Astérisque

AST

Pages préliminaires

Astérisque, tome 198-199-200 (1991), p. 1-34

<http://www.numdam.org/item?id=AST_1991__198-199-200__1_0>

198-199-200 ASTÉRISQUE

1991

JOURNÉES ARITHMÉTIQUES de LUMINY 17-21 JUILLET 1989

Gilles LACHAUD, éditeur

SOCIÉTÉ MATHÉMATIQUE DE FRANCE

Publié avec le concours du CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

Classification A.M.S. : 11, 12, 14

AVERTISSEMENT

Ce volume rassemble les textes de certains exposés présentés aux seizièmes Journées Arithmétiques qui se sont tenues au Centre International de Rencontres Mathématiques (C.I.R.M.) à Luminy du 17 au 21 Juillet 1989.

Ce congrès a bénéficié en premier lieu du soutien du Centre National de la Recherche Scientifique, et aussi de la Ville de Marseille et du Conseil Régional de Provence, Alpes et Côte d'Azur : nous remercions ces organismes pour leur collaboration.

Je remercie également Anna Zeller-Meier, qui s'est chargée de l'organisation administrative, et aussi Christiane Faure et Dominique Bally pour la dactylographie de certains des textes présentés ici.

Le liste des participants figure en tête de ce volume : on observera que plus de vingt nationalités sont représentées. Elle est suivie de la liste de l'ensemble des exposés qui ont été donnés durant ces Journées.

Georges Poitou est décédé peu après ces Journées. Le C.I.R.M. et les Journées Arithmétiques sont deux réalisations qui n'existeraient pas sans lui.

Gilles Lachaud

Table des Matières

J.-P. ALLOUCHE - **SUR LA TRANSCENDANCE DE LA SERIE FORMELLE II**

We prove by elementary means that the formal series II is transcendental, using the theorem of Christol, Kamae, Mendès France and Rauzy.

A.-M. BERGÉ et J. MARTINET - **RESEAUX EXTREMES POUR UN GROUPE D'AUTOMORPHISMES**

Soit E un espace euclidien, et soit G un sous-groupe fini du groupe orthogonal de E. On caractérise les réseaux stables par G qui réalisent un maximum local de la densité des empilements de sphères qui leur sont associés (réseaux G-extrêmes). L'étude est complète pour les groupes cycliques $\mathbb{Q}$-irréductibles d'ordres ≤ 9, ce qui conduit pour certains groupes à une minoration de la densité meilleure que la minoration générale.

M. CAR - **LE PROBLEME DE WARING POUR LES CORPS DE FONCTIONS**

Soit $\mathbb{L}$ un corps de fonctions sur le corps des constantes $\mathbb{F}_q$. Soit S un ensemble fini non vide de valuations de L et soit O_S l'anneau des S-entiers de $\mathbb{L}$.

On s'intéresse au problème de Waring dans O_S en imposant des conditions de valuation, plus précisément, on s'intéresse aux représentations de $b \in O_S$ comme somme

$$b = b_1^k + \cdots + b_m^k$$

telles que $v(b_j) \geq [v(b)/k]$ pour tout $j = 1, \ldots, m$, tout $v \in S$.
On traite ce problème par la méthode du cercle.

J. CHERLY - **SOMMES D'EXPONENTIELLES CUBIQUES DANS L'ANNEAU DES POLYNOMES EN UNE VARIABLE SUR LE CORPS A 2 ELEMENTS, ET APPLICATION AU PROBLEME DE WARING**

L'exposé porte sur le problème de Waring pour un anneau de polynômes sur un corps fini $\mathbb{F}_q$. Ce problème est complètement ouvert lorsque le degré des puissances est supérieur à la caractéristique de $\mathbb{F}_q$, "le premier" cas étant les sommes de cubes dans $\mathbb{F}_2[X]$, c'est ce cas que nous avons étudié. Les deux piliers de ces résultats sont les majorations des sommes trigonométriques et l'encadrement de la série singulière. Nous obtenons ainsi par la méthode du cercle adapté à l'anneau $\mathbb{F}_2[X]$ en suivant Carlitz le résultat suivant :

Les éléments $\mathbf{F}_2[X]$ qui peuvent s'exprimer comme une somme de cubes sont exactement ceux qui sont congrus à 0 ou 1 modulo $1 + X + X^2$. En outre, soit M un tel élément de degré $\leq 3n$ (n un entier suffisamment grand). On peut le représenter comme somme de 18 cubes de polynômes dont chacun a son degré majoré par n.

P. COHEN et J. WOLFART – MONODROMIE DES FONCTIONS D'APPELL, VARIETES ABELIENNES ET PLONGEMENT MODULAIRE

The monodromy groups of Appel's hypergeometric functions F_1 in two variables are sometimes discontinuous, but in general are not arithmetically defined ([DM],[M]). However we associate to them families of abelian varieties which give natural modular embeddings of the monodromy groups into arithmetic groups. We describe these embeddings and sketch some applications to automorphic functions and transcendence questions.

E. DUBOIS et R. PAYSANT-LEROUX – SUR LA LONGUEUR DU DEVELOPPEMENT EN FRACTION CONTINUE DE $\sqrt{f(n)}$

On étudie la longueur $\ell(n)$ du développement en fraction continue de l'irrationnel quadratique $\sqrt{f(n)}$ lorsque f est un polynôme à coefficients entiers et on donne une version effective d'un résultat de Schinzel [9] en minorant, pour tout entier n dans un sous-ensemble de $\mathbf{Z}$, $\ell(n)$ par $1 + 2[\log(\sqrt{f(n)})/\log c]$ où c est une constante ne dépendant que de f. La démonstration fait intervenir certaines notions de meilleures approximations dans les réels et dans un corps de fonctions.

W. DUKE et H. IWANIEC – SUMS OVER PRIMES OF THE FOURIER COEFFICIENTS OF HALF-INTEGRAL WEIGHT CUSP FORMS

This is a brief summary of work presented in detail elsewhere. We give non-trivial estimates for various bilinear forms in the Fourier coefficients of half-integral weight cusp forms. These are applied in Vinogradov's method to give an estimate for the sum of these coefficients over primes.

N. ELKIES – DISTRIBUTION OF SUPERSINGULAR PRIMES

Fix an elliptic curve E over $\mathbf{Q}$ without complex multiplication. Let $\pi_0(x)$ be the number of primes $p < x$ at which E has supersingular reduction. Various approaches to estimating the growth of $\pi_0(x)$ are described, including the recent unconditional proof of the upper bound $\pi_0(x) \ll x^{3/4}$, which was previously only known (by a different method) under the assumption of the Generalized Riemann Hypothesis.

B. EREZ – **A SURVEY OF THE SQUARE ROOT OF THE INVERSE DIFFERENT**

We give a survey of recent work done by several authors on the Galois-Hermitian module obtained by restricting the bilinear trace form of a Galois extension K/F to the ideal $A(K/F)$in K which -when it exists- is the square root of the inverse different of K/F. In many ways the study of $A(K/F)$ as a Galois module is completely analogous to the study of rings of integers, so for instance Galois-Gauss sums play an important role. Howewer we show that -since $A(K/F)$ is self-dual with respect to the trace form- its hermitian structure can also be described very precisely, thus leading to new results on the ring of integers $\mathbf{Z}_K$ (which it contains). Two appendices due to D. BURNS are included.

D.R. HEATH-BROWN – **THE NUMBER OF ABELIAN GROUPS OF ORDER AT MOST x**

Let $A(x)$ denote the number of isomorphism classes of Abelian groups of order at most x. Then

$$A(x) = \sum_{j=1}^{5} c_j x^{1/j} + \Delta(x),$$

with certain coefficients c_j. It is shown that

$$\int_0^X \Delta(x)^2 dx \ll X^{4/3} (\log X)^{89},$$

which is best possible, apart from the log power. The proof uses mean-value estimates for $\zeta(s)$. Using similar techniques it is shown that $\beta_5 \leq \frac{9}{20}$, in the usual notation of the generalized divisor problem. This result has been stated without proof by ZHANG [11].

M.N. HUXLEY – **EXPONENTIAL SUMS AFTER BOMBIERI AND IWANIEC**

We present a summary of the main lines of argument in the new method for estimating exponential sums introduced by BOMBIERI and IWANIEC in 1986. The key ideas are to dissect the exponential sum into sections corresponding to the rational numbers of bounded height, and to bound these subsums in the mean using the large sieve. Applications include bounds for the Riemann zeta function, both mean and pointwise, and the number of integer points in a plane domain with smooth convex boundary. Some problems are posed on the Diophantine behaviour of a smooth curve at integer arguments. The bibliography lists all papers related to the new method up to the end of 1989.

D.-O. JACQUET – **CLASSIFICATION DES RESEAUX DANS $\mathbf{R}^7$ (Via la notion de formes parfaites).**

According to Voronoï, in order to determine all the classes of perfect forms with n variables, it is sufficient to prove that for each class the neighbouring forms of a given representative always

belong to a class which is already known.
The results for $n \leq 6$ have been known for over thirty years. Therefore this article communicates results of the $n = 7$ dimension.

J.-F. JAULENT – **NOYAU UNIVERSEL ET VALEURS ABSOLUES**

We discuss some of the relations involving Gross and Leopoldt conjectures between the ℓ-part of the universal kernel in the K-theory of number fields, the Kummer radical of the compositum of $\mathbf{Z}_\ell$-extensions, and the kernel of the principal ℓ-adic absolute values, given by the ℓ-adic class field theory.

M. LAURENT – **SUR QUELQUES RESULTATS RECENTS DE TRANSCENDANCE**

Cet article se compose de deux parties. La première consiste en une présentation de quelques résultats récents de transcendance et d'indépendance algébrique ; on y examine aussi leurs applications à la conjecture de Leopoldt et à certaines questions de géométrie diophantienne. La deuxième partie propose une nouvelle démonstration du théorème des six exponentielles évitant l'emploi du principe des tiroirs.

R. MASSY – **SUR LES BASES NORMALES D'ENTIERS RELATIVES**

Soient K un corps de nombres quelconque, et E une extension quadratique ou biquadratique de K. On donne des conditions nécessaires pour qu'il existe un corps N, respectivement cyclique de degré 4, diédral ou quaternionien de degré 8, sur K, qui admette une base normale d'entiers sur E. Lorsque K est de nombre de classe $h(K) = 1$, on montre que ces conditions sont aussi suffisantes, et l'on fournit des formules explicites de construction de bases normales d'entiers de N sur E.

T. MATALA-AHO – **ON RECURRENCES FOR SOME HYPERGEOMETRIC TYPE POLYNOMIALS**

Four and five term recurrences are found for some special ${}_3F_2$ and ${}_4F_3$ type hypergeometric polynomials. As a consequence we shall get the Apéry recurrences for the sums $\sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}^i$ $(i = 1, 2)$ and some other three term recurrences - like $A(n)G_n + B(n)G_{n-2} + C(n)G_{n-4} = 0$ for $G_n = \sum_{k=0}^{n} \binom{n}{k}^4 (-1)^k (\deg A(n) = \deg B(n) = \deg C(n) = 6)$.

F. MORAIN – **ELLIPTIC CURVES, PRIMALITY PROVING AND SOME TITANIC PRIMES.**

We describe how to generate large primes using the primality proving algorithm of Atkin.

L. MURATA – **ON THE MAGNITUDE OF THE LEAST PRIMITIVE ROOT**

Let p be an odd prime, $g(p)$ be the least primitive root modulo p and $G(p)$ be the least prime primitive root mod p.

We consider the distribution of $g(p)$ and $G(p)$, and obtain the following results, which show that, in most cases, $g(p)$ and $G(p)$ are very small.

We assume the Generalized Riemann Hypothesis (G.R.H.). Let $\psi(x)$ be a monotone increasing positive function with the properties

$$\lim_{x\to\infty}\psi(x)=+\infty, \psi(x)\ll(\log x)^A \text{ for some } A>0, \psi(x)\ll\psi(\frac{x}{\log x})\cdot$$

Then we have

$$|\{p\le x\ ;\ G(p)>\psi(p)\}|\ \ll\ \frac{\pi(x)}{\log\psi(x)}\cdot$$

We assume G.R.H. For any $\varepsilon>0$, we have

$$\pi(x)^{-1}\sum_{p\le x}g(p)\ll\pi(x)^{-1}\sum_{p\le x}G(p)\ll\ (\log x)(\log\log x)^{1+\varepsilon}.$$

If $\delta<\frac{1}{2}$, then we have

$$\pi(x)^{-1}\sum_{p\le x}g(p)^\delta=E_\delta+o(1)\ ,\quad \pi(x)^{-1}\sum_{p\le x}G(p)^\delta=E'_\delta+o(1)$$

where E_δ and E'_δ are constants depending only on δ.

H. NAKADA et G. WAGNER – **DUFFIN-SCHAEFFER THEOREM OF DIOPHANTINE APPROXIMATION FOR COMPLEX NUMBERS.**

We consider the following inequality for a complex number z and a real-valued function f :

$$|z-\frac{a}{r}|<\frac{f(r)}{|r|}\ ,(a,r)=1\ ,$$

where a and r are integers in an imaginary quadratic field $\mathbf{Q}(\sqrt{d})$, $d<0$. We denote by A_f the set of z having infinitely many solutions a/r to the above inequality. We show that either A_f

or A_f^c is a set of Lebesgue measure 0 (in the complex plane). We also give a sufficient condition on f so that A_f^c is a set of Lebesgue measure 0, which is a complex version of Duffin-Schaeffer's condition.

J. PAS - SOME APPLICATIONS OF UNIFORM p-ADIC CELL DECOMPOSITION

In this paper we summarize some applications of uniform p-adic cell decomposition. The technique of p-adic cell decomposition was developed by Denef, using ideas of Cohen. We obtain cell decomposition theorems which are uniform in a certain class of p-adic fields. We prove a cell decomposition for a class of henselian valued fields of equicharacteristic zero.

R. QUÊME - ON DIOPHANTINE APPROXIMATION BY ALGEBRAIC NUMBERS OF A GIVEN NUMBER FIELD : A NEW GENERALIZATION OF DIRICHLET APPROXIMATION

Let K be a number field of degree n and signature (r, s). In this note, we propose a new generalization of Dirichlet approximation theorem (approximation of $\alpha \in \mathbf{R}$ by $p/q \in \mathbf{Q}$) to the approximation of $\alpha \in \mathbf{R}^r \times \mathbf{C}^s$ by $\sigma(p/q)$ where $p/q \in K$ and $\sigma(p/q)$ is the canonical embedding of K in $\mathbf{R}^r \times \mathbf{C}^s$.

P. RAMBOUR - ELEMENTS FIXES DU COMPLETE D'UNE CLOTURE SEPARABLE SOUS L'ACTION DE SON GROUPE DE GALOIS

En 1969, Ax a montré que l'ensemble des points fixes sous l'action de son groupe de Galois de la clôture algébrique d'un corps local n'est autre que l'adhérence d'une clôture radicielle contenue dans cette clôture algébrique.

Ici R désigne un anneau noethérien, normal, intègre, de corps des fractions K, I un idéal de R qui n'est pas R tout entier. On considère R_s l'anneau des entiers sur R d'une clôture séparable K_s de K, G le groupe $\mathrm{Gal}(K_s/K)$, $\widehat{R}_s$ le complété de R_s pour la topologie définie par IR_s. G agit sur $\widehat{R}_s$ par uniforme continuité et on cherche à déterminer l'ensemble des points de $\widehat{R}_s$ fixes sous l'action de G.

PH. SATGÉ - QUELQUES PROBLEMES DE RATIONALITE LIES AU THEOREME DE PONCELET

Let S be a non singular projective plane conic and c a positive integer. Poncelet's theorem associates a projective plane curve of degree c to any linear system of dimension 1 of effective divisors on S. In this paper we are interested in the field of definition of the curves Poncelet's theorem produces. We pay special attention to the case $c = 2$.

N. SCHAPPACHER – **LES CONJECTURES DE BEILINSON POUR LES COURBES ELLIPTIQUES**

Dans ce rapport qui se veut une *introduction pour non-spécialistes*, on essaie de décrire ce qu'on sait — et ce qu'on ignore — des conjectures de Beilinson relatives aux valeurs spéciales aux points entiers de la fonction L d'une courbe elliptique sur $\mathbf{Q}$. Les problèmes non résolus de K-théorie dans ce contexte sont expliqués. Les deux hypothèses souvent évoquées dans l'arithmétique des courbes elliptiques sur $\mathbf{Q}$ — à savoir, soit l'hypothèse d'une paramétrisation modulaire, soit celle de multiplications complexes — font leur apparition avec des résultats correspondants plus ou moins récents en direction de la conjecture de Beilinson.

H.-P. SCHLICKEWEI – **RESULTATS QUANTITATIFS EN APPROXIMATION DIOPHANTIENNE**

A quantitative version of a general subspace theorem is given. Let K be an algebraic number field, $M(K)$ the set of absolute values $\| \ \|_v$ of K, let S be a finite subset of $M(K)$, and for each $v \in S$, let $L_1^v, \ldots, L_n^v$ be linearly independent linear forms in n variables and with coefficients in K. Solutions $\beta \in K^n$ of the inequality

$$\prod_{v \in S} \prod_{i=1}^{n} \frac{\|L_i^v(\beta)\|_v}{\|L_i^v\|_v \|\beta\|_v} < H(\beta)^{-n-\delta},$$

are considered. Here $\delta > 0, H(\beta)$ denotes the height, and $\|(\beta)\|_v$, $\|L_i^v\|_v$ denote respectively the maximum norm of a vector β and of the coefficient vector of a linear form. It is shown that these solutions are contained in the union of t proper subspaces of K^n and of a set "small" βs. Here t is bounded in terms of n, deg K, card S, δ (but independently of the L_i^v), and the small βs have $H(\beta)$ under some effective bound (depending on the above data, as well as on the heights of the forms L_i^v).

As applications, uniform estimates on the number of solutions of S-unit equations in n variables are obtained.

J.-P. SERRE – **MOTIFS**

This article is a survey of the theory of motives ; some excerpts of letters of A. Grothendieck are included.

J.-P. SERRE – **Lettre à M. Tsfasman**

In this letter, a majoration of the number of points of an hypersurface defined over a finite field is established.

C. SOULÉ – **GEOMETRIE D'ARAKELOV ET THEORIE DES NOMBRES TRANSCENDANTS**

On résume les travaux de GILLET et l'auteur sur l'extension en dimension arbitraire de la géométrie d'ARAKELOV des surfaces arithmétiques. On indique comment cette théorie intervient dans les travaux récents de VOJTA et FALTINGS. On montre que la hauteur des variétés projectives introduites par FALTINGS se compare à celle de leurs coordonnées de CHOW, notion utilisée précédemment par MESTERENKO et PHILIPPON.

W. VEYS - RELATIONS BETWEEN NUMERICAL DATA OF AN EMBEDDED RESOLUTION

Let k be an algebraically closed field of characteristic zero, $f \in k[x_1, \ldots, x_n]$, and (X, h) an embedded resolution of $f = 0$. To each irreducible component E_i of $h^{-1}(f^{-1}\{0\})$, we associate the numerical data (N_i, ν_i), where N_i and $v_i - 1$ are the multiplicities of E_i in the divisor of respectively $f \circ h$ and $h^*(dx_1 \wedge \ldots \wedge dx_n)$ on X. For curves ($n = 2$) there is the well-known relation

$$\frac{\nu}{N} = \frac{\sum_{i=1}^{k}(\nu_i - 1) + 2}{\sum_{i=1}^{k} N_i}$$

between the numerical data of a fixed irreducible component E and its intersecting other components $E_1, \ldots, E_k$. In this paper we present a generalization of this relation, together with new kinds of relations, for all dimensions.

JOURNÉES ARITHMÉTIQUES 1989

LISTE DES PARTICIPANTS

ALLOUCHE J.P., UFR de Math., Ing. Math. et Info., Univ. de Bordeaux I, 351, cours de la Libération, 33405-Talence cedex, France

AMARA H., Dépt. de Math., Fac. des Sciences, Université de Tunis, Campus El Manzah, 1060-Tunis, Tunisie

AMICE Y., UFR de Mathématiques, Tour 45-55, Univ. Paris 7, 2, place Jussieu, 75251-Paris cedex 05, France

AMOROSO F., Scuola Normale Superiore, Piazza dei Cavalieri 7, 56100-Pisa, Italie

ANTONIADIS J.A., Dept. of Mathematics, University of Crete, P.O. Box 1470, Iraklion, Crète, Grèce

ARENAS SOLA A., Dépt. de Mathématiques, Université de Barcelone, Gran Via 585, 08007-Barcelone, Espagne

ARNOUX P., UFR de Mathématiques, Tour 45-55, Université Paris 7, 2 pl. Jussieu, 75251-Paris cedex 05, France

BACHOK C., UFR de Math., Ing. Math. et Info., Univ. de Bordeaux I, 351, cours de la Libération, 33405-Talence cedex, France

BAKER R.C., Dept. of Mathematics, Royal Holloway & Bedford New College, Egham Hill, Egham, Surrey TW20 0EX, England, G.B.

BALASUBRAMANIAN R., U.A. 763 Problèmes Diophantiens, Institut Henri Poincaré, 11, rue Pierre et Marie Curie, 75231-Paris cedex 05, France

BARBOLOSI D., 3 Allée Maurice Blondel, 13100-Aix-en-Provence, France

BARSKY D., UFR de Mathématiques, Tour 45-55, Univ. Paris 7, 2, place Jussieu, 75251-Paris cedex 05, France

BAYER P., Dépt. de Mathématiques, Université de Barcelone, Gran Via 585, 08007-Barcelone, Espagne

BAYER E., Section de mathématiques, Univ. de Genève, C.P. 240, 1211 Genève 24, Suisse

BECKER P.-G., Math. Institut der Univ., Universitt zu Kóln, Weyertal 86-90, 5000 Kóln 41, R.F.A.

BERGÉ A.-M., UFR de Math., Ing. Math. et Info., Univ. de Bordeaux I, 351, cours de la Libération, 33405-Talence cedex, France

BERNDT R., Math. Seminar, Universitât Hamburg, Bundesstrasse 55, 2000-Hamburg 13, R.F.A.

BERTIN M.J., Inst. Math. pures & appli., Univ. Paris 6, tours 45-46, 4 place Jussieu, 75252-Paris cedex 05, France

BERTRAND A., Univ. de Poitiers, 27 rue Boyssonne, 31400-Toulouse, France

BERTRAND D., Inst. Math. pures & appli., Univ. Paris 6, tours 45-46, 4 place Jussieu, 75252-Paris cedex 05, France

BEUKERS F., Mathematics Institute, Univ. of Utrecht, Budapestlaan 6, PO Box 80010, 3508-TA Utrecht, Pays-Bas

BILLOT P., Mathématiques, Bât. 425, Université Paris-Sud, 91405-Orsay cedex, France

BIRCH B., Math. Institute, University of Oxford, 24-29 St. Giles, Oxford OX1 5DQ, England, G.B.

BLANCHARD F., UFR Mathématiques, Informatique, Mécanique, Université de Provence, 3 pl. Victor Hugo, 13288-Marseille cedex 9, France

BLASCO L., Mathématiques, Bât. 425, Univ. de Paris-Sud, 91405-Orsay cedex, France

BOREL J.P., Dépt. de Mathématiques, Univ. de Limoges, 123, rue Albert Thomas, 87060-Limoges cedex, France

BOST J.-B., IHES, 35 rte de Chartres, 91440-Bures sur Yvette, France

BUNDSCHUH P., Mathematisches Institut, Universitt zu Kóln, Weyertal 86-90, D-5000-Kóln 41, R.F.A.

