a :

$$\frac{a^2}{2}(1-\tau) = N\theta = \theta' = \theta_{S', K/K'}.$$

Mais, K/K' étant quadratique, on a, par le lemme 1 du cas (c) :

$$\theta' = \frac{2^{|S'| - 2} |\text{Coker}|}{w} (1-\tau).$$

Dans la situation envisagée, $w = 2$, sinon, il y aurait une racine de l'unité $\zeta \in K$, $\zeta \notin K'$ (qui, lui, est réel), donc $K = k_0(\zeta, K')$ serait abélienne sur k_0 . Donc on a :

$$a^2 = 2^{|S'| - 2} |\text{Coker}|$$

où Coker est le "Coker" du (c) pour S' et K/K' , et pour démontrer la conjecture pour K/k il nous faut montrer, pour chaque idéal α de K , que $\alpha^{a(1-\tau)} = (\alpha)$ avec $\alpha \in K^\circ$ tel que $K(\sqrt{\alpha})/k$ soit abélienne.

En fait, nous allons voir que $a^{a(1-\tau)} = (\beta^2)$ avec $\beta \in K$. Le fait que K' est totalement réel implique (parce que chaque place archimédienne de k devient deux places dans K) que $|S'| \geq |S| + [k : \mathbb{Q}] \geq |S| + 2 \geq 4$, donc :

$$a^2 = 2^{2+n} |\text{Coker}|$$

avec $n \in \mathbb{Z}$, $n \geq 0$. Le "Coker" est un $\mathbb{Q} \xrightarrow{\text{def}} \text{Gal}(K/k_{\mathbb{Q}})$ -module fini sur lequel τ agit comme -1 .

LEMME. - Soit $\mathbb{Q}$ un groupe non-abélien d'ordre 8 dont le centre est $\{1, \tau\}$.

Soit M un $\mathbb{Q}$ -module fini sur lequel τ agit comme -1 . Alors $|M| = m^2$ ou $\frac{1}{2}m^2$ pour un entier $m > 0$, et l'on a $mM = (0)$.

Admettons ce lemme pour le moment. Alors pour $M = \text{Coker}$, on a $(a/2)^2 = 2^n |M| = 2^n m^2$ ou $2^{n-1} m^2$, donc $(a/2) \in m\mathbb{Z}$. On en déduit que $(a/2)$ tue Coker, donc

$$a^{a/2} = \gamma c b,$$

où c est un idéal de k , $\gamma \in K^*$, et b un idéal de K à support au-dessus de S , comme à la fin de (c). On peut supposer $G_v \neq (1)$ pour tout v dans S comme toujours, donc $\tau \in G_v$ pour tout $v \in S$, donc $b^{\tau} = b$. Il en résulte que

$$a^{(a/2)(1-\tau)} = (\gamma^{1-\tau})$$

donc on peut prendre $\beta = \gamma^{1-\tau} \in K^{\circ}$.

Démonstration du lemme. - On peut supposer que M est indécomposable, donc

$|M|$ est une puissance d'un nombre premier p . Supposons d'abord $p \neq 2$ pour le $\mathbb{Q}$ -module M . Alors chaque quotient simple $N_v = M_v / M_{v+1}$ est tué par p , donc est l'espace d'une représentation irréductible de $\mathbb{Q}$ sur $\mathbb{F}_p$, sur lequel τ agit comme -1 . Pour $p \neq 2$, p ne divise pas $|\mathbb{Q}|$, donc les représentations de $\mathbb{Q} \pmod{p}$ sont relevables sur $\mathbb{Z}_p$. Une représentation irréductible de $\mathbb{Q}$ sur $\mathbb{Q}_p$ avec τ agissant par -1 est de dimension 2. Donc N_v est de dimension 2, $|N_v| = p^2$, $|M| = p^{2\ell}$, et (par induction sur ℓ) $p^{\ell} M = 0$. Pour $p = 2$, on peut gagner en considérant M comme un module sur $\mathbb{Z}[\gamma]$, où γ est un élément de G tel que $\gamma^2 = \tau$, au-lieu de $\mathbb{Z}[\mathbb{Q}]$.

En effet, puisque $\gamma^2 = \tau$ agit comme -1 , M est un module sur l'anneau de Gauss $\mathbb{Z}[i] = \mathbb{Z} + \mathbb{Z}i$, avec $i^2 = -1$; M étant indécomposable d'ordre une puissance de 2, on a $M \approx \mathbb{Z}[i] / (1+i)^\ell$ pour $\ell =$ longueur de M . Donc $|M| = 2^\ell$, et $m^2 = 2^\ell$ ou $2^{\ell+1}$ est divisible par $(1+i)^\ell$, donc tue M , C.Q.F.D.

§.4. - Choses à faire

Je crois que la conjecture générale sera longue à démontrer. Néanmoins, on peut essayer de la démontrer dans des situations particulières ; il peut être aussi possible de faire des calculs numériques pour la tester.

Calculs numériques. - Le cas où $k = \mathbb{Q}$ étant réglé, on doit commencer par des corps k quadratiques réels. Alors, le corps K étant totalement imaginaire, ce qui entraîne que $[K:k]$ est divisible par 2, et le cas où K/k est une extension quadratique étant réglé, le premier cas ouvert est $[K:k] = 4$; le corps K est déjà de degré 8, et c'est probablement à cause de l'importance du degré que personne, à ma connaissance, n'a entrepris d'étude numérique. Mais cela doit être possible à l'aide d'un ordinateur. Bien entendu, si $K/\mathbb{Q}$ est galoisienne non abélienne, on est dans le cas (c) et il est inutile de faire des calculs. Si $K/\mathbb{Q}$ est une extension abélienne, la démonstration doit pouvoir se faire sans calcul à l'aide du théorème de Stickelberger. Donc, pour faire des calculs numériques, il faudrait commencer par les extensions K/k de degré 4, telles que K n'est pas une extension galoisienne de $\mathbb{Q}$. Pour calculer θ , on peut utiliser les formules de Siegel ([S]) ou de Shintani ([Sh]).

Cas spéciaux à considérer. - D'abord, il y a la situation dans laquelle K est une extension abélienne de $\mathbb{Q}$, le sous-corps k de K n'étant pas le corps $\mathbb{Q}$ lui-même. Je crois possible de traiter le cas où K est contenu dans un corps cyclotomique $\mathbb{Q}(e^{2i\pi/p^n})$, p premier impair, en utilisant les idées discutées dans la propriété (4) des groupes $\mathcal{T}_{S, K/k}^*$, mais je n'ai pas écrit les détails.

Un autre cas abordable doit être celui d'un groupe G d'exposant 2 .
 Dans ce cas, on peut donner une formule explicite pour θ à l'aide du lemme
 utilisé dans (c) qui permet de trouver l'image de θ dans $\mathbb{Q}[G']$ pour tous
 les quotients G' de G d'ordre 2 . En particulier, le cas du groupe de Klein
 d'ordre 4 doit être étudié en détail.

-:-:-:-

BIBLIOGRAPHIE

- [C] J. COATES, $\mathbb{P}$ -adic L functions and Iwasawa's theory, in Algebraic
 Number Fields, A. Fröhlich éd., Academic Press, London, 1977,
 269-353.
- [D - R] P. DELIGNE, K.A. RIBET, Values of L-functions at Negative Integers
 over Totally Real Fields, Invent. Math. 59 (1980), 227-286.
- [S] C.L. SIEGEL, Über die Fourierschen Koeffizienten von Modulformen,
 Nachr. Akad. Wiss. Göttingen (1970), 15-56.
- [Sh] T. SHINTANI, On evaluation of zeta functions of totally real algebraic
 number fields at non-positive integers, J. Fac. Sc. Tokyo 23 (1976),
 393-417.
- [St IV] H.M. STARK, L-Functions at $s=1$, IV. First Derivatives at $s=0$.
 Advances in Math. 35 (1980), 197-235.
- [T] J. TATE, Les conjectures de Stark sur les fonctions L d'Artin en $s=0$,
 notes d'un cours à Orsay rédigées par D. Bernardi et N. Schappacher,
 à paraître.
- [W-W] E. WHITTAKER, G. WATSON, A Course of Modern Analysis, 4e ed.,
 Cambridge University Press, 1965.

(texte reçu le 22 mai 1981)

-:-:-:-

John TATE
 Département de Mathématiques
 Université de Paris-Sud
 F 91405 ORSAY CEDEX

 Department of Mathematics
 Harvard University
 CAMBRIDGE MA 02138
 (U.S.A.)

ZEROS OF p -ADIC L -FUNCTIONS

by

Lawrence C. WASHINGTON

-:-:-:-

Let χ be a non-trivial even Dirichlet character and let $L_p(s, \chi)$ be the associated p -adic L -function. It is natural to consider the location of the zeros of this function. For example, is there a disc around $s=1$, independent of χ , in which there are no zeros? This could be regarded as a possible analogue of the Riemann Hypothesis. However, the following result shows that this is probably false; in particular, it yields 3-adic L -functions with zeros very close to $s=1$.

THEOREM. - Let χ be a non-trivial even quadratic character of conductor f and assume 3 does not divide f . Let ε be the fundamental unit of $\mathbb{Q}(\sqrt{f})$. Suppose that

$$3^m \mid h(\mathbb{Q}(\sqrt{f})) = h^+$$

$$3^n \mid \varepsilon^8 - 1 \quad (\Leftrightarrow 3^n \mid \log_3(\varepsilon)),$$

$$m+n \geq 3,$$

$$9 \nmid h(\mathbb{Q}(\sqrt{-3f})) = h^-.$$

Then $L_p(s, \chi)$ has a unique zero β , $\beta \in \mathbb{Z}_p$ with

$$\beta \equiv 1 \pmod{3^{m+n-2}}.$$

Examples. - To obtain examples, we can either use h^+ (i.e., make m large) or use ϵ (n large).

(1) With h^+

f	h^+	h^-	n	zero
21 433	27	60	1	$\beta \equiv 1 \pmod{9}$
36 073	27	84	1	$\beta \equiv 1 \pmod{9}$
94 865	54	156	3	$\beta \equiv 1 \pmod{81}$

(2) With ϵ

f or $f/4$	h^+	h^-	n	zero
$122 = 11^2 + 1$	2	12	5	$\beta \equiv 1 \pmod{27}$
$48\ 845 = 221^2 + 4$	12	192	6	$\beta \equiv 1 \pmod{243}$
$64\ 517 = 254^2 + 1$	6	276	7	$\beta \equiv 1 \pmod{729}$

The proof of the theorem may be sketched as follows. Leopoldt's class number formula says that

$$\frac{2h^+ \log_3 \epsilon}{\sqrt{f}} \left(1 - \frac{\chi(3)}{3}\right) = L_3(1, \chi).$$

It follows that 3^{m+n-1} divides $L_3(1, \chi)$, so $L_3(1, \chi)$ is small 3-adically.

Also,

$$L_3(0, \chi) = -B_{1, \chi \omega^{-1}} = h^-,$$

where ω is the Teichmüller character. Iwasawa has proved that there is a power series

$$f(T) = b_0 + b_1 T + \dots \in \mathbb{Z}_3[[T]]$$

such that

$$L_3(s, \chi) = f((1+3f)^s - 1).$$

It follows easily from the above that 3 divides b_0 but 3 does not divide b_1 . The p-adic Weierstrass Preparation Theorem implies that

$$f(T) = (T - \alpha) U(T)$$

with $U(T)$ invertible and $\alpha \in 3\mathbb{Z}_3$. It follows that there is exactly one zero β of $L_3(s, \chi)$. Since $L_3(1, \chi)$ is small, β must be near $s = 1$. This completes the sketch of the proof.

In classical analytic number theory, the possibility of zeros near 1 ("Siegel zeros") arises in problems such as the Brauer-Siegel theorem. The main result needed is that there is, in a certain sense, at most one such zero. However, in the p-adic case there is the additional possibility of many such zeros, and correspondingly (but not as a consequence) the p-adic Brauer-Siegel theorem fails.

THEOREM. - There exists a sequence of totally real fields K such that

$$\frac{[K : \mathbb{Q}]}{v_p(d_K)} \longrightarrow 0$$

but

$$\frac{v_p(h_K R_{K,p})}{v_p(\sqrt{d_K})} \longrightarrow \infty$$

(v_p = p-adic valuation, h_K = class number, $R_{K,p}$ = p-adic regulator).

The p-adic analogue of the Brauer-Siegel theorem would have required the limit to be 1, not ∞ . However, there is a result analogous to the "easy" half of the Brauer-Siegel theorem (where Siegel zeros do not play a role).

PROPOSITION. - If K is a sequence of totally real number fields such that

$$\frac{[K : \mathbb{Q}]}{v_p(d_K)} \longrightarrow 0,$$

then

$$\liminf \frac{v_p(h_K R_{K,p})}{v_p(\sqrt{d_K})} \geq 1.$$

Finally, we consider a function field k over a finite field $\mathbb{F}_q$. The classical zeta function has the form

$$\zeta_k(s) = \frac{P(q^{-s})}{(1-q^{-s})(1-q^{1-s})}, \quad P(T) \in \mathbb{Z}[T].$$

Let ℓ be a prime not dividing q . To get a continuous ℓ -adic function, we replace q by $\langle q \rangle$, where $q = \omega(q)\langle q \rangle$ with $\langle q \rangle \equiv 1 \pmod{\ell}$. Then

$$\zeta_{k,\ell}(s) = \frac{P(\langle q \rangle^{-s})}{(1-\langle q \rangle^{-s})(1-\langle q \rangle^{1-s})}.$$

PROPOSITION. - Let $\ell \neq p$ be two primes and let $S = \{s \in \mathbb{Z}_\ell \mid \text{there exists } q = \text{a power of } p, \text{ and there exists } k \text{ of genus } 1 \text{ and constant field } \mathbb{F}_q \text{ with } \zeta_{k,\ell}(s) = 0\}$. Then S is dense in $\mathbb{Z}_\ell$.

This shows in particular that there are examples of zeros arbitrarily close to 1 in the function field case, and it is likely that a similar result holds for number fields. Note that although the polynomial $P(T)$ satisfies a Riemann Hypothesis, $\zeta_{k,\ell}$ does not. In the number field case, one might therefore expect the Iwasawa power series $f(T)$ to satisfy some type of Riemann Hypothesis. However, $f(T)$ depends on the choice of a generator of the Galois groups of a certain $\mathbb{Z}_p$ -extension, and at present there is no obvious way to make this choice.

(texte reçu le 29 septembre 1981)

--:--:--

Lawrence C. WASHINGTON
University of Maryland
Department of Mathematics
College Park
MARYLAND 20 742, U. S.A.

SUR L'HISTOIRE DES ÉQUATIONS INDETERMINÉES DE GENRE 1
DEPUIS DIOPHANTE

par

André WEIL

-:-:-:-

Parmi les problèmes mathématiques qui remontent à l'antiquité grecque, il n'y en a peut-être que deux qui demeurent ouverts, et un seul qui reste actuel ; celui-ci consiste en la recherche des points rationnels sur une courbe de genre 1, donnée sur $\mathbb{Q}$; l'autre étant le problème de l'existence de nombres parfaits impairs.

Les problèmes traités dans la collection qui nous est parvenue sous le nom de Diophante (III^e siècle de notre ère) se ramènent tous à la recherche de points rationnels sur des courbes de genre 0 ou 1 ; chez Diophante il s'agit toujours d'équations ou de systèmes d'équations qui, lorsque nous les considérons comme définissant des courbes dans des espaces projectifs, ont au moins un point rationnel évident (s'il s'agit du genre 0) ou en ont au moins deux (s'il s'agit du genre 1).

Dans l'un et l'autre cas chacun sait à présent qu'on peut, par voie purement algébrique, déduire d'autres points rationnels, et même le plus souvent une infinité de tels points, de ceux qui sont connus. Le cas du genre 0 est relativement trivial, et en tout cas a été complètement et définitivement résolu par Lagrange ; il sera laissé de côté dans le présent exposé.