CALDERON GARCIA C., Dep. de Matematicas, Univ. des Pais Vasco, Apartado 644, Bilbao, Espagne

CAR M., Dépt. de Mathématiques, Centre de Saint-Jérôme, Rue Henri Poincaré, 13397-Marseille cedex 13, France

CHASSE G., PAA / TIM, C.N.E.T, 38-40, rue du Général Leclerc, 92130-Issy les Moulineaux, France

CHERLY J., Dépt. de Mathématiques, Univ. de Bretagne Occidentale, 6 av. Victor Le Gorgeu, 29287-Brest cedex, France

CODECA P., Dip. di Matematica, Univ. di Ferrara, Via Machiavelli 35, 4410-Ferrara, Italie

COHEN H., UFR de Math., Ing. Math. et Info., Univ. de Bordeaux I, 351, cours de la Libération, 33405-Talence cedex, France

COLLIOT-THÉLÈNE J.L., Mathématiques - Bât. 425, Université de Paris-Sud, 91405-Orsay cedex, France

COMALADA S., Dpto. Mathematica, Univ. auton. de Barcelona, Bellaterra 08193 (Barcelona), Espagne

CORAY G., Institut de Mathématiques, Université de Genève, 2-4 rue du lièvre, CH-1211 Genève, Suisse

CORRALES R. C., Dpto. Algebra, Fac. Ciencas Mat., Univ. Complutense Madrid, 28040-Madrid, Espagne

COUGNARD J., Dépt. de Mathématiques, Univ. de Franche-Comté, Route de Gray, 25030-Besançon cedex, France

CRESPO T., E.U. d'Arquitectura Tecnica, Auda Dr. G. Maranon s/n, 08028-Barcelona, Espagne

DALAWAT C.S., Mathématiques, Bat. 425, Univ. de Paris-Sud, 91405-Orsay cedex, France

DAVID S., U.A. 763 Problèmes Diophantiens, Institut Henri Poncaré, 11, rue Pierre et Marie Curie, 75231-Paris cedex 05, France

DEBBACHE A., Mathématiques, Bat. 425, Université de Paris-Sud, 91405-Orsay cedex, France

DELAUNAY M., U.A. 763 Problèmes Diophantiens, Institut Henri Poincaré, 11, rue Pierre & Marie Curie, 75231-Paris cedex 05, France

DELGADO J.R., Dept. of Algebra, Fac. Matematicas, Univ. Complutense, Madrid, 28040, Espagne

DELMER F., UFR de Math., Ing. Math. et Info., Univ. de Bordeaux I, 351, cours de la Libération, 33405-Talence cedex, France

DENINGER C., F.B. Mathematik, Universitt Regensburg, Universittstr.31, 8400-Regensburg, R.F.A.

DENIS L., U.A. 763 Problèmes Diophantiens, Institut Henri Poincaré, 11, rue Pierre & Marie Curie, 75231-Paris cedex 05, France

DESCHAMPS M., C.N.R.S., 29 rue Reinhardt, 92100-Boulogne, France

DESHOMMES B., 15, rue de l'Ancienne Comédie, 75006-Paris, France

DESHOUILLERS J.-M., UFR de Math., Ing. Math. et Info., Univ. de Bordeaux I, 351, Cours de la Libération, 33405-Talence cedex, France

DEWISME A., 9, rue des Chardonnerêts, 59134-Le Maisnil, France

DIAZ G., Univ. de St. Etienne, 23, rue du Docteur Paul Michelon, 42023-St. Etienne cedex 2, France

DIAZ Y DIAZ F., Mathématiques - Bât. 425, Université de Paris-Sud, 91405-Orsay cedex, France

DOUAI J.-C., 35 rue du Coquelet, 60123-Eméville, France

DRESS F., UFR de Math., Ing. Math. et Info., Univ. de Bordeaux I, 351, cours de la Libération, 33405-Talence cedex, France

DUBOIS E., Dépt. de Mathématiques, Univ. de Caen, Esplanade de la Paix, 14032-Caen cedex, France

DUKE W., Dept. of Math., Rutgers University, New Brunswick, NJ 08903, USA

DUMONT J.M., UFR des Sciences de Luminy, Mathématiques Informatique, Luminy - Case 901, 13288-Marseille cedex 9, France

ELKIES N., Dept. of Mathematics, Harvard University, Cambridge, Mass. 02138, U.S.A.

EMSALEM M., UFR de Mathématiques, Tour 45-55, Univ. Paris 7, 2, place Jussieu, 75251-Paris cedex 05, France

ERDÖS P., Matematikai Kutato Intezete, A Magyar Tudomanyos Akademia, Realtanoda u. 13-15, Pf. 127, H1364-Budapest, Hongrie

EREZ B., Section Mathématiques, Univ. de Genève, 2-4 rue du Lièvre, CH-1211 Genève, Suisse

EVERTSE J.H., Dept. of Mathematics, Rijksuniversiteit Leiden, P.O. Box 9512, 2300 RA Leiden, Pays-Bas

FAIVRE M., UFR de Math., Info., Mécanique, Université de Provence, 3 place Victor Hugo, 13331-Marseille cedex 3, France

FAKIR S., UFR de Mathématiques, Univ. Scientifique de Lille, B.P. 36, 59655-Villeneuve d'Ascq cedex, France

FAURE H., UFR de Math., Info., Mécanique, Univ. de Provence, 3, pl. Victor-Hugo, 13331-Marseille cedex 3, France

FERENCZI S., Dépt. de Mathématiques, CNRS - URA 225, Luminy - case 916, 13288-Marseille cedex 9, France

FLAJOLET P., Domaine de Voluceau, I.N.R.I.A., B.P. 105, 78153-Le Chesnay cedex, France

FLECKINGER V., Dépt. de Mathématiiques, Univ. de Besançon, Route de Gray, 25030-Besançon, France

FOUVRY E., Mathématiques-Bâtiment 425, Université Paris-Sud, 91405 - Orsay cedex, France

FREI G., Dépt. de Mathématiques, ETH, CH-8092 Zurich, Suisse

FRESNEL J., UFR de Math., Ing. Math. et Info., Univ. de Bordeaux I, 351, cours de la Libération, 33405-Talence cedex, France

GEROLDINGER A., Institut f. Mathematik, Univ. Graz, Halbrthgasse 1/1, 8010-Graz, Autriche

GIAN-GIACOMO J.L., UFR. Méca., Info & Math., Univ. de Metz, Ile du Saulcy, 57012-Metz cedex, France

GOLDSTEIN C., Mathématiques - Bât. 425, Université de Paris-Sud, 91405-Orsay cedex, France

GRANDET M., UER de Mathématiques, Univ. de Toulouse Le Mirail, 5, allée A. Machado, 31058-Toulouse cedex, France

GREEN B.W., Math. Institut, Univ. Heidelberg, Im Neuenheimer Feld 288, Heidelberg 06900, RFA

GREKOS G., Dépt. de Mathématiques, UFR des Sciences et Techniques, 23, rue du Docteur P. Michelon, 42023-Saint-Etienne cedex, France

GROSS B., Dept. of Mathematics, Harvard University, Cambridge, Mass. 02138, U.S.A.

HARAN D., School of Mathematical Sciences, Tel Aviv University, Tel Aviv 69978, Israel

HEATH-BROWN D.R., Mathematical Institute, Magdalen College, Oxford OX14AU, England, G.B.

HEDI A., Dépt. de Math., Fac. des Sciences, Université de Tunis, Campus El Manzah, 1060-Tunis, Tunisie

HELLEGOUARCH Y., Dépt. de Mathématiques, Univ. de Caen, Esplanade de la Paix, 14032-Caen cedex, France

HENNECART F., UFR de Math., Ing. Math. et Info., Univ. de Bordeaux I, 351 cours de la Libération, 33405-Talence cedex, France

HILDEBRAND A., Dept. of Mathematics, Univ. of Illinois, Urbana, Ill.61801, U.S.A.

HINDRY M., UFR de Mathématiques, Tour 45-55, Univ. Paris 7, 2 place Jussieu, 75251-Paris cedex 05, France

HIRATA-KOHNO N., Dept. of Math., Nara Women's Univ, Kita-Uoya-Nishi-Machi, Nara 630, Japon

HOOLEY M., Dept. of Pure Mathematics, University College, P.O. Box 78, Cardiff CF1 1XL, Wales, G.B.

HUXLEY M., School of Mathematics, UWCC, Senghenydd Rd., Cardiff CF2 4AG, Wales, G.B.

ITO S., Dept. of Mathematics, Tsuda College, 2-1-1 Tsuda-machi, Kodaim-shi, Tokyo (187), Japon

JAGER H., Mathematics Institute, Universiteit van Amsterdam, Roetersstraat 15, 1018 WB-Amsterdam, Pays-Bas

JANNSEN U., F.B. Mathematik, Universitt Regensburg, Universittstr.31, 8400-Regensburg, R.F.A.

JAQUET D.-O., Université de Neuchatel, Chantemerle 20 (IMI), 2000 Neuchatel, Suisse

JAULENT J.F., UFR de Math., Ing. Math. et Info., Univ. de Bordeaux I, 351 cours de la Libération, 33405-Talence cedex, France

KACZOROWSKI J., Fachbereich Mathematik, Marburg Univ., Hans-Meerwein-str., D-3550-Marburg/Lahnberge, R.F.A.

KANI E., Dept. of mathematics, Queen's University, Jeffrey Hall, Kingston, Ont. K7L 3N6, Canada

KERADA M., 16 place Bertie Albrecht, 93100- Montreuil, France

KIM M.-H., Dept. of Mathematics, Seoul National University, Kwanak-Gu, Seoul 151 742, Corée

KISILEVSKY H., Dépt. de Mathématiques, Concordia Univ., 1455 De Maisonneuve Blvd. West, Montréal, Québec H3G 1M8, Canada

KRAAIKAMP C., Fac. Wiskunde & Informatica, Roetersstraat 15, 101PWB Amsterdam, Pays-Bas

KRAMMER D., Postbus 880010, Univ. of Utrecht, 3508 TA Utrecht, Pays-Bas

KWON S.-H., UFR de Math., Ing. Math. et Info., Univ. de Bordeaux I, 351 cours de la Libération, 33405-Talence cedex, France

LACHAUD G., C.N.R.S, Luminy Case 916, 13288-Marseille Cedex 9, France

LAHZAMI F., Dépt. de Math., Fac. des Sciences, Université de Tunis, Campus El Manzah, 1060-Tunis, Tunisie

LAMPRECHT E., F.M. Mathematik, Universitt des Saarlandes, Bau 36, 6600-Saarbrcken, R.F.A.

LARIO J.C., Facultat d'Informatica UPS, Pau Gargallo, 5, 08029-Barcelona, Espagne

LAUBIE F., Dépt. de Mathématiques, Univ. de Limoges, 123, rue Albert Thomas, 87060-Limoges cedex, France

LAURENT M., U.A. 763 Problèmes Diophantiens, Institut Henri Poincaré, 11 rue Pierre & Marie Curie, 75231-Paris cedex 05, France

LECACHEUX O., Inst. Math. pures & appli., Univ. Paris 6, tours 45-46, 4 place Jussieu, 75252-Paris cedex 05, France

LEDGARD R.C., Dept. of Mathematics, University of Manchester, Manchester, M13 9PL, England, G.B.

LEVESQUE C., Dépt. de Mathématiques, Université Laval, Québec, P.Q. G1K 7P4, Canada

LIARDET P., UFR de Math., Info., Mécanique, Univ. de Provence, 3, pl. Victor-Hugo, 13331-Marseille cedex 3, France

LIU Q., UFR de Math., Ing. Math. et Info., Univ. de Bordeaux I, 351, cours de la Libération, 33405-Talence cedex, France

MARTINET J., UFR de Math., Ing. Math. et Info., Univ. de Bordeaux I, 351, cours de la Libération, 33405-Talence cedex, France

MASSER D., Dept. of Mathematics, Univ. of Michigan, Ann Arbor, Michigan 48109, U.S.A.

MASSY R., Dépt. de Math., Le Mont-Houy, Univ. de Valenciennes, 29283-Valenciennes, France

MATALA-AHO T., Dept. of Mathematics, Univ. of Oulu, Linanmaa, 90570-Oulu, Finlande

MATIGNON M., UFR de Math., Ing. Math. et Info., Univ. de Bordeaux I, 351, cours de la Libération, 33405-Talence cedex, France

MATTHES R, Univ. Kassel, Henkelstr. 1, D-3500 Kassel, R.F.A.

MATZAT B.H., Mathematisches Institut, Univ. Heidelberg, Im Neuenheimer Feld 288, D-6900 Heidelberg, R.F.A.

MAUDUIT C., UFR des Sciences de Luminy, Université Aix-Marseille II, Luminy Case 901, 13288 - Marseille Cedex 9, France

MAURESO M., Facultat d'Informatica UPS, Pau Gargallo, 5, 08029-Barcelona, Espagne

MAXSEIN T., FB Math der Univ. Frankfurt, Robert-Mayer-str. 10, D-6000 Frankfurt a. M. 11, R.F.A.

McCALLUM W., Dept. of Mathematics, University of Arizona, Tucson, Arizona 85721, U.S.A.

MERCIER A., Dépt. de Mathématiques, Université du Québec à Chicoutimi, 555, Bd. de l'Université, Chicoutimi, P.Q. G7H 2B1, Canada

MESTRE J.-F., DMI, Ecole Normale Supérieure, 45, rue d'Ulm, 75230 - PARIS CEDEX 05, France

MONACI L., Institut Fourier, U.S.M. Grenoble I, B.P. 74, 38402-St. Martin d'Hères Cedex, France

MONTES PERAL J., Dpto. Algebra Geometria, Univ. de Barcelona, Gran Via 585, 08007 Barcelona, Espagne

MORAIN F., Domaine de Voluceau, I.N.R.I.A., BP 105, 78153-Le Chesnay, France

MOROZ B.Z., Dépt. de Mathématiques, Univ. Louis Pasteur, 7, rue René Descartes, 67084-Strasbourg, France

MOSSE B., UFR Mathématiques, Informatique, Mécanique, Université de Provence, 3 pl. Victor Hugo, 13288-Marseille cedex 9, France

MURATA L., Dépt. de Mathématiques, Université de Nancy I, B.P. 239, 54506-Vandoeuvre lès Nancy, France

NAIMI M., Dépt. de Mathématiques, Faculté des Sciences de Tunis, Campus Universitaire, 1060 Tunis, Tunisie

NAIR M., Dep. of Mathematics, Univ.of Glasgow, Gardens, Glasgow G12 8QW, G.B.

NAKADA H., Dept. of Mathematics, Keio Univ. Hiroshi 3-14-1, Kohoku, Yokohama 223, Japon

NAKAGAWA J., Dept. of Mathematics, Joetsu Univ. of Education, Joetsu 943, Japon

NAKAJIMA S., Dept. of Math., College of Arts & Sci., Univ. of Tokyo, 3-8-1 Komaba, Maguroku, Tokyo 153, Japon

NART E., Dpto. Matematica, Université de Barcelone, Gran Via 585, 08007-Barcelone, Espagne

NGUYEN N.T., Mathématiques - Bât. 425, Université de Paris-Sud, 91405-Orsay cedex, France

NGUYEN QUANG DO T., Dépt. de Mathématiques, Univ. de Franche-Comté, Route de Gray, 25030-Besançon cedex, France

NICOLAS J.L., Inst. de Mathématiques & Informatique, Univ. Claude Bernard-Lyon I, 43, Bd. du 11 novembre 1918, 69622-Villeurbanne cedex, France

NOGUEIRA A., Mathématiques, Bât. 425, Univ. de Paris-sud & Univ. de Rio de Janeiro, 91405-Orsay cedex, France

PAS J., Kath. Univ. Leuven, Celestijnenlaan 200-B, 3030 Heyerlee, Belgique

PASCUAL-XUFRE G., Dépt. de Mathématiques, Université de Barcelone, Gran Via 585, 08007-Barcelone, Espagne

PAYSANT-LE-ROUX R., Dépt. de Mathématiques, Univ. de Caen, Esplanade de la Paix, 14032-Caen cedex, France

PERELLI A., Dip. di Matematica, Universita di Genova, Via L.8. Alberti 4, 16132-Genova, Italie

PERRET M., C.N.R.S., Luminy - case 916, 13288-Marseille cedex 9, France

PHILIBERT G., Dépt. de Mathématiques, UFR des Sciences et Techniques, 23, rue du Docteur P. Michelon, 42023-Saint-Etienne cedex, France

PHILIPPON P., U.A. 763 Problèmes Diophantiens, Institut Henri Poincaré, 11, rue Pierre et Marie Curie, 27170-Le Plessis Ste Opportune, France

POITOU G., DMI, Ecole Normale Supérieure, 45, rue d'Ulm, 75230-Paris cedex 05, France

POP F., Math. Institut, Im Neuenheimer Feld 288, D-6900- Heidelberg, RFA

POULAKIS D., Dépt. de Mathématiques, Univ. de Théssalonique, 54006-Thessalonique, Grèce

QUEME R., 32 Hameau de la Caravelle, 91650-Breuillet, France

QUER J., Facultat d'Informatica UPS, Pau Gargallo, 5, 08029-Barcelona, Espagne

RAMBOUR M., Résidence "Les Bourgognes", 95000-Cergy, France

RAOUJ A., Dépt. de Mathématiques, Univ. de Nancy I, BP 239, 54506-Vandoeuvre les Nancy, France

RAUZY G., UFR des Sciences de Luminy, Mathématiques Informatique, Luminy - Case 901, 13288-Marseille cedex 9, France

RAYNER F., Dept. of Pure Mathematics, University of Liverpool, Liverpool, L69 3BX, England, G.B.

REVERSAT M., Département de Mathématiques, Univ. Paul Sabatier, 118, rte de Narbonne, 31062-Toulouse cedex, France

REYSSAT Y., Inst. Math. Pures & Appli., Univ. Paris 6, tours 45-46, 4 place Jussieu, 75252-Paris cedex 05, France

RHIN G., Dépt. de Mathématiques, UFR. Méca., Info & Math., Univ. de Metz, Ile du Saulcy, 57012-Metz cedex, France

RIEGER G.J., Institut f. Mathematik, Universitt Hannover, 3000-Hannover, R.F.A.

RIO A., Dept. Algebra i Geometria, Gran Via 585, 08007-Barcelona, Espagne

ROY D., UA 763 - Problèmes Diophantiens, Institut Henri Poincaré, 11, rue Pierre & Marie Curie, 75231-Paris cedex 05, France

RUDOLPH D., c/o W. Parry, Math. Institute, Univ. of Warwick, Coventry CV4 7AL, G.B.

SAIAS E., 44 rue du Fer à Moulin, 75005-Paris, France

SALBERGER P., 20-22 rue d'Arcueil, 75014-Paris, France

SAMPRE G., Ecole des Mines, Cours Fauriel, 42-Saint-Etienne, France

SANDER J.W., Institut f. Mathematik, Univ. Hannover, Welfengarten 1, 3000-Hannover 1, RFA

SATGE P., Dépt. de Mathématiques, Univ. de Caen, Esplanade de la Paix, 14032-Caen cedex, France

SCHÄFFER V., Institut f. Mathematik, Univ. Hannover, Welfengarten 1, D-3000 Hannover 1, France

SCHAPPACHER N., Max-Planck Institut f. Mathematik, Gottfiried-Clarrenstr.. 26, 5300-Bonn 3, R.F.A.

SCHERTZ R., Institut f. Mathematik, Universitt Augsburg, Memmingerstr. 6, D-8900-Augsburg, R.F.A.

SCHLICKEWEI H.P., Abteilung f. Mathematik, Universitt Ulm, Oberer Eselsberg, D-7900-Ulm, R.F.A.

SCHOEN C., Mathematisches Institut, Universitt Erlangen, Bismarckstr. 1/2, D-8520 Erlangen, R.F.A.

SCHOLL A., Dept. of Mathematics, Durham University, South Rd., Durham DH1 3LE, England, G.B.

SCHWARZ W., Institut f. Mathematik, Frankfurt Univ., Robert-Mayer-Str. 10, d-6000 Frankfurt a. M., R.F.A.

SERRE J.P., Collège de France, 11, Place Marcelin Berthelot, 75231 - PARIS CEDEX 05, France

SHIOKAWA I., Dept. of Mathematics, Keio University, Hiyoshi Kohoku, Yokohama, Japon

SILVERMAN R., MITRE Corp., Burlington Rd., Bedford, Ma., U.S.A.

SMADJA R., UFR des Sciences de Luminy, Université Aix-Marseille II, Luminy Case 901, 13288-Marseille cedex 9, France

SMATI A, Dépt. de Mathématiques, Univ. de Limoges, 123, rue Albert Thomas, 87060-Limoges cedex, France

SMITH P., F.B. Mathematik sze Univ. Frankfurt, Robert-Mayer-Str. 10, D-6000 Frankfurt a. M. 11, R.F.A.

SODAIGUI B., Section de Mathématiques, Université de Genève, 2-4 rue du Lièvre, 1211-Genève, Suisse

SOUL Christophe, I.H.E.S., 35, route de Chartres, 91440 - Bures su Yvette, France

SPIRO-Silverman C., Dept. of Pure Math., MIT, Cambridge, Mass., U.S.A.

STOLARSKY K., Mathematics Dept., Univ. of Illinois, 1409 W. Green, Urbana, Ill. 61801, U.S.A.

TAN E.-T., Dept. of Math. Sciences, National Shenghi Univ., Mucha, Taipei 11623, Taiwan, République de Chine

TAUSSAT Y., UFR de Math., Ing. Math. et Info., Univ. de Bordeaux I, 351, cours de la Libération, 33405-Talence cedex, France

TENENBAUM G., Dépt. de Mathématiques, Univ. de Nancy I, B.P. 239, 54506-Vandoeuvre-les-Nancy, France

THEROND J.D., Dépt. de Mathématiques, U.S.T. du Languedoc, Place E. Bataillon, 34060-Montpellier cedex, France

TICHY R., Abt. f. Tech. Math., Tech. Univ. Vienna, Wiedner Hauptstr. 8-10, 1040-Wien, Autriche

TILOUINE J., Mathématiques - Bât. 425, Université de Paris-Sud, 91405-Orsay cedex, France

TOFFIN P., Dépt. de Mathématiques, Univ. de Caen, Esplanade de la Paix, 14032-Caen cedex, France

TOP J., Math. Inst., Univ. of Utrecht, P.O. Box 80010, 3508 TA Utrecht, Pays-Bas

TOPUZOGLU A., Maths. Dept., Middle East Techn. University, 06531-Ankara, Turquie

TOUIBI L., Dépt. de Math., Fac. des Sciences, Université de Tunis, Campus El Manzah, 1060-Tunis, Tunisie

TRAVERSA GRAU A., Dept. Algebra, Geometria, Univ. de Barcelona, Gran Via 585, 08007-Barcelona, Espagne

TSFASMAN M., Institute of Information Transmission, 19 Ermolovoi Street, Moscow, URSS

VALLEE B., Dépt. de Mathématiques, Univ. de Caen, Esplanade de la Paix, 14032-Caen cedex, France

VERANT M., 28, chemin de Palenté, 25000- Besançon, France

VERGER-GAUGRY J.-L., Institut Fourier, Univ J. Fourier, BP 74, 38402-St. Martin d'Hères cedex, France

VEYS W., K.U. Leuven, Celestijnenlaan 20013, B-3030 Leuven, Belgique

VILA N. P., Dépt. de Mathématiques, Université de Barcelone, Gran Via 585, 08007-Barcelone, Espagne

VIOLA C., Istituto di Matematica "L. Tonelli", Universita di Pisa, 56100-Pisa, Italie

VOJTA P., Dept. of Mathematics, Univ. of California, Berkeley, Ca 94720, U.S.A.

WALDSCHMIDT M., UA 763-Problèmes Diophantiens, Institut Henri Poincaré, 11, rue Pierre & Marie Curie, 75231 - PARIS CEDEX 05, France

WANG W., Math. Institute, Oxford University, 24-29 St. Giles, Oxford, G.B. OX13LB

WILSON S.M.J., Dept. of Mathematics, Durham University, South Rd., Durham DH1 3LE, England, G.B.

WOLFART J., FB Mathematik, Universitt Frankfurt, Robert-Mayer str.6-10, 6000-Frankfurt a.M., R.F.A.

WOLFMANN J., G.E.C.T., Université de Toulon & du Var, 83130-La Garde, France

WU J., Mathématiques, Bat. 425, Univ. de Paris-Sud, 91405-Orsay cedex, France

YOGANANDA, Matscience 1, Taramant, 600113 Madras, Inde

ZRAN ZANKOE T.S., UFR de Math., Ing. Math. et Info., Univ. de Bordeaux I, 351, cours de la Libération, 33405-Talence cedex, France

JOURNEES ARITHMETIQUES 1989

CONFERENCES ET COMMUNICATIONS

CONFERENCES

BOST J.B.	Moyennes arithmético-géométriques et périodes des courbes algébriques : un aperçu historique
GROSS B.	Kolyvagin's work on modular elliptic curves
HILDEBRAND A.	Irregularities in the distribution of primes
HOOLEY C.	On nonary cubic sums
LAURENT M.	Progrès récents en transcendance
RAUZY G.	Systèmes de numération
SCHAPPACHER N.	Beilinson's conjecture for elliptic curves : the state of the art
SERRE J.-P.	Motifs
SOULÉ C.	Arithmetic Riemann-Roch and ampleness
TSFASMAN M.	Global fields, codes and sphere packings

COMMUNICATIONS

ALLOUCHE J.P.	Sur la transcendance de la série formelle Π
BALASUBRAMANIAN R.	On Erdös-Woods conjecture

BAYER E.	Bases normales autoduales
BECKER P.G.	On effective measures for algebraic independence
BERGÉ A.M., MARTINET J.	Réseaux extrêmes pour un groupe d'automorphismes
BERNARDI D.	Présentation du logiciel PARI
BERTRAND A.	Nombres de Perron et séries rationnelles
BIRCH B.J.	Calculations for, and questions about, elliptic curves
BLANCHARD F.	Numération en base thêta
BOREL J.P.	Sur une fonction liée à certains ensembles normaux
BOURGAIN J.	The Riesz-Raikov theorem for algebraic numbers
CAR M.	Problème de Waring pour l'anneau des S-entiers d'un corps de fonctions algébriques
CHERLY J.	Résolution du problème de Waring pour les cubes dans $F_2[X]$
COLLIOT-THÉLÈNE J. L.	Théorèmes de finitude pour les cycles de codimension 2
CRESPO T.	Réalisation explicite de doubles recouvrements comme groupes de Galois
DAVID S.	Minoration de hauteurs dans les variétés abéliennes
DENINGER C.	Groupes formels et fonctions L
DESCHAMPS M.	Nombre de points des jacobiennes sur les corps finis
DESHOMMES B.	Résolution semi-locale d'équations diophantiennes

DIAZ G.	Approximation de π par les éléments d'un corps cyclotomique
DUBOIS E.	Sur le développement de $\sqrt{P(n)}$ en fraction continue
DUKE W.	Sums over primes of half-integral weights Fourier coefficients
DUMONT J.M.	Formules sommatoires et substitutions
ELKIES N.	Distribution of supersingular primes
EREZ B.	Structure galoisienne de la racine carrée de la codifférente
EVERTSE J.H.	Effective finiteness theorems for binary forms with given discriminant
FAIVRE C.	Distribution des constantes de Levy des irrationnels quadratiques
FERENCZI S.	Bounded remainder sets
FLAJOLET P.	Transformation de Mellin et analyse d'algorithmes informatiques
FREIMAN G.	analytic number theory and integer programming
GEROLDINGER A.	Factorization of algebraic integers
HEATH-BROWN D.R.	The number of abelian groups of order at most x
HELLEGOUARCH Y.	Factorisation des différentielles galoisiennes
HINDRY M.	Hauteurs sur les courbes et les variétés abéliennes
HIRATA-KOHNO N.	Formes linéaires de points algébriques sur les groupes algébriques
HUXLEY M. N.	Exponential sums after Bombieri and Iwaniec
ITO S.	On continued fractions, substitutions and characteristic sequences

JANNSEN U.	Principe de Hasse cohomologique
JAQUET D.O.	Classification des réseaux dans R^7
JAULENT J.F.	Noyau universel et noyau des valeurs absolues
KIM M.H.	The canonical decomposition of Siegel modular forms
KRAAIKAMP C.	Good approximations and continued fractions
LIARDET P.	Propriétés harmoniques de la numération suivant Ostrowski
MASSER D.	Endomorphismes de variétés abéliennes
MASSY R.	Bases normales d'entiers relatives
MATALA-AHO T.	Recurrences for some hypergeometric type polynomials
MESTRE J.-F.	Extensions groupe de Galois A_n
MORAIN F.	Courbes elliptiques, tests de primalité et nombres de Chudnovsky
MOROZ B.Z.	On representation of integers by integral quadratic forms
MURATA L.	On the magnitude of the least primitive root
NAKADA H.	On Duffin-Schaeffer theorem on diophantine approximation for complex numbers
NGUYEN QUANG DO T.	Lois de réciprocité primitives
NOGUEIRA A.	Interval exchange transformations
PAS J.	p-adic cell decomposition and Igusa's local zeta function
PERRET M.	Nombre de points des courbes sur les corps finis
POP F.	On the Galois structure of finitely generated fields

QUÈME R.	Sur l'approximation diophantienne par un nombre algébrique d'un corps donné
RAMBOUR P.	Points fixes du complémentaire de la clture séparable d'un corps sous l'action du groupe de Galois
RAYNER F.	Weak uniform distribution for divisor functions
RUDOLPH D.J.	Normal numbers base 2 and base 3 and entropy
SALBERGER P.	On the Hasse principle and weak approximation for surfaces defined by two quadratic forms
SANDER J.W.	On $4/n = 1/x + 1/y + 1/z$ and Iwaniec' half-dimensional sieve
SATGÉ P.	Systèmes linéaires de degré 3 et involution d'Atkin-Lehner sur $X_0(3)$
SCHLICKEWEI H.P.	Le théorème du sous-espace quantitatif pour les corps de nombres
SCHOLL A.	Heights pairings and motives
SCHWARZ W.	New proof for a theorem connecting spaces of almost-periodical arithmetic functions
SERRE J.-P.	Points rationnels et crible
SHIOKAWA I.	Explicit constructions of normal numbers
SILVERMAN R.	Practical, average case analysis of the elliptic curve factoring algorithm
SMITH P.R.	On discriminants of binary quadratic forms with one class in each genus
SODAÏGUI B.	Structure galoisienne des anneaux d'entiers
SPIRO-SILVERMAN C.	Asymptotic expansion for the property that an integer is coprime to $j(n)$

STOLARSKY K.B.	Beatty sequences and general Wythoff pairs via substitutions of non constant length
TAMURA J.	Infinite products and ascending continued fractions
TAN E.T.	Le scindage du corps de classes de Hilbert et les noeuds de nombres
TENENBAUM G.	Sommes oscillantes sur les entiers sans grand facteur premier
VALLÉE B.	Éléments de petit carré modulaire et factorisation entière
VEYS W.	Numerical data of resolutions and Igusa's local zeta function
VOJTA P.	Recent work on Hall's conjecture
WILSON S.M.J.	Projective invariants from non-projective Galois modules
WOLFART J.	Monodromie et plongement modulaire
WU J.	Sur la suite des nombres premiers jumeaux

SÉANCE DE PROBLÈMES

1) Pour tout entier N tel que la courbe $X_0(N)$ soit de genre ≥ 1, on note h_N la hauteur de Faltings de $J_0(N)/\mathbf{Q}$.

La fonction $N \mapsto h_N$ est-elle majorée par un monôme en N ? Une réponse positive serait déjà intéressante pour N sans facteurs carrés ou même pour N premier.

D. BERTRAND, M. HINDRY

2) Let $\varphi : X_0(N) \to E$ be the Weil map. What can be said about $\deg(\varphi)$, in particular :

a) does $\deg(\varphi)/\sigma(N)$ tend to infinity with N ?

b) estimate $\limsup \dfrac{\log \deg(\varphi)}{N}$ (is it zero ?)

B.J. BIRCH

3) Suppose α is algebraic of degree d, such that $\mathbf{Q}(\alpha^n) = \mathbf{Q}(\alpha)$ for all $n > 0$. Is there a constant $C(\alpha)$ (or, better, $C(d)$) such that for any $(d-1)$-dimensional subspace W of $\mathbf{Q}(\alpha)$ there are at most $C(\alpha)$ powers of α in W ?

J. BOURGAIN

4) Set $f(x)$ equal to the number of discriminants D of an imaginary quadratic field such that $h(D)$ is a power of 2 and $|D| \leq x$. Can one prove that $f(x) = o(x)$?

H. COHEN

5) Let $h(\Delta)$ be the class number of $\mathbf{Q}(\sqrt{\Delta})$ for any fundamental discriminant $\Delta \in \mathbf{Z}$. Is it true that

$$\sum_{\substack{p \equiv 1 \pmod 4 \\ p \text{ prime } \leq x}} h(p) \sim \frac{x}{8} \quad \text{as} \quad x \to \infty \ ?$$

H. COHEN,C. HOOLEY

6) Soit q une puissance d'un nombre premier p, et soit $a \in \mathbf{F}_q^\times$. La *somme de Kloosterman* d'indice a est

$$Kl_q(a) = \sum_{x \in \mathbf{F}_q^\times} \exp\left(\frac{2i\pi}{p}\, Tr_{\mathbf{F}_q/\mathbf{F}_p}\,(ax + x^{-1})\right).$$

L'application $a \mapsto Kl_q(a)$ de $\mathbf{F}_q^\times$ dans le corps cyclotomique $\mathbf{Q}(\zeta_p)$ des racines p-ièmes de l'unité (où $\zeta_p^p = 1$) est contenue dans l'ensemble

$$X_q = \{K \in \mathbf{R} \cap \mathbf{Z}[\zeta_p] \mid |K| \leq [2\sqrt{q}] \text{ et } K \equiv -1 \bmod (1-\zeta_p)\mathbf{Z}[\zeta_p]\}\ .$$

Quelle est l'image de l'application Kl_q ?

L'image de l'application Kl_q est égale à X_q si $p = 2$ (G. LACHAUD et J. WOLFMANN, C.R.A.S. 1987) et si $p = 3$ (N. KATZ et R. LIVNÉ, C.R.A.S. 1989) ; des calculs sur machine faits par R. ROLLAND et R. SMADJA ont montré qu'il n'en est pas ainsi pour $p \geq 5$.

G. LACHAUD

7) (Calcul de lois de réciprocité explicites par le corps de normes de FONTAINE ET WINTENBERGER.) Soit K un corps local de caractéristiques $(0, p)$, contenant μ_{p^n}. On veut calculer le symbole de Hilbert $(.,.)_{p^n}$ par la méthode suivante : soit K_∞/K une extension APF (e.g. la $\mathbf{Z}_p$-extension cyclotomique) ; FONTAINE et WINTENBERGER lui associent le corps de normes $X_{K_\infty}(K)$ qui s'identifie à un corps de séries formelles sur le corps résiduel de K. On a $X_{K_\infty}(K)^* = \varprojlim K_n^*$; une addition est définie dans le même style.

Calculer le symbole de Hilbert dans K à partir du symbole de Witt dans $X_{K_\infty}(K)$. On s'intéresse surtout au cas où $n > 1$, le cas $n = 1$ ayant été résolu partiellement par DRAOUIL. Eventuellement, retrouver les lois de réciprocité explicites dans le style de BRÜCKNER, VOSTOKOV, etc...

T. NGUYEN QUANG DO

8) Soient $N \geq 1$ et $u_1 < u_2 < \cdots < u_N$ une suite arbitraire d'entiers. Pour $n > N$, on prolonge cette suite de la manière suivante : u_n est le plus petit entier supérieur à u_{n-1} tel que

$$u_n \neq u_p + u_q$$

quels que soient $p, q < n$. Est-il vrai que la suite $u_{n+1} - u_n$ est périodique à partir d'un certain rang ?

Exemple : $N = 2$, $u_1 = 1$, $u_2 = 4$.Alors u_3 est différent de $5 = u_1 + u_2$ et de $8 = u_2 + u_2$, donc $u_3 = 6$.Ensuite u_4 doit être différent de $7 = u_1 + u_3$, de $8 = u_2 + u_2$,de $10 = u_2 + u_3$ et de $12 = u_3 + u_3$, donc $u_4 = 9$, et ainsi de suite : $1, 4, 6, 9, 11, 14 \ldots$

G. RAUZY

9) L'application de $\mathbf{N}^{*2}$ dans $\mathbf{Q}$

$$(m,n) \longmapsto \frac{3^m - 1}{2^n - 1}$$

est-elle injective ?

C. SAIAS

10) Existe-t-il une suite de polynômes unitaires f_λ, à coefficients dans $\mathbf{Z}$ tels que :

1) $\deg f_\lambda \to \infty$;

2) $\text{disc}\,(f_\lambda) \neq 0$;

3) $|\text{disc}\,(f_\lambda)|^{1/\deg f_\lambda}$ est borné ?

Le cas le plus intéressant est celui où les f_λ sont irréductibles.

J-P. SERRE

11) An equilateral triangle of side L is placed in the plane. How far can its perimeter be from the unit lattice ?

K.B. STOLARSKY

12) Let $d \leq q+1$. What is the value of

$$M_{d,q,n} = \max_F |\{(x_1,\ldots,x_n) | x_i \in \mathbf{F}_q \ , \ F(x_1,\ldots,x_n) = 0\}\,,$$

the maximum being taken over all non-zero homogeneous forms of degree d ? Is it true that

$$M_{d,q,n} = d(q^{n-1} - q^{n-2}) + q^{n-2} \ ?$$

(*réponse : oui* (J-P. SERRE,A.B.SORENSEN))

M. TSFASMAN

13) For any sequence $\{K_i\}$ of number fields with $[K_i : \mathbf{Q}] \to \infty$, and

$$\frac{1}{[K_i : \mathbf{Q}]} \log |\mathcal{D}_{K_i}| < d \ ,$$

it can be shown that

$$M(\{K_i\}) = \limsup_{K_i} \frac{h(K_i)}{[K_i : \mathbf{Q}]} \leq c_1(d) \ ,$$

where

$$h(K) = \min_{\substack{f \in K^* \\ h(f) \neq 0}} h(f),$$

$$h(f) = \sum_v |\log \|f\|_v| .$$

Do there exist such sequences $\{K_i\}$ with

$$M(\{K_i\}) \geq c_2(d) > 0 \ ?$$

M. TSFASMAN

14) Let K be a number field,

$$\varphi : K \to \mathbf{R}^s \times \mathbf{C}^t \simeq \mathbf{R}^n$$

and $L = \varphi(\mathcal{O}_K)$. What is the minimum length

$$d(L) = \min_{\substack{v \in L \\ v \neq 0}} |v| \ ?$$

Is it true that

$$d(L) = \sqrt{s+t} \ ?$$

It is known that $\sqrt{s+t} \geq d \geq \sqrt{\frac{s}{2} + t}$; if $s = 0$ or $t = 0$ then $d = \sqrt{s+t}$.

M. TSFASMAN

15) a) Let

$$A(q) = \limsup_{X/\mathbf{F}_q} \frac{|X(\mathbf{F}_q)|}{g} \ , \ g \to \infty.$$

Is it true that

$$A(q) = \sqrt{q} - 1 \ ?$$

i.e. is the DRINFELD-VLĂDUŢ bound exact ?

b) Are the ODLYZKO-SERRE bounds for

$$\liminf_K \frac{1}{[K : \mathbf{Q}]} \log |\mathcal{D}_K|$$

asymptotically exact ?

M. TSFASMAN

Astérisque

JEAN-PAUL ALLOUCHE

Sur la transcendance de la série formelle II

Astérisque, tome 198-199-200 (1991), p. 35-39

<http://www.numdam.org/item?id=AST_1991__198-199-200__35_0>

Sur la transcendance de la série formelle Π

PAR JEAN-PAUL ALLOUCHE

Résumé : Nous donnons une preuve élémentaire de la transcendance de la série formelle Π, qui utilise le théorème de Christol, Kamae, Mendès France et Rauzy.

Abstract : We prove by elementary means that the formal series Π is transcendental, using the theorem of Christol, Kamae, Mendès France and Rauzy.

I. Introduction

A la réception d'un paquet de tirés à part d'une note aux Compte-Rendus, nous nous sommes aperçu que quelques exemplaires d'une autre note s'étaient glissés dans notre tas : cette deuxième note, due à Damamme et Hellegouarch [8], donne des résultats sur la fonction zéta de Carlitz. Notre attention, ayant été ainsi attirée, le fut une seconde fois par une faute d'impression dans une quantité notée Π, annoncée comme transcendante, et dont l'expression (erronée) était clairement algébrique, ([8]). Nous nous sommes donc lancé dans une quête bibliographique, puis avons obtenu des résultats que nous nous proposons de décrire ici.

Dans deux articles, parus en 1935 et en 1942 ([5] et [6]), Carlitz définit, sur le corps des séries formelles sur un corps fini, une fonction qui joue le rôle de l'exponentielle, son inverse qui joue celui du logarithme, et une fonction appelée depuis fonction zéta de Carlitz. Il introduit en particulier une quantité notée ξ_∞ (actuellement plutôt notée Π) qui joue le rôle de π=3,14159... Quelques années plus tard, Wade donne différentes propriétés de transcendance dont celle de cette série formelle Π, ([9], [10]).

Nous présentons ici une nouvelle démonstration de ce résultat, plus élémentaire et qui utilise le théorème de Christol, Kamae, Mendès France et Rauzy ([7]). En conclusion nous indiquerons nos espoirs d'obtenir, par des moyens élémentaires analogues, d'autres résultats de transcendance.

Ce texte est une version courte d'un article au titre identique accepté pour publication au Séminaire de Théorie des Nombres de Bordeaux (2ème série) [2], où on trouvera une bibliographie plus importante.

S.M.F.
Astérisque 198-199-200 (1991)

II. La série formelle Π

Dans ce qui suit $\mathbb{F}_q$ est le corps fini de cardinal $q = p^s$ (et de caractéristique p). On note $\mathcal{F} = \bigcup_{m\geq 1} \mathbb{F}_q((x^{-m}))$, et on utilise les notations traditionnelles :

$$[k] = x^{q^k} - x,$$

$$F_k = [k][k-1]^q[k-2]^{q^2}...[1]^{q^{k-1}},$$

$$L_k = [k][k-1]...[1],$$

$$F_0 = L_0 = 1.$$

On pose aussi :

$$\psi(t) = \sum_{j=0}^{+\infty} \frac{(-1)^j}{F_j} t^{q^j} \qquad (t \in \mathcal{F}),$$

$$\Pi = \xi_\infty = \prod_{j=1}^{+\infty} \left(1 - \frac{[j]}{[j+1]}\right) \qquad \text{[c'est un élément de } \mathbb{F}_q((x^{-1}))\text{]},$$

$$\xi = (x^q - x)^{1/q-1}\xi_\infty.$$

La fonction ψ est linéaire et joue un peu le rôle de l'exponentielle ; l'on a :

$$\forall t \in \mathcal{F} \qquad \forall E \in \mathbb{F}_q[x], \qquad \psi(t + \xi E) = \psi(t)$$

(autrement dit ξ joue le rôle de $\pi i = (3,14159...)i$).

Enfin, la fonction ζ (fonction zéta de Carlitz) est définie par :

$$\forall m \geq 1 \quad \zeta(m) = \sum_P{}' P^{-m},$$

où $\sum'$ signifie que la somme est prise sur l'ensemble des polynômes (dans $\mathbb{F}_q[x]$) de coefficient directeur égal à 1.

Notons que Carlitz a prouvé :

$$\text{si } (q-1)|m, \text{ alors } \zeta(m) = \xi^m r_m, \text{ avec } r_m \in \mathbb{F}_q[x],$$

et que Wade a prouvé (entre autres) la transcendance (sur $\mathbb{F}_q(x)$) de la série formelle Π.

III. Le théorème de Christol, Kamae, Mendès France et Rauzy

Ce théorème, donné dans [7] (voir [1] pour un survol d'applications en théorie des nombres), donne en particulier une équivalence entre la transcendance sur $\mathbb{F}_q(x)$ d'une série formelle et une propriété combinatoire de ses coefficients :

THEORÈME. *La série formelle* $\sum a(n)x^{-n}$, *à coefficients dans* $\mathbf{F}_q$, *est algébrique sur* $\mathbf{F}_q(x)$ *si et seulement si l'ensemble de sous-suites :*

$$\{n \to a(q^k n + r); \quad k \geq 0; \quad 0 \leq r \leq q^k - 1\}$$

est fini.

Remarque : cette propriété combinatoire équivaut à la reconnaissabilité par automate fini de la suite $(a(n))$, voir [7] par exemple.

IV. Preuve élémentaire de la transcendance de la série formelle Π

En utilisant le théorème de Christol, Kamae, Mendès France et Rauzy rappelé au paragraphe précédent, on peut donner une preuve élémentaire de la transcendance de $\Pi = \prod_{j=1}^{+\infty}(1 - \frac{[j]}{[j+1]})$, et nous proposons ci-dessous les étapes d'une telle preuve (les détails sont laissés au lecteur... ou peuvent être trouvés dans [2]).

1. Posons $\alpha = \prod_{j=0}^{+\infty}(1 - \frac{x^{q^j}}{x^{q^{j+1}}})$, alors α est algébrique sur $\mathbf{F}_q(x)$ et $\alpha/\Pi = \sum_{n=0}^{+\infty} a(n)x^{-n}$, où $a(n) = 0$ si n ne peut pas s'écrire $\sum_{j\in J}(q^j - 1)$ pour un ensemble fini d'indices J, et $a(n) = (-1)^{CardJ}$ si $n = \sum_{j\in J}(q^j - 1)$ (une telle écriture, si elle existe, est nécessairement unique).

2. Montrer que Π est transcendant, ou ce qui revient au même que α/Π est transcendant, équivaut à montrer que l'ensemble de suites $\{n \to a(q^k n + r); \quad k \geq 0, \quad 0 \leq r \leq q^k - 1\}$ est infini. Il suffit même de montrer que l'ensemble de suites

$$\mathcal{S} = \{n \to |a(q^k n + r)|; \quad k \geq 0, \quad 0 \leq r \leq q^k - 1\}$$

est infini.

3. Soit $b_k(n)$ la suite définie (pour $k \geq 2$), par

$$b_k(n) = |a(q^k n + q^k - k)|.$$

Alors, toujours pour $k \geq 2$, on a :

$$b_k(n) = \begin{cases} 0 \text{ si } 0 \leq n < \dfrac{q^k - 1}{q - 1} - 1 \\ 1 \text{ si } n = \dfrac{q^k - 1}{q - 1} - 1 \end{cases}$$

les suites $b_k(n)$ sont donc toutes distinctes, et l'ensemble $\mathcal{S}$ est infini.