Quant au genre 1, il se présente toujours chez Diophante sous la forme soit d'une équation $P(x) = y^2$ où P est un polynôme de degré 3 ou 4, soit d'une "double équation" $F(x) = y^2$, $G(x) = z^2$, où F et G sont du second degré. Dans ce dernier cas, qui est le plus fréquent, il se trouve toujours que les coefficients de x^2 dans F et G , ou bien les coefficients constants, sont des "carrés parfaits" ; de notre point de vue moderne, si les coefficients de x^2 sont des carrés, cela veut dire que, dans l'espace projectif, la courbe a quatre points rationnels à l'infini. De même, si le coefficient de x^4 dans P est un carré, la courbe $P(x) = y^2$, regardée comme droite projective double, a deux points à l'infini ; etc. Le caractère systématique des procédés que Diophante applique aux problèmes de cette espèce indique qu'il avait conscience d'un début de classification

Diophante fut redécouvert au XVI^e siècle par Bombelli, puis par Viète ; celui-ci, le plus grand algébriste de son époque, donna la transcription des procédés de Diophante en notation algébrique moderne (ce qui incidemment, comme le fit en substance observer Fermat, montre qu'ils restent valables sur un corps quelconque). Bachet, qui édita, traduisit et commenta Diophante en 1621, n'y ajouta rien d'utile ; mais c'est son Diophante qui servit de point de départ à Fermat.

En ce qui concerne les équations de genre 1, l'œuvre de Fermat se divise en deux parties. D'une part il fut le premier à voir que l'application répétée des procédés de Diophante permet en général d'obtenir une infinité de solutions d'un problème donné ; parfois il semble même admettre qu'on trouve ainsi toutes les solutions, mais il ne s'explique jamais clairement sur ce point. Mais sa contribution la plus originale à ces questions fut la "méthode de descente", au moyen de laquelle il put démontrer que certaines équations de genre 1 n'ont pas de

solution non triviale ; par exemple l'équation $x^4 - 1 = y^2$ (ou, ce qui revient au même, l'équation $X^4 - Z^4 = Y^2$ à résoudre en nombres entiers) n'a que les solutions évidentes ; nous possédons même sa démonstration pour cette dernière équation, mais il est certain qu'il en traita aussi beaucoup d'autres (y compris l' "équation de Fermat" pour les cubes, $X^3 - Z^3 = Y^3$).

S'inspirant de Fermat, Euler reprit l'œuvre de celui-ci dans l'une et l'autre des directions indiquées, et d'abord reconstitua les démonstrations perdues de Fermat. Aux divers types d'équations hérités de Diophante et de Fermat, il en ajouta un nouveau : c'est le type $F(x,y) = 0$, où F est de degré 2 en x et de degré 2 en y ; ce type, qui apparaît vers la fin de la vie d'Euler, est celui même qui joue le rôle principal dans ses recherches sur les intégrales elliptiques. Par exemple, lorsqu'il s'agit de trouver des intégrales algébriques pour une équation différentielle

$$\frac{dx}{\sqrt{P(x)}} = \frac{dy}{\sqrt{P(y)}} ,$$

où P est un polynôme de degré 4 (problème équivalent à l'addition des fonctions elliptiques), c'est sous la forme $F(x,y) = 0$ qu'Euler les obtient, avec F comme ci-dessus. C'est ce qui a fait dire à Jacobi qu'Euler, même s'il n'en dit rien, avait dû avoir conscience du lien entre ces deux genres de questions.

Effectivement Jacobi s'aperçut du fait que les courbes de genre 1 s'uniforment par les fonctions elliptiques et que par conséquent les théorèmes d'addition et de multiplication de ces fonctions rendent parfaitement compte des procédés de Diophante, de Fermat et d'Euler pour trouver de nouvelles solutions à partir de solutions connues. Après quoi les équations diophantiennes disparurent pour un siècle du champ de vision des mathématiciens, et il fallut Mordell pour faire voir, en 1922, qu'en fait, sur toute courbe de genre 1, il suffit de connaître des solutions en nombre fini (les "générateurs" du groupe des solutions) pour avoir toutes les autres par voie algébrique. Quant à trouver ces solutions en nombre fini, nous ne sommes guère plus avancés que Diophante.

(texte reçu le 20 octobre 1981)

-:-:-:-

André WEIL
The Institute for Advanced Study
School of Mathematics
PRINCETON, NEW-JERSEY 08540
(U. S. A.)

A NEW METHOD IN THE ELEMENTARY THEORY OF PRIMES

by

Mohan NAIR

--:--:--

Let $\pi(x)$ denote the number of primes not exceeding x and $\psi(x)$ denote, as usual, the Chebyshev ψ -function. It is well-known and easily proved that the Prime Number Theorem,

$$\pi(x) \sim \frac{x}{\log x} \quad (x \rightarrow \infty),$$

is equivalent to

$$\psi(x) \sim x \quad (x \rightarrow \infty)$$

and also to

$$\psi_1(x) \sim \frac{1}{2} x^2 \quad (x \rightarrow \infty)$$

where

$$\psi_1(x) = \sum_{m \leq x} \psi(m) .$$

It is also well-known that, for $n \in \mathbb{N}$, $\psi(n) = \log d_n$ where

$$d_n = \text{L. C. M. } \{m\} . \\ 1 \leq m \leq n$$

In this talk, I shall describe a new method to obtain good lower bounds for the functions $\psi(x)$ and $\psi_1(x)$. This has the surprising feature, in elementary prime number theory, of leading directly to a lower bound for $\psi_1(x)$ rather than for $\psi(x)$ as may be expected. The bound for $\psi(x)$ can then be deduced from the one obtained for $\psi_1(x)$ although some precision is lost in the process. For this reason, we shall only describe the technique for obtaining lower bounds for $\psi_1(x)$.

An expanded version of this talk has been submitted for publication in the Journal of the London Mathematical Society.

We begin with a simple application of the ideas involved.

THEOREM 1. - For sufficiently large x ,

$$\psi_1(x) \geq (0.47459) x^2 .$$

Proof. - Cauchy proved that, for $n \in \mathbb{N}$,

$$\det \left(\frac{1}{a_i + b_j} \right)_{i,j=1}^n = \frac{\prod_{i>j} (a_i - a_j)(b_i - b_j)}{\prod_{i,j} (a_i + b_j)} .$$

A proof may be found in [1]. Put $a_i = m+i$, $b_j = j$ where $m \in \mathbb{N}$. Then

$$D = \begin{vmatrix} \frac{1}{m+2} & \frac{1}{m+3} & \cdots & \frac{1}{m+n+1} \\ \frac{1}{m+3} & \frac{1}{m+4} & \cdots & \frac{1}{m+n+2} \\ \vdots & & & \\ \frac{1}{m+n+1} & \cdots & & \frac{1}{m+2n} \end{vmatrix} = \frac{\prod_{i>j} (i-j)^2}{\prod_{i,j} (m+i+j)} . \quad (1)$$

Note that $d_{m+n+1} \times D$ makes the first row of D into integers,

$d_{m+n+1} \cdot d_{m+n+2} \times D$ makes the first two rows of D into integers and in general,

$$\prod_{i=1}^n d_{m+n+i} \times D$$

is a determinant with integer entries which is positive and hence its value is a natural number. Therefore we have that

$$\prod_{i=1}^n d_{m+n+i} \times D \geq 1$$

so that, taking logs,

$$\sum_{i=1}^n \psi(m+n+i) \geq -\log D$$

or

$$\psi_1(m+2n) - \psi_1(m+n) \geq -\log D. \quad (2)$$

It only remains to evaluate $\log D$ from (1) and this can easily be done, via Stirling's formula, to obtain

$$\begin{aligned} \log D = & -\frac{(2n+m)^2 \log(2n+m)}{2} + (n+m)^2 \log(n+m) + n^2 \log n \\ & - \frac{m^2 \log m}{2} + O((n+m) \log(n+m)). \end{aligned} \quad (3)$$

Put $m = [sn]$ where s is a real parameter in $[0, 1]$ to deduce, from (2) and (3), that

$$\begin{aligned} \psi_1((2+s)n) - \psi_1((1+s)n) & \geq \left\{ \frac{(2+s)^2 \log(2+s)}{2} + (1+s)^2 \log(1+s) - \frac{s^2 \log s}{2} \right\} n^2 + O(n \log n), \\ & \geq f(s) n^2 + O(n \log n), \quad \text{say.} \end{aligned} \quad (4)$$

For any $x \geq 3$, we may put $n = [x/(2+s)]$ to obtain from (4) that

$$\psi_1(s) - \psi_1\left(\frac{1+s}{2+s}x\right) \geq \frac{f(s)}{(2+s)^2} x^2 + O(x \log x).$$

This quickly leads, by summation, to

$$\psi_1(x) \geq \frac{f(s)}{2s+3} x^2 + O(x \log^2 x).$$

We now choose s appropriately. Note that for $s = 0$, $f(s)/(2s+3) = 2 \log 2/3$ so that we obtain

$$\begin{aligned} \psi_1(x) & \geq \left(\frac{2 \log 2}{3}\right) x^2 + O(x \log^2 x) \\ & \geq (0.4634) x^2 \quad \text{for large } x. \end{aligned}$$

The optimal choice of s is $s = 0.222676$ which gives

$$\psi_1(x) \geq (0.47459) x^2 \quad \text{for large } x.$$

This completes the proof of Theorem 1.

In order to proceed further with these ideas, we may observe that the entries of D are of the form

$$\int_0^1 t^r dt$$

for suitable $r \in \mathbb{N}$. We should therefore consider determinants with entries of the form

$$\int_0^1 t^r w(t) dt$$

where $w(t)$ is a suitable non-negative polynomial weight function.

THEOREM 2. - For sufficiently large x ,

$$\psi_1(x) \geq (0.49517) x^2.$$

Proof. - Let $n, p, q \in \mathbb{N}$ and let $w(t) = t^q(1-t)^p$. Put, for $r \in \mathbb{N}$,

$$c_r = \int_0^1 t^r w(t) dt = \int_0^1 t^{r+q} (1-t)^p dt = \sum_{j=0}^p (-1)^j \binom{p}{j} \frac{1}{r+q+j+1}.$$

Note that $d_{p+q+r+1} c_r$ is a natural number. By repeated integration by parts, we get

$$1/c_r = (r+q+1) \binom{p+q+r+1}{p}.$$

Hence taking logarithms and choosing $p = q$ and $r = 0$ already leads to

$$\psi(2p+1) \geq (2 \log 2) p.$$

(For full details of this argument and also of a corresponding upper bound, see [2].) We, however, proceed in the spirit of Theorem 1 and consider the determinant

$$\Delta = |c_{i+j}|, \quad (1 \leq i, j \leq n), \quad n \in \mathbb{N}.$$

Before we can proceed any further, we need to confirm that Δ is non-zero.

Fortunately we can write Δ as the following n -dimensional integral (see e. g. [3] for details).

$$\Delta = \frac{1}{n!} \int_0^1 \int_0^1 \dots \int_0^1 \prod_{i=1}^n w(t_i) \prod_{i>j} (t_i - t_j)^2 dt_1 dt_2 \dots dt_n .$$

In particular, since $w(t)$ is non-negative for $0 \leq t \leq 1$, we have that $\Delta > 0$. As before, we may now observe that

$$\Delta \prod_{i=1}^n d_{p+q+n+1+i}$$

is a positive determinant with integer entries and hence is ≥ 1 . Thus, taking logs, we obtain

$$\sum_{i=1}^n \psi(p+q+n+1+i) \geq -\log \Delta$$

or

$$\psi_1(p+q+2n+1) - \psi_1(p+q+n+1) \geq -\log \Delta . \quad (5)$$

The problem now is to determine $\log \Delta$. Let, for $0 \leq t_i \leq 1$,

$$T(t_1, t_2, \dots, t_n) = \prod_{i=1}^n w(t_i) \prod_{i>j} (t_i - t_j)^2 .$$

Since $T(t_1, t_2, \dots, t_n)$ is a continuous function defined on a compact set,

$$\sup_{0 \leq t_i \leq 1} T(t_1, t_2, \dots, t_n) = T$$

exists and from the above integral representation for Δ , we have

$$\Delta \leq \frac{1}{n!} T$$

so that, from (5), we get

$$\psi_1(p+q+2n+1) - \psi_1(p+q+n+1) \geq \log(n!) - \log T . \quad (6)$$

We now evaluate $\log T$. Rather surprising, T can be exactly determined.

LEMMA

$$T = \frac{\binom{n+p-1}{n}^p \binom{n+q-1}{n}^q \prod_{i=1}^n i^{i-2n+2} (i+q-1)^{i-1} (i+p-1)^{i-1} (n+p+q+i+2)^{n-i}}{\binom{2n+p+q-2}{n}^{2n+p+q-2}} .$$

Details of the proof of this lemma may be found in my paper. The idea of the proof goes back to Stieltjes in the 1850's. We show that $t_1, \dots, t_n$ which attain T are the zeros of a certain Jacobi polynomial normalised to $[0, 1]$. Results for the discriminant of this polynomial are required because of the term

$$\prod_{i>j} (t_i - t_j)^2$$

in the expression for $T(t_1, t_2, \dots, t_n)$.

Assuming the lemma, we proceed as in Theorem 1. Put $p = q = \lfloor sn \rfloor$ where $s \in (0, 1)$ to get from (6) that

$$\psi_1((2s+2)n) - \psi_1((2s+1)n) \geq \frac{g(s)}{2} n^2 + O(n \log n)$$

where

$$g(s) = 2(1+s)^2 \log(1+s) + 4(1+s)^2 \log 2 - (1+2s)^2 \log(1+2s) + 2s^2 \log s$$

For any $x \geq 4$, put $n = \lfloor x/(2s+2) \rfloor$ to deduce

$$\psi_1(s) \geq \frac{g(s)}{8s+6} x^2 + O(x \log^2 x) .$$

Note that for $s = 1/2$, $g(1/2) = 9 \log 3/2$ so that we get

$$\begin{aligned} \psi_1(x) &\geq \left(\frac{9}{20} \log 3\right) x^2 + O(x \log^2 x) \\ &\geq (0.494375) x^2 \quad \text{for large } x . \end{aligned}$$

The optimal value of s is $s = 0.39191162$ which leads to

$$\psi_1(x) \geq (0.49517) x^2 \quad \text{for large } x .$$

This completes the proof of Theorem 2.

In conclusion, it is perhaps appropriate to mention that there are good reasons for believing that weight functions of the form

$$w(x) = x^q (1-x)^p (1-2x)^{2r}$$

and

$$w(x) = x^q (1-x)^p (1-2x)^{2r} (5x^2 - 5x + 1)^{2s},$$

where $p, q, r, s \in \mathbb{N}$, would lead to better results but the exact limit of this method is not known.

-:-:-:-

REFERENCES

- [1] G. PÓLYA and G. SZEGÖ, Aufgaben und Lehrsätze aus der Analysis, vol. II.
- [2] M. NAIR, On Chebyshev-type inequalities for primes, to appear in the American Maths Monthly.
- [3] G. SZEGÖ, Orthogonal Polynomials, American Mathematical Society Colloquium Publications, vol. XXIII.

(texte reçu le 22 juin 1981)

-:-:-:-

M. NAIR
Department of Mathematics
University of Glasgow
GLASGOW, Scotland

TWO RESULTS IN METRICAL DIOPHANTINE APPROXIMATION

by

Kunrui YU

-:-:-:-

I. - Hausdorff dimension and simultaneous rational approximation

Let us recall the definition of the Hausdorff dimension of a set S in $\mathbb{R}^k$. By $\mathcal{C}$ we signify a finite or denumerable set of k -dimensional cubes C whose sides have length $\ell(C)$. The Hausdorff dimension of S , termed $\dim S$, is defined as the supremum of the values of $s > 0$ for which there exists $\rho > 0$ such that

$$\inf_{\mathcal{C}} \sum_{C \in \mathcal{C}} (\ell(C))^s \neq 0,$$

where the infimum is taken over all coverings $\mathcal{C}$ of S with $\ell(C) \leq \rho$ for all C in $\mathcal{C}$.

For real numbers x , let $\|x\| = \min_{\ell \in \mathbb{Z}} |x - \ell|$, $\bar{x} = \max(1, |x|)$. Let δ be a given positive number. Denote by $E(m, n; \delta)$ the set of all

$(\theta_{11}, \dots, \theta_{1n}, \dots, \theta_{m1}, \dots, \theta_{mn})$ in $\mathbb{R}^{mn}$ for which there exist infinitely many $(q_1, \dots, q_n) \in \mathbb{Z}^n$ satisfying

$$(\bar{q}_1 \dots \bar{q}_n)^{1+\delta} \prod_{i=1}^m \left\| \sum_{j=1}^n \theta_{ij} q_j \right\| < 1. \quad (1)$$

We have the following.