V. Le cas $q = 2$ et la définition des entiers d'après von Neumann

Le cas $q = 2$ dans le paragraphe précédent montre un rapport inattendu entre la série formelle Π et la définition de von Neumann des entiers.

Soit en effet (A_n) la suite d'ensembles définie par :

$A_0 = \emptyset$

$A_1 = \{\emptyset\}$

$A_2 = \{\emptyset, \{\emptyset\}\}$

...

qui, on le sait, permet de définir les entiers ([4]) en appelant n le cardinal de A_n.

Écrivons ces ensembles A_n à l'aide des symboles { et } :

$A_0 = \{\}$

$A_1 = \{\{\}\}$

$A_2 = \{\{\}\{\}\}\}$

...

Alors la suite de "mots" (A_n) converge vers une suite infinie A, qui est point fixe de la substitution $\{ \to \{\{, \quad \} \to \}$, (voir [3]).

Le lecteur vérifiera que si l'on remplace dans la suite A les { par des 1 et les } par des 0, on obtient une suite $A' = u(0)u(1)u(2)... = 110...$, qui est telle que, si l'on écrit la série formelle α/Π dans le cas $q = 2$ (voir IV.1) :

$$\frac{\alpha}{\Pi} = \prod_{j=0}^{+\infty}\left(1 - \frac{1}{x^{2^j}}\right) \Big/ \prod_{j=1}^{+\infty}\left(1 - \frac{x^{2^j} - x}{x^{2^{j+1}} - x}\right) = \sum_{n=0}^{+\infty} a(n)x^{-n},$$

alors, $|a(n)| = u(n)$ quel que soit l'entier n.

VI. Espoirs

En utilisant une propriété de la fonction zéta de Carlitz donnée dans l'introduction et la transcendance de la série formelle Π, on obtient sans mal la transcendance de $\zeta(m)$ pour les entiers m divisibles par $q - 1$. Yu a démontré récemment (voir [11], [12], [13]), via l'étude des modules de Drinfeld, la transcendance de toutes les valeurs de la fonction zéta de Carlitz. Il serait donc très intéressant de donner une preuve élémentaire de ce résultat, via le théorème de Christol, Kamae, Mendès France et Rauzy. Nous n'avons pas encore une telle preuve, mais nous avons obtenu de cette façon d'autres résultats de transcendance, par exemple la transcendance sur $\mathbb{F}_q(x)$ de la "série des crochets" $\sum_{k=1}^{+\infty} [k]^{-1}$ démontrée pour la première fois par Wade ([9]).

Note ajoutée en septembre 1990 : G. Damamme a obtenu récemment une preuve élémentaire (mais qui n'utilise pas les automates finis) de la transcendance de toutes les valeurs de la fonction zéta de Carlitz (*Transcendance de la fonction zéta de Carlitz par la méthode de Wade*, Université de Caen, 1990).

BIBLIOGRAPHIE

[1] J.-P. ALLOUCHE *Automates finis et théorie des nombres*, Expo. Math. **5** (1987), 239–266.

[2] J.-P. ALLOUCHE *Sur la transcendance de la série formelle* Π, Sém. de Théorie des Nombres de Bordeaux **1,1** $2^{\text{ème}}$ **série** (1989), 163–187.

[3] J.-P. ALLOUCHE, J. BÉTRÉMA et J. SHALLIT *Sur des points fixes de morphismes d'un monoïde libre*, R.A.I.R.O., Informatique théorique et Applications **23,3** (1989), 235–249.

[4] N. BOURBAKI "Théorie des ensembles," chap. 3, Hermann, Paris, 1963, p. 39.

[5] L. CARLITZ *On certain functions connected with polynomials in a Galois field*, Duke Math. J., **1** (1935), 137–168.

[6] L. CARLITZ *Some topics in the arithmetic of polynomials*, Bull. Amer. Math. Soc. **48** (1942), 679–691.

[7] G. CHRISTOL, T. KAMAE, M. MENDÈS FRANCE et G. RAUZY *Suites algébriques, automates et substitutions*, Bull. Soc. Math. France **108** (1980), 401–419.

[8] G. DAMAMME et Y. HELLEGOUARCH *Propriétés de transcendance des valeurs de la fonction zéta de Carlitz*, C.R. Acad. Sci. Paris **307, Série I** (1988), 635–637.

[9] L.I. WADE *Certain quantities transcendental over* $GF(p^n, x)$, Duke Math. J., **8** (1941), 701–720.

[10] L.I. WADE *Certain quantities transcendental over* $GF(p^n, x)$, *II*, Duke Math. J., **10** (1943), 587–591.

[11] J. YU *Transcendence and Drinfeld modules*, Inv. Math. **83** (1986), 507-517.

[12] J. YU *Transcendence and Drinfeld modules, II*, Math. Res. Cent. Rep. (1986), 172–181, Symp. Taipei/Taiwan.

[13] J. YU . In Zbl. Math. 644.12005.

C.N.R.S. URA 0226 Mathématiques
Université Bordeaux I
351, cours de la Libération
33405 Talence Cedex
FRANCE
(Reçu le 31 octobre 1989)

Astérisque

A.-M. BERGÉ
J. MARTINET

Réseaux extrêmes pour un groupe d'automorphismes

Astérisque, tome 198-199-200 (1991), p. 41-66
<http://www.numdam.org/item?id=AST_1991__198-199-200__41_0>

RÉSEAUX EXTRÊMES POUR UN GROUPE D'AUTOMORPHISMES

par A-M. BERGÉ et J. MARTINET

1. Introduction. Soit V un espace vectoriel euclidien dont la dimension est notée n. Étant donné un réseau Λ de V, on note $\|\Lambda\| = \inf_{x\in\Lambda-\{0\}} \|x\|$ la norme du réseau, et $\Delta(\Lambda)$ son discriminant ($\Delta^2(\Lambda)$ est le déterminant de la matrice de Gram d'une base du réseau). On pose alors

$$\gamma_n(\Lambda) = \frac{\|\Lambda\|^2}{\Delta(\Lambda)^{\frac{2}{n}}}.$$

C'est un invariant de la classe de similitude de Λ. La *constante d'Hermite* pour la dimension n est

$$\gamma_n = \sup_{\Lambda} \gamma_n(\Lambda) \ ;$$

ses valeurs sont connues pour $n \leq 8$, et l'on dispose au-delà des majorations de Rogers.

Cette constante intervient dans de nombreuses inégalités utilisant la géométrie des nombres, par exemple dans les minorations à la Remak des régulateurs, ce qui a été le point de départ de cette étude (cf. [5], § 7 où est résumée une partie des résultats de cet article).

Soit maintenant G un sous-groupe fini du groupe orthogonal $O(V)$ de V. Si l'on se restreint aux réseaux Λ stables par G (les *G-réseaux*), on définit naturellement une "G-constante d'Hermite" $\gamma_{n,G}$. On peut alors améliorer la majoration classique chaque fois que les groupes d'automorphismes des *réseaux critiques* (i.e. qui réalisent γ_n) ne fournissent pas par restriction la représentation donnée de G. C'est ainsi que les minorations géométriques des régulateurs peuvent être améliorées pour certains types d'extensions galoisiennes.

Dans cet article, nous nous intéressons à la détermination des *maxima locaux* de $\gamma_n(\Lambda)$ sur les G-réseaux pour un groupe G donné (plus généralement, il est utile de se donner plutôt une représentation de G dans $O(V)$) ; les maxima globaux s'en déduisent : c'est le principe qui a été utilisé par Korkine et Zolotareff en 1877 pour calculer γ_5. Par analogie avec la situation classique, on introduit la notion de *réseau G-extrême*, qui se réduit à la notion habituelle de *réseau extrême* lorsque G est réduit à $\{\mathrm{Id}\}$ ou à $\{\pm\mathrm{Id}\}$, et, comme dans

le cas classique traité par Voronoï, on caractérise les réseaux G-extrêmes comme étant G-parfaits et eutactiques. C'est l'objet du § 2, où nous nous inspirons de la méthode qui a permis à Barnes de simplifier considérablement la démonstration de Voronoï.

Des résultats du § 2, on déduit dans le § 3 une minoration du nombre d'orbites de vecteurs minimaux sous l'action de G pour tout réseau G-parfait. C'est cette minoration qui est à la base de la détermination des réseaux G-parfaits (et donc des réseaux G-extrêmes) pour certaines représentations $G \to O(V)$ examinées au cours des §§ 4 et 5 : groupes cycliques irréductibles lorsque $\dim V = 4$ ou 6, puis, pour $\ell = 3$ ou 5, groupes cycliques d'ordre $\ell = \dim V$. En particulier, dans le cas d'un groupe cyclique irréductible d'ordre 5 ou 7, nous obtenons une majoration non triviale de la constante d'Hermite des G-réseaux, retrouvant dans le cas de l'ordre 5 un résultat obtenu par Schoof et Washington ([14]) à l'aide d'un calcul d'extremum. Un court § 6 est consacré à l'énoncé de quelques résultats obtenus postérieurement à l'exposé.

Il est à noter que, en établissant la liste des réseaux G-extrêmes dans les cas couverts par le § 4,nous retrouvons 4 des 5 constructions "cyclotomiques" trouvées par Craig ([10]) pour des réseaux extrêmes de dimension 6. L'idée d'utiliser des groupes d'automorphismes donnés *a priori* intervient également dans un travail d'Eva Bayer ([3]) dans lequel l'auteur s'intéresse à des formes quadratiques entières unimodulaires possédant un automorphisme de polynôme caractéristique donné.

2. Caractérisation des réseaux G-extrêmes . Dans tout ce §, on adoptera les notations suivantes : V désigne un espace *euclidien* de dimension $n > 0$, $\mathrm{Gl}(V)$ et $\mathrm{O}(V)$ ses groupes *linéaire* et *orthogonal*, $\mathcal{S}(V) = \mathcal{S}$ (resp. $\mathcal{S}^+(V) = \mathcal{S}^+$) l'ensemble des endomorphismes symétriques (resp. symétriques et à valeurs propres ≥ 0) de V. Rappelons que dans $\mathcal{S}^+$ tout élément a une unique racine carrée, d'où l'on déduit :

2.1 LEMME. *(i) Tout $u \in Gl(V)$ s'écrit de façon unique $u = sf$, avec $s \in \mathcal{S}^+$ et $f \in O(V)$.*

(ii) Soient $s \in \mathcal{S}^+$ et $g \in O(V)$. Alors on a l'équivalence : $s^{-1}gs \in O(V) \Leftrightarrow sg = gs$.

Démonstration. (i) : on prend pour s la racine carrée positive de ${}^t uu \in \mathcal{S}^+$. (ii) : on a les équivalences $s^{-1}gs \in \mathrm{O}(V) \Leftrightarrow {}^t(s^{-1}gs) = (s^{-1}gs)^{-1} \Leftrightarrow sg^{-1}s^{-1} = s^{-1}g^{-1}s \Leftrightarrow s^2 = (g^{-1}sg)^2 \Leftrightarrow s = g^{-1}sg$.

On note $\mathcal{R}$ l'ensemble des *réseaux de V*. Il est muni d'une *topologie naturelle* que l'on peut décrire ainsi : les sous-ensembles $\mathcal{V}'$ de $\mathcal{R}$ de la forme $\mathcal{V}\Lambda$ $(=\{s\Lambda, s \in \mathcal{V}\})$ où $\mathcal{V}$ est un voisinage de l'identité dans $\mathrm{Gl}(V)$ constituent un système fondamental de voisinages d'un réseau Λ. Alors, l'application $s \mapsto s\Lambda$

de $\mathcal{V}$ dans $\mathcal{V}'$ ci-dessus est bijective si on se limite à des voisinages de l'identité assez petits, puisque le *stabilisateur* $\mathrm{Gl}(\Lambda)$ *de* Λ *dans* $\mathrm{Gl}(V)$ est discret. (La condition "assez petit" dépend du réseau Λ.) L'ensemble des *classes d'isométrie* de réseaux est également muni d'une topologie naturelle, à savoir la topologie quotient de $\mathcal{R}$ par l'action du groupe orthogonal.

Soit Λ un réseau de V ; son groupe d'automorphismes $\mathrm{Aut}(\Lambda) = \{u \in \mathrm{O}(V) \mid u\Lambda \subset \Lambda\}$ est un sous-groupe compact donc fini de $\mathrm{Gl}(\Lambda)$, dont l'espace vectoriel $W = \mathbb{Q}\Lambda$ est une représentation rationnelle. Inversement, soit G un groupe fini tel que V provienne d'une représentation W de G dans $\mathrm{O}(V)$ rationnelle sur $\mathbb{Q}$. Le sous-ensemble $\mathcal{R}_G$ de $\mathcal{R}$ formé des réseaux stables par G ("*G-réseaux*") n'est pas vide. (Si $e_1, e_2, ..., e_n$ est une $\mathbb{Q}$-base de W, le sous-groupe Λ de W engendré par les $s(e_i), s \in G, i = 1, 2, ..., n$ est un réseau de $\mathcal{R}_G$.) *Nous supposons désormais que les couples (V, G) vérifient les hypothèses ci-dessus.* Notons que l'on peut se ramener facilement au cas où la représentation W est fidèle, ce qui revient à supposer que G est un sous-groupe de $\mathrm{O}(V)$.

On munit $\mathcal{R}_G$ de la topologie induite par celle de $\mathcal{R}$. Soit $\Lambda \in \mathcal{R}_G$ et soit $\mathcal{V}'$ un voisinage de Λ dans $\mathcal{R}$ provenant d'un voisinage $\mathcal{V}$ de Id dans $\mathrm{Gl}(V)$. Si $\mathcal{V}$ est assez petit, les éléments u de $\mathcal{V}$ qui s'appliquent sur $\mathcal{V}' \cap \mathcal{R}_G$ par la bijection $u \mapsto u\Lambda$ sont ceux qui commutent avec G (puisque, pour tout $g \in G$, ils doivent vérifier $gug^{-1}\Lambda = u\Lambda$). D'après 2.1., la composante symétrique $s \in \mathcal{S}^+$ d'un tel u doit aussi commuter avec G. Notons $\mathcal{S}_G$ (resp. $\mathcal{S}_G^+$) le *commutant de G dans $\mathcal{S}$* (resp. *dans $\mathcal{S}^+$*). Les images canoniques des ensembles $\{s\Lambda \mid s \in \mathcal{V} \cap \mathcal{S}_G^+\}$ forment, quand $\mathcal{V}$ décrit l'ensemble des voisinages de Id dans $\mathrm{Gl}(V)$, un système fondamental de voisinages de la classe d'isométrie de Λ.

2.2 DÉFINITION. Un G-réseau est dit *G-extrême* (resp. *G-critique*) s'il réalise un maximum local (resp. absolu) de la fonction γ_n dans $\mathcal{R}_G$.

Notons que cette notion ne dépend que de la classe de similitude du réseau.

Rappelons quelques notions et notations relatives à la *méthode de Korkine et Zolotareff* (cf. [11], [1] et [4]) ; on note $S(\Lambda)$, ou simplement S, l'ensemble des *vecteurs minimaux* de Λ.

Pour $x \neq 0$, on note φ_x la forme linéaire $u \mapsto x.u(x)$ sur $\mathcal{S}$ et p_x la projection orthogonale de V sur la droite $\mathbb{R}x$. Un réseau de V est dit *parfait* si le dual $\mathcal{S}^*$ de $\mathcal{S}$ est engendré par les formes φ_x, $x \in S$, et *eutactique* si l'endomorphisme Trace est combinaison linéaire à coefficients *strictement* positifs des φ_x, $x \in S$.

En termes de projections, "parfait" signifie que les $(p_x)_{x \in S}$ engendrent $\mathcal{S}$, et "eutactique" que l'identité est combinaison linéaire à coefficients > 0 des p_x (la traduction se fait par dualité par rapport à la forme quadratique définie positive $u \mapsto \mathrm{Tr}(u^2)$ sur $\mathcal{S}$, cf. [4], rem. 3.12).

2.3 DÉFINITION. On dit qu'un G-réseau est *G-parfait* si le dual $\mathcal{S}_G^*$ de $\mathcal{S}_G$ est engendré par les restrictions à $\mathcal{S}_G$ des formes linéaires φ_x, $x \in S$, et qu'il est *G-eutactique* si la restriction à $\mathcal{S}_G$ de la forme linéaire Trace est combinaison linéaire à coefficients positifs des restrictions à $\mathcal{S}_G$ des φ_x.

Notons que ces notions ne font intervenir que l'ensemble S des vecteurs minimaux du G-réseau. Le groupe G opère sur cet ensemble, et les restrictions à $\mathcal{S}_G$ des formes linéaires φ_x, $x \in S$ sont constantes sur les orbites de S sous G : on a en effet, pour tous $x \in S$, $g \in G$ et $u \in \mathcal{S}$, $\varphi_{gx}(u) = \varphi_x(g^{-1}ug)$. On en déduit immédiatement :

2.4 PROPOSITION. *Le nombre d'orbites sous G de couples $\{\pm x\}$ de vecteurs minimaux d'un réseau G-parfait est au moins égal à la dimension de l'espace $\mathcal{S}_G$ des endomorphismes symétriques de V commutant avec G.*

(Quitte à grossir G en le remplaçant par $G \cup -G$, on pourrait supposer que deux vecteurs opposés sont toujours dans une même orbite.)

Remarquons que la G- perfection peut s'écrire ainsi : le système

$$\forall x \in S, \qquad \varphi_x(u) = 0$$

n'a pas de solution non triviale $u \in \mathcal{S}_G$. Cela permet d'obtenir pour les G-réseaux parfaits une caractérisation par *rigidité* analogue au mystérieux

"Toute forme extrême a au moins $\frac{n(n+1)}{2}$ représentations de son minimum qui déterminent complètement cette forme, en supposant que son minimum soit donné"
de Korkine et Zolotareff (Math. Annalen 11 (1877), p. 252) :

2.5 PROPOSITION. *Tout réseau G-parfait a au moins* $\dim \mathcal{S}_G$ *orbites de couples $\{\pm x\}$ de vecteurs minimaux, dont la configuration par rapport au réseau le détermine complètement à isométrie près. En particulier, $\gamma_{n,G}^n \in \mathbb{Q}$.*

[Précisons le sens que nous donnons dans le cas des G-réseaux au mot configuration : étant donnés deux réseaux Λ et Λ' *munis de bases $\mathcal{B}$ et $\mathcal{B}'$*, on dit que leurs ensembles S et S' de vecteurs minimaux ont *mêmes configurations par rapport à ces bases* s'il existe une bijection de $S(\Lambda)$ sur $S(\Lambda')$ *respectant les orbites sous G* telle que la matrice de S dans $\mathcal{B}$ ait pour image la matrice de S' dans $\mathcal{B}'$.]

Comme dans le cas classique, cette propriété d'unicité assure réciproquement la G-perfection. Comme la perfection (et du reste également l'eutaxie) ne dépend que du sous-réseau engendré par les vecteurs minimaux, on en déduit :

2.6 PROPOSITION. *Pour qu'un G-réseau Λ soit G-parfait, il faut et il suffit qu'une matrice de Gram d'une base de Λ soit déterminée de façon unique par les composantes dans cette base des vecteurs minimaux de Λ.*

Nous reviendrons sur cette question d'unicité au paragraphe suivant (prop. 3.12).

Remarquons que si H est un sous-groupe de G, tout réseau H-parfait (resp. H-eutactique, resp. H-extrême) est G-parfait (resp. G-eutactique, G-extrême), et que pour $G = \{\mathrm{Id}\}$ ou $\{\pm\mathrm{Id}\}$, on retrouve les notions usuelles. En fait, pour un G-réseau, les notions de G-eutaxie et d'eutaxie sont équivalentes :

2.7 LEMME. *Pour qu'un G-réseau soit G-eutactique, il faut et il suffit qu'il soit eutactique.*

Démonstration. Que la condition soit suffisante résulte des remarques ci-dessus. Pour la réciproque, on observe qu'à tout $u \in \mathcal{S}$ on peut associer de façon naturelle un endomorphisme symétrique u_G commutant avec G : on pose

$$u_G = \frac{1}{\operatorname{card} G} \sum_{g \in G} gug^{-1}.$$

On a alors $\mathrm{Tr}(u_G) = \mathrm{Tr}(u)$, et $\varphi_x(u_G) = \frac{1}{\operatorname{card} G} \sum_{g \in G} \varphi_x(u)$, d'où l'équivalence

$$\mathrm{Tr}(u_G) = \sum_{x \in S} \rho_x \varphi_x(u_G) \Leftrightarrow \mathrm{Tr}(u_G) = \sum_{x \in S} \alpha_x \varphi_x(u)$$

avec $\alpha_x = \frac{1}{\operatorname{Card} G} \sum_{g \in G} \rho_{gx}$. On en déduit immédiatement 2.4.

Par dualité, la G-perfection peut être caractérisée ainsi :

2.8 PROPOSITION. *Un G-réseau est G-parfait si et seulement si les endomorphismes $p_{x,G} = \frac{1}{\operatorname{card} G} \sum_{g \in G} gp_x g^{-1} = \frac{1}{\operatorname{card} G} \sum_{g \in G} p_{gx}$ engendrent $\mathcal{S}_G$.*

Comme conséquence immédiate des définitions, on obtient le résultat important suivant :

2.9 PROPOSITION. *Les vecteurs minimaux d'un réseau G-parfait ou G-eutactique engendrent l'espace vectoriel V.*

Démonstration. Soit V' le sous-espace de V orthogonal à tous les vecteurs minimaux du réseau. Il est stable par G, donc la projection orthogonale u de V sur V' appartient à $\mathcal{S}_G$, et l'on a $\varphi_x(u) = 0$ pour tout $x \in S$, d'où, si le réseau est G-parfait (resp. eutactique), u=0 (resp. $\mathrm{Tr}(u)$=0), donc $V' = \{0\}$.

Les notions introduites ci-dessus permettent une caractérisation des réseaux G-extrêmes analogue à celle obtenue par Voronoï et dont la démonstration que nous donnons est inspirée par la démonstration très simple donnée par Barnes ([1]) dans le cas classique :

2.10 THÉORÈME. *Pour qu'un G-réseau soit G-extrême, il faut et il suffit qu'il soit G-parfait et eutactique.*

On démontre d'abord le lemme suivant :

2.11 LEMME. *Soit Λ un G-réseau.*
1. Les conditions suivantes sont équivalentes :
(i) Λ est G-extrême ;
(ii) dans $\mathcal{S}_G$, le système d'inégalités

$$(1) \qquad \begin{cases} x.u(x) \geq 0 \text{ pour tout } x \in S(\Lambda) \\ Tru \leq 0 \end{cases}$$

n'a pas d'autre solution que $u = 0$.
2. Si Λ est G-extrême, on a $\gamma_n(\Lambda') < \gamma_n(\Lambda)$ pour tout G-réseau Λ' suffisamment voisin de Λ et non semblable à Λ.