THEOREM 1. - $\dim E(m, n; \delta) = mn - 1 + 2/(2+\delta)$.

This generalizes the well-known theorem of Jarnik [8] and Besicovitch [5] (on taking $m=n=1$ in Theorem 1) and the theorem of Bovey and Dodson [6] (on taking $n=1$). Our proof requires some techniques from linear algebra together with the basic method of Bovey and Dodson.

Note that this theorem implies, in particular, that $E(m, n; \delta)$ has Lebesgue measure zero (see also Wang and Yu [8]). On the other hand, the famous Thue-Siegel-Roth-Schmidt theorem [11] asserts that (1) (with $n=1$) has only finitely many solutions in positive integers q_1 when $\theta_{11}, \dots, \theta_{m1}$ are algebraic numbers with $1, \theta_{11}, \dots, \theta_{m1}$ linearly independent over $\mathbb{Q}$; and the important theorem of Baker [1] shows that the same holds for $\theta_{i1} = e^{\gamma_{i1}}$ where $\gamma_{11}, \dots, \gamma_{m1}$ are distinct non-zero rationals. These theorems lead one to conjecture that (1) has only finitely many solutions in $(q_1, \dots, q_n) \in \mathbb{Z}^n$ when θ_{ij} are algebraic numbers which, together with 1, are linearly independent over $\mathbb{Q}$; further the same probably holds when $\theta_{ij} = e^{\gamma_{ij}}$ with γ_{ij} distinct non-zero rationals; in fact the latter conjecture almost certainly holds more generally when the γ_{ij} ($1 \leq j \leq n$) are distinct non-zero rationals and $(\gamma_{i1}, \dots, \gamma_{in})$ are distinct vectors for $1 \leq i \leq n$.

II. - A note on a problem of Baker in metrical Diophantine approximation

Let $P(x) = a_0 + a_1 x + \dots + a_n x^n \in \mathbb{Z}[x]$ have degree n and height $h = \max_{0 \leq i \leq n} |a_i|$. Mahler conjectured in 1932 that for almost all real numbers θ , any positive integer n and any positive number ε there exist only finitely many polynomials P as above such that

$$|P(\theta)| < h^{-(n+\varepsilon)}; \quad (2)$$

he further conjectured that a similar result would hold for almost all complex numbers θ , in terms of planar Lebesgue measure, with the exponent n in (2) replaced by $\frac{1}{2}n$. Mahler originally proved that, in both cases, the conjecture is true if the exponent n in (2) is replaced by $4n$, and $4n$ was reduced to $3n$ and $\frac{5}{2}n$ in the real and complex cases respectively by Koksma in 1939. Leveque improved these in 1953 to $2n$ and $\frac{5}{3}n$, and Volkmann further reduced them in 1964 to $\frac{4}{3}n$ and $\frac{2}{3}n$. Moreover in the cases $n=2$ and $n=3$ proofs of Mahler's conjecture were obtained by Kubilyus, Kasch and Volkmann. Finally Sprindžuk [13] established in 1965 a complete proof of the conjecture for all n , and indeed with the best possible exponent $\frac{1}{2}(n-1)$ instead of $\frac{1}{2}n$ in the complex case. His paper contains references to the earlier works.

In 1966, Baker [2] obtained a refinement of Sprindžuk's theorem to the effect that (2) can be replaced by

$$|P(\theta)| < (\psi(h))^n \quad \text{and} \quad |P(\theta)| < (\psi(h))^{\frac{1}{2}(n-1)}$$

in the real and complex cases respectively, where $\psi(h)$ is any positive monotonic decreasing function such that $\sum \psi(h)$ converges. Further, as Baker pointed out in [2], the refinement implies that for almost all real θ and any positive integer n , there exist only finitely many positive integers q such that

$$\max_{1 \leq j \leq n} \|q\theta^j\| < q^{-1/n} (\phi(q))^n,$$

where $\phi(q)$ is a positive monotonic decreasing function of the integer variable $q > 0$ such that $\sum \phi(q)/q$ converges. In particular it follows from the truth of Mahler's conjecture that, for any $\varepsilon > 0$, the inequality

$$\max_{1 \leq j \leq n} \|q\theta^j\| < q^{-(1/n)-\varepsilon}$$

has only finitely many solutions for almost all real θ .

In his book [3] (see also Sprindžuk [14]), Baker raised the problem of confirming the stronger proposition in which the above inequality is replaced by

$$q^{1+\varepsilon} \|q\theta\| \dots \|q\theta^n\| < 1.$$

Again, by transference (see, for example, Wang, Yu and Zhu [19]), the problem is equivalent to showing that for any n and ε as above, there exist for almost all real numbers θ only finitely many polynomials $P(x) = a_0 + a_1 x + \dots + a_n x^n \in \mathbb{Z}[x]$ such that

$$|P(\theta)| < (\bar{a}_1 \bar{a}_2 \dots \bar{a}_n)^{-(1+\varepsilon)}. \quad (3)$$

So far, the problem has been solved only in the case $n=2$; the solution is given in Sprindžuk [15]. The argument utilizes a result similar to that of Schmidt [10] established in 1964 which generalized the work of Kasch [9] mentioned earlier. Sprindžuk derives in fact a theorem to the effect that the inequality

$$q^{1+\varepsilon} \|q f_1(\theta)\| \|q f_2(\theta)\| < 1$$

has only finitely many solutions in positive integers q for almost all real θ in any given interval, where $f_1(x)$ and $f_2(x)$ are functions satisfying $f_1' f_2'' \neq f_1'' f_2'$ almost everywhere on the interval, and f_1', f_2'' are assumed continuous.

The above problem of Baker concerns the real case. An analogous problem can be formulated in the complex case. In fact, in analogy with (3), one would conjecture that for any $n \geq 2$, any $\mu > \frac{1}{2}(1 - \frac{1}{n})$ and for almost all complex numbers θ there exist only finitely many polynomials $P(x) = a_0 + a_1 x + \dots + a_n x^n \in \mathbb{Z}[x]$ such that

$$|P(\theta)| < (\bar{a}_1 \bar{a}_2 \dots \bar{a}_n)^{-\mu}. \quad (4)$$

The condition on μ is best possible for it is easily shown by means of Dirichlet's "pigeonhole principle" that, for any complex transcendental number θ , there exist infinitely many $P(x)$ as above satisfying $|P(\theta)| < h^{-\frac{1}{2}(n-1)}$ (see Schneider [12]) whence satisfying (4) with $\mu = \frac{1}{2}(1 - \frac{1}{n})$.

Our purpose here is threefold. First we shall refine the work of Kasch [9] to give a sharper form of the result of Sprindžuk in the case $f_1(x) = x$, $f_2(x) = x^2$. Accordingly, let $\psi(q)$ denote a positive monotonic decreasing function of the integer variable q such that $\sum \psi(q)$ converges. We prove :

THEOREM 2. - For almost all real numbers θ there exist only finitely many polynomials $P(x) = ax^2 + bx + c \in \mathbb{Z}[x]$ such that

$$|P(\theta)| < \psi(\bar{a}) \psi(\bar{b}) .$$

Further, let $\varphi(q)$ denote a positive function of the integer variable q such that $q \varphi(q)$ decreases monotonically and $\sum \varphi(q)$ converges. Then by the transference method of Baker [1] we obtain the following result.

THEOREM 3. - For almost all real numbers θ there exist only finitely many positive integers q such that

$$q \|q\theta\| \|q\theta^2\| < (q \varphi(q))^4 .$$

Our method of proof of Theorem 2 depends on the estimation of weighted sums involving the discriminant of P . The paper of Kasch [9] depends on an analysis of similar but unweighted sums. Kasch's work was extended by Volkmann [17] to deal with the real case $n=3$ of Mahler's conjecture; the proof depended on a theorem of Davenport [7] concerning binary cubic forms. It might be expected that an analogous extension to $n=3$ would apply to our analysis but unfortunately this does not seem to be so. However, we are able to solve the problem for $n=3$ in the complex case, and this is our second purpose.

We shall prove that for almost all complex numbers θ , for $n=2$ and 3 , the inequality (4) has only finitely many solutions. In fact rather more will be proved. Let $\psi(q)$ be a function of the integer variable q such that $\sum \psi(q)$ converges and $0 < \psi(q) < C/q$, where C is an absolute constant. We have :

THEOREM 4. - For almost all complex numbers θ , there exist only finitely many polynomials $P(x) = ax^2 + bx + c \in \mathbb{Z}[x]$ such that

$$|P(\theta)| < (\bar{a} \bar{b})^{\frac{1}{4}} (\psi(\bar{a}) \psi(\bar{b}))^{\frac{1}{2}} .$$

THEOREM 5. - For almost all complex numbers θ , there exist only finitely many polynomials $P(x) = ax^3 + bx^2 + cx + d \in \mathbb{Z}[x]$ such that

$$|P(\theta)| < (\bar{a} \bar{b} \bar{c})^{1/6} (\psi(\bar{a}) \psi(\bar{b}) \psi(\bar{c}))^{\frac{1}{2}} .$$

The demonstrations will involve a modification of the method of Volkmann [16]. As already remarked, it is known (see Schneider [12]) that Theorems 4 and 5 are best possible ; in fact they become false with $\psi(q) = 1/q$.

Thirdly we calculate the Hausdorff dimension of the set referred to in Theorem 2 in the case $\psi(q) = q^{-(1+\epsilon)}$. We have :

THEOREM 6. - For any given $\epsilon > 0$, the Hausdorff dimension of the set of all real numbers θ for which there exist infinitely many quadratic polynomials $P(x) = ax^2 + bx + c \in \mathbb{Z}[x]$ such that $|P(\theta)| < (\bar{a} \bar{b})^{-(1+\epsilon)}$ is $2/(2+\epsilon)$.

Theorem 6 leads us to conjecture that, more generally, the Hausdorff dimension of the set of all real numbers θ for which (3) has infinitely many solutions is $2/(2+\epsilon)$. This conjecture is true for $n=2$ by Theorem 6 and the theorem of Jarník [8] and Besicovitch [5]. An analogous conjecture can be made in the complex case, namely the Hausdorff dimension of the set of all complex numbers θ for which (4) has infinitely many solutions is $2/(\mu+1)$ for $\mu > 1$ and $(n+1)/(n\mu+1)$ for $\frac{1}{2}(1-\frac{1}{n}) < \mu \leq 1$. This conjecture can be verified for $n=2$ with $\mu > \frac{1}{4}$ and for $n=3$ with $\frac{1}{3} < \mu \leq 1$ following the proofs of Theorems 4 and 5 and utilizing Theorem 6 and some results of Baker and Schmidt [4]

-:-:-:-

REFERENCES

- [1] BAKER A., On some Diophantine inequalities involving the exponential function, Canadian J. Math. 17 (1965), 616-626.
- [2] BAKER A., On a theorem of Sprindžuk, Proc. Roy. Soc. London A 292 (1966), 92-104.
- [3] BAKER A., Transcendental number theory (Cambridge University Press, 1975).
- [4] BAKER A. and SCHMIDT W.M., Diophantine approximation and Hausdorff dimension, Proc. London Math. Soc. 21 (1970), 1-11.

- [5] BESICOVITCH A.S., Sets of fractional dimensions (IV) : On rational approximation to real numbers, J. London Math. Soc. 9 (1934), 126-131.
- [6] BOVEY J.D. and DODSON M.M., The fractional dimension of sets whose simultaneous rational approximations have errors with a small product, Bull. London Math. Soc. 10 (1978), 213-218.
- [7] DAVENPORT H., A note on binary cubic forms, Mathematika 8 (1961), 58-62.
- [8] JARNIK V., Diophantische Approximationen und Hausdorffsches Mass, Math. Sbornik 36 (1929), 371-382.
- [9] KASCH F., Über eine metrische Eigenschaft der S-Zahlen, Math. Zeit. 70 (1958), 263-270.
- [10] SCHMIDT W.M., Metrische Sätze über simultane Approximation abhängiger Grössen, Monatsh. Math. 68 (1964), 154-166.
- [11] SCHMIDT W.M., Simultaneous approximation to algebraic numbers by rationals, Acta Math. 125 (1970), 189-201.
- [12] SCHNEIDER Th., Einführung in die transzendenten Zahlen, Springer Verlag Berlin, Göttingen, Heidelberg, 1957).
- [13] SPRINDŽUK V.G., Proof of the conjecture of Mahler on the measure of the set of S-numbers, Izv. Akad. Nauk SSSR (ser. mat.) 29 (1965), 379-436 (in Russian).
- [14] SPRINDŽUK V.G., Metric theory of diophantine approximations, Current problems of analytic number theory, In Proc. Summer School on Analytic Number Theory, Minsk (1972), 178-198, (Izd. Nauka i Tekhnika, Minsk, 1974) (in Russian).
- [15] SPRINDŽUK V.G., Metric theory of diophantine approximations, V.H. Winston, Washington, D.C. 1979.
- [16] VOLKMANN B., Zur Mahlerschen Vermutung in Komplexen, Math. Ann. 140 (1960), 351-359.
- [17] VOLKMANN B., The real cubic case of Mahler's conjecture, Mathematika 8 (1961), 55-57.

- [18] WANG Y. and YU K.R., A note on some metrical theorems in Diophantine approximations, Publications Mathématiques 297, Institut des Hautes Etudes Scientifiques, Paris, 1979).
- [19] WANG Y., YU K.R. and ZHU Y.C., On a transference theorem on linear forms, Acta Math. Sinica 22 (1979), 237-240.

(texte reçu le 27 juillet 1981)

-:-:-:-

Kunrui YU
Institute of Mathematics
Chinese Academy of Sciences
PEKING

MULTIPLICITIES OF BINARY RECURRENCES

by

R. TIJDEMAN

-:-:-:-

1. - Let $\alpha_1, \alpha_2, \dots, \alpha_n$ and $c_0, c_1, \dots, c_{n-1}$ be elements of a ring R .
A (homogeneous linear) recursive sequence $\{c_\nu\}_{\nu=0}^\infty$ is a sequence satisfying

$$(1) \quad c_\nu = \alpha_1 c_{\nu-1} + \alpha_2 c_{\nu-2} + \dots + \alpha_n c_{\nu-n} \quad (\nu = n, n+1, \dots)$$

with $\alpha_n \neq 0$. Here n is called the order of the recurrence. In this paper we shall restrict ourselves to $R = \mathbb{C}$ (a complex sequence), $R = \overline{\mathbb{Q}}$ (an algebraic sequence), $R = \mathbb{Q}$ (a rational sequence) and $R = \mathbb{Z}$ (an integer sequence).

From the companion polynomial

$$(2) \quad z^n - \alpha_1 z^{n-1} - \dots - \alpha_n = \prod_{i=1}^m (z - \omega_i)^{\rho_i}, \quad \omega_i \neq \omega_j \text{ if } i \neq j,$$

and the initial values $c_0, c_1, \dots, c_{n-1}$, one can deduce an explicit expression for c_ν of the form

$$(3) \quad c_\nu = \sum_{i=1}^m P_i(\nu) \omega_i^\nu, \quad \nu = 0, 1, 2, \dots,$$

where P_i is a polynomial of degree at most $\rho_i - 1$ ($i = 1, \dots, m$) and $\sum_{i=1}^m \rho_i = n$. On the other hand, every sequence (3) satisfies the recurrence (1) where the α_j 's are determined by (2). Since both the Taylor coefficients of a rational function and the values of the exponential polynomial (3) at integers satisfy a recurrence relation (1), any result on recurrences can be transformed into statements about these functions (cf. Loxton and van der Poorten [12]).

We shall deal with the multiplicity of a recursive sequence. For any complex number a the a -multiplicity of a sequence $\{c_v\}$ is the number of indices v for which $c_v = a$. The multiplicity of the sequence is the supremum of the a -multiplicities taken over all $a \in \mathbb{C}$. Since every exponential polynomial (3) satisfies relation (1), the multiplicity of a recursive sequence of order n is equal to the 0-multiplicity of a recursive sequence of order at most $n+1$. On the other hand, if the characteristic polynomial of a recursive sequence of order n has a simple zero, then its 0-multiplicity is at most the multiplicity of some recursive sequence of order $n-1$. Indeed, if ω_m is a simple zero of (2), then P_m is a constant and the 0-multiplicity of $\{c_v\}_{v=0}^{\infty}$ is equal to the $(-P_m(0))$ -multiplicity of $\left\{ \sum_{i=1}^{m-1} P_i(v) \left(\omega_i / \omega_m \right)^v \right\}_{v=0}^{\infty}$.