Démonstration du lemme. Soit Λ' un G-réseau voisin de Λ et non semblable à Λ ; il peut s'écrire

$$\Lambda' = v\Lambda, \quad \text{avec } v = \mathrm{Id} + \epsilon u,\ \epsilon > 0, u \neq 0 \in \mathcal{S}_G.$$

Il s'agit de comparer les constantes d'Hermite donc les normes et les discriminants de Λ et $v\Lambda$. On suppose ϵ assez petit pour que les vecteurs minimaux de $v\Lambda$ proviennent de ceux de Λ. Soit $x \in V$; avec les notations ci-dessus, la relation

$$\|v(x)\|^2 - \|x\|^2 = 2\epsilon x.u(x) + \epsilon^2 \|u(x)\|^2 \qquad (x \in V)$$

montre l'équivalence

$$\|v(x)\|^2 \geq \|x\|^2 \iff x.u(x) \geq 0\,,$$

d'où aussi

$$(2) \qquad \|v\Lambda\| \geq \|\Lambda\| \Longleftrightarrow \forall x \in S(\Lambda),\ \varphi_x(u) \geq 0.$$

Notons $X^n - T_1(u)X^{n-1} + T_2(u)X^{n-2} + \ldots + (-1)^n T_n(u) = \prod_i (X - \lambda_i)$ le polynôme caractéristique de u, où T_1 est la forme linéaire Trace, et où $T_2(u) = \frac{1}{2}(T_1(u)^2 - \sum \lambda_i^2)$ est $< \frac{1}{2}T_1(u)^2$. Le développement

$$\frac{\Delta(v\Lambda)}{\Delta(\Lambda)} - 1 = \epsilon T_1(u) + \epsilon^2 T_2(u) + \ldots$$

fournit les implications (pour $u \neq 0 \in \mathcal{S}$)

$$\begin{aligned} T_1(u) > 0 &\Rightarrow \Delta(v\Lambda) > \Delta(\Lambda) \\ T_1(u) \leq 0 &\Rightarrow \Delta(v\Lambda) < \Delta(\Lambda). \end{aligned} \tag{3}$$

Supposons alors que Λ ne vérifie pas la conditon (ii) du lemme, et soit $u \in \mathcal{S}_G$ une solution non triviale de (1). Le réseau $v\Lambda$ correspondant vérifie $\|v\Lambda\| \geq \|\Lambda\|$ d'après (2) et $\Delta(v\Lambda) < \Delta(\Lambda)$ d'après (3), d'où $\gamma_n(v\Lambda) > \gamma_n(\Lambda)$: le réseau Λ n'est pas G-extrême. Réciproquement, supposons (ii) vérifiée par Λ et soit Λ' un G-réseau voisin de Λ, non semblable à Λ, que l'on peut supposer de même norme que Λ (quitte à le remplacer par un réseau homothétique). L'endomorphisme non nul $u \in \mathcal{S}_G$ correspondant à Λ' vérifie alors les inégalités $\varphi_x(u) \geq 0$ pour tout $x \in S$ d'après (2) ; comme il ne peut vérifier (1) (condition (ii)), on a $\mathrm{Tr}u > 0$ d'où, par (3), $\Delta(\Lambda') > \Delta(\Lambda)$ et $\gamma_n(\Lambda') < \gamma_n(\Lambda)$, ce qui prouve que Λ est G-extrême et démontre aussi 2.

La caractérisation des réseaux G-extrêmes à l'aide de la condition (ii) du lemme 2.11 repose sur un théorème de Stiemke très utile en programmation linéaire et que Barnes ([1]) a eu l'idée d'exhumer pour l'étude de la situation classique :

2.12 LEMME (STIEMKE, 1915). *Soit E un espace vectoriel réel de dimension finie et soient $\varphi_1, ..., \varphi_p$ des formes linéaires sur E. Les conditions suivantes sont équivalentes :*
(i) Il existe des nombres réels $\rho_1, ..., \rho_p$ positifs tels que $\rho_1\varphi_1 + ... + \rho_p\varphi_p = 0$;
(ii) Toute solution $v \in E$ au système d'inéquations $\varphi_j(v) \geq 0$, $j = 1, ..., p$ vérifie les égalités $\varphi_j(v) = 0$ pour $j = 1, ..., p$.

Démonstration du théorème. On applique 2.11 aux formes linéaires φ_x, $x \in S$ et $-\mathrm{Tr}$ sur $E = \mathcal{S}_G$, de sorte que la condition (i) du lemme exprime l'eutaxie du G-réseau.

Notons, pour $u \in \mathcal{S}_G$, (1) la condition "$\forall x \in S$, $\varphi_x(u) \geq 0$ et $-\mathrm{Tr}u \geq 0$", et (2) la condition "$\forall x \in S$, $\varphi_x(u) = 0$".

Par 2.11, "Λ G-extrême " équivaut à "(1) implique $u = 0$ ". Par définition, "Λ G-parfait " équivaut à "(2) implique $u = 0$ ". Par 2.11., "Λ eutactique " équivaut à "(1) implique (2) et $-\mathrm{Tr}u \geq 0$".

Supposons le réseau G-extrême, et soit $u \in \mathcal{S}_G$ vérifiant (2); u ou $-u$ vérifie (1), donc est nul. Si $u \in \mathcal{S}_G$ vérifie (1), il est nul, donc vérifie (2) et $-\mathrm{Tr}u \geq 0$.

Réciproquement, supposons Λ G-parfait et eutactique, et soit $u \in \mathcal{S}_G$ vérifiant (1) ; il vérifie aussi (2), donc $u = 0$, **c.q.f.d.**

3. Calculs de dimensions. Dans ce §, nous déterminons la dimension de l'espace vectoriel $\mathcal{S}_G$ des endomorphismes symétriques de V qui commutent

avec G. Nous donnons en outre la structure des G-réseaux extrêmes qui sont sommes directes orthogonales de sous-réseaux stables. Nous conservons les notations du § 2.

Soit $V = V_1 \perp V_2 \perp \ldots \perp V_r$ une décomposition de V en somme directe orthogonale de sous-espaces stables par G. Pour tout i, soit p_i la projection orthogonale de V sur V_i. Soit $u \in \mathrm{End}(V)$. Il se décompose de manière unique en somme $\sum u_{ij}$ où $u_{ij} \in \mathrm{End}(V)$ est nul sur les V_k pour $k \neq i$ et a une image contenue dans V_j : on a en fait $u_{ij} = p_j \circ u \circ p_i$. On identifiera souvent $u_{ij} \in \mathrm{End}(V)$ avec l'homomorphisme de V_i dans V_j qu'il définit. Pour tout couple (i, j), on a ${}^t(u_{ij}) = ({}^t u)_{ji}$, et, en particulier, u est symétrique si et seulement si les u_{ij} vérifient les relations ${}^t u_{ij} = u_{ji}$. De même, u commute avec G si et seulement tous les u_{ij} commutent avec G. Par ailleurs, pour tout $x \in V_i$, $\varphi_x(u_{jk})$ est nul sauf peut-être si $i = j = k$ (cf. § 2 après 2.2 pour la définition de φ_x). En particulier :

3.1 PROPOSITION. *Soit i, $1 \leq i \leq r$, soit $x \in V_i$ et soit $u = \sum_{jk} u_{jk} \in End(V)$. Alors, $\varphi_x(u) = \varphi_x(u_{ii})$.*

Pour tout caractère $\mathbb{R}$-irréductible χ de G, et pour tout sous-espace stable V' de V, notons V'_χ la somme des sous-espaces de V' de caractère χ. L'espace V' est somme directe orthogonale de ses sous-espaces stables V'_χ. En particulier, on a $V = \perp_\chi V_\chi$. Comme $\mathrm{Hom}_{\mathbb{R}[G]}(V_\chi, V_{\chi'})$ est réduit à zéro pour $\chi \neq \chi'$, on a

$$\mathcal{S}_G(V) = \oplus_\chi \mathcal{S}_G(V_\chi)\,, \tag{3.2}$$

d'où en particulier

$$\dim_{\mathbb{R}} \mathcal{S}_G(V) = \sum_\chi \dim_{\mathbb{R}} \mathcal{S}_G(V_\chi)\,.$$

Rappelons (cf. [12], § 13.2, pp. 122-123) qu'*un caractère $\mathbb{R}$-irréductible* (i.e. le caractère d'une représentation irréductible de G sur $\mathbb{R}$) χ est de l'un des trois types suivants : (I) χ est un caractère "réel", i.e. le caractère d'une représentation $\mathbb{C}$-irréductible de G réalisable sur $\mathbb{R}$; (II) $\chi = \varphi + \bar{\varphi}$, où φ est un caractère $\mathbb{C}$-irréductible qui prend au moins une valeur non réelle ; (III) $\chi = 2\varphi$ où φ est à valeurs réelles, mais n'est pas le caractère d'une représentation réalisable sur $\mathbb{R}$. Les commutants de ces trois types de caractères sont isomorphes respectivement à $\mathbb{R}$, $\mathbb{C}$ et $\mathbb{H}$ ($\mathbb{H}$ désigne le corps des quaternions de Hamilton). Notons maintenant a_χ le nombre de fois que le caractère de V_χ contient χ, $K_\chi = K$ le commutant de χ, et soit $b_\chi = [K_\chi : \mathbb{R}]$ (donc, $b_\chi = 1$, 2 ou 4).

3.3 PROPOSITION. *On a :*

$$\dim_{\mathbb{R}} \mathcal{S}_G(V_\chi) = \begin{cases} \dfrac{a_\chi(a_\chi+1)}{2} & \text{si } K = \mathbb{R} ; \\ a_\chi^2 & \text{si } K = \mathbb{C} ; \\ a_\chi(2a_\chi-1) & \text{si } K = \mathbb{H} . \end{cases}$$

Démonstration. Écrivons V_χ sous la forme d'une somme directe de sous-espaces irréductibles stables W_i, $1 \leq i \leq a_\chi$, chacun des W_i étant isomorphe à un même espace W irréductible sur $\mathbb{R}$. Alors, $\mathrm{End}_{\mathbb{R}[G]}(V_\chi)$ est isomorphe à $\mathcal{M}_{a_\chi}(\mathrm{End}_{\mathbb{R}[G]}(W)) = \mathcal{M}_{a_\chi}(K)$, et son sous-espace $\mathrm{End}^s(V_\chi)$ formé des endomorphismes symétriques s'identifie au sous-espace de $\mathcal{M}_{a_\chi}(\mathrm{End}_{\mathbb{R}[G]}(W))$ dont les éléments diagonaux sont symétriques, c'est-à-dire réels, et tels que deux éléments symétriques par rapport à la diagonale soient transposés l'un de l'autre. (Dans l'identification à une algèbre de matrices $\mathcal{M}_m(K)$ du facteur simple associé à une représentation irréductible, la transposée d'une matrice P est ${}^t\bar{P}$, où $\bar{}$ désigne la conjugaison dans K.) On a donc $\dim_{\mathbb{R}} \mathcal{S}_G(V_\chi) = a_\chi + b_\chi \frac{a_\chi(a_\chi-1)}{2}$, ce qui est bien la formule de la prop. 3.3. Revenons maintenant à des décompositions orthogonales plus générales que la décomposition canonique.

3.4 PROPOSITION. *Soit $V = V_1 \perp V_2 \perp \ldots \perp V_r$ une décomposition de V en somme directe orthogonale de sous-espaces stables par G. Alors, $\mathcal{S}_G(V)$ contient la somme des $\mathcal{S}_G(V_i)$, et l'égalité a lieu si et seulement si les V_i sont sans composantes irréductibles communes.*

Démonstration. L'inclusion $\mathcal{S}_G(V) \supset \oplus \mathcal{S}_G(V_i)$ est évidente. Si les V_i sont sans composantes irréductibles communes, alors, pour tout χ, V_χ est égal à l'un des $V_{i,\chi}$, et l'inclusion est une égalité par 3.2. Dans le cas contraire, il existe un couple (i,j) pour lequel $\mathrm{Hom}_{\mathbb{R}[G]}(V_i, V_j)$ contient un élément $v \neq 0$. Alors, l'élément $u \in \mathrm{End}_{\mathbb{R}[G]}(V)$ défini par $u_{ij} = v$, $u_{ji} = {}^t v$ et $u_{kl} = 0$ pour $\{k,l\} \neq \{i,j\}$ appartient à $\mathcal{S}_G(V)$ mais pas à $\oplus \mathcal{S}_G(V_k)$.

Nous appliquons maintenant ce qui précède à l'étude des G-réseaux décomposables.

3.5 PROPOSITION. *Soit Λ un réseau, somme directe orthogonale de réseaux relatifs $\Lambda_1, , \Lambda_2, \ldots, \Lambda_r$. Alors :*

(i) *$S(\Lambda)$ est égal à la réunion des $S(\Lambda_i)$ pour les i tels que $\|\Lambda_i\|$ soit minimal.*

(ii) *Λ est eutactique si et seulement si les réseaux Λ_i sont eutactiques et ont même norme.*

Démonstration. L'assertion (i) est évidente, et elle entraîne que l'endomorphisme identité de V, qui est somme des projections p_{V_i} sur les V_i, ne peut s'écrire comme combinaison des p_x, $x \in S(\Lambda)$ que si $S(\Lambda)$ contient tous les $S(\Lambda_i)$, ce qui donne la condition d'égalité des normes dans l'assertion (ii). Lorsque cette condition est satisfaite, comme la restriction de p_{V_i} à V_i est l'identité de V_i pour tout i, il est clair que Λ est eutactique si et seulement si tous les Λ_i le sont.

3.6 THÉORÈME. *Soit Λ un G-réseau, somme directe orthogonale de G-réseaux relatifs $\Lambda_1, \Lambda_2, ..., \Lambda_r$. Pour que le réseau Λ soit G-parfait (resp. G-extrême), il faut et il suffit que les trois conditions suivantes soient satisfaites :*

(i) *Les réseaux Λ_i ont même norme ;*
(ii) *Les réseaux Λ_i sont G-parfaits (resp. G-extrêmes) ;*
(iii) *Les restrictions aux sous-espaces V_i de la représentation définie par V sont sans composantes irréductibles communes.*

Démonstration. Étudions d'abord la perfection du réseau Λ. Un argument analogue à celui qui a été utilisé pour démontrer 3.5 montre tout de suite que les conditions (i) et (ii) sont vérifiées lorsque Λ est G-parfait. Lorsqu'elles sont vérifiées, on a, quel que soit $x \in S$ et $u_{ij} \in \mathrm{Hom}_{\mathbf{R}[G]}(V_i, V_j)$ avec $i \neq j$, $\varphi_x(u_{ij}) = 0$ (cf. 3.1 et 3.5, (i)). La proposition 3.4 montre que le sous-espace de $\mathrm{End}(V)^*$ engendré par les φ_x, $x \in S(\Lambda)$ est somme directe de ses sous-espaces engendrés par les φ_x , $x \in S(\Lambda_i)$ si et seulement si la condition (iii) est satisfaite.

Comme Λ est G-extrême si et seulement s'il est G-parfait et eutactique (th. 2.10), l'assertion relative au caractère extrémal de Λ est une conséquence immédiate de la prop. 3.5.

Le cas où V est $\mathbf{R}$-irréductible est particulièrement simple : en effet, il résulte de la proposition 3.3 que $\mathcal{S}_G(V)$ est alors de dimension 1 sur $\mathbf{R}$ (et la réciproque est du reste exacte). La description de la topologie de $\mathcal{R}_G$ faite au début du § 2 montre alors tout de suite le résultat suivant :

3.7 PROPOSITION. *Lorsque V est $\mathbf{R}$-irréductible, tous les G-réseaux de V sont G-extrêmes.*

C'est en particulier le cas en dimension 2 pour le réseau hexagonal lorsque G est cyclique d'ordre 3 ou 6 et pour le réseau carré lorsque G est cyclique d'ordre 4 ; de façon générale, cela se produit chaque fois que le groupe G est "gros" relativement à la dimension de V.

La proposition 2.4 se réduit dans le cas classique où $G = \{\mathrm{Id}\}$ à l'inégalité $s \geq n(n+1)/2$ de Korkine et Zolotareff que doit vérifier le nombre s de couples $\{\pm x\}$ de vecteurs minimaux de tout réseau parfait. C'est cette inégalité qui

est à la base de leur détermination des réseaux parfaits de dimension ≤ 5. Une analyse de leurs démonstrations montre qu'ils ont en fait prouvé le résultat plus fort suivant :

3.8 THÉORÈME (KORKINE ET ZOLOTAREFF, 1877). *Un réseau parfait de dimension $n \leq 5$ est extrême, et est semblable à l'un des réseaux A_1, A_2, A_3, D_4, A_4, D_5, A_5^3 ou A_5. En outre, pour $n \leq 4$, l'inégalité $s \geq n(n+1)/2$ assure la perfection.*

Rappelons brièvement les notations (cf. [6]).

Pour tout $n \geq 1$, A_n désigne la section du réseau cubique $\mathbb{Z}^{n+1} \subset \mathbb{R}^{n+1}$ par l'hyperplan orthogonal au vecteur $(1, 1, ..., 1)$. C'est un réseau extrême ; on a $\|A_n\|^2 = 2$, $s(A_n) = n(n+1)/2$ et $\Delta^2(A_n) = n+1$. Il possède une base $e_1, ..., e_n$ de vecteurs minimaux pour laquelle on a $e_i.e_j = 1$ pour $j \neq i$. Son dual A_n^*, pour lequel $s = n+1$, n'est pas parfait lorsque n est ≥ 3. L'opération de $\mathrm{Aut}(A_n) = \mathrm{Aut}(A_n^*)$ sur $S(A_n^*)$ permet d'identifier ce groupe à $\{\pm\mathrm{Id}\} \times S_{n+1}$. En particulier, pour ℓ premier, A_ℓ possède un automorphisme de polynôme caractéristique $X^\ell - 1$, et $A_{\ell-1}$ possède un automorphisme $\mathbb{Q}$-irréductible d'ordre ℓ.

Le réseau A_n^t (notation de Coxeter) est défini pour $1 \leq t \leq n+1$, $t|(n+1)$, en ajoutant à la base précédente de A_n le vecteur $\frac{e}{t}$ où $e = e_1 + ... + e_n$. Il est stable par $\mathrm{Aut}(A_n)$. Son dual est semblable à $A_n^{t'}$ où $tt' = n+1$. (Le réseau A_n^t est noté $A_n[t']$ dans [6], ch. 4, § 6.6, et A_n^{+t} dans [7], § 5.)

Pour tout $n \geq 4$, D_n désigne le sous-réseau de $\mathbb{Z}^n$ formé des points dont la somme des coordonnées est paire. C'est un réseau extrême ; on a $\|D_n\|^2 = 2$, $s = n(n-1)$, et $\Delta^2(D_n) = 4$. Le dual de D_n est un réseau cubique centré. Pour $n \geq 5$, il n'est pas parfait, car $s(D_n^*) = n$, et l'opération de $\mathrm{Aut}(D_n)$ sur D_n^* identifie ce groupe à $\{\pm\mathrm{Id}\}^n \times S_n$. Pour $n = 4$, D_4 et D_4^* sont semblables, et leur groupe d'automorphismes est une extension du groupe précédent par un groupe d'ordre 3. En particulier, si ℓ est premier, $\mathrm{Aut}(D_\ell)$ contient un automorphisme de polynôme caractéristique $X^\ell - 1$, et D_4 possède des automorphismes irréductibles d'ordre 8 et 12.

La détermination des réseaux parfaits de dimension 6 a été effectuée par Barnes ([2]) en 1957, qui a prouvé qu'il existe à similitude près exactement 7 réseaux parfaits, dont 6 extrêmes. La démonstration de Barnes utilise l'algorithme de Voronoï, et ne permet pas de prouver la perfection des réseaux ayant suffisamment de vecteurs minimaux. Du reste, l'énoncé analogue à 3.8 est faux en dimension $n \geq 6$, comme le montre l'exemple de la somme othogonale $D_{n-1} \perp A_1$, qui est un réseau non parfait possédant $(n-1)(n-2)+1 \geq n(n+1)/2$ vecteurs minimaux. (En dimension 5, l'énoncé est correct à condition de se limiter aux réseaux ne possédant pas de section hyperplane isométrique à D_4.)

Nous décrivons maintenant ceux de ces réseaux que nous aurons à utiliser dans la suite. Deux d'entre eux, dont le réseau non extrême, ont un groupe d'automorphismes réductible. Les 5 autres sont A_6, D_6, le réseau critique E_6 (cf. ci-dessous), son dual E_6^*, et le réseau P_6 de Barnes (noté $A_6^{(2)}$ dans [7]), qui est le sous-réseau de A_6 formé des points de $\mathbb{Z}^7$ dont les coordonnées vérifient la congruence $\sum_i ix_i \equiv 0 \mod 7$. Il est semblable à son dual, et possède un automorphisme d'ordre 7. Les réseaux E_6 et E_6^* (ce dernier est semblable au réseau appelé L_6^3 par Barnes et noté $A_{6,0}$ dans [7]) possèdent un automorphisme d'ordre 9.

On note E_8 le réseau A_8^3 (autre construction : E_8 est le réseau D_8^+ engendré par D_8 et le vecteur de composantes $\frac{1}{2}$). En coupant E_8 par un sous-espace orthogonal à un vecteur minimal (resp. à un plan hexagonal de vecteurs minimaux), on obtient E_7 (resp. E_6) ; E_7 est semblable à A_7^2, et possède donc un automorphisme d'ordre 7.

Dans la suite, les évaluations de $\dim \mathcal{S}_G$ que nous avons données seront utilisées comme minorations des nombres d'orbites de vecteurs minimaux des réseaux G-parfaits. L'énoncé suivant, facile mais d'usage constant, apporte quelques précisions sur ces vecteurs minimaux :

3.9 PROPOSITION. *Soit Λ un réseau G-parfait engendrant l'espace vectoriel V.*

(i) *Si V est $\mathbb{Q}$-irréductible, l'orbite d'un vecteur non nul de Λ engendre V ;*

(ii) *Si en outre G est abélien et fidèle, le nombre de couples $\{\pm x\}$ de vecteurs contenus dans l'orbite d'un vecteur non nul de Λ est égal à l'ordre de G si $-Id$ n'appartient pas à G, et à la moitié de l'ordre de G sinon.*

Démonstration. L'assertion (i) résulte de la définition même de l'irréductibilité. Pour prouver (ii), il suffit de remarquer que la seule réalisation comme groupe de permutations fidèle d'un groupe abélien est la permutation régulière.

Pour terminer ce §, nous donnons, en suivant Korkine et Zolotareff, des résultats concernant l'indice dans un réseau Λ d'un sous-réseau Λ' de même norme ($S(\Lambda)$ et $S(\Lambda')$ engendrant tous deux l'espace V). On supposera dans la suite que les deux réseaux sont de norme 1, ce que l'on peut faire sans restreindre la généralité.

3.10 PROPOSITION.

(i) *L'indice $[\Lambda : \Lambda']$ est majoré par $\{\gamma_n/\gamma_n(\Lambda')\}^{n/2}$, avec égalité si et seulement si Λ est critique ; en particulier, on a la majoration $[\Lambda : \Lambda'] \leq \gamma_n^{n/2}$ indépendante de Λ.*

(ii) *On suppose que* Λ *possède une base* $e_1, e_2, \ldots, e_n$ *formée de vecteurs de* $S(\Lambda)$. *Soient* $e'_1, e'_2, \ldots, e'_r$ $(r \leq n)$ *des vecteurs de* $S(\Lambda)$. *Alors, les déterminants d'ordre* $\leq r$ *extraits de la matrice des composantes des* e'_j *dans la base* e_i *de* V *sont* $\leq \gamma_n^{n/2}$.

En effet, $\gamma_n(\Lambda)^{-n/2}$ est égal au discriminant $\Delta(\Lambda)$ du réseau Λ, ce qui prouve les deux assertions de (i), compte tenu de l'inégalité $\Delta(\Lambda) \leq 1$ valable pour tout réseau engendré par des vecteurs de norme 1, qui découle de l'inégalité de Hadamard appliquée à un sous-réseau de Λ ayant une base formée de tels vecteurs. L'assertion (ii) est évidente lorsque les e'_i sont dépendants. Dans le cas contraire, on complète cet ensemble de vecteurs en une base de V par $n-r$ vecteurs convenablement choisis parmi les e_i. Le déterminant de ce système de vecteurs dans la base (e_i) est alors précisément le déterminant extrait que l'on cherche, **c.q.f.d.**

Compte tenu des valeurs de la constante d'Hermite, connues pour $n \leq 8$, on obtient les majorations suivantes pour $[\Lambda : \Lambda']$:

3.11 PROPOSITION. *Avec les notations de 3.10, l'indice* $[\Lambda : \Lambda']$ *est majoré par 1 pour* $n \leq 3$, *par 2 pour* $n = 4, 5$, *par 4 pour* $n = 6$, *par 8 pour* $n = 7$ *et par 16 pour* $n = 8$. *En outre, pour* $n = 4$ *(resp. 8), on peut remplacer 2 par 1 (resp. 16 par 15) si* Λ *n'est pas critique.*

Combinés avec les résultats du § 2, les majorations d'indice permettent de démontrer une assertion de finitude :

3.12 PROPOSITION. *L'ensemble des classes de similitude de réseaux G-parfaits est fini.*

Démonstration. Soit Λ un réseau G-parfait de V et soit Λ' le sous-réseau de Λ engendré par les vecteurs de $S(\Lambda)$. L'indice $m = [\Lambda : \Lambda']$ ne prend qu'un nombre fini de valeurs (prop. 3.10, (i)), et la double inclusion $\Lambda' \subset \Lambda \subset \frac{1}{m}\Lambda'$ montre que, pour Λ' fixé, il n'y a qu'un nombre fini de réseaux Λ possibles. On est donc ramené au cas où Λ est engendré par ses vecteurs minimaux.

Comme Λ est engendré par des vecteurs minimaux, son discriminant est borné. Il existe donc (Hermite) une borne B_n telle que Λ possède une base $\mathcal{B}$ constituée de vecteurs de norme $\leq B_n$. En raisonnant comme dans 3.10 (ii), on montre qu'il existe une constante C_n majorant les composantes dans une telle base des vecteurs de $S(\Lambda)$. Le nombre de vecteurs de $S(\Lambda)$ (le *kissing number*) étant majoré par une fonction qui ne dépend que de n, la proposition 2.6 permet de conclure.

3.13 REMARQUE. La démonstration précédente s'applique en particulier dans le cas des réseaux parfaits au sens ordinaire. Il serait intéressant de trouver un "G-algorithme de Voronoï" produisant un graphe connexe pour l'ensemble

des faces associées aux G-réseaux G-parfaits (mais il faut –remarque de Sigrist–considérer les familles de réseaux *appartenant à une classe donnée de représentations intégrales* (i.e. sur $\mathbb{Z}$) de G). Par ailleurs, il est vraisemblable que des énoncés analogues (algorithme de Voronoï compris) s'appliquent aux réseaux "dual-extrêmes" au sens de [4] stables sous l'action d'un sous-groupe fini de $O(V)$.

4. Groupes cycliques irréductibles. On conserve dans ce § les notations du § 3, mais on suppose maintenant que G est cyclique et que V provient d'une représentation $\mathbb{Q}$-irréductible et fidèle de G. On note q l'ordre de G, σ un générateur de G, et l'on suppose que q est ≥ 3 (si $q = 1$ ou 2, V est de dimension 1, et l'unique réseau à similitude près est A_1, semblable à $\mathbb{Z}$). Si l'ordre de G est congru à 2 mod 4, G est produit direct de $\{\pm \mathrm{Id}\}$ par un groupe G' d'ordre moitié. Comme les notions de G- et de G'-réseaux coïncident, on peut supposer, ce que nous ferons dans la suite, que q est impair ou divisible par 4.

Soit ζ une racine de l'unité d'odre q. Un G-réseau Λ de V possède une structure de module (de rang 1, sans torsion) sur l'anneau des entiers $\mathbb{Z}[\zeta]$ du corps cyclotomique $K_q = \mathbb{Q}(\zeta)$, définie par la règle $\zeta x = \sigma x$ (il y a $\varphi(q)$ structures de module possibles, dépendant du choix de ζ). On note K'_q le sous-corps réel maximal de K_q. Lorsque q est une puissance de nombre premier et est ≤ 19, ce qui est le cas dans les applications que nous avons en vue, l'anneau $\mathbb{Z}[\zeta]$ est principal et ses unités sont de la forme $\zeta^i \eta$ où η est une unité de K'_q.

Comme G est irréductible, les vecteurs minimaux de Λ engendrent V. Soit Λ' un sous-réseau de Λ engendré par des vecteurs de $S(\Lambda)$. On a vu précédemment (prop. 3.10) comment majorer l'indice $[\Lambda : \Lambda']$; en particulier, on a $[\Lambda : \Lambda'] = 1$ pour $n \leq 3$, et même pour $n = 4$ si Λ n'est pas critique, $[\Lambda : \Lambda'] \leq 2$ pour $n \leq 5$ et $[\Lambda : \Lambda'] \leq 4$ pour $n = 6$. Lorsque l'on suppose en outre que Λ' est lui aussi un G-réseau, on a $[\Lambda : \Lambda'] = N_{K_q/\mathbb{Q}}(\mathfrak{a})$ où $\mathfrak{a}$ désigne le $\mathbb{Z}[\zeta]$-indice (au sens de [13], ch. III, § 1) de Λ' dans Λ. Le fait que $[\Lambda : \Lambda']$ soit une norme permet de limiter les valeurs possibles de cet indice. En particulier, on a :

4.1 PROPOSITION. *Soit Λ un G-réseau, et soit Λ' un sous-G-réseau de Λ engendré par des vecteurs minimaux de Λ. Alors :*

(i) *Si Λ' est strictement contenu dans Λ, $[\Lambda : \Lambda']$ est au moins égal au plus petit diviseur premier de q ;*
(ii) *Si q est une puissance d'un nombre premier p, $[\Lambda : \Lambda']$ est une puissance de p ou est $\geq q + 1$;*
(iii) *Si $q = 5$ ou 7, on a $\Lambda' = \Lambda$;*
(iv) *Si $q = 9$, $[\Lambda : \Lambda'] = 1$ ou 3.*

Démonstration. La norme minimale d'un idéal de K_q est évidemment une puissance de nombre premier. La loi de décomposition des nombres premiers dans les corps cyclotomiques montre que les idéaux premiers non ramifiés ont une norme $\equiv 1 \mod q$, d'où (i) et (ii). Les assertions (iii) et (iv) sont des conséquences immédiates de (i) et (ii) et des majorations d'indices rappelées au début de ce §.

La dimension de V est $n = \varphi(q)$. Comme q est ≥ 3, n est pair. On pose $m = n/2$. L'espace V contient m sous-espaces $\mathbb{R}$-irréductibles, qui sont des plans deux à deux non isomorphes que nous notons $P_1, P_2, ..., P_m$, P_i étant caractérisé par le fait que σ induit sur P_i une rotation d'angle $\pm 2i\pi/q$ (l'angle n'est défini qu'au signe près) ; l'indexation des P_i dépend du choix de σ.

Chaque plan P_i est un $\mathbb{C}$-espace vectoriel de dimension 1, et les calculs de dimension effectués au § 3 montrent tout de suite l'égalité $\dim_{\mathbb{R}} \mathcal{S}_G = m$. En utilisant la prop. 2.5, on en déduit une minoration du nombre de vecteurs minimaux des réseaux G-parfaits :

4.2 LEMME. *Pour tout réseau G-parfait, on a $s \geq q\varphi(q)/2$ si q est impair, et $s \geq q\varphi(q)/4$ si q est pair.*

Lorsque q est égal à 3 ou à 4, on est dans le cas évoqué en 3.7 dans lequel V est $\mathbb{R}$-irréductible. Sinon, m est ≥ 2, et les classes de similitude de G-réseaux ne sont pas isolées. C'est le cas dès la dimension 4, pour laquelle les valeurs possibles pour q sont 5, 8 et 12. On a vu (cf. prop. 2.4) qu'un réseau G-parfait possède au moins $m = 2$ orbites de vecteurs minimaux dans le cas de la dimension 4. Cette condition caractérise en fait les réseaux parfaits, et même extrêmes, comme dans le cas du théorème 3.8 de Korkine et Zolotareff :

4.3 THÉORÈME. *Soit V un $\mathbb{R}$-espace vectoriel de dimension 4, soit G un sous-groupe cyclique irréductible de $O(V)$, et soit Λ un G-réseau possédant au moins deux orbites de vecteurs minimaux. Alors, Λ est G-extrême, et :*

(i) *Si G est d'ordre 5, Λ est semblable à A_4 ;*
(ii) *Si G est d'ordre 8 ou 12, Λ est semblable à D_4 .*

4.4 COROLLAIRE (SCHOOF ET WASHINGTON, [14]). *Si Λ est un réseau de dimension 4 muni d'un automorphisme d'ordre 5, on a $\gamma_4(\Lambda)^4 \leq \frac{16}{5}$ $(< \gamma_4^4 = 4)$.*

En effet, $\gamma_4(A_5)^4 = \frac{16}{5}$.

Démonstration de 4.4. D'après le lemme 4.2, pour $q = 5$ (resp. 8, resp. 12), $s(\Lambda)$ est ≥ 10 (resp. 8, resp. 12). Le théorème 3.8 montre tout de suite que pour q=5 et q=12, le réseau Λ est extrême. Comme 5 ne divise pas $s(D_4)$, Λ est semblable à A_4 lorsque q=5, et, pour q=12, l'inégalité $s(\Lambda) \geq 12$ montre

que Λ est semblable à D_4. Comme on sait qu'il existe des G-réseaux admettant ces groupes comme groupes d'automorphismes (cf. § 2, après le th. 3.8)), il est clair que, réciproquement, ces réseaux conviennent.

Il reste à traiter le cas $q = 8$; c'est une conséquence immédiate du lemme suivant :

4.5 LEMME. *Un G-réseau non critique a une seule orbite de couples $\{\pm x\}$ de vecteurs minimaux.*

En effet, tout vecteur minimal constitue alors une base de Λ sur $\mathbb{Z}_{\mathbb{Q}(\zeta)}$, de sorte que si x et y sont deux vecteurs minimaux de Λ, on a

$$y = \lambda x, \ \lambda \text{ unité de } \mathbb{Q}(\zeta), \tag{1}$$

où, quitte à échanger les rôles de x et y et à remplacer y par un de ses conjugués, on peut supposer $\lambda = \epsilon^k$, ϵ désignant l'unité fondamentale $1 + \zeta + \zeta^{-1}$ de $\mathbb{Q}(\zeta)$, et k un entier ≥ 0. Posant alors $x_k = \epsilon^k x$, où x est minimal, on voit immédiatement les relations

$$\|x_{k+1}\|^2 = 3\|x_k\|^2 + 4x_k.\zeta x_k \quad \text{et} \quad x_{k+1}.\zeta x_{k+1} = 2\|x_k\|^2 + 3x_k.\zeta x_k \ . \tag{2}$$

On en tire d'abord, puisque $x_0 = x$ est minimal, que $x_0.\zeta x_0$ est $\geq -\frac{1}{2}$, l'égalité équivalant à $\|x_1\| = 1$, mais aussi à $\|x + \zeta x\| = 1$, impossible d'après (1), puisque $1 + \zeta$ est de norme 2 : x_1 n'est donc pas minimal. Les relations (2) montrent aussi par récurrence que, pour $k \geq 1$, on a $x_k.\zeta x_k \geq \frac{1}{2}$ et donc $\|x_{k+1}\|^2 \geq 5$. Ainsi, les vecteurs minimaux de Λ se répartissent sur une seule orbite, celle de $x = x_0$, **c.q.f.d.**

Par des arguments de nature combinatoire analogues à ceux qui ont permis de démontrer le théorème précédent dans le cas $q = 8$, on peut trouver tous les réseaux G-parfaits pour $n = 6$, ce qui impose $q = 7$ ou 9. Ici encore, la minoration de s donnée par 3.3 suffit :

4.6 THÉORÈME. *Soit V un espace vectoriel euclidien de dimension 6, soit G un sous-groupe cyclique irréductible de $O(V)$, d'ordre $q \not\equiv 2 \mod 4$, et soit Λ un G-réseau contenant au moins 3 orbites de couples $\pm x$ de vecteurs minimaux. Alors, Λ est extrême, et l'on est dans l'un des deux cas suivants :*

(i) *$q = 7$, et Λ est semblable à A_6 ou à P_6 ;*
(ii) *$q = 9$, et Λ est semblable à E_6 ou à E_6^*.*

4.7 COROLLAIRE. *Un réseau de dimension 6 invariant sous l'action d'un sous-groupe cyclique d'ordre 7 de $O(V)$ vérifie l'inégalité*

$$\gamma_6(\Lambda)^6 \leq \frac{2^{12}}{7^3} < 11,942 \ (< \gamma_6^6 = \frac{64}{3} = 21,333...)$$

En effet, on a $\gamma_6(A_6)^6 = \frac{2^6}{7} < \gamma_6(P_6) = \frac{2^{12}}{7^3}$.

Démonstration de 4.6. Soit Λ un réseau vérifiant les hypothèses du théorème. En combinant les prop. 3.11 et 4.1, on voit tout de suite que le réseau Λ' engendré par les vecteurs minimaux de Λ est égal à Λ lorsque $q = 7$, et est d'indice 1 ou 3 lorsque $q = 9$. Pour faire la démonstration, on supposera d'abord que Λ est engendré par ses vecteurs minimaux, ce qui est loisible puisque Λ' satisfait aussi aux hypothèses du théorème.

Dans les deux cas $q = 7$ et $q = 9$, le corps $\mathbb{Q}(\zeta)$ est cyclique de degré 6 et possède deux unités fondamentales e et f, que l'on peut prendre égales à $\zeta+\zeta^{-1}$ et $\zeta^2+\zeta^{-2}$ respectivement. Ce sont deux éléments conjugués du sous-corps réel maximal K'_q de $\mathbb{Q}(\zeta)$; on note g le conjuqué autre que f de e. On a $g = \zeta^4 + \zeta^{-4}$ $(= \zeta^3 + \zeta^{-3}$ si $q = 7)$. Les unités e, f, g vérifient les relations $efg = 1$ et $e+f+g = -1$ lorsque $q = 7$, et $efg = -1$ et $e+f+g = 0$ lorsque $q = 9$.

Dans l'énoncé du lemme ci-dessous, lorsque q=9, on note π l'élément $\zeta-\zeta^{-1}$ de $\mathbb{Z}[\zeta]$; c'est un générateur de l'unique idéal premier au-dessus de 3 de $\mathbb{Z}[\zeta]$.

4.8 LEMME. *Il existe trois vecteurs minimaux x, y, z de Λ appartenant à des orbites distinctes de $\pm G$ et des unités η et η' de K'_q telles l'une des conditions suivantes soit vérifiée :*

(i) $y = \eta x$ *et* $z = \eta' x$;
(ii) $y = \eta x$ *et* $z = \eta' \pi x$;
(iii) $y = \eta \pi x$ *et* $z = \eta' \pi x$;

Démonstration. On a vu que Λ possède au moins trois orbites de vecteurs minimaux. On prend pour x, y, z des représentants de ces orbites. On a vu également que Λ est un module libre sur $\mathbb{Z}[\zeta]$. Soit a une $\mathbb{Z}[\zeta]$-base de Λ. Il existe des éléments λ, μ et ν de $\mathbb{Z}[\zeta]$ tels que $x = \lambda a$, $y = \mu a$ et $z = \nu a$. Quitte à permuter x, y, z, on peut supposer λ, μ, ν rangés par normes croissantes. La proposition 4.1 montre que ces éléments sont de la forme ε ou $\varepsilon\pi$, ε désignant une unité de K_q. Vu les propriétés de K_q rappelées au début du §, ces unités sont de la forme $\zeta^i\eta$ où η est une unité de K'_q. Il est alors clair que l'on est dans le cas (i) si π divise 0 ou 3 des éléments λ, μ, ν, dans le cas (ii) si π en divise 2, et dans le cas 3 si π en divise 1.

Nous allons maintenant étudier de plus près ce que peuvent être η et η'.

4.9 LEMME. *Soient x et y deux vecteurs minimaux indépendants de Λ et soit η une unité de K'_q telle que $y = \eta x$. Alors, $\pm\eta$ ou $\pm\eta^{-1} \in \{e, f, g\}$.*

Démonstration. Écrivons $\eta = u + ve + wf$, $u, v, w \in \mathbb{Z}$ avec $(v, w) \neq (0,0)$. On sait (cf. § 3) que tous les déterminants formés par 2 composantes sur la base ζ^i, $-2 \leq i \leq 3$ de 2 vecteurs $\zeta^j y$, $\zeta^k y$ sont ≤ 4. On vérifie que l'on peut faire apparaître les valeurs w^2, v^2, et $u^2 - v^2$ de ces déterminants. Par exemple, si $q = 7$, il suffit d'utiliser successivement $(j,k) = (0,1)$ avec $i \in \{-2,3\}$, $(1,3)$ avec $i \in \{1,2\}$ et $(3,-3)$ avec $i \in \{1,3\}$. On en déduit que les valeurs absolues de u, v, w sont ≤ 2. Les triplets (u', v', w') obtenus à partir d'un triplet (u,v,w) en faisant opérer $\mathrm{Gal}(K_q'/\mathbb{Q})$ doivent vérifier les mêmes propriétés, ainsi que ceux obtenus par les transformations $\eta \mapsto \eta^{-1}$ (car $x = \eta^{-1} y$) et $\eta \mapsto -\eta$. Les triplets admissibles se répartissent donc en orbites de 12 éléments sous l'action d'un groupe abélien de type $(6,2)$. On vérifie alors facilement que ces contraintes limitent les valeurs de η à deux orbites, à savoir celles de e et de $e^2 f$, pour $q = 7$ comme pour $q = 9$.

Pour simplifier l'écriture des calculs qui vont suivre, nous normalisons Λ par la condition $\|\Lambda\| = 1$. Nous allons calculer les normes de certains vecteurs de Λ en fonction des produits scalaires $\alpha = x.\zeta x$, $\beta = x.\zeta^2 x$ et $\gamma = x.\zeta^4 x$ ($\gamma = x.\zeta^3 x$ si $q = 7$). La somme $\alpha + \beta + \gamma$ est égale à $-\frac{1}{2}$ si $q = 7$ et à 0 si $q = 9$; en outre, $x.\zeta^3 x = -\frac{1}{2}$ si $q = 9$: cela se voit simplement en utilisant l'égalité $\|x\|^2 = 1$. En écrivant les inégalités $\|z\| \geq 1$ pour $z = x \pm \zeta^i x$, on obtient $-\frac{1}{2} \leq \alpha, \beta, \gamma \leq \frac{1}{2}$, d'où, pour $q = 7$ (resp. 9), $\alpha + \beta \leq 0$ (resp. $-\frac{1}{2} \leq \alpha + \beta \leq \frac{1}{2}$).

Occupons-nous maintenant du cas $q = 7$. En calculant $\|efx\|$ par l'égalité $ef = -1 - f$, on obtient $\alpha - \beta \leq \frac{1}{2}$. On trouve enfin $\|e^2 fx\|^2 = \|(1 - e + f)x\|^2 = 6 - 6\alpha + 8\beta = 6 + 2\beta - 6(\alpha - \beta) \geq 3 - 2\beta \geq 2$, inégalité qui prouve que $e^2 fx$ ne peut pas être un vecteur minimal.

Lorsque $q = 9$, on obtient par un calcul analogue $\|efx\|^2 = \|(1 - e)x\|^2 = 3 - 4\alpha + 2\beta \geq 1$, d'où $2\alpha - \beta \leq 1$, puis $\|e^2 fx\|^2 = \|(2 - e + f)x\|^2 = 10 - 14\alpha + 8\beta = 10 + \beta - 7(2\alpha - \beta) \geq 3 + \beta > 2$, ce qui achève la démonstration du lemme 4.9.

4.10 LEMME. *Si Λ vérifie l'hypothèse (i) du lemme 4.8, on peut choisir x, y, z de façon que $(\eta, \eta') = (ef, f)$ ou (ef, e).*

Démonstration. Écrivons $\eta = \pm e^a f^b$ et $\eta' = \pm e^c f^d$. En examinant l'effet des 6 permutations de $\{x, y, z\}$ sur le quadruplet (a, b, c, d), on voit tout de suite que l'on peut se limiter aux cas où l'on a $a \geq c \geq 0$ et $d \geq 0$ lorsque $c = 0$. Il suffit alors de considérer les couples $(\eta, \eta') = (ef, e)$, (ef, f), et (e, f). Or, on a $\|ex\|^2 = 2 + \beta$ et $\|fx\|^2 = 2 + \gamma$. Donc, si ex et fx sont minimaux, on a $\beta = \gamma = -\frac{1}{2}$. Cela entraîne l'égalité absurde $\alpha = 1$ lorsque $q = 9$ et, pour $q = 7$, l'égalité $\alpha = \frac{1}{2}$ qui entraîne à son tour l'égalité absurde $\|efx\| = 0$.

Fin de la démonstration de 4.6, (i). Il résulte du lemme 4.10 qu'un réseau

vérifiant les hypothèses du th. 4.6, (i) est semblable à un réseau possédant 3 orbites de vecteurs minimaux de la forme x, efx, ex ou x, efx, fx. Ces données fixent le système α, β, γ une fois que l'on a imposé $\|x\|$. Donc, à similitude près, au plus 2 réseaux conviennent. Or, nous connaissons deux réseaux acceptables, à savoir A_6 et P_6. Ce sont donc certainement ces 2 réseaux, **c.q.f.d.**

(Pour $\|x\| = 1$, les valeurs respectives du triplet (α, β, γ) sont $(0, -\frac{1}{2}, \frac{1}{2})$ et $(\frac{1}{4}, -\frac{1}{4}, -\frac{1}{2})$. La forme quadratique $t \mapsto 2\|t\|^2$ étant entière pour le premier réseau mais non pour le second, le premier réseau est semblable à A_6 et le second à P_6.)

Nous devons maintenant examiner les autres possibilités prévues par le lemme 4.8. Nous supposons donc que $q = 9$. Toutefois, vu l'absence d'application comparable au cor. 4.7, nous n'écrirons pas tous les détails.

4.11 LEMME. *Si Λ possède un couple de vecteurs minimaux $(x, \eta\pi x)$, alors η est l'une des unités ± 1, $\pm e$, $\pm(1-e)$, pour lesquelles on a respectivement $\beta = \frac{1}{2}$, $\gamma = \frac{1}{2}$, $\alpha = \frac{1}{2}$.*

Démonstration. On écrit $\eta = u + ve + wf$. Par des considérations analogues à celles qui ont été utilisées dans la démonstration de 4.9, on montre les majorations $|u| \leq 3$, $|v| \leq 2$, $|w| \leq 1$, et, en utilisant la conjugaison dans K_9', on limite les triplets (u, v, w) à 4 orbites de 3 éléments (au signe près). En écrivant les inégalités $\|t\| \geq 1$ pour quelques vecteurs bien choisis, on trouve finalement qu'une seule orbite convient, en l'occurence $\{\pm 1, \pm e, \pm(1-e)\}$; la fin du lemme est évidente.