2. - The so-called Lech-Mahler theorem gives a simple property of recurrences with infinite multiplicities :

THEOREM A. - If $c_v = 0$ for infinitely many v , then those v for which $c_v = 0$ form a periodic sequence for $v > v_0$.

The result was proved by Skolem [22] for rational sequences, by Mahler [13] for algebraic sequences, by Lech [11] for sequences in a field of characteristic 0, and later once more by Mahler [14] for complex sequences. It does not hold for fields of positive characteristic. It is an immediate consequence of the theorem that if $\{c_v\}_{v=0}^{\infty}$ has an infinite 0-multiplicity, then ω_i / ω_j is a root of unity for some indices i, j with $i \neq j$. A recurrence satisfying the latter property is said to be degenerate, while the other recursive sequences are called non-degenerate.

It follows from the preceeding remarks that the multiplicity of a non-degenerate recursive sequence of order n (≥ 2) is bounded. The proof of the Lech-Mahler theorem is ineffective and no general method to find an upper bound for the multiplicity of a non-degenerate recurrence is available. Even for integer sequences hardly any results for recurrences of arbitrary order are known. Berstel and Mignotte [4] showed that it is a decidable question whether a given recursive integer sequence $\{c_\nu\}$ of order n is degenerate or not (cf. Robba [19]). Loxton and van der Poorten [12] indicated how known techniques involving the theorem of Strassman on p -adic analytic functions can be used to estimate the multiplicity of a given recursive integer sequence. If all numbers w_j are real, then a straightforward estimation suffices. A result of Mignotte [17] can be used to give an upper bound for the multiplicity of a recursive sequence (1) if the number of w_j of maximal modulus is at most three and each of these w_j is a simple zero of (2). For more details I refer to the survey paper of Loxton and van der Poorten [12]. They state the remarkable conjecture that there should exist an upper bound for the multiplicity of a non-degenerate recursive integer sequence which depends only on the order of the recurrence.

3. - Most attention has been paid to binary recurrences, recurrences of order 2. The more specific conjecture that the multiplicity of a non-degenerate binary integer sequence is at most 5 is known as Ward's conjecture. This conjecture has been established by Kubota [7, 8] who showed that the multiplicity is even at most 4. He improved upon previous partial results of Skolem, Chowla and Lewis [23], Chowla, Dunton and Lewis [6], Laxton [10] and Alter and Kubota [1]. Beukers [5] has obtained a further improvement by showing that the sum of the a -multiplicity and the $(-a)$ -multiplicity of a non-degenerate binary integer sequence is at most 3, with essentially five exceptions, namely

$$\alpha_1 = 1, \quad \alpha_2 = -2, \quad c_0 = c_1 = 1, \quad \text{where } c_0 = c_1 = 1, \quad c_2 = c_4 = c_{12} = -1,$$

$$\alpha_1 = 1, \quad \alpha_2 = -2, \quad c_0 = 1, \quad c_1 = -1, \quad \text{where } c_0 = 1, \quad c_1 = c_3 = c_{11} = -1,$$

$$\alpha_1 = 3, \quad \alpha_2 = -4, \quad c_0 = c_1 = 1, \quad \text{where } c_0 = c_1 = 1, \quad c_2 = c_6 = -1,$$

$$\alpha_1 = 2, \quad \alpha_2 = -3, \quad c_0 = c_1 = 1, \quad \text{where } c_0 = c_1 = c_5 = 1, \quad c_2 = -1,$$

$$\alpha_1 = 1, \quad \alpha_2 = 1, \quad c_0 = 1, \quad c_2 = -1, \quad \text{where } c_0 = 1, \quad c_1 = c_3 = c_4 = -1.$$

It is easy to show that there are infinitely many binary integer recursive sequences of multiplicity three : for any positive integer N take $\alpha_1 = -1$, $\alpha_2 = N$, $c_0 = c_1 = 1$. Then also $c_3 = 1$. I conjecture that all binary recursive sequences have the property that if $c_{v_1} = c_{v_2} = c_{v_3}$ with $v_1 < v_2 < v_3$, then $v_3 - v_1$ is bounded by an absolute constant. Such a result does not hold for recursive sequences of multiplicity two, as is shown by the following example :

For any positive integer N take

$$c_v = 5c_{v-1} - 6c_{v-2}, \quad c_0 = 3^N - 2^N, \quad c_1 = 2 \cdot 3^N - 3 \cdot 2^N.$$

Then $c_0 = c_N = 3^N - 2^N$.

Shorey [21] has shown that the gap N between the indices is essentially maximal with respect to the sizes of the initial values.

Closely related is the question of the 0-multiplicity of ternary sequences (i. e. $n = 3$). There is a claim of Kubota [9] that a non-degenerate ternary integer sequence has 0-multiplicity at most 6. The following example due to Berstel [3] shows that this bound is sharp :

$$c_v = 2c_{v-1} - 4c_{v-2} + 4c_{v-3} \quad \text{with} \quad c_0 = c_1 = c_4 = c_6 = c_{13} = c_{52} = 0.$$

(cf. Mignotte [15].) If the three zeros of (2) are distinct, non-zero and real, then the 0-multiplicity of a corresponding non-degenerate ternary sequence is at most 3. This was shown by Smiley [24] in 1956 (cf. Scott [20], Picon [18]). More history on the problem and further results can be found in a survey paper of M. Ward [25].

4. - Non-integral binary recursive sequences have not been studied so intensively. Kubota [9] proved that the multiplicity of a binary non-degenerate recursive sequence of algebraic integers in a fixed algebraic number field K is bounded above by an effectively computable number M depending only on the degree of K over $\mathbb{Q}$ and wondered whether a bound would exist which is independent of this degree. Quite recently Beukers extended Kubota's result by giving an explicit value of M for general algebraic sequences. His results will be published later.

5. - As an illustration of some of the underlying ideas we shall deal with a related problem which Beukers and I investigated. It follows from Beukers' paper [5] that for computing the multiplicity of a binary integer sequence it is important to know how many powers of ω_1 are lying on a line. For example, in the above mentioned first exceptional example $\omega = \frac{1}{2} \pm \frac{1}{2}\sqrt{-7}$ whereas $\omega^2, \omega^3, \omega^5$ and ω^{13} are on the lines $\text{Im } z = \pm \frac{1}{2}\sqrt{7}$. We might consider any complex number z and wonder how many of its powers z^j ($j \in \mathbb{Z}$) can be on a straight line. Obviously infinitely many among them are located on a line if z is real or a root of unity. We have proved :

If L is a line in the complex plane not passing through the origin and z is a number such that infinitely many of its powers are on L , then z is a root of unity.

If $|z|=1$, then L intersects the unit circle in at most two points and the assertion is valid (even for three powers of z on a line). Now let L be a line not passing through the origin and z a complex number, not a root of unity. We know that L contains only finitely many powers of z and we want to give an upper bound for that number. Without loss of generality we may assume that $|z|>1$, since the cases $z=0$ and $|z|=1$ are trivial and we might consider powers of z^{-1} instead of z . Since we can divide all powers of z by the lowest power of z in the sequence, we may assume without loss of generality that the powers of z on L are given by $1 = z^0, z^{\nu_1}, z^{\nu_2}, \dots, z^{\nu_N}$ with $0 < \nu_1 < \dots < \nu_N$. We suppose $N \geq 3$ and put $\nu_1 = p, \nu_2 = q, \nu_3 = r$. The connection with recursive sequences becomes clear when one looks at the real binary recursive sequence $\{z_{\nu}\}_{\nu=0}^{\infty}$ defined by

$$(4) \quad z_{\nu} = (1 - \bar{z}^p) z^{\nu} + (z^p - 1) \bar{z}^{\nu}.$$

It is a recursive sequence, for it is of the form (3). If $1, z^p, z^{\nu}$ are on L , we have $(z^p - 1)/(\bar{z}^p - 1) = (z^{\nu} - 1)/(\bar{z}^{\nu} - 1)$ and hence

$$(5) \quad z_{\nu} = (1 - \bar{z}^p) z^{\nu} + (z^p - 1) \bar{z}^{\nu} = (1 - \bar{z}^p) + (z^p - 1) = z_0.$$

Thus $z_0 = z_{\nu_1} = \dots = z_{\nu_N}$ and the multiplicity of the sequence is at least $N+1$.

I shall sketch the proof of the following result.

THEOREM (Beukers and Tijdeman). - If L is a line not passing through the origin and z is a complex number with $|z| \geq e$, then there are at most nine powers of z on L .

The proof consists of three steps. Of course we may assume that z is not real.

Step 1. - If four powers of z are on L , then z is an algebraic number of bounded degree and height.

Step 2. - If z is an algebraic number of degree d and height H , then the number of powers of z on L can be bounded in terms of d and H .

Step 3. - The powers of z on L are so far from each other that there can be no more than nine together.

Ad step 1. - The basic principle can be found in the paper of Lech [11], but for this special case there is an elegant argument due to Beukers.

Assume $1, z^p, z^q, z^r$ are on L and $0 < p < q < r$. Without loss of generality we may assume $(p, q, r) = 1$. Put

$$F(X, Y) = (X^p - 1) Y^q - (X^q - 1) Y^p + X^q - X^p,$$

$$G(X, Y) = (X^p - 1) Y^r - (X^r - 1) Y^p + X^r - X^p.$$

Hence,

$$F(z, \bar{z}) = G(z, \bar{z}) = 0.$$

It is clear that F and G have simple factors $X-1$, $Y-1$, $X-Y$ in common.

Write

$$F(X, Y) = F_1(X, Y) P(X, Y) (X-1) (Y-X) (Y-1)$$

$$G(X, Y) = G_1(X, Y) P(X, Y) (X-1) (Y-X) (Y-1)$$

with $(F_1, G_1) = 1$. Let α be a primitive r -th root of unity. It follows from $G(\alpha, Y) = (\alpha^p - 1)(Y^r - 1)$ that every root $Y = \beta$ of $P(\alpha, Y)$ is a simple r -th root of unity with $\beta \neq 1, \alpha$. Moreover, we can apply a geometric argument to the equation

$$(\alpha^p - 1) \lambda - (\alpha^q - 1) \mu + \alpha^q - \alpha^p = 0, \quad |\lambda| = |\mu| = 1,$$

to conclude that there are at most two solutions, (λ_1, μ_1) and (λ_2, μ_2) say. Since $(\lambda, \mu) = (1, 1)$ and $(\lambda, \mu) = (\alpha^q, \alpha^p)$ provide solutions, we can deduce that $\beta = 1$ or α , a contradiction. Hence $P(\alpha, Y)$ is a constant, that is $P(X, Y) \in \mathbb{Z}[X]$.

It is not hard to show that $G_2(X, Y) := G_1(X, Y)P(X, Y)$ has no factors $Y-X$ or $Y-1$. Hence the greatest common factor of F and G_2 is a constant with respect to Y . The resultant R of F and G_2 is therefore a non-trivial polynomial in X . A simple calculation gives that its degree is at most $2qr$ and its height at most 2^{4qr} . We know that z and $\bar{z}$ are zeros of R . A standard argument in transcendental number theory (cf. Mignotte [16]) implies that z and $\bar{z}$ are algebraic numbers of heights at most 2^{5qr} .

Ad step 2. - Here we apply an estimate of Baker on linear forms of logarithms of algebraic numbers twice (Baker [2, Theorem 2]). Better estimates could be used, but they would not yield a far better final result. J. Oesterlé has obtained part of this step independently.

Suppose $1, z^{\nu_1}, z^{\nu_2}, \dots, z^{\nu_N}$ with $0 < \nu_1 < \nu_2 < \dots < \nu_N$ are on L and $N \geq 3$. Put $\nu_1 = p$, $\nu_2 = q$, $\nu_3 = r$, $\nu_{N-1} = \ell$, $\nu_N = m$. We have

$$(6) \quad \frac{z^\ell - 1}{\bar{z}^\ell - 1} = \frac{z^m - 1}{\bar{z}^m - 1}$$

and

$$(7) \quad \left| \frac{z^j - 1}{\bar{z}^j - 1} - \frac{z^j}{\bar{z}^j} \right| = \left| \frac{z^j - \bar{z}^j}{\bar{z}^j (\bar{z}^j - 1)} \right| \leq \left| \frac{z^j - 1}{\bar{z}^j (\bar{z}^j - 1)} \right| + \left| \frac{\bar{z}^j - 1}{\bar{z}^j (\bar{z}^j - 1)} \right| \leq \frac{2}{|z|^j}$$

for every j . Hence, by the triangle inequality,

$$\left| \left(\frac{z}{\bar{z}} \right)^{m-\ell} - 1 \right| = \left| \left(\frac{z}{\bar{z}} \right)^m - \left(\frac{z}{\bar{z}} \right)^\ell \right| \leq \frac{2}{|z|^m} + \frac{2}{|z|^\ell} \leq \frac{4}{|z|^\ell}.$$

Since $\|e^{\pi i \varphi} - 1\| \geq 4\|\varphi\|$ for all real φ , there is an integer h with $|2h| \leq m - \ell$ such that

$$(8) \quad \left| (m - \ell) \log \frac{z}{\bar{z}} - 2h \log(-1) \right| \leq \frac{\pi}{|z|^\ell}.$$

A straightforward application of Baker's estimate gives

$$\left| (m-\ell) \log \frac{z}{\bar{z}} - 2h \log(-1) \right| \geq \exp(-(12qr)^{804} \log m)$$

and hence, by $|z| > e$,

$$(9) \quad \ell \leq (12qr)^{805} \log m.$$

Similarly, from (6) and (7) with $j=m$, we have

$$\left| \frac{z^m}{\bar{z}^m} \cdot \frac{\bar{z}^\ell - 1}{z^\ell - 1} - 1 \right| \leq \frac{2}{|z|^m}$$

and hence

$$\left| m \log \frac{z}{\bar{z}} + 2h_1 \log(-1) - \log \frac{z^\ell - 1}{\bar{z}^\ell - 1} \right| \leq \frac{2}{|z|^m}.$$

Standard arguments can be used to estimate the heights of the algebraic numbers in the logarithms. Then Baker's estimate implies

$$m \leq (10qr)^{1212} \ell \log m.$$

On combining this with (9) we obtain

$$m \leq (12qr)^{2015} (\log m)^2$$

and therefore

$$(10) \quad m \leq (12qr)^{2021}.$$

Ad step 3. - The basic idea behind this step is well known by the work of Thue and Siegel.

As in step 2 we assume that $z^0, z^{\nu_1}, \dots, z^{\nu_N}$ with $0 < \nu_1 < \dots < \nu_N$ are on L and that $N \geq 3$. The letters p, q, r, ℓ, m have the same meaning and further $i, j, k \in \{0, \nu_1, \dots, \nu_N\}$ with $i < j < k$. Hence, for suitable integers h_2 and h_3 we have like in (8)

$$\left| (j-i) \log \frac{z}{z} - 2h_2 \log(-1) \right| \leq \frac{\pi}{|z|^i}$$

and

$$\left| (k-j) \log \frac{z}{z} - 2h_3 \log(-1) \right| \leq \frac{\pi}{|z|^j}.$$

It follows from a geometrical argument that $h_2/(j-i) \neq h_3/(k-j)$. The observation that the argument of z^x/z^i for $x \geq i$ is strictly monotonic leads to a proof that equality of both sides cannot hold. Hence, by the triangle inequality,

$$\frac{1}{(j-i)(k-j)} \leq \left| \frac{h_2}{j-i} - \frac{h_3}{k-j} \right| \leq \frac{1}{(j-i)|z|^i} + \frac{1}{(k-j)|z|^j} \leq \frac{1}{|z|^i} \left(\frac{1}{j-i} + \frac{1}{k-j} \right).$$

Thus

$$k-i \geq |z|^i \geq e^i.$$

This implies $v_5 - v_3 \geq e^r$, $v_7 - v_5 \geq e^{e^r}$, $v_9 - v_7 \geq e^{e^{e^r}}$, but since

$$e^{e^{e^r}} \geq (12 r^2)^{2021}$$

for all $r \geq 3$, this is a contradiction. Hence $N \leq 8$, and the theorem follows.

The theorem can be modified in a number of ways.

1. - By splitting the sequence of v 's in subsequences it is possible to show that the number of points on L which is a power of some complex number z is at most

$$9 (|\log |z||)^{-1}.$$

2. - It is possible to give bounds in terms of p, q and r . If r is large, then the bound can be improved. Bounds for small r could be investigated separately.