Fin de la démonstration de 3.6, (ii). On remarque d'abord que le cas (iii) du lemme 4.8 ne se produit pas, car 2 des α, β, γ ne peuvent prendre la valeur $\frac{1}{2}$ à cause de la relation $\alpha + \beta + \gamma = 0$. On essaie alors les diverses possibilités provenant du cas (ii) de ce lemme, et on constate que, compte tenu des inégalités $|\alpha|, |\beta|, |\gamma| \leq \frac{1}{2}$ et $\|x - \zeta^i x - \zeta^{-i} x\| \geq 1$, les orbites de vecteurs minimaux doivent être de l'une des formes

$$(x, efx, (1-e)\pi x),\ (x, ex, e\pi x),\ (x, fx, (1-e)\pi x).$$

Dans les 3 cas, on retrouve le réseau rencontré dans le lemme 4.10, réseau qui possède en fait 4 orbites de vecteurs minimaux.

On obtient donc un résultat analogue à celui que nous avons démontré dans le cas $q = 7$: il y a au plus 2 classes de similitude de G-réseaux engendrés par leurs vecteurs minimaux. Or, on connaît *a priori* deux réseaux de ce type, à savoir E_6 et son dual E_6^*. Ce sont donc ces deux réseaux que nous avons trouvés. Comme le premier est critique, et que le quotient des discriminants de E_6^* et E_6 (ramenés à la norme 1) est < 2, il n'existe pas pour $q = 9$ de

G-réseau qui ne soit pas engendré par ses vecteurs minimaux. Cela achève la démonstration du th. 4.6.

4.12 REMARQUE. Pour n=8, les groupes cycliques irréductibles sont d'ordre 15 (ou 30), 16, 20, 24. En examinant la table des caractères donnée par l'Atlas ([8]) pour les groupes liés à $O_8^+(2)$, on voit que E_8 fournit des représentations $\mathbb{Q}$-irréductibles pour les groupes cycliques d'ordre 15, 20 et 24, ce qui résulte aussi du travail d'Eva Bayer ([3], exemple 5.8). En revanche, E_8 ne possède pas d'automorphisme d'ordre 16 ; en conséquence, la classification des G-réseaux possédant un tel automorphisme permettrait d'améliorer la G-constante d'Hermite correspondante.

Une remarque analogue peut être faite en dimension 10 avec un groupe cyclique d'ordre 11, le réseau conjecturalement critique ne possédant pas d'automorphisme d'ordre 11 (les vecteurs minimaux de son dual engendrent un réseau plan hexagonal, cf. [4], rem. 4.8).

Nous reviendrons sur les réseaux de dimension 8 dans un article ultérieur. (Voir aussi l'appendice (§ 6) ci-dessous.)

5. Autres groupes cycliques. Dans ce §, pour lequel nous conservons les notations des § précédents, nous étudions quelques exemples dans lesquels le groupe G est un sous-groupe cyclique de $O(V)$ dont la représentation associée n'est pas irréductible, et classons complètement les réseaux G-parfaits lorsque G est cyclique d'ordre 3 ou 5 et V de dimension égale à l'ordre de G . Toutefois, comme les réseaux critiques font partie des listes que nous dressons, nous ne reproduirons pas tous les détails des démonstrations.

Soit ℓ un nombre premier impair, et supposons que l'on ait $\mathrm{Card}\, G = \dim V = \ell$. Une représentation rationnelle fidèle de G est unique à isomorphisme près, et le polynôme caractéristique d'un générateur σ de G est alors $X^\ell - 1$. Notons toujours ζ une racine de l'unité d'ordre ℓ, et soit $T \in \mathbb{Z}[G]$ la "trace" $\sum_{i=0}^{\ell-1} \sigma^i$. L'algèbre $\mathbb{Q}[G]$ s'identifie au produit $\mathbb{Q} \times \mathbb{Q}(\zeta)$, le premier facteur étant associé à l'idempotent $e = \frac{T}{\ell}$ et le second à l'idempotent orthogonal $1 - e$. Plus précisemment, on identifie l'élément

$$\sum_{i \bmod \ell} a_i \sigma^i \text{ de } \mathbb{Q}[G] \text{ au couple } \Big(\sum_{i \bmod \ell} a_i, \sum_{i \bmod \ell} a_i \zeta^i \Big) \text{ de } \mathbb{Q} \times \mathbb{Q}(\zeta).$$

L'espace V est somme directe de l'image de T, qui est une droite stable notée D, et du noyau de T, qui est l'hyperplan H orthogonal à cette droite.

L'anneau $\mathbb{Z}[G]$ est contenu dans l'unique ordre maximal $\mathfrak{M}$ de $\mathbb{Q}[G]$, engendré par $\mathbb{Z}[G]$ et e. Le quotient $\mathfrak{M}/\mathbb{Z}[G]$ est un groupe cyclique d'ordre ℓ. Comme Λ est de rang 1, l'une des deux conditions suivantes est réalisée : ou

bien Λ possède une structure de $\mathfrak{M}$-module, ou bien il est projectif sur $\mathbb{Z}[G]$, et donc libre pour $\ell \leq 19$.

5.1 PROPOSITION. *Si Λ est un $\mathfrak{M}$-module, ses vecteurs minimaux sont dans l'image ou le noyau de e.*

Démonstration. Soit $x \in S(\Lambda)$. Si $\sigma x = x$, on a $ex = x$. Sinon, on a $\|x \pm \sigma x\| \geq 1$, d'où $|x.\sigma x| \leq \frac{1}{2}$, ce qui entraîne $\|\sum \sigma^i x\|^2 \leq \frac{\ell(\ell+1)}{2}$, d'où $\|ex\|^2 \leq \frac{(\ell+1)}{2\ell} < 1$. (On a normalisé Λ par $\|\Lambda\| = 1$.) Cette somme est donc nulle, **c.q.f.d.**

La représentation de G définie par V est somme de $\frac{\ell+1}{2}$ représentations $\mathbb{R}$-irréductibles (une de dimension 1, la droite D, et $\frac{\ell-1}{2}$ de dimension 2). Il en résulte (cf. 2.4) que, si Λ est G-parfait, $S(\Lambda)$ contient au-moins $\frac{\ell+1}{2}$ orbites de couples $\{\pm x\}$ de vecteurs minimaux, formées de ℓ vecteurs sauf au plus une qui peut être réduite à un élément. Nous allons voir que pour $\ell = 3$ ou 5, cette condition est suffisante. Le cas $\ell = 3$ est facile :

5.2 THÉORÈME. *Si G est d'ordre 3 et opère fidèlement sur V, les réseaux Λ possédant deux orbites de vecteurs minimaux sont G-extrêmes, et semblables à $A_1 \perp A_2$, A_3 ou A_3^*.*

Démonstration. Le cas d'un réseau réductible est une conséquence immédiate du th. 3.6. Par ailleurs, si les orbites de vecteurs minimaux ont 3 éléments, le th. 3.8 montre que Λ est semblable à A_3. Il reste à considérer le cas où $S(\Lambda)$ contient un vecteur x fixe par G et une orbite Gy non contenue dans H. Alors, l'orbite de y engendre V, donc aussi Λ (prop. 3.11). Écrivons $x = ay + b\sigma y + c\sigma^2 y$, avec $a, b, c \in \mathbb{Z}$. On a $a = b = c$ (car $\sigma x = x$), puis $a = \pm 1$ (car x est minimal). Les produits scalaires $y.\sigma^{\pm 1} y$ sont égaux, et valent $-\frac{1}{3}$, comme on le voit en calculant $\|y\|$. On reconnaît alors le réseau A_3^*. On vérifie sans peine l'indépendance de φ_x et de φ_y, ce qui prouve que le réseau est G-parfait. Comme les réseaux A_n^* sont eutactiques ([9], 12.7), A_3^* est G-extrême. Les deux autres le sont également (th. 3.6 pour $A_1 \perp A_2$ et th. 3.8 pour A_3), **c.q.f.d.**

Passons maintenant au cas où $\ell = 5$.

5.3 THÉORÈME. *Si G est d'ordre 5 et opère fidèlement sur V, et si $S(\Lambda)$ contient 3 orbites de vecteurs minimaux, Λ est G-extrême, et semblable à l'un des 5 réseaux suivants : D_5, A_5^3, A_5, Λ_5 ou $A_1 \perp A_4$, où Λ_5, normé par*

$\|\Lambda_5\|^2 = 10$, *a pour déterminant 19602 et est défini par la matrice de Gram*

$$\begin{pmatrix} 10 & -5 & 1 & 1 & -5 \\ -5 & 10 & -5 & 1 & 1 \\ 1 & -5 & 10 & -5 & 1 \\ 1 & 1 & -5 & 10 & -5 \\ -5 & 1 & 1 & -5 & 10 \end{pmatrix}.$$

Démonstration. Rappelons (prop. 3.11) que le sous-réseau de Λ engendré par l'orbite d'un vecteur minimal qui n'est ni dans D ni dans H est d'indice 1 ou 2, et que sa projection sur H engendre la projection de Λ sur H (cf. prop. 4.1).

5.4 LEMME. *Soient x et y deux vecteurs minimaux d'un G-réseau Λ engendrant des orbites distinctes, avec $x \notin H$. Alors, quitte à remplacer y par l'un des vecteurs $\pm\sigma^i y$, on peut supposer que l'une des relations suivantes est vérifiée :*

(i) *Gx et Gy engendrent des réseaux de même indice dans Λ, $y = (\sigma + \sigma^{-1} - 1)x$ ou $y = (\sigma^2 + \sigma^{-2} - 1)x$ (on passe d'un cas à l'autre en échangeant x et y) ;*

(ii) *Gy engendre un réseau d'indice 2 et Gx un réseau d'indice 1, $y = (1 + \sigma^i)x$, avec $i = 1$ ou 2 (à l'échange près de x et de y) ;*

(iii) *$y \in H$, $y = (\sigma - 1)x$, $(\sigma^2 - 1)x$, $(1 - \sigma + \sigma^{-1} - \sigma^2)x$ ou $(1 - \sigma - \sigma^{-1} + \sigma^2)x$.*

Démonstration (indications). (i) En utilisant l'isomorphisme de $\mathbb{Z}[G]/T\mathbb{Z}$ sur $\mathbb{Z}[\zeta]$, on montre que les unités de $\mathbb{Z}[G]$ sont de la forme $\pm\sigma^i(\sigma + \sigma^{-1} - 1)^m$, $m \in \mathbb{Z}$. Un argument d'indice déjà utilisé montre que l'on doit choisir m pour que les coefficients de y sur la base $\{\sigma^i x\}$ soient bornés par 2, ce qui impose $m = \pm 1$. Pour (ii), on montre de même que les éléments de $\mathbb{Z}[G]$ de norme ± 2 sont de la forme $\pm\sigma^i(\sigma + \sigma^{-1})(\sigma + \sigma^{-1} - 1)^m$, et on limite les valeurs de m à 0, -1 par un argument d'indice. Pour (iii), on écrit $y = \lambda x$, avec λ dans l'idéal d'augmentation de $\mathbb{Z}[G]$. Un argument d'indice montre encore que les coefficients de λ sont bornés par 1, ce qui permet de conclure facilement.

Soit maintenant Λ un G-réseau avec 3 orbites de vecteurs minimaux. Comme un réseau de dimension 4 a au plus 12 vecteurs minimaux, une au moins de ces orbites n'est pas contenue dans H. On note x, y, z des vecteurs engendrant chacune de ces orbites, en supposant que x n'est pas dans H, et l'on discute selon le nombre d'orbites contenues dans H. On pose $\alpha = x.\sigma x$ et $\beta = x.\sigma^2 x$.

Si y et z sont dans H, on utilise 5.4, (iii). On trouve *a priori* pour (α, β) ou (β, α) l'une des possibilités $(\frac{1}{2}, \frac{1}{2})$, $(\frac{1}{2}, 0)$ et $(\frac{1}{2}, \frac{2}{3})$. La dernière est clairement impossible, et les deux premières correspondent pour le réseau engendré par les

orbites de x, y, z à A_5 et D_5 respectivement. L'indice 2 est alors impossible, les discriminants de A_5 et de D_5 étant trop petits. On a donc $\Lambda \sim A_5$ ou $\Lambda \sim D_5$.

Si z est dans H mais non y, on utilise 5.4, (i) et (iii) si Gx et Gy engendrent le même réseau, et 5.4, (ii) et (iii) sinon. En échangeant éventuellement α et β, on se ramène à $\alpha = -\frac{1}{2}$ et $\beta \in \{0, \frac{1}{2}, \frac{1}{3}\}$. L'inégalité $\|x\| \geq 1$ ne laisse plus que la possibilité $\alpha = -\frac{1}{2}$, $\beta = 0$, qui correspond à D_5, Gx et Gy engendrant toutes les deux Λ.

(Compte tenu des échanges de α et de β, D_5 est apparu quatre fois, ce qui correspond à l'existence pour ce réseau de 4 orbites de vecteurs minimaux, dont 2 dans H.)

Enfin, si Λ ne possède aucune orbite dans H, on peut, compte tenu du lemme 5.4, supposer que Gx engendre Λ et que Gz engendre un sous-réseau d'indice 2, Gy étant d'indice 1 ou 2 dans Λ. Un très petit nombre d'essais permet de voir que le réseau cherché peut être défini par $\alpha = -\frac{1}{2}$ et $\beta = \frac{1}{4}$. L'unique réseau que nous avons trouvé ne peut être alors que le réseau A_5^3, ce qui qui n'est pas difficile à vérifier directement.

Ainsi, lorsque le nombre de vecteurs minimaux du G-réseau Λ est un multiple de 5, Λ est semblable à l'un des 3 réseaux extrêmes qui existent en dimension 5.

Nous étudions maintenant le cas où $s(\Lambda)$ est congru à 1 modulo 5. Il y a alors un vecteur minimal stable par G, que nous notons x, et deux vecteurs minimaux y et z ayant des orbites à 5 éléments. Si y et z sont dans H, les vecteurs minimaux engendrent un réseau semblable à $A_1 \perp A_4$, qui est égal à Λ tout entier vu son discriminant, et qui est G-extrême d'après le th. 3.6.

Sinon, on suppose que y n'est pas dans H. L'indice $Q = [\Lambda : Gy]$ vaut 1 ou 2, et l'on peut supposer que l'indice $[\Lambda : Gz]$ est $\geq Q$ si z n'est pas dans H. On pose maintenant $\alpha = y.\sigma y$ et $\beta = y.\sigma^2 y$. Du fait que x est minimal, on a $\alpha + \beta = \frac{Q^2-5}{10}$. Nous avons alors examiné les trois possibilités $z \in H$, $z \notin H$ et $[\Lambda : Gz] = Q$, et enfin $z \notin H$, $Q = 1$ et $[\Lambda : Gz] = 2$, et avons éliminé les réseaux de discriminant trop petit (ce qui signifie que x, y, z ne sont en fait pas minimaux). Seule a subsisté la possibilité (α, β) (ou (β, α)) $= (-\frac{1}{2}, \frac{1}{10})$, qui donne la matrice de Gram annoncée. Nous avons alors vérifié que x, y, z sont effectivement des vecteurs minimaux, et contrôlé que l'équation

$$\mathrm{Tr} = a\varphi_x + b\varphi_y + c\varphi_z$$

possède pour unique solution le triplet $(\frac{15}{33}, \frac{50}{33}, \frac{100}{33})$.

L'unicité confirme que Λ_5 est G-parfait, et Λ_5 est même G-extrême, puisque a, b, c sont > 0, **c.q.f.d.**.

5.5 REMARQUE. L'étude du cas $\ell = 7$ semble possible avec des calculs limités. Toutefois, le réseau critique E_7 possédant un automorphisme d'ordre 7, on ne

peut pas espérer améliorer la majoration classique de $\gamma_7(\Lambda)$ sur les G-réseaux Λ. (6 des 33 réseaux parfaits figurant dans [7], à savoir $p_7^1 \sim E_7$, $p_7^2 \sim E_7^*$, $p_7^4 \sim D_7$, p_7^{15}, p_7^{30} et $p_7^{33} \sim A_7$, possèdent un automorphisme d'ordre 7.)

De même, l'étude des automorphismes de polynôme minimal X^2+X+1 ou X^2+1 en dimensions n =4, 6 ou 8 n'améliore pas $\gamma_n(\Lambda)$, les réseaux critiques D_4, E_6 et E_8 possédant des automorphismes de ce type.

6. Compléments (mai 1990). Nous décrivons brièvement dans ce § quelques résultats concernant le degré 8 qui ont été obtenus postérieurement à l'exposé fait aux journées arithmétiques.

Nous avons déterminé les réseaux G-parfaits pour les groupes cycliques $\mathbb{Q}$-irréductibles d'ordres 15,16 et 24, ce qui couvre trois des quatre possibilités en dimension 8. (Le cas des groupes d'ordre 20 reste en suspens ; il est probable (mais non démontré) que le seul réseau G-parfait est dans ce cas E_8.) Ces réseaux sont engendrés en tant que $\mathbb{Z}[G]$-modules par un vecteur minimal convenable x et sont déterminés à isométrie près par les 4 produits scalaires $\alpha_i(x) = x.\sigma^i(x)$, $i = 0, 1, 2, 3$. Pour les décrire, nous les normalisons de façon que que $\alpha_0(x) = \|x\|^2$ soit le plus petit entier qui rende le réseau entier. Pour $q = 15$ (resp. 16, resp. 24), on trouve à similitude près 1 (resp. 3, resp. 2) réseaux G-parfaits, qui sont tous G-extrêmes, donc en particulier eutactiques, mais seuls D_8 (trouvé pour $q = 16$) et E_8 (trouvé pour $q = 15$ et $q = 24$) sont parfaits au sens usuel du terme.

Voici ces six réseaux, pour lesquels nous donnons α_0, un triplet $(\alpha_1, \alpha_2, \alpha_3)$, et le déterminant noté det.

$q = 15$: 2 ; (-1, 0, 0) ; det=1 (E_8).
$q = 16$: 8 ; (-2,-4, 3) ; det=$(2.241)^2$.
$q = 16$: 2 ; (-1,-0,-0) ; det=4 (D_8).
$q = 16$: 4 ; (-2, 0, 1) ; det=$(2.17)^2$).
$q = 24$: 2 ; (-1,-0,-0) ; det=1 (E_8).
$q = 24$: 4 ; (0,-1,-2) ; det=5^4.

Les constantes d'Hermite des trois réseaux G-parfaits trouvés pour $|G| = 16$, arrondies aux deux décimales les plus proches, sont respectivement 72,21 ; 64,00 et 56,69 . On en déduit :

THÉORÈME. *Soit Λ un réseau d'un espace euclidien de dimension 8, invariant sous l'action d'un groupe cyclique ($\mathbb{Q}$-irréductible) d'ordre 16. Alors, la constante d'Hermite de Λ vérifie l'inégalité*

$$\gamma_8(\Lambda)^8 \leq 2^{22}241^{-2} = 72,214... \quad (< \gamma_8^8 = 256).$$

On peut également montrer (M. Laïhem) que les seuls réseaux de dimension 8 parfaits pour le groupe quaternionien d'ordre 8 sont (à similitude près) D_8 et E_8.

Signalons enfin que François Sigrist a calculé les "G-voisins" d'un certain nombre de G-réseaux considérés dans cet article pour l'adaptation naturelle aux G-réseaux de l'algorithme classique de Voronoï. Bien que l'on n'ait pas encore de résultats de connexité au sens de la remarque 3.13 qui permettraient d'effectuer des classifications, on a dès à présent un procédé intéressant de construction de G-réseaux. En outre, les résultats de Sigrist corroborent ceux de notre article dans le cas des groupe cycliques $\mathbb{Q}$-irréductibles d'ordre 5 et 7 (th. 4.3 et 4.6) ainsi que dans le cas des groupes d'ordre 5 en dimension 5, où il y a une composante connexe de 4 classes de G-réseaux (correspondants à ceux qui sont projectifs sur $\mathbb{Z}[G]$) et une composante réduite à la classe de $A_1 \perp A_4$, conformément à ce que laissait prévoir le th. 5.3. Enfin, dans le cas $|G| = n = 7$, il trouve à partir de A_7 les 6 réseaux évoqués dans la remarque 5 et deux réseaux supplémentaires analogues au réseau Λ_5 du th. 5.3.

BIBLIOGRAPHIE

[1] E.S. Barnes, *On a theorem of Voronoï*, Proc. Cambridge Phil. Soc. **53** (1957), 537–539.
[2] E.S. Barnes, *The perfect and extreme senary forms*, Canad. J. Math. **9** (1957), 235–242.
[3] E. Bayer-Fluckiger, *Definite unimodular lattices having an automorphism of given characteristic polynomial*, Comm. Math. Helvet. **59** (1984), 509-538.
[4] A-M. Bergé et J. Martinet, *Sur un problème de dualité lié aux sphères en géométrie des nombres*, J. Number Theory **32** (1989), 14–42.
[5] A-M. Bergé et J. Martinet, *Sur les minorations géométriques des régulateurs*, "Séminaire de Théorie des Nombres de Paris," Birkhäuser, Bâle, 1989, pp. 23–50.
[6] J.H. Conway et N.J.A. Sloane, "Sphere Packings, Lattices and Groups," Springer-Verlag, Grundlehren no 290, Heidelberg, 1988.
[7] J.H. Conway et N.J.A. Sloane, *Low-dimensional lattices. III. Perfect forms*, Proc. R. Soc. London **418** (1988), 43–80.
[8] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker et R.A. Wilson, "ATLAS of Finite Groups," Oxford Univ. Press, 1988.
[9] H.S.M. Coxeter, *Extreme forms*, Canad. J. Math **3** (1951), 391–441.
[10] M. Craig, *Extreme Forms ans Cyclotomy*, Mathematika **25** (1978), 44–56.
[11] A. Korkine et G. Zolotareff, *Sur les formes quadratiques positives*, Math. Ann. **11** (1877), 242–292.
[12] J-P. Serre, "Représentations linéaires des groupes finis (2ième édition)," Hermann, Paris, 1971.
[13] J-P. Serre, "Corps locaux (3ième édition)," Hermann, Paris, 1980.
[14] R. Schoof et L. Washington, *Quintic Polynomials and Real Cyclotomic Fields with Large Class Numbers*, Math. Comp. **50** (1988), 543–556.

mots clés : automorphismes, réseaux, géométrie des nombres

Laboratoire de Mathématiques
351, cours de la Libération
F-33405 TALENCE cedex

(Reçu le 3 novembre 1989)

Astérisque

ANNE BERTRAND

Nombres de Perron et problèmes de rationalité

Astérisque, tome 198-199-200 (1991), p. 67-76

<http://www.numdam.org/item?id=AST_1991__198-199-200__67_0>

NOMBRES DE PERRON ET PROBLEMES DE RATIONALITE

par

Anne BERTRAND

1. Le Théorème de Perron.

On dit qu'une matrice carrée B est primitive s'il existe un entier k tel que B^k ait tous ses coefficients strictement positifs. Le Théorème de PERRON, qui date du siècle dernier, affirme que :

THÉORÈME DE PERRON : *Toute matrice primitive B à coefficients positifs ou nuls admet une valeur propre λ strictement positive telle que pour toute autre valeur propre μ de B :*

$$|\mu| < \lambda.$$

Le nombre λ est dit valeur propre strictement dominante de B.

Ceci est vrai en particulier pour les matrices à coefficients strictement positifs, qui sont forcément primitives.