3. - It is possible to use hypergeometric functions instead of or in combination with Baker's bound. In the general case this gives bounds which are in certain respects far better.

REFERENCES

- [1] R. ALTER and K. KUBOTA, Multiplicities of second order linear recurrences, Trans. Amer. Math. Soc. 178 (1973), 271-284.
- [2] A. BAKER, The theory of linear forms in logarithms, Ch. 1 of Transcendence Theory : Advances and Applications, Proc. Conf. Cambridge 1976, Academic Press, 1977.
- [3] J. BERSTEL, Sur le calcul des termes d'une suite récurrente linéaire, exposé fait à l'I. R. I. A. (Rocquencourt) en mars 1974.
- [4] J. BERSTEL et M. MIGNOTTE, Deux propriétés décidables des suites récurrentes linéaires, Bull. Soc. Math. France 104 (1976), 175-184.
- [5] F. BEUKERS, The multiplicity of binary recurrences, Compositio Math. 40 (1980), 251-267.
- [6] S. CHOWLA, M. DUNTON and D. J. LEWIS, Linear recurrences of order two, Pacific J. Math. 11 (1961), 833-845.
- [7, 8, 9] K. KUBOTA, On a conjecture of M. Ward, I, II, III, Acta Arith. 33 (1977), 11-28, 29-48, 99-109.
- [10] R. R. LAXTON, Linear recurrences of order 2, J. Austral. Math. Soc. 7 (1967), 108-114.
- [11] C. LECH, A note on recurring series, Ark. Mat. 2 (1953), 417-421.
- [12] J. H. LOXTON and A. J. van der POORTEN, On the growth of recurrence sequences, Math. Proc. Camb. Phil. Soc. 81 (1977), 369-376.
- [13] K. MAHLER, Eine arithmetische Eigenschaft der Taylor-Koeffizienten rationaler Funktionen, Akad. Wetensch. Amsterdam Proc. 38 (1935), 50-60.
- [14] K. MAHLER, On the Taylor coefficients of rational functions, Proc. Cambridge Philos. Soc. 52 (1956), 39-48 and 53 (1957), 544.
- [15] M. MIGNOTTE, Suites récurrentes linéaires, Sémin. Delange-Pisot-Poitou, 15e année (1973/74), n° G14.
- [16] M. MIGNOTTE, An inequality about factors of polynomials, Math. Comput. 28 (1974), 1153-1157.
- [17] M. MIGNOTTE, A note on linear recursive sequences, J. Austral. Math. Soc. (A) 20 (1975), 242-244.

- [18] P. A. PICON, Sur certaines suites récurrentes cubiques ayant deux ou trois termes nuls, Discrete Math. 21 (1978), 285-296.
- [19] Ph. ROBBA, Zéros de suites récurrentes linéaires, Groupe d'étude d'analyse ultramétrique, 5e année (1977/78), n° 13.
- [20] S. J. SCOTT, On the number of zeros of a cubic recurrence, Amer. Math. Monthly 67 (1960), 169-170.
- [21] T. N. SHOREY, On the equation $u_m = u_n$ with $\{u_m\}$ a binary recursive sequence, (unpublished).
- [22] Th. SKOLEM, Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen und diophantischer Gleichungen, 8. Skand. Mat. Kongr. (1935), 163-188.
- [23] Th. SKOLEM, S. CHOWLA and D. J. LEWIS, The diophantine equation $2^{n+2} - 7 = x^2$ and related problems, Proc. Amer. Math. Soc. 10 (1959), 663-669.
- [24] M. F. SMILEY, On the zeros of a cubic recurrence, Amer. Math. Monthly 63 (1956), 171-172.
- [25] M. WARD, Some diophantine problems connected with linear recurrences, Report Institute Th. Numbers (Univ. Colorado) (1959), 250-257.

(texte reçu le 19 juin 1981)

-:-:-:-

R. TIJDEMAN
 Mathematisch Instituut der
 Rijksuniversiteit te Leiden
 Wassenaarseweg 80 - Postbus 9512
 2300 RA LEIDEN
 (Pays Bas)

ON IRRATIONALITY OF THE VALUES OF CERTAIN SERIES

by

Iekata SHIOKAWA

-:-:-:-

§.I. - Introduction

In 1916, Bernstein and Szász studied the irrationality of certain values of the series

$$\sum_{n=0}^{\infty} q^{n^2} z^n,$$

which is the right half of the Jacobi's theta series

$$\theta_3(v, \tau) = 1 + 2 \sum_{n=1}^{\infty} q^{n^2} \cos 2n\pi v = \sum_{n=-\infty}^{\infty} q^{n^2} z^n,$$

where $z = \frac{1}{2} (e^{2\pi i v} + e^{-2\pi i v})$ and $q = e^{i\pi \tau}$ with $\text{Im } \tau > 0$.

They proved in [1] that, if $q = q_1/q_2$ with $q_1, q_2 \in \mathbb{Z}$ and $|q_2| \geq |q_1|^3 \geq 1$, $|q_2| \geq 2$, then $\sum_{n=0}^{\infty} q^{n^2} z^n \notin \mathbb{Q}$ for any non-zero $\alpha \in \mathbb{Q}$. Their method is to apply an irrationality criterion for continued fractions to the Eisenstein's continued fraction

$$\sum_{n=0}^{\infty} q^{n^2} z^n = 1 + \frac{qz}{1} - \frac{q^3 z}{1} + \frac{q^3(1-q^2)z}{1} - \dots - \frac{q^{4n-1}z}{1} + \frac{q^{2n+1}(1-q^{2n})z}{1} - \dots$$

Szasz [6] gave another proof using the following series of functional equations :

$$\left. \begin{aligned} \mathfrak{D}_{2\nu}(z) &= \mathfrak{D}_{2\nu+1}(z) - q^{4\nu+1} z \mathfrak{D}_{2\nu+2}(z) \\ \mathfrak{D}_{2\nu+1}(z) &= \mathfrak{D}_{2\nu+2}(z) + q^{2\nu+1} (1-q^{2\nu+2}) z \mathfrak{D}_{2\nu+3}(z) \end{aligned} \right\} (\nu=0, 1, 2, \dots)$$

where

$$\left. \begin{aligned} \mathfrak{D}_{2\nu}(z) &= 1 + \sum_{n=1}^{\infty} q^{n(2\nu+n)} \frac{(1-q^{2\nu})(1-q^{2\nu+2}) \dots (1-q^{2\nu+2n-2})}{(1-q^2)(1-q^4) \dots (1-q^{2n})} z^n \\ \mathfrak{D}_{2\nu+1}(z) &= 1 + \sum_{n=1}^{\infty} q^{n(2\nu+n)} \frac{(1-q^{2\nu})(1-q^{2\nu+2}) \dots (1-q^{2\nu+2n})}{(1-q^2)(1-q^4) \dots (1-q^{2n})} z^n \end{aligned} \right\}$$

($\nu=0, 1, 2, \dots$), and so especially $\mathfrak{D}_1(z) = \sum_{n=0}^{\infty} q^{n^2} z^n$.

Tschakaloff [8] considered the entire function

$$f(z) = \sum_{n=0}^{\infty} a^{-\frac{1}{2}n(n-1)} z^n,$$

where a is any given complex number with $|a| > 1$, and proved the following theorem : let $a = s/r$ with $r, s \in \mathbb{Z}$ and

$$(1) \quad |s| > |r|^{(3+\sqrt{5})/2} > 0.$$

Then $f(\alpha) \notin \mathbb{Q}$ for any non-zero $\alpha \in \mathbb{Q}$. Noticing the relation

$$\sum_{n=0}^{\infty} q^{n^2} y^n = \sum_{n=0}^{\infty} a^{-\frac{1}{2}n(n-1)} z^n \quad \text{with } q^{-2} = a, \quad qy = z,$$

we can deduce the theorem of Bernstein and Szász with a weaker condition

$$|q_2| > |q_1|^{(3+\sqrt{5})/2} \geq 1.$$

Tschakaloff [8] has also obtained a linear independence results for $f(z)$.

In 1974, Bundschuh [4] improved the above mentioned theorem of Tschakaloff by proving the following.

THEOREM 1. - Let K be any given imaginary quadratic field and let $a = s/r$ with integers $s, r \in K$ satisfying (1). Then $f(\alpha) \notin K$ for any non-zero $\alpha \in K$.

THEOREM 2. - Let K , a , and α be as in Theorem 1 and let

$$= 1 + \frac{1 + \sqrt{5}}{2 - (3 + \sqrt{5})^\gamma} \text{ with } \gamma = \frac{\log |r|}{\log |s|}.$$

Then for any given $\varepsilon > 0$ the inequality

$$(2) \quad |f(\alpha) - \frac{p}{q}| < |q|^{-\kappa - \varepsilon}$$

has only finitely many solutions in non-zero integers $p, q \in K$.

Bundschuh's proof is of an analytic nature. He made use of a Newton interpolation series for $f(z)$; i. e.

$$f(z) = A_0 + \sum_{n=1}^{\infty} A_n \prod_{v=1}^n (z - z_v),$$

with

$$A_{n-1} = \frac{1}{2\pi i} \int_{\Gamma_n} \frac{f(\zeta)}{\prod_{v=1}^n (\zeta - z_v)} d\zeta,$$

$$z_n = \begin{cases} a^{1-\mu} \alpha & \text{if } n = [\beta \mu] + \mu \text{ for some } \mu \in \mathbb{Z}, \\ 0 & \text{otherwise,} \end{cases}$$

where $\beta > 0$ is a parameter and Γ_n is a circle containing $0, z_1, z_2, \dots, z_n$.

By a similar method Bundschuh [2], [3], [4], and Walliser [10] have obtained some irrationality results for the values of entire functions satisfying certain kind of functional equations.

In this note we prove Theorem 1 and 2 by an elementary method [7] which is a refinement of that of Tschakaloff.

§. 2. - The auxiliary function

In this section a with $|a| > 1$ and $\alpha \neq 0$ are any given complex numbers not necessarily in K . We start with the functional equation for $f(z)$;

$$\begin{aligned} f(z) &= 1 + z + \sum_{k=2}^{\infty} a^{-\frac{1}{2}k(k-1)} z^k \\ &= 1 + z + z \sum_{k=1}^{\infty} a^{-\frac{1}{2}k(k-1)} a^{-k} z^k = 1 + z f(a^{-1}z), \quad \text{i. e.} \\ f(z) &= 1 + z f(a^{-1}z). \end{aligned}$$

Repeating this we have

$$(3) \quad f(z) = 1 + z + a^{-1} z^2 + \dots + a^{-\frac{1}{2}k(k-1)} z^k + a^{-\frac{1}{2}(k+1)k} z^{k+1} f(a^{-k-1}z)$$

or equivalently

$$a^{\frac{1}{2}k(k+1)} f(z) = a^{\frac{1}{2}k(k+1)} \sum_{j=0}^k a^{-\frac{1}{2}(k-j)(k-j-1)} z^{k-j} + z^{k+1} f(a^{-k-1}z).$$

Let n be a large integer. We define

$$(4) \quad F(z) = \sum_{k=0}^n c_{n-k} a^{\frac{1}{2}k(k+1)} \sum_{j=0}^k a^{-\frac{1}{2}(k-j)(k-j-1)} z^{k-j},$$

where $c_0, c_1, \dots, c_n \in \mathbb{Z}[a, \alpha]$ will be chosen in the sequel.

Then by the functional equation

$$F(z) = F(0) f(z) - G(z),$$

where

$$(5) \quad G(z) = \sum_{k=0}^n c_{n-k} z^{k+1} f(a^{-k-1}z).$$

Hence, since $f(0) = 1$ and $G(0) = 0$, we have

$$(6) \quad p F(0) - q F(\alpha) = F(0) (p - q f(\alpha)) + q G(\alpha),$$

where p and q are any complex numbers.

It follows from (4) that :

$$\begin{aligned}
 F(z) &= \sum_{k=0}^n \sum_{j=0}^k c_{n-k} a^{k(j+1) - \frac{1}{2}j(j+1)} z^{k-j} \\
 &= \sum_{j=0}^n \sum_{k=0}^{n-j} c_k a^{(n-k)(j+1) - \frac{1}{2}j(j+1)} z^{n-k-j} \\
 &= \sum_{j=0}^n a^{\frac{1}{2}j(j+1)} \sum_{k=0}^{n-j} c_k -a^{j+1} z^{n-k-j},
 \end{aligned}$$

and so

$$F(z) = f_0(z) + f_1(z) + \dots + f_n(z),$$

where

$$(7) \quad f_k(z) = a^{\frac{1}{2}k(k+1)} \sum_{j=0}^{n-k} c_j (a^{k+1} z)^{n-k-j} \quad (0 \leq k \leq n).$$

Using this with $k=0$, we define $c_0, c_1, \dots, c_n \in \mathbb{Z}[a, \alpha]$ as follows ;

$$\begin{aligned}
 f_0(z) &= \sum_{j=0}^n c_j (a z)^{n-j} \\
 (8) \quad &= (a z)^\lambda \prod_{h=1}^{\mu} (a z - a^h \alpha) \quad (= a^n z^\lambda \prod_{h=1}^{\mu} (z - a^{h-1} \alpha)),
 \end{aligned}$$

where $\lambda, \mu \in \mathbb{Z}$ with $\lambda + \mu = n$ and $\lambda - 1 > \mu > 1$. Then

$$(9) \quad c_j = \begin{cases} (-\alpha)^j \omega_j & (0 \leq j \leq \mu) \\ 0 & (\mu < j \leq n) \end{cases}$$

where $\omega_0 = 1$ and ω_j ($1 \leq j \leq \mu$) is the j^{th} elementary symmetric polynomial in $a, a^2, \dots, a^\mu$, which can be written, in the depending order of the exponents of a , as

$$\begin{aligned}
 \omega_j &= a^{\mu + \mu - 1 + \dots + \mu - j + 1} + \dots + a^{j + j - 1 + \dots + 1} \\
 (10) \quad &= a^{\mu j - \frac{1}{2}j(j-1)} + \dots + a^{\frac{1}{2}j(j+1)}.
 \end{aligned}$$

Thus we have polynomials $f_k(0), f_k(\alpha)$ ($1 \leq k \leq n$) and $F(0), F(\alpha) \in \mathbb{Z}[a, \alpha]$.

LEMMA 1. - If we write $F(0)$ and $F(\alpha)$ in the descending order of the exponents of a , then

$$(i) \quad F(0) = a^{\frac{1}{2}n(n+1)} + \dots \pm \alpha^\mu a^{\frac{1}{2}\lambda(\lambda+1) + \frac{1}{2}\mu(\mu+1)}, \quad \deg_\alpha F(0) = \mu$$

$$(ii) \quad F(\alpha) = a^{\frac{1}{2}n(n+1)} + \dots \pm \alpha^\lambda a^{\lambda(\mu+1)}, \quad \deg_\alpha F(\alpha) = \lambda.$$

For any polynomial $P(a)$ in a , we denote by $D(P)$ and $d(P)$ the maximal and minimal exponent of a in P .

Proof. - (i) By (7) and (9) we have

$$(11) \quad f_k(0) = a^{\frac{1}{2}k(k+1)} c_{n-k} = \begin{cases} 0 & (0 \leq k < \lambda), \\ (-\alpha)^{n-k} a^{\frac{1}{2}k(k+1)} w_{n-k} & (\lambda \leq k \leq n), \end{cases}$$

where noticing (10)

$$\left. \begin{aligned} D(f_k(0)) &= \frac{1}{2}n(n+1) - \lambda(n-k) \\ d(f_k(0)) &= \frac{1}{2}k(k+1) + \frac{1}{2}(n-k)(n-k+1) \end{aligned} \right\} \quad (\lambda \leq k \leq n).$$

So we have

$$(11)' \quad \left\{ \begin{aligned} \max_{\lambda \leq k < n} D(f_k(0)) &< D(f_n(0)) = \frac{1}{2}n(n+1), \\ \min_{\lambda < k \leq n} d(f_k(0)) &> d(f_\lambda(0)) = \frac{1}{2}\lambda(\lambda+1) + \frac{1}{2}\mu(\mu+1). \end{aligned} \right.$$

(i) follows from (11) with (11)'.

(ii) Case 1. - Let $0 \leq k \leq \lambda$. Then it follows from (7), (8) and (9) that

$$\begin{aligned} f_k(z) &= a^{\frac{1}{2}k(k+1)} \sum_{j=0}^{\mu} c_j (a^{k+1} z)^{n-k-j} \\ &= z^{-k} a^{-\frac{1}{2}k(k+1)} \sum_{j=0}^{\mu} c_j (a^{k+1} z)^{n-j} \\ &= z^{\lambda-k} a^{(k+1)(\lambda-k/2)} \prod_{h=1}^{\mu} (a^{k+1} z - a^h \alpha). \end{aligned}$$

Thus we have

$$(12) \quad f_k(\alpha) = \begin{cases} 0 & (0 \leq k < \mu) \\ \alpha^{n-k} a^{(k+1)(\lambda-k/2)} \prod_{h=1}^{\mu} (a^{k+1} - a^h) & (\mu \leq k \leq \lambda) \end{cases}$$

where

$$D(f_k(\alpha)) = (k+1)(n-k/2), \quad d(f_k(\alpha)) = (k+1)(\lambda-k/2) + \frac{1}{2}\mu(\mu+1) \quad (\mu \leq k \leq \lambda)$$

and so

$$(12)' \quad \begin{cases} \max_{\mu \leq k \leq \lambda} D(f_k(\alpha)) < \frac{1}{2}n(n+1), \\ \min_{\mu < k \leq \lambda} d(f_k(\alpha)) > d(f_{\mu}(\alpha)) = \lambda(\mu+1). \end{cases}$$

Case 2. - Let $\lambda < k \leq n$. We have by (7) and (9)

$$(13) \quad f_k(\alpha) = \alpha^{n-k} a^{(k+1)(n-k/2)} \sum_{j=0}^{n-k} (-1)^j w_j a^{-(k+1)j} \quad (\lambda < k \leq n),$$

where noticing (10)

$$D(f_k(\alpha)) = (k+1)(n-k/2), \quad d(f_k(\alpha)) = \frac{1}{2}k(k+1) + \frac{1}{2}(n-k)(n-k+1).$$

Hence

$$(13)' \quad \begin{cases} \max_{\lambda < k < n} D(f_k(\alpha)) < D(f_n(\alpha)) = \frac{1}{2}n(n+1), \\ \min_{\lambda < k \leq n} d(f_k(\alpha)) > \lambda(\mu+1) = d(f_{\mu}(\alpha)). \end{cases}$$

(12) with (12)' and (13) with (13)' imply (ii).

§. 3. - A lemma

We restrict n , from now on to integers of the form

$$n = \lambda + \mu \quad \text{with} \quad \lambda = [\beta \mu],$$

where $\beta > 1$ is a parameter and $[x]$ is the greatest integer less than or equal to a real number x .

LEMMA 2. - Let $a = s/r$ and $\alpha = \sigma/\rho$ with non-zero integers $s, r, \sigma, \rho \in K$ such that each " s and r ", " σ and ρ ", and " s and σ " have no common factor except units in K . Then there are positive integers μ_0 and ℓ depending only on β such that, if $\mu > \mu_0$,

$$p F(0) - q F(\alpha) \neq 0$$

for at least one $n \in \{[\beta \mu'] + \mu' \mid \mu \leq \mu' \leq \mu + \ell, \mu' \in \mathbb{Z}\}$ and for all integers $p, q \in K$ not both zero.

Proof. - We denote by $F_1(z)$ and $F_2(z)$ the auxiliary function $F(z)$ defined by (4) with $n = [\beta \mu] + \mu$ and $n = [\beta(\mu + \ell)] + \mu + \ell$ respectively, and assume that

$$p F_1(0) - q F_1(\alpha) = 0 \quad \text{and} \quad p F_2(0) - q F_2(\alpha) = 0$$

for some integers $p, q \in K$ not both zero. Then

$$(14) \quad F_1(0) F_2(\alpha) = F_2(0) F_1(\alpha) .$$

It follows from Lemma 1 that

$$(15) \quad F_1(0) F_2(\alpha) = a^D + \dots \pm \alpha^{\delta_1} a^{d_1}, \quad \deg_{\alpha} F_1(0) F_2(\alpha) = \delta_1 ,$$

$$(15)' \quad F_2(0) F_1(\alpha) = a^D + \dots \pm \alpha^{\delta_2} a^{d_2}, \quad \deg_{\alpha} F_2(0) F_1(\alpha) = \delta_2 ,$$

where the right-hand sides are written in the descending order of exponents of a and

$$d_1 = \frac{1}{2} \lambda(\lambda+1) + \frac{1}{2} \mu(\mu+1) + [\beta(\mu+\ell)](\mu+\ell+1) < D ,$$

$$d_2 = \frac{1}{2} [\beta(\mu+\ell)]([\beta(\mu+\ell)]+1) + \frac{1}{2}(\mu+\ell)(\mu+\ell+1) + \lambda(\mu+1) < D$$

$$\delta_1 = \mu + [\beta(\mu+\ell)] \geq \delta_2 = \mu + \ell + [\beta \mu] .$$

Here, using the relation $x-1 < [x] \leq x$, we find

$$d_2 - d_1 \geq \mu \{ \ell(\beta-1)^2 - (\beta+2) \} - C ,$$

where C is a constant depending only on β and ℓ . So, if we choose $\ell = [(\beta+2)/(\beta-1)^2] + 1$ and μ_0 large enough

$$(16) \quad d_2 > d_1 \quad (\mu > \mu_0) .$$

Now we prove $F_1(0) F_2(\alpha) \neq 0$. For this we assume $F_1(0) F_2(\alpha) = 0$ and put $u = \rho^{\delta_1} r^D (F_1(0) F_2(\alpha) \mp \alpha^{\delta_1} a^{d_1})$. Then $u \neq 0$ and by (15) $s^{d_1+1} \mid u$. But at the same time u can be written as $u = \mp \sigma^{\delta_1} r^{D-d_1} s^{d_1}$, where both " s and σ " and " s and r " have no common factor except units in K ; which is a contradiction.

So the number $v = \rho^{\delta_1} r^D F_1(0) F_2(\alpha)$ is a non-zero integer in K with $s^{d_1+1} \nmid v$ (by (15)) and $s^{d_2} \mid v$ (by (14) and (15)'); which is impossible because of (16), and the lemma is proved.

§.4. - Proof of Theorem 1

Let $a = s/r$ and $\alpha = \sigma/\rho$ with non-zero integers $s, r, \sigma, \rho \in K$ such that " s and r " and " σ and ρ " have no common factor except units.

Case 1. - Let s and σ have no common factor except units in K .

Suppose that $f(\alpha) \in \mathbb{Q}$, so that $p - q f(\alpha) = 0$ for some integers $p, q \in K$ not both zero.

By Lemma 1 $a^{-\lambda(\mu+1)} (p F(0) - q F(\alpha)) \in \mathbb{Z}[a, \alpha]$ with degree $\frac{1}{2} n(n+1) - \lambda(\mu+1)$ and λ in a and α respectively, and so

$$R = T(p F(0) - q F(\alpha)) \text{ with } T = \rho^{\lambda} r^{\frac{1}{2} n(n+1) - \lambda(\mu+1)} a^{-\lambda(\mu+1)}$$

is an integer in K . Using now Lemma 2, as we may in this case, we obtain

$$|R| \geq 1 \text{ for infinitely many } \mu.$$

On the other hand, we have by (6)

$$R = T q G(\alpha).$$

Here

$$(17) \quad \log |T| = \left\{ \frac{1}{2} (\beta+1)^2 - \beta \right\} \mu^2 \log |r| - \beta \mu^2 \log |a| + B\mu$$

$$= \left\{ \frac{1}{2} (\beta+1)^2 \gamma - \beta \right\} \mu^2 \log |s| + B\mu ,$$

where γ is given in Theorem 2, and

$$(18) \quad \log |G(\alpha)| \leq \frac{1}{2} (1-\gamma) \mu^2 \log |s| + B\mu ,$$

since by (5) and (8)

$$|G(\alpha)| \leq B^n \sum_{j=0}^{\mu} |C_j| \leq B^n \prod_{h=1}^{\mu} (1+|a|^{h-1}) \leq B^n |a|^{\frac{\mu}{2}} \mu^2 ,$$

where and in what follows B denotes constants, independent of μ , which are not necessarily the same at each occurrence. Thus

$$\log |R| \leq \left\{ \frac{1}{2} (\beta^2 + 2\beta) \gamma - \beta + \frac{1}{2} \right\} \mu^2 \log |s| + B\mu .$$

So, if $\gamma < (2\beta-1)/(\beta^2 + 2\beta) = h(\beta)$ say, we get

$$\log |R| < 0 \quad \text{for all large } \mu ,$$

which is a contradiction. We have assumed (1), since

$$\max_{\beta > 1} h(\beta) = h\left(\frac{1+\sqrt{5}}{2}\right) = \frac{2}{3+\sqrt{5}} .$$

Case 2. - Let s and σ have common factors except units in K . We can choose a positive integer k for which $a^{-k}\alpha$ can be written as $a^{-k}\alpha = \frac{\sigma'}{\rho'}$, where σ' and ρ' are integers in K such that both " s and σ' " and " σ' and ρ' " have no common factor except units in K . The functional equation (3) with $\alpha' = a^{-k}\alpha$ implies

$$(19) \quad f(\alpha') = \frac{A}{B} + \frac{C}{D} f(\alpha) \quad \text{with integers } A, B, C, D \in K .$$

So Case 2 can be reduced to Case 1, and the proof is completed.

§. 5. - Proof of theorem 2

Let a and α be as in the beginning of the preceeding section. We suppose that there is an ε with $0 < \varepsilon < 1$ such that the inequality (2) has infinitely many solution in non-zero integers in K .

Case 1. - Let s and σ have no common factor except units in K . Choose a solution p, q of (2) with $|q|$ sufficiently large and then a positive integer v such that

$$\xi(1 - \frac{\delta}{k})v^2 \log |s| \leq \log |q| \leq \xi(1 - \frac{\delta}{k})(v+1)^2 \log |s| ,$$

where

$$\xi = \beta - \frac{1}{2} - \frac{1}{2}(\beta^2 + 2\beta)\gamma \quad \text{with} \quad \beta = \frac{1+\sqrt{5}}{2} ,$$

so that, by the condition (1),

$$\xi > 0 \quad \text{and} \quad \xi\kappa = \frac{1}{2}(\beta^2 + 2\beta)(1-\gamma) .$$

By lemma 2, there is a $\mu \in \mathbb{Z}$ with $v \leq \mu \leq v+l$ such that $pF(0) - qF(\alpha) \neq 0$ with $n = [\beta\mu] + \mu$, and so

$$|R| \geq 1 ,$$

where R is defined in the preceeding section.

On the other hand, we have by (6)

$$\log |R| = \log |T| + \log |q| + \log |F(0)(\frac{p}{q} - f(\alpha)) + G(\alpha)| .$$

Here

$$\log |q| = \xi(1 - \frac{\delta}{k})\mu^2 \log |s| + B\mu$$

and, by (11) and Lemma 1 (i),

$$\begin{aligned} |F(0)| &\leq B^n \sum_{k=\lambda}^n |a|^{\frac{1}{2}k(k+1)} |w_{n-k}| \\ &\leq B^n n^{2\mu} |a|^{D(F(0))} \leq B^n |a|^{\frac{1}{2}n(n+1)} , \end{aligned}$$

and so

$$\begin{aligned} \log |F(0)(\frac{p}{q} - f(\alpha))| &\leq \log |F(0)| - (\kappa + \varepsilon) \log |q| \\ &\leq \left\{ \frac{1}{2}(\beta+1)^2(1-\gamma) - \xi(\kappa + \varepsilon)(1 - \frac{\varepsilon}{\kappa}) \right\} \mu^2 \log |s| + B\mu \\ &= \left\{ \frac{1}{2}(1-\gamma) + \xi \frac{\varepsilon^2}{\kappa} \right\} \mu^2 \log |s| + B\mu , \end{aligned}$$

which together with (18) lead to

$$\log |F(0) \left(\frac{p}{q} - f(\alpha) \right) + G(\alpha)| \leq \left\{ \frac{1}{2}(1-\gamma) + \xi \frac{\varepsilon^2}{\kappa} \right\} \mu^2 \log |s| + B \mu.$$

Using this and (17), we obtain

$$\begin{aligned} \frac{\log |R|}{\mu^2 \log |s|} &\leq \frac{1}{2} (\beta+1)^2 \gamma - \beta + \xi \left(1 - \frac{\varepsilon}{\kappa}\right) + \frac{1}{2}(1-\gamma) + \xi \frac{\varepsilon^2}{\kappa} + o(1) \\ &\leq \xi \frac{\varepsilon}{\kappa} (\varepsilon-1) + o(1) < 0, \end{aligned}$$

a contradiction.

Case 2. - Let s and σ have common factors except units in K choose α' as in §.4 Case 2. Then by (19)

$$\left| f(\alpha') - \frac{p'}{q'} \right| < |q'|^{-\kappa - \varepsilon/2} \quad \text{with } p' = A D q + B C p, \quad q' = B D q$$

holds for all integral solutions $p, q \in K$ of (2) with $|q|$ sufficiently large.

Thus Case 2 is reduced to case 1, and the proof is completed.

-:-:-:-

REFERENCES

- [1] F. BERNSTEIN und O. SZASZ, Über Irrationalität unendlicher Kettenbrüche mit einer Anwendung auf die Reihe $\sum_{v=0}^{\infty} q^{v^2} x^v$, Math. Ann. 76 (1915),
- [2] P. BUNDSCHUH, Arithmetische Untersuchungen unendlicher Produkte, Inventiones math. 6 (1969), 275-295.
- [3] P. BUNDSCHUH, Ein Satz über ganze Funktionen und Irrationalitätsaussagen, Inventiones math. 9 (1970), 175-184.
- [4] P. BUNDSCHUH, Verschärfung eines arithmetischen Satz von Tschakaloff, Portugaliae Math. 33 (1974), 1-17.
- [5] P. BUNDSCHUH, Arithmetische Eigenschaften ganzer Funktionen mehrerer variablen, J. reine angew. math. 313 (1980), 116-132.

- [6] O. SZASZ, Über Irrationalität gewisser unendlicher Reichen, Math. Ann. 76 (1915), 485-489.
- [7] I. SHIOKAWA, On the improvement of a theorem of Tschakaloff, to appear.
- [8] L. TSCHAKALOFF, Arithmetische Eigenschaften der unendlichen Reihe
 $\sum_{v=0}^{\infty} a^{-\frac{1}{2}v(v-1)} x^v$, Math. Ann. 80 (1920), 62-74.
- [9] L. TSCHAKALOFF, Arithmetische Eigenschaften der unendlichen Reihe
 $\sum_{v=0}^{\infty} a^{-\frac{1}{2}v(v-1)} x^v$ (2), Math. Ann. 84 (1921), 100-114.
- [10] R. WALLISSER, Über die arithmetische Natur der Werte der Lösungen einer Funktionalgleichung von H. Poincaré, Acta Arith. XXV (1973), 81-92.

(texte reçu le 9 juillet 1981)

-:-:-:-

Iekata SHIOKAWA
 U.E.R. de Mathématiques et
 d'Informatique
 Université de Bordeaux I
 F 33405 TALENCE CEDEX
 and

Department of Mathematics
 Keio University
 HIYOSHI, YOKOHAMA (Japan)

Correction to my paper :

ARITHMETIC PROPERTIES OF CERTAIN POWER SERIES
WITH ALGEBRAIC COEFFICIENTS

(Séminaire de Théorie des Nombres, année 1979-1980, exposé n°27)

by Iekata SHIOKAWA

-:-:-:-

Theorem 5 could be corrected as follows :

THEOREM 5. - Let $f(z)$ be the power series defined by (5) with (6). If $\alpha_1, \dots, \alpha_t$ are t algebraic numbers with $0 < |\alpha_t| < \dots < |\alpha_1| < R_f^*$ such that

$$\prod_{\tau=1}^t \frac{P_k(\alpha_\tau)}{Q_k(\alpha_\tau)} \neq 0 \quad (k \in M) \quad \text{and}$$

$$\lim_{k \rightarrow \infty, k \in M} \left| \frac{P_k(\alpha_{\tau+1})}{Q_k(\alpha_{\tau+1})} \frac{Q_k(\alpha_\tau)}{P_k(\alpha_\tau)} \right| \left| \frac{\alpha_{\tau+1}}{\alpha_\tau} \right|^{e_k} = 0 \quad (1 \leq \tau \leq t)$$

for some infinite sequence M of integers, then $f(\alpha_1), \dots, f(\alpha_t)$ are algebraic independent.

ON THE STRUCTURE OF SELFGENERATING SEQUENCES

by

F. M. DEKKING

-:-:-:-

Consider the sequence $x = x_0 x_1 \dots$ defined by the following rules.

(i) $x_0 = 1$, (ii) x consists of single 2's separated by 1's, (iii) the sequence of lengths of runs of 1's in x equals x :

$$\begin{array}{ccccccccccc} \underbrace{1} & 2 & \underbrace{1 \quad 1} & 2 & \underbrace{1} & 2 & \underbrace{1} & 2 & \underbrace{1 \quad 1} & \dots \\ 1 & & 2 & & 1 & & 1 & & 2 & \dots \end{array}$$

The sequence x is a typical example of a selfgenerating sequence as defined in Section 2.4.4 of [5].

Since x is clearly generated by the substitution $([1, p. 902]) \theta$ given by $\theta(1) = 12$, $\theta(2) = 112$, a lot is known about the structure of x . We mention the following properties.

Recurrence. - Every word which occurs in x , occurs infinitely often in x .

In fact x is almost periodic, i.e., every word occurs with bounded gap (cf. [1, p. 904]).

Linear subword complexity. - Let $\beta_x(n)$ be the number of subwords of length n which occur in x . Then $\beta_x(n) \leq cn$ for some $c > 0$ (cf. [1, Prop. 4.2]).

In fact $\beta_x(n) = n+1$. This can be seen as follows. From Markov's Theorem (cf. ref. 31 in [1]), one infers that $\theta(1) \theta^2(1) \theta^3(1) \dots = z$, where $z = z_1 z_2 \dots$ is defined by

$$z_k = [(k+1)(\sqrt{2}-1)] - [k(\sqrt{2}-1)] + 1.$$

Therefore, $\beta_x(n) \leq \beta_z(n)$ (x starts with $\theta^k(1)$ for all k). Now either by a result of Knuth [4], or by ref. 4 in [1] (noting that z is a Sturmian sequence ([1, p. 903]) $z = (z_k^\alpha)$ with $\alpha = \sqrt{2}-1$ and $I = [1-\alpha, 1)$, since $[(k+1)\alpha] - [k\alpha] = 1$ iff $k\alpha \in I$), one has $\beta_z(n) = n+1$. Since $\beta_x(n) > n$ for all n (by [1, prop. 4.1]), $\beta_x(n) = n+1$ follows.

In the sequel we shall consider another remarkable selfgenerating sequence y (cf. [1, Ex. 4]) defined in a similar way. (i) $y_0 = 2$, (ii) y consists of 1's and 2's, (iii) the sequence of lengths of runs of y equals y :

$$\begin{array}{ccccccc} \underbrace{2 \ 2} & \underbrace{1 \ 1} & \underbrace{2 \ 1} & \underbrace{2 \ 2} & \underbrace{1} & \dots & \\ 2 & 2 & 1 & 1 & 2 & 1 & \dots \end{array}$$

The **mirror image** of a word is the word obtained by the interchange of 1's and 2's. Words occurring in y are called **admissible**. In [3] the reader is asked to prove or disprove the following two properties for y .

Mirror invariance. - A word is admissible iff its mirror image is admissible.

Recurrence. - Every admissible word occurs infinitely often in y .

To the best of my knowledge these two problems are still unsolved. I shall merely offer some simple propositions connected to these problems (*), and show that y has polynomial subword complexity, which immediately implies that y has zero entropy (cf [1, p. 905]).

Any word W of 1's and 2's in which neither 111 nor 222 occur will be called differentiable, and its derivative W' is the word whose j^{th} symbol equals the length of the j^{th} run of W , discarding the first and/or the last run if these have length 1.

For example $(22112122)' = 22112$, $(12211)' = 22$ and $(212)' = 1$.

We put $\Lambda' = \Lambda$, where Λ is the empty word. Also $(12)' = (21)' = 2' = 1' = \Lambda$ (in accordance with the definition). A word V such that $V' = W$ is called a primitive of W . A word can have at most 8 primitives (the primitives of 22 are 1122, 2211, 21122, 12211, 11221, 22112, 122112, and 211221). The two primitives with minimal length are called principal primitives.

PROPOSITION 1. - Mirror invariance implies recurrence.

Proof. - Since any admissible word occurs in some begin segment of y , it suffices to show that any begin segment occurs infinitely often. It even suffices to show that any begin segment $y_0 \dots y_m$ occurs twice. (Suppose $y_0 \dots y_m$ occurs twice for all m . Given k , choose m such that $y_0 \dots y_k$ occurs twice in $y_0 \dots y_m$. Then $y_0 \dots y_k$ occurs at least three times, since $y_0 \dots y_m$ occurs twice, etc... .) Choose n such that $(y_0 \dots y_n)' = y_0 \dots y_m$. By assumption, the mirror image $\tilde{y}_0 \dots \tilde{y}_n$ of $y_0 \dots y_n$ occurs in y . But then $(\tilde{y}_0 \dots \tilde{y}_n)' = y_0 \dots y_m$ occurs in y , not as a begin segment. Hence $y_0 \dots y_m$ occurs at least twice. $\square$

We call a word a C^∞ -word if it is arbitrarily often differentiable. (221122 is a differentiable word which is not C^∞ .) Obviously any admissible word is a C^∞ -word.

(*) After giving this talk, I received a letter from C. Kimberling, who was so kind to send me a copy of a private letter (dated Dec. 7, 1979) addressed to him by F. Galvin. This letter mentions most of these results.

PROPOSITION 2. - Mirror invariance holds iff each C^∞ -word is admissible.

Proof. - Clearly the set of C^∞ -words is mirror invariant. Hence admissibility of all C^∞ -words implies mirror invariance of all admissible words. To prove the converse, suppose W is a C^∞ -word which is not admissible. We may assume that W is the shortest such word, and that 11 or 22 occurs in W . Then W' is a shorter C^∞ -word than W , so W' is admissible. But then at least one, and by mirror invariance both principal primitives of W' are admissible. One of these must be equal to W . Contradiction. $\square$

PROPOSITION 3. - Let $\gamma(n)$ be the number of C^∞ -words of length n . Then $\gamma(n) \leq n^p$, where $p = \log(8)/\log(4/3)$.

Proof. - Let $|W|$ denote the length of W . Let W be a C^∞ -word. Let c be the number of 1's, and d the number of 2's in W' . Suppose W' starts and ends with 2. Then (by differentiability of W') $c \leq 2d$, and

$$|W| \geq c + 2d = c + 4/3d + 2/3d \geq 4/3c + 4/3d = 4/3|W'|.$$

Treating the other 3 cases similarly, we find that for all non-empty C^∞ -words W , one has

$$|W'| \leq 3/4|W|.$$

This implies that $|W^{(k)}| < 1$ as soon as $k \geq \log|W|/\log(4/3)$, where $W^{(k)}$ denotes the k^{th} derivative of W . Since a word has no more than 8 primitives, it follows that

$$\gamma(n) \leq 8^{\log(n)/\log(4/3)} = n^{\log 8/\log(4/3)}.$$

 $\square$

Since all admissible words are C^∞ , and hence $\beta_y(n) \leq \gamma(n)$, we obtain :

COROLLARY. - The sequence y has zero entropy.

It is easy to give sharper estimates for the exponent p .

CONJECTURE. - For some constant c , $\beta_y(n) \sim cn^q$ as $n \rightarrow \infty$, where $q = \log(3)/\log(3/2)$.

PROPOSITION 4. - $\gamma(n) \geq c n^r$, where $c > 0$ and $r = \log(3)/\log(5/3)$.

Proof. - Let W a non-empty C^∞ -word. The degree d of W is defined by $W^{(d)} \neq \Lambda$, $W^{(d+1)} = \Lambda$. The trace sequence $(t_0, t_1, \dots, t_d)$ of W is determined by (i) t_0 is the first symbol of W , (ii) t_j equals the first symbol of $W^{(j)}$ if $W^{(j-1)}$ does not start with 122 or 211, and $t_j = 2^+$ in the remaining case. Example : 1221121122 has trace sequence $(1, 2^+, 2, 1)$. Conversely any sequence of symbols 1, 2 and 2^+ determines at least one C^∞ -word in an obvious way, and it is easily proved by induction that these C^∞ -words are different (in the strong sense that neither is a begin segment of the other) if the corresponding trace sequences are distinct - unless one of these begins with 2 and the other with 2^+ . An argument similar to the one given in the proof of Proposition 3 shows that $|W| \leq 5/3 |W'| + 8/3$ for all C^∞ -words W . This implies that the length of a C^∞ -word with degree d is less than $5(5/3)^d$. Since any C^∞ -word can be extended (to the right) to a longer C^∞ -word, we can conclude to

$$\gamma(5(5/3)^d) \geq 2 \cdot 3^{d-1}.$$

This yields the desired lower bound. □

It is known ([2]) that $\beta_z(n) \leq cn^2$ ($c > 0$, $n = 1, 2, \dots$) if z is a sequence generated by a substitution. Since $\log(3)/\log(5/3) > 2^1/10$ we obtain as a corollary to Proposition 4 (applying Proposition 2), that y cannot be generated by a substitution if mirror invariance holds.

Finally we cannot restrain ourselves from giving a (computer generated) list of the first 39 values of $\gamma(n)$: 2, 4, 6, 10, 14, 18, 26, 34, 42, 50, 62, 78, 94, 110, 126, 142, 162, 186, 218, 250, 282, 314, 346, 378, 410, 446, 486, 534, 590, 654, 718, 782, 846, 910, 974, 1038, 1102, 1166, 1234. This sequence has two peculiar (unexplained) properties. Firstly $\gamma(n+1) - \gamma(n)$ tends to be a power of 2, and secondly $\gamma(3n) = 3\gamma(2n-1)$ holds for $n = 1, 2, \dots, 12$ (but not for $n = 13$). The latter formula is connected to the conjecture above.

REFERENCES

- [1] DEKKING F.M. , Regularity and irregularity of sequences generated by automata, Sémin. Th. des Nombres de Bordeaux, 1979-1980, exposé n° 9.
- [2] EHRENFEUCHT A. , LEE K.P. and ROZENBERG G. , Subword complexities of various classes of deterministic developmental languages without interactions, Theoret. Comput. Sci. 1 (1975), 59-76.
- [3] KIMBERLING C. , Problem 6281* , Amer. Math. Monthly 86 (1979), 793.
- [4] KNUTH D. , Solution to Problem E 2307, Amer. Math. Monthly 79 (1972), 773-774.
- [5] SLOANE N.J.A. , A Handbook of integer sequences, Academic Press, New York, 1973.

(texte reçu le 27 juillet 1981)

--:--:--

F. M. DEKKING
 Department of Mathematics
 Delft University of Technology
 Julianalaan 132
 2628 BL DELFT
 The Netherlands

THE ARITHMETIC OF FUNCTION FIELDS

by

David GOSS

--:--:--

Introduction

The purpose of this article is to give a summary of the arithmetic of function fields as it now stands. We present here, without proofs, the main ideas and results.

§.1. - Background

Let C be a geometrically connected, irreducible curve over $\mathbb{F}_r$, $r = p^n$, p a rational prime. Let $\infty \in C$ be a rational point and let $A = \Gamma(C - \infty, \mathcal{O}_C)$. Thus A is a Dedekind domain with unit group equal to $\mathbb{F}_r^*$. The general theory concerns the ring A and its ring of integers in finite extensions. For simplicity we set $A = \mathbb{F}_r[T]$; though most of the results are entirely general. We set

$k = \mathbb{F}_r(T)$, $K = \mathbb{F}_r((\frac{1}{T})) = k_\infty$ and for $x \in K^*$, we set $D(x) = \text{ord}_\infty(x^{-1})$.

If v is a finite prime, then we set A_v to be the local ring of integers in k_v . Finally we let $\pi = \frac{1}{T} + \sum_{i=2}^{\infty} c_i T^{-i} \in K$ be a fixed uniformizer at ∞ .

An element $x \in K^*$ is said to be monic if and only if $\pi^{D(x)} x \in \mathcal{U}_1 = \{1\text{-units} \subseteq K\}$. If X is monic, then we put $\langle x \rangle_\infty = \pi^{D(x)} x$. If a lower case Roman letter denotes an element of k , then it denotes a monic element.

Let $p \in \text{Spec}(A)$ and set, for $j \in \mathbb{N}$, $\mathfrak{I}(p^j)$ to be the group of A fractional ideals prime to p^j . We set $P(p^j)$ to be the group of principal ideal generated by all $a \in k$ with $a \equiv 1 \pmod{p^j}$. We set $P(p^j \pi^m)$ to be the group generated by all $a \in k$ with $a \equiv 1 \pmod{p^j}$ and $\langle a \rangle_\infty \equiv 1 \pmod{\pi^m}$.

1.1. - LEMMA. - $\mathfrak{I}(p^j)/P(p^j \pi^m)$ is a finite abelian group.

By class field theory $\mathfrak{I}(p^j)/P(p^j \pi^m)$ is canonically the Galois group of an abelian extension $k(p^j \pi^m)$ of k . We set $\mathcal{O}(p^j \pi^m)$ to be the corresponding ring of integers. Let $G(p^j \pi^m)$ be the associated Galois group.

§. 2. - Explicit constructions via the Carlitz-module

Let F be the r^{th} -power map and let $k\{F\}$ be the ring (under composition) of finite polynomials $\{\sum_{i=0}^j a_i F^i \mid a_i \in k \text{ all } i\}$. It is easy to see that $k\{F\}$ is a non commutative ring of endomorphism of $\bar{k}$. Let $C(T) = TF^\circ + F \in k\{F\}$ and for $\alpha \in \mathbb{F}_r$ let $C(\alpha) = \alpha F^\circ$. As F is $\mathbb{F}_r$ -linear, we can extend C to an injection of A into $k\{F\}$. If $M \in A$, then for $x \in \bar{k}$, we have

$$C(M)(x) = \sum_{i=0}^{D(M)} c_i x^{r^i}, \quad c_0 = M, \quad c_i \in A \text{ all } i, \quad c_{D(M)} \in \mathbb{F}_r^*.$$

We call C the Carlitz-module. It is an A -analogue of $\mathbb{G}_m$. Let $p \in \text{Spec}(A)$, with $p = (f)$. Let

$$C[p^j] = \{\text{roots of } C(f^j)(X) \text{ in } \bar{k}\}.$$

One knows that $C[p^j]$ forms an A -module $\simeq A/p^j$. Any generator $\alpha(p^j)$ of $C[p^j]$ is called a primitive p^j -th division point.

2.1. - THEOREM. - a) $k(p^j) = k(\alpha(p^j))$

b) $\mathcal{O}(p^j) = A[\alpha(p^j)]$

c) $\mathcal{O}(p^j)$ is totally ramified at p and unramified elsewhere.

Note that $\mathfrak{F}(p^j)/\mathfrak{P}(p^j) \simeq A/p^{j*}$. Let $k(p^j)_+$ be the fixed field of $\mathbb{F}_r^* \subseteq A/p^{j*}$.

2.2. - THEOREM. - a) $k(p^j)_+/k$ is totally split at infinity.

b) $k(p^j)/k(p^j)_+$ is totally ramified at all infinite primes.

Thus $k(p^j)$ is analogous to $\mathcal{O}(\mu_{p^n})$ and $k(p^j)_+$ to $\mathcal{O}(\mu_{p^n})_+$.

2.3. - PROPOSITION. - $\mathcal{O}(p^n \pi^m)^* = \mathcal{O}(p^n)_+^*$.

2.4. - THEOREM. - Let α_1, α_2 be two primitive p^j -th division points.

Then $\alpha_1/\alpha_2 \in \mathcal{O}(p^j)_+^*$.

We call the group generated by all such units, the group of C -units of level p^j . We denote it by $E(p^j)$.

Let $[i] = T^{r^i} - T$, and let $\lambda = \prod_{i=1}^{\infty} (1 - \frac{[i]}{[i+1]}) \in \mathcal{U}_1$.

Let α be any $(r-1)$ -st root of $-[1]$ and let $\bar{\lambda} = \alpha \lambda$. It is known that $\bar{\lambda}$ is transcendental. Let $L = A\bar{\lambda}$ and let

$$e_L(z) = z \prod_{\substack{\alpha \in L \\ \alpha \neq 0}} (1 - z/\alpha).$$

2.5. - PROPOSITION. - a) $e_L(z)$ is every where convergent.

b) $e_L(z)$ is $\mathbb{F}_r$ -linear.

c) Let $M \in A$. Then $e_L(Mz) = C(M)(e_L(z))$.

Thus $e_L(z)$ is the A -analogue of the classical exponential function.

Let $\alpha \in A$ with $D(\alpha) < D(f^j)$. Clearly all the division points of level p^j are of the form $e_L((\alpha/f^j)\bar{\lambda})$.

As $e'_L(z) \equiv 1$, we see $e_L(z)^{-1} = \sum_{\delta \in L} (z+\delta)^{-1}$. Thus we see the C -units have the description

$$\sum_{\delta \in A} (\alpha + f^j \delta)^{-1} / \sum_{\delta \in A} (\beta + f^j \delta)^{-1}$$

where $(f, \alpha) = (f, \beta) = 1$ and the level is p^j .

§. 3. - The two-variable zêta-functions

We now present the theory of zeta-functions that goes along with the construction of §. 2. Let $S_\infty = K^* \times \mathbb{Z}_p$ and let $s = (s_0, s_1) \in S_\infty$. Let $a \in A$. We set

$$a^s = s_0^{D(a)} < a >_s^1.$$

This definition has all the usual formal properties and the integer powers occur as (π^{-i}, i) . We set $\zeta_\infty(s) = \sum_{a \in A} a^{-s} = \prod_{f \text{ prime}} (1 - f^{-s})^{-1}$.

Clearly $\zeta_\infty(s)$ converges for all s with $D(s_0) > 0$.

3.1. - THEOREM. - a) $\zeta_\infty(s)$ can be analytically continued to a continuous K -valued function on all of S_∞ .

b) For each fixed s_1 , $\zeta_\infty(s_0, s_1)$ is a power series in s_0^{-1} with an infinite radius of convergence.

We call such functions two variable. Theorem 3.1. is proved by resumming the series for $\zeta_\infty(s_0, s_1)$ according to degree.

3.2. - THEOREM. - a) Let $i \in \mathbb{N}^+$. Then $\zeta_\infty(s_0^{-1}, -i)$ is a polynomial in s_0^{-1} .

$$b) \quad \zeta_\infty(-i) = \sum_{j=0}^{\infty} \left(\sum_{D(a)=j} n^i \right) \in A.$$

Indeed the expression in parathesis can be shown to be zero for $j \gg 0$.

3.3. - PROPOSITION. - $\zeta_{\infty}(-i) = 0$ for $i \in \mathbb{N}^*$, $i \equiv 0 \pmod{r-1}$.

Let $\bar{\zeta}(X, -i) = \zeta_{\infty}(X\pi^i, -i)$. Then $\bar{\zeta}(X, -i) \in A[X^{-1}]$. Let $\bar{\zeta}'(X, -i) = \frac{d}{dX} \bar{\zeta}(X, -i)$.
We set $\beta(0) = 0$, $\beta(1) = 1$, and for $i > 0$

$$\beta(i) = \begin{cases} \zeta_{\infty}(-i) & \text{for } i \not\equiv 0 \pmod{r-1} \\ \bar{\zeta}'(1, -i) & \text{for } i \equiv 0 \pmod{r-1} \end{cases}$$

3.4. - PROPOSITION. - a) $\beta(i) \neq 0$ for $i \neq 0$.

b) Let $r = p$. Then $\beta(i)$ is a constant ($= 1$) if and only if the sum of the p-adic digits of $i \leq p-1$.

3.5. - COROLLAIRE. - ζ_{∞} has a simple zero at $-i$, $i \equiv 0 \pmod{r-1}$.

3.5. is the exact analogue of the result for Riemann's zêta function.

Let $(f) = \mathfrak{p} \in \text{Spec}(A)$ and let

$$S_{\mathfrak{p}} = \varprojlim_j \mathbb{Z}/((r^{D(\mathfrak{p})} - 1)p^j)$$

and let $X_{\mathfrak{p}} = k_{\mathfrak{p}}^* \times S_{\mathfrak{p}}$.

3.6. - THEOREM. - a) $(1-f^i) \beta(i)$ interpolates to a continuous function

$$\beta = S_{\mathfrak{p}} \longrightarrow A_{\mathfrak{p}}.$$

b) $(1-f^i X^{-D(\mathfrak{p})}) \zeta(X, -i)$ interpolates to a continuous function $\zeta_{\mathfrak{p}} : X_{\mathfrak{p}} \longrightarrow k_{\mathfrak{p}}$. This function is represented by everywhere convergent power series in the first variable.

It is important to notice that 3.6. gives a very strong relationship between the zeroes of ζ_w for all the places w of k . We will present measures for β a bit later.

We next discuss the theory at the positive integers. At this point there is no functional equation relating the two.

3.7. - THEOREM. - Let $i \in \mathbb{N}^+$ with $i \equiv 0 \pmod{r-1}$. Then $0 \neq \zeta_{\infty}(-i)(\bar{\lambda})^{-i} \in \mathbb{F}_r(T)$.

3.7. is shown with the use of $e_L(z)$.

Let $D_0 = 1$ and for $i > 0$, $D_i = [i][i-1] \dots [1]^{r^{i-1}}$.

Let $m \in \mathbb{N}^+$ with $m = \sum_{j=0}^t \alpha_j r^j$, $0 \leq \alpha_j \leq (r-1)$. We set

$$\Gamma_m = \prod_{j=0}^t D_j^{\alpha_j}$$

The elements Γ_m have all the classical properties of a "factorial".

We also put

$$B_m = \begin{cases} 0 & \text{if } m \not\equiv 0 \pmod{r-1} \\ \Gamma_m \zeta_{\infty}(m)(\bar{\lambda})^{-m} & m \equiv 0 \pmod{r-1}. \end{cases}$$

The next result is a von-Staudt type result. We present it only for the case $p^n = r \neq 2$. When $r = 2$ there are appropriate modifications.

3.8. - THEOREM. - Let $i = \sum_{e=0}^v \beta_e p^e$ be written in its p-adic expansion.

We have two conditions on i :

$$1) \quad (\sum \beta_e) / (n(p-1)) = h \in \mathbb{Z}$$

$$2) \quad (r^h - 1) \mid i.$$

If i satisfies these conditions then the denominator of $B_i = \prod_{\substack{f \text{ prime} \\ D(f)=h}} f$. If not, then $B_i \in A$.

3.9. - COROLLAIRE. - Let $r = p \neq 2$. Then the denominator of $B_i = T^P - T$ if $\beta(i) = 1$.

Proof. - Follows directly from 3.8 and 3.4.

We now show how Γ_m may be interpolated at all the places of k to two-variable Γ -functions. We begin first with ∞ . We put $\overline{D_i(X)} = \overline{X}^{D(D_i)} D_i(X)$.

It is immediate that as $i \rightarrow \infty$, $\overline{D_i(X)} \rightarrow 1$, $\frac{1}{X}$ -adically. Let

$m = \sum_{j=0}^{\infty} \alpha_j r^j$, $0 \leq \alpha_j < r$, be a p -adic integer. Let $X \in K$ be monic. We then set

$$\Gamma_{\infty}(X, m) = \prod_{j=0}^{\infty} \overline{D_j}(\langle X \rangle_{\infty}^{-1})^{\alpha_j}.$$

It is immediate that $\Gamma_\infty(X, m)$ converges to a continuous function which is locally-analytic in the first variable.

Next, let $\mathfrak{P} \in \text{Spec}(\mathbb{F}_r[X])$. It is known that $D_i(X) = \prod_{\substack{f \in \mathbb{F}_r[X] \\ f \text{ monic} \\ D(f) = i}} f$.

We set $\overline{D}_i(X)_{\mathfrak{P}} = \prod_{\substack{f \in \mathbb{F}_r[X] \\ D(f) = i \\ (f, \mathfrak{P}) = 1}} f$.

It is not too hard to show that $\overline{D}_i(X) \rightarrow 1$ $\mathfrak{P}$ -adically as $i \rightarrow \infty$. Now let $a \in A$ and $\mathfrak{p} \in \text{Spec}(A)$. We have a map from $\text{Spec}(A) \rightarrow \text{Spec}(\mathbb{F}_r[X])$ which is dual to the map $X \mapsto a$. Set $a(\mathfrak{p})$ to be the image of $\mathfrak{p}$ under this map. We then set for

$$m = \sum \alpha_i r^i \in \mathbb{Z}_p$$

$$\Gamma_p(a, m) = \prod_{i=0}^{\infty} (-D_i(a)_{a(\mathfrak{p})})^{\alpha_i}.$$

3.10. - THEOREM. - $\Gamma_p(a, m)$ interpolates to a two-variable function

$\Gamma_p : A_p \times \mathbb{Z}_p \longrightarrow A_p^*$. It is analytic in the first variable on each coset of A_p/p .

The above constructions are similar to the classical construction of the p -adic Γ -function.

§.4. - Kummer and Herbrand criterion and Iwasawa theory

We now show how the β -function appears in Kummer and Herbrand criterion for the fields $k(\mathfrak{p})$. By using the classical Weil zeta-function associated to the curves defined by $k(\mathfrak{p}^n)$, $k(\mathfrak{p}^n)_+$, one can show the following : let $h(\mathfrak{p}^n)$, $h(\mathfrak{p}^n)_+$ be the class number of the fields $k(\mathfrak{p}^n)$, $k(\mathfrak{p}^n)_+$ resp.. Let

$$\Theta(\mathfrak{p}^n) = - \sum_{\substack{D(a) < D(\mathfrak{p}^n) \\ (a, \mathfrak{p}) = 1}} \sigma_a^{-1}$$

$\Theta(\mathfrak{p}^n)_+ = \sum -D(a) \sigma_a^{-1}$, where σ_a represents the associated Galois element of $k(\mathfrak{p}^n)$ or $k(\mathfrak{p}^n)_+$. Then we have

$$4.1. - \text{THEOREM.} - a) \quad h(p) = h(p)_+ \prod_{\substack{\chi \in G(p) \\ \chi|_{\mathbb{F}_r^*} \neq 1}} \chi(\theta(p))$$

$$b) \quad h(p)_+ = \prod_{\substack{\chi \in G(p)_+ \\ \chi \neq \chi_0}} \chi(\theta(p)_+) .$$

Following classical theory it is clear how to deduce a plus and minus part for $h(p)$. Both of these numbers are integers and

$$h(p)^- = h(p) / h(p)^+ .$$

Let ζ be a primitive $(r^{D(p)} - 1)$ -st root of 1.

Set $B = \mathbb{Z}_p[\zeta]$ and choose an isomorphism of $B/(p)$ with A/p . Via this, we have a B^* -valued character ω with

$$\omega(\alpha + (p)) + (p) = \alpha + (p) .$$

Thus we have

$$4.2. - \text{THEOREM.} - a) \quad h(p)_+ + (p) = \prod_{\substack{i=0 \\ (r-1) \nmid i}}^{r^{D(p)}-2} \beta(i) + p .$$

$$b) \quad h(p)^- + (p) = \prod_{\substack{i=0 \\ (r-1) \nmid i}}^{r^{D(p)}-2} \beta(i) + p .$$

4.2. is an obvious Kummer criterion. Via it and previous results one can show that, when $r = p > 2$, there are an infinite number of primes with $p \mid h(p)^-$.

Let $Cl(p^n)$, $Cl(p^n)_+$ be the class groups of $k(p^n)$, $k(p^n)_+$ resp. . Let $Cl(p^n)^{(p)}$, etc, be the p -primary component of such groups. Of course $Cl(p^n)^{(p)}$, $Cl(p^n)_+^{(p)}$ are Galois-modules. We may decompose these groups into isotypic components for $\{\omega^i\}$ by tensoring with B . Our next goal, a Herbrand criterion, is to give a sufficient criterion for these isotypic components to vanish. To do so we first present a Stickelberger Theorem due to Tate.

4.3. - THEOREM. - a) $\theta(p^n)$ annihilates $Cl(p^n)$.

b) $\theta(p^n)$ annihilates $Cl(p^n)_+$.

4.3. is proved thru the use of the Jacobian and it is valid quite generally. By reducing mod p , we have as before.

4.4. - COROLLARY. - Let $0 < i < (r^{D(p)} - 1)$. Then $Cl(p)(w^i) \neq 0 \Rightarrow p \mid \beta(r^{D(p)} - 1 - i)$.

4.5. - COROLLARY. - Let the sum of the p-adic coefficients of $(r^{D(p)} - 1 - i) \leq (p-1)$. Then $Cl(p)(w^i) = 0$ when $r = p$.

Let $\eta(p^n) = \theta(p^n) - N/(r-1)$

$$\eta(p^n)_+ = \sum_{\substack{(a, p) = 1 \\ D(a) < D(p^n)}} (n D(p) - D(a) - 1) \sigma_a^{-1} - N/(r-1)$$

where N is the norm element. Both elements are in the p -adic group ring and give rise to distributions. They also annihilate $Cl(p^n)^{(p)}$, $Cl(p^n)_+^{(p)}$ etc.

One can therefore, in classical Iwasawa-theory fashion extend the results of 4.5 to arbitrary level.

We let μ, μ_+ be the p -adic measures on $\mathcal{U} = A_p^*$ determined by $\eta(p^n)$, $\eta(p^n)_+$. Let $\bar{\mu}, \bar{\mu}_+$ denote their reductions mod p .

4.6. - THEOREM. - a) Let $i \in \mathbb{N}$, $i \neq 0$ $(r-1)$. Then

$$\int_{A_p^*} x^{-i} d\bar{\mu}(x) = \zeta_\infty(-i) .$$

b) Let $i \equiv 0$ $(r-1)$. Then

$$\int_{A_p^*} x^{-i} d\bar{\mu}_+(x) = \beta(i) .$$

It is known that cyclicity of the Galois modules $Cl(p)$, $Cl(p)_+$ implies the converse to Herbrand and gives a complete global Iwasawa theory.

§.5. - C-units

We finish by representing the main Theorems in the C-units.

5.1. - THEOREM. - $(\mathcal{O}_{p^n}^+)^* / E(p^n)$ is a finite group of order equal to the class number of $\mathcal{O}_{p^n}^+$.

Let $S(p^n)$ be the group of divisors of degree zero supported at infinity. Let $\mathcal{O}(p^n)$ be the divisors of elements in $E(p^n)$. Let $Q(p^n) = S(p^n) / \mathcal{O}(p^n)$.

5.2. - THEOREM. - $Q(p^n)$ is a finite group of order $h(p^n)_+$.

5.3. - THEOREM. - $Q(p^n)(p) \simeq \mathbb{Z}_p[A/p^{n*} / \mathbb{F}_r^*] / (\mathbb{N}, \theta(p^n))$.

5.3. implies that $Q(p^n)(p)$ should be isomorphic to $Cl(p^n)_+(p)$. This would then imply cyclicity !

§.6. - Open Problems

It is quite important to show the converse to the Herbrand criterion, whether by cyclicity or by Ribet's method. This, perhaps, will involve finding the meaning of the Bernoulli-Carlitz numbers.

It is equally important to find the meaning of the two variable zeta functions themselves, not just their special values theory. This, no doubt, will include the meaning of the associated two-variable Γ -functions.

REFERENCES

- [1] S. GALOVICH, M. ROSEN, The Class Number of Cyclotomic Function Fields, (to appear in Journal of Number Theory).
- [2] D. GOSS, v-adic Zeta Functions, L-series and measures for Function Fields, *Inventiones Mathematicae* 55 (1979), 107-119.
- [3] D. GOSS, The Γ -ideal and Special Zeta-Values, *Duke Journal* (june 1980), 345-364.
- [4] D. GOSS, Kummer and Herbrand Criterion in the Theory of Function Fields, (to appear).
- [5] D. GOSS, The Arithmetic of Function Fields, 2 : The "Cyclotomic" Theory, (to appear).
- [6] D. GOSS, Local Iwasawa Theory for Function Fields, (to appear).
- [7] D. HAYES, Explicit Class Field Theory for Rational Function Fields, *Trans. A.M.S.* vol. 189 (1974), 77-91.
- [8] E. THOMAS, On the Zeta Function for Function Fields over $\mathbb{F}_p$ (to appear).

(texte reçu le 10 septembre 1981)

-:-:-:-

David GOSS
 Department of Mathematics
 Brandeis University
 Waltham
 MASSACHUSETTS 02254
 (Etats-Unis)