On dit qu'une matrice carrée d'ordre $B = (b_{ij})$ est réductible s'il existe une partition de $\{1, \ldots, n\}$ en deux ensembles non vides I et J tels que

$$\forall (i,j) \in I \times J \quad b_{ij} = 0.$$

Si cela n'est pas vrai B est dite irréductible. FROBENIUS a complété les résultats de PERRON en établissant que :

THÉORÈME DE FROBENIUS : *Soit B une matrice carrée irréductible à coefficients positifs ou nuls ; alors B admet une valeur propre réelle positive λ telle que toute autre valeur propre μ vérifie*

$$|\mu| \leq \lambda$$

et si $|\mu| = \lambda$, alors il existe une racine de l'unité $e^{2i\pi/h}$ telle que $\mu = e^{2i\pi/h}\lambda$; le spectre de B est invariant par rotation d'angle $\dfrac{2\pi}{h}$.

Exemples : la matrice $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ est primitive : son carré est $\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$ et ses valeurs propres sont $\dfrac{1+\sqrt{5}}{2}$ ($\sim 1,6$) et $\dfrac{1-\sqrt{5}}{2}$ ($\sim -0,6$).

La matrice $\begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$ est irréductible, la matrice $\begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$ ne l'est pas ($b_{ij} = 0$ si $(i,j) \in \{1,2\} \times \{3\}$).

Dans le cas où B est à coefficients dans $\mathbb{N}$ (c'est à ce cas précis que nous nous intéresserons), les valeurs propres de B sont des entiers algébriques racines du polynôme caractéristique de B ; si λ est valeur propre strictement dominante d'une matrice primitive B sur $\mathbb{N}$, les conjugués de λ sont aussi valeurs propres de B et donc tous les conjugués de λ distincts de λ sont en module strictement inférieur à λ. Douglas LIND a baptisé *Nombres de Perron* les entiers algébriques qui sont strictement supérieurs aux modules de leurs conjugués. On peut se poser la question suivante : quels sont exactement les nombres entiers algébriques qui sont valeur propre strictement dominante d'au moins une matrice primitive à coefficients dans $\mathbb{N}$? Et bien, ce sont exactement les nombres de PERRON comme le montre le théorème suivant :

THÉORÈME (LIND - HANDLEMAN, 1980-1984) : *Soit λ un nombre de Perron ; alors il existe une matrice primitive B à coefficients dans $\mathbb{N}$ dont λ est la valeur propre strictement dominante.*

Exemple : $\dfrac{1+\sqrt{5}}{2}$ est un Perron, mais par $\sqrt{2}$ dont le conjugué est $-\sqrt{2}$. Les démonstrations de LIND et HANDLEMAN sont de nature géométrique ; nous voulons présenter ici la trame d'une preuve algébrique basée sur des problèmes de rationalité (de langages et de séries).

2. Langages.

Soit A un alphabet fini, c'est à dire un ensemble fini de symboles ; soit A^* l'ensemble des mots sur A, c'est à dire des suites finies sur A (y compris le mot vide) ; on munit A^* du produit de concaténation (le concatené de $u_1 \cdots u_k$ et $v_1 \cdots v_h$ est $u_1 \cdots u_k\ v_1 \cdots v_h$) ; on appelle langage une partie de A^*.

Etant donné un langage L sur un alphabet A, on définit une relation d'équivalence sur les mots de A^* : $u \sim v$ si et seulement si

$$\forall a, b \in A^* \quad aub \in L \iff avb \in L$$

(u et v ont les mêmes contextes dans L).

Le langage L est dit rationnel si le nombre de classes de A^* modulo cette relation d'équivalence est fini. Par exemple, si $A = \{0,1\}$, si L_1 est l'ensemble des mots sur A dans lesquels n'apparaissent jamais deux 1 consécutifs ($L_1 = \{0,1,00,01,10,000,001,010,100,101,\ldots\}$) alors L_1 est rationnel car les classes modulo L_1 ont pour système de représentants dans A^* :

$$\begin{array}{ll} 0 & (a0b \in L_1 \text{ si } a,b \in L_1) \\ 1 & (a1b \in L_1 \text{ si } a,b \in L_1, a \text{ finit et } b \text{ débute par } 0) \\ 01 & (a01b \in L_1 \text{ si } a,b \in L_1, b \text{ commence par } 0) \\ 10 & (a10b \in L_1 \text{ si } a,b \in L_1 \text{ et } a \text{ finit par } 0) \\ 11 & (a11b \text{ n'est jamais dans } L_1). \end{array}$$

L'ensemble des langages rationnels est aussi la plus petite classe de langages contenant les langages finis et stables pour la réunion, le "produit" $L_1L_2 = \{uv; u \in L_1, v \in L_2\}$ et par l'opération "étoile" : $L^* = L \cup L^2 \cup L^3 \cup \cdots$ (ceci constitue le Théorème de Kleene).

Exemple : si $C = \{0,10\}$, alors C^* est l'ensemble des mots de L_1 finissant par 0 ; on remarque que

$$L_1 = C^*U(C^*1).$$

3. Matrices sur $\mathbb{N}$ et systèmes dynamiques.

Un langage L est dit factoriel si, dès que uvw est dans L, v y est aussi ; il est dit prolongeable si pour tout u appartenant à L on peut trouver des mots de A^*, a et b, tels que aub soit dans L ; il est dit transitif si, dès que u et v sont dans L, on peut trouver un mot w de A^* tel que uwv soit dans L.

Le langage A^*, le langage L_1 du §.2 possèdent ces trois propriétés.

Systèmes dynamiques symboliques. Considérons l'ensemble $A^{\mathbf{N}} = \{a_1a_2a_3\cdots;\ a_i \in A\}$ des suites sur A, muni de la transformation T dite shift : $T(a_1a_2a_3\cdots) = (a_2a_3a_4\cdots)$. Etant donné un langage L factoriel et prolongeable on appelle système dynamique symbolique S associé à L l'ensemble $S = \{a_1a_2a_3\cdots; \forall n,p,\ a_{n+1}\cdots a_{n+p} \in L\}$ dont on vérifie qu'il est invariant par T. Lorsque L est rationnel on dit que L est un système sofique ; le système est dit transitif si le langage L est transitif et il est dit mélangeant s'il existe un entier k tel que pour tout $h \geq k$ et pour tout couple u,v de mots de L (apparaissant donc dans les suites de S) on peut trouver un mot w de longueur h (la longueur d'un mot est le nombre de lettres qui le composent) tel que uwv soit encore dans L.

Si, par exemple, $L = L_1$, S_1 est l'ensemble des suites de 0 et 1 dans lesquelles on n'observe jamais deux 1 consécutifs.

Les systèmes de MARKOV sont un cas particulier des systèmes sofiques : soit P un ensemble fini de mots, et L le langage formé par les mots ne contenant aucun mot de P ; il est facile de voir qu'il existe un entier k et un ensemble fini M de mots de longueur $k+1$ tel que le système dynamique associé à L soit $S = \{a_1 a_2 \cdots ; \forall n,\ a_n \cdots a_{n+k} \in M\}$: la connaissance des k lettres $a_n \cdots a_{n+k-1}$ détermine les valeurs possibles de a_{n+k} ; de tels langages sont bien sûr rationnels. Par exemple le système S_1 est un système de MARKOV mélangeant d'ordre 1 pour lequel $M = \{00, 01, 10\}$. On peut associer à ce système dynamique la matrice suivante :

$$\begin{pmatrix} b_{00} & b_{10} \\ b_{01} & b_{11} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} : \begin{pmatrix} 1 \text{ car } 00 \in M & 1 \text{ car } 10 \in M \\ 1 \text{ car } 01 \in M & 0 \text{ car } 11 \in M \end{pmatrix}$$

Autre exemple : considérons le système d'ordre 2 dans lequel 111 n'apparaît jamais ; on peut lui associer la matrice d'ordre 4 sur $\mathbb{N}$:

$$\begin{pmatrix} b_{00,00} & b_{00,01} & b_{00,10} & b_{00,11} \\ b_{01,10} & b_{01,01} & b_{01,10} & b_{01,11} \\ b_{10,00} & b_{10,01} & b_{10,10} & b_{10,11} \\ b_{11,00} & b_{11,01} & b_{11,10} & b_{11,11} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

dans laquelle $b_{c_1c_2,d_1d_2} = 1$ s'il existe un mot $u_1u_2u_3$ de $L \cap A^3$ tel que $u_1u_2 = c_1c_2$ et $u_2u_3 = d_1d_2$; $b_{c_1c_2,d_1d_2} = 0$ sinon. De même, à tout système de MARKOV d'ordre k sur un alphabet de p lettres on associe la matrice carrée d'ordre p^k $b = (b_{c_1 \cdots c_k, d_1 \cdots d_k})$ où $b_{c_1 \cdots c_k, d_1 \cdots d_k}$ vaut 1 si $d_1 \cdots d_{k-1} = c_2 \cdots c_k$ et $d_1 \cdots d_k \in M$ et 0 sinon. Lorsque le système est mélangeant la matrice B est primitive ; d'une façon générale et par un procédé plus sophistiqué (sic), *à tout système sofique mélangeant on peut associer une matrice primitive B sur $\mathbb{N}$.*

Que représente pour le système la valeur propre λ strictement dominante de B ? Remarquons que le nombre de mots de longueur $k+1$ apparaissant dans une chaîne de MARKOV est égal à la somme des coefficients de la matrice B ; de même, le nombre de mots de longueur $k+n$ apparaissant dans une chaîne de MARKOV est égal à la somme des coefficients de la matrice B^n ; par exemple, pour le système L_1 avec la matrice $B = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$, $B^2 = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$, $B^3 = \begin{pmatrix} 3 & 2 \\ 2 & 1 \end{pmatrix}$ ... ; la somme des coefficients de B vaut 3, celle de B^2, 5, celle de B^3, 8 ; or il y a trois mots de longueur deux (00,01,10), cinq mots de longueur 3 (000,001,010,100,101) et huit mots de longueur 4 (0000,0001,0010,0100,0101,1000,1001,1010). Les 2-mots sont ainsi formés à partir des mots de longueur 1 :

$$0 \xrightarrow{b_{00}=1} 00$$

ou bien

$$0 \xrightarrow{b_{01}=1} 01$$

et

$$1 \xrightarrow{b_{10}=1} 10$$

Les 3-mots sont obtenus comme suit :

$$0 \xrightarrow{b_{00}=1} 00 \xrightarrow{b_{00}=1} 000$$

ou bien

$$0 \xrightarrow{b_{01}=1} 01 \xrightarrow{b_{10}=1} 010$$

et

$$1 \xrightarrow{b_{10}=1} 10 \xrightarrow{b_{00}=1} 100$$

ou bien

$$1 \xrightarrow{b_{10}=1} 10 \xrightarrow{b_{01}=1} 101$$

et

$$B^2 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1.1+1.1 & 1.1 \\ 1.1 & 1.1 \end{pmatrix}$$

$$= \begin{pmatrix} b_{0,0} & b_{0,0} + b_{0,1} & b_{1,0} & b_{0,0} & b_{0,1} + b_{0,1} & b_{1,1} \\ b_{1,0} & b_{0,0} + b_{1,1} & b_{1,0} & b_{1,0} & b_{0,1} + b_{1,1} & b_{1,1} \end{pmatrix}$$

qui correspondent aux mots :

$$\begin{pmatrix} 000 & \text{et} & 010 & 001 \\ 100 & & & 101 \end{pmatrix}$$

Or la somme des coefficients de B^n est de l'ordre de λ^n ; il s'ensuit que si ω_n désigne le nombre de mots de longueur n du langage associé à S alors

$$\lim_{n\to\infty} \sqrt[n]{\omega_n} = \lambda \, .$$

Dans notre exemple ou $L = L_1$, $\lambda = \dfrac{1+\sqrt{5}}{2}$ et $(\omega_1, \omega_2, \omega_3 \ldots) = (2, 3, 5, 8 \ldots)$ où l'on retrouve la suite de FIBONACCI : ω_n peut se mettre sous la forme

$$\alpha\left(\frac{1+\sqrt{5}}{2}\right)^n + B\left(\frac{1-\sqrt{5}}{2}\right)^n \quad \sim \alpha\left(\frac{1+\sqrt{5}}{2}\right)^n.$$

Le nombre *Log* λ est dit *entropie* du système dynamique ; on définit de même l'entropie de tout système dynamique symbolique.

Pour terminer ce paragraphe, donnons l'exemple d'un système sofique qui n'est pas un système de Markov : soit

$$S_2 = \{a_1 a_2 \ldots \ ; \ a_i \in \{0,1,2\} \ ; \ \forall i, j : a_i \ldots a_{i+j} \neq 211 \ldots 12\}$$

sur l'alphabet $\{0,1,2\}$. Ce n'est pas un système de Markov car le nombre de mots exclus (les $211 \ldots 12$) ne peut être fini et si l'on voit arriver $11 \ldots 1$, il faut aller regarder vers la gauche, à une distance qui peut être aussi grande qu'on veut, le premier terme différent de 1 pour savoir si après on peut mettre 2 où si l'on doit se limiter à 0 ou 1. Par contre il est sofique (les classes modulo L_2 sont représentées par (0,1,21,20,121,02,12). L'entropie du système est Log $\left(\dfrac{3+\sqrt{5}}{2}\right)$.

Bien entendu, si Log λ est l'entropie d'un tel système, alors λ est toujours un nombre de Perron et *pour prouver le théorème de Lind, il suffit de montrer qu'à tout nombre de Perron on peut associer un système sofique S dont l'entropie est* Log λ : λ *sera alors valeur propre strictement dominante de la matrice primitive B associée à S.*

4. Séries $\mathbb{N}$-rationnelles.

Considérons l'ensemble E des séries rationnelles $\sum_{n\geq 0} a_n X^n$ à coefficients dans $\mathbb{C}$; on dit qu'une série est propre si le coefficient a_0 est nul et on définit alors l'"étoile" S^* de la série propre $S = \sum_{n\geq 1} a_n X^n$ comme :

$$S^* = \frac{1}{1-S} = 1 + S + S^2 + \cdots + S^n + \cdots$$

Définissons maintenant l'ensemble des séries $\mathbb{N}$-rationnelles : on l'obtient à partir des polynômes (séries "finies") sur $\mathbb{N}$ comme l'ensemble des langages

rationnels à partir des langages finis : l'ensemble des séries $\mathbb{N}$-rationnelles est par définition le plus petit sous-ensemble de E contenant les polynômes à coefficients dans $\mathbb{N}$, stable par addition, par multiplication et par l'opération "étoile" appliquée aux séries propres.

Remarque : si dans la définition ci-dessus on remplace $\mathbb{N}$ par $\mathbb{C}$ on obtient l'ensemble des fractions rationnelles habituelles sans pôle en 0 ; si on remplace $\mathbb{N}$ par $\mathbb{Z}$ on obtient l'ensemble des fractions rationnelles s'écrivant $\dfrac{P(X)}{Q(X)}$ avec P et Q dans $\mathbb{Z}[X]$ et $Q(0) = 1$. Une série entière à coefficients dans $\mathbb{Z}$ est rationnelle si et seulement si ses coefficients vérifient une relation de récurrence linéaire à coefficients dans $\mathbb{Z}$.

Une série $\mathbb{N}$-rationnelle est forcément $\mathbb{Z}$-rationnelle et à coefficient dans $\mathbb{N}$; mais toutes les séries $\mathbb{Z}$-rationnelles à coefficients dans $\mathbb{N}$ ne sont pas $\mathbb{N}$-rationnelles :

THÉORÈME (SOITTOLA) : *Une série $\mathbb{Z}$-rationnelle à coefficients dans $\mathbb{N}$ est $\mathbb{N}$-rationnelle si et seulement si elle est l'emboîtement de séries rationnelles possédant une racine strictement dominante*

Quelques explications : on dit que la série $V = v_0 + v_1X + v_2X^2 + \cdots$ est l'emboîtement des séries $S_0, \ldots, S_{p-1}$ si pour tout m, v_{mp+i} est le $m^{\text{ème}}$ coefficient de S_i : par exemple l'emboîtement de $1 + 3X + 9X^2 + \cdots$ et $14 + 2X + 2X^2 + \cdots$ est $1 + 14X + 3X^2 + 2X^3 + 9X^4 + 2X^5 + \cdots$

Mettons une série $\mathbb{Z}$-rationnelle V sous la forme $\dfrac{P}{Q}$ où P et Q sont des polynômes de $\mathbb{Z}[X]$ premiers entre eux avec $Q(0) = 1$; soit λ le rayon de convergence de la série : alors $\dfrac{1}{\lambda}$ est racine de Q et est inférieur ou égal aux modules des autres racines ; si $\dfrac{1}{\lambda}$ est strictement inférieur aux modules des autres racines de Q on dit que la série admet λ comme série strictement dominante ; λ est alors un nombre de Perron !

En plagiant la preuve de ce théorème on peut montrer que :

LEMME : *Soit λ un nombre de Perron ; alors il existe une série $\mathbb{N}$-rationnelle $\sum_{n\geq 1} a_n X^n$ telle que $1 = \dfrac{a_1}{\lambda} + \dfrac{a_2}{\lambda^2} + \cdots + \dfrac{a_n}{\lambda^n} + \cdots$; de plus on peut supposer que le PGCD des entiers n tels que $a_n \neq 0$ vaut 1.*

Comme les a_i sont ≥ 0 et le PGCD égal à 1, λ est racine strictement

dominante de la série

$$\frac{1}{1-(a_1X+a_2X^2+\cdots)}.$$

Exemples de séries $\mathbb{N}$*-rationnelles* : si L est un langage rationnel, si a_n désigne le nombre de mots de longueur n de L (la longueur d'un mot est par définition le nombre de mots qui le composent) alors la série $\sum_{n\geq 1} a_n X^n$ est $\mathbb{N}$-rationnelle.

5. Codes et systèmes dynamiques.

On appelle code sur un alphabet A un ensemble C de mots de A^* tels que si m,p,q,r sont des mots de C alors $mp = qr$ implique $m = q$ et $p = r$ (C engendre par concaténation un monoïde libre). Par exemple $\{0,10\}$ est un code ; $C_2 = \{0,1,20,210,2110,\ldots,21111\ldots10,\ldots\}$ en est un aussi ; $\{a,ab,ba\}$ n'en est pas car $aba = (ab)a = a(ba)$. Soit $C^* = \{m,m_2\ldots m_k; k = 1,2\ldots; m_i \in C\}$. Soit $L(C)$ l'ensemble des mots facteurs de mots de C^* (un mot q est facteur d'un mot r s'il existe deux mots u et v sur A tels que $r = uqv$) ; $L(C)$ est un langage factoriel prolongeable et transitif ; à ce langage on peut associer comme au §3 un système dynamique symbolique $S(C)$; par exemple si $C = \{0,12\}$, C^* est l'ensemble des mots commençant et finissant par 0 et ne comportant jamais deux 1 consécutifs ; $L(C)$ est le langage L_1 du §2. On peut montrer que si C est un langage rationnel le langage $L(C)$ est rationnel et $S(C)$ est sofique ; s'il est fini c'est un système de Markov (conditions suffisantes mais non nécessaires) ; soit c_n le nombre de mots de longueur n du code C : si le PGCD des entiers n avec $c_n \neq 0$ est 1, le système $S(C)$ est mélangeant (c'est le cas pour $C = \{0,10\}$; si $C = \{00,11\}$ le nombre de 0 entre 10 et 01 est toujours pair dans $L(C)$: il n'y a pas mélange). La série c_nX^n est $\mathbb{N}$-rationnelle si le code est rationnel. L'entropie du système est égale à Log λ où λ est le seul réel > 0 tel que

$$1 = \frac{c_1}{\lambda} + \frac{c_2}{\lambda^2} + \cdots$$

car le nombre de mots de longueur n de $L(C)$ est comparable au nombre de mots d_n de longueur n de C^* et

$$\sum_{n\geq 0} d_n X^n = \frac{1}{1-(c_1X+c_2X^2+c_3X^3+\cdots)}.$$

Si le système est mélangeant, λ est racine strictement dominante de $\sum d_nX^n$. Selon le §3 il existe une matrice primitive B dont λ est la valeur propre strictement dominante.

Pour prouver le Théorème de Lind, nous allons donc associer à tout nombre de Perron λ un code C de PGCD 1 tel que si c_n est le nombre de mots de longueur n de C alors $1 = \frac{c_1}{\lambda} + \frac{c_2}{\lambda^2} + \cdots$ Pour cela il suffit de prouver le lemme :

LEMME : *A toute série propre* $\mathbb{N}$*-rationnelle* $\sum_{n\geq 1} c_n X^n$ *on peut associer un code rationnel* C *comportant* c_n *mot de longueur* n.

Ceci se montre en prouvant que l'ensemble des séries "génératrices" des codes $\sum_{n\geq 1} c_n X^n$ contient les polynômes sur $\mathbb{N}$ (par exemple pour $3X + 2X^2 + X^3$ prendre un alphabet de 10 lettres $q_1 \ldots q_{10}$ et le code $\{a_1, a_2, a_3, a_4a_5, a_6a_7, a_8a_9a_{10}\}$ est stable pour l'addition (prendre la réunion de deux codes sur deux alphabets différents), par multiplication (concatener deux codes sur deux alphabets distincts) et par l'opération étoile (au coefficient constant près !).

Or la plus petite classe possédant ces propriétés est celle des séries $\mathbb{N}$-rationnelles propres.

6. Trame de la preuve du théorème.

Prenons un nombre de Perron λ ; trouvons une série $\mathbb{N}$-rationnelle $\sum_{n\geq 1} c_n X^n$ telle que $1 = \frac{c_1}{\lambda} + \cdots + \frac{c_n}{\lambda^n} + \cdots$ et telle que le PGCD des entiers n avec $c_n \neq 0$ soit 1 ; à cette série associons un code C rationnel, à ce code associons un système dynamique sofique mélangeant S ; à ce système associons une matrice primitive B sur $\mathbb{N}$; λ est alors valeur propre strictement dominante de B. ∎

N.B. Remarquons qu'on peut choisir B à coefficient 0 ou 1 ; par ailleurs les conjugués de λ sont valeurs propres de B mais en général B en a d'autres : ces "parasites" sont-ils toujours les mêmes ? y-a-t-il des "conjugués" sur $\mathbb{N}$? Quelle est la taille minimale de B ? autant de questions sans réponse.

REFERENCES

[1] LIND D., *The entropies of topological Markov shifts and a related class of algebraic integers. Ergodic Th. and Dynam. Systems* (1984) 283-300.

[2] BERSTEL B.J. et PERRIN D., *Theory of codes*, Orlando Academic Press, (1985).

[3] WEISS B., *Subshifts of finite type and sofic systems. Monats. Math.* 77 (1973) 462-474.

[4] WILLIAMS R.F, *Classification of subshifts of finite type.* Ann. of Math. 98 (1973), 120-153 and 99 (1974), 380-381.

[5] BLANCHARD F. et HANSEL G., *Systèmes codés.* Theor. Comp. Sci. North Holland 44 (1986) 17-44.

[6] BERSTEL B.J. et REUTENAUER C., *Les séries rationnelles et leurs langages.* Masson, Paris (1984).

Anne BERTRAND
Département de Mathématiques
Université de Poitiers
40, avenue du Recteur Pineau
86022 POITIERS

(Reçu le 23 Novembre 1989)

Astérisque

MIREILLE CAR

Le problème de Waring pour les corps de fonctions

Astérisque, tome 198-199-200 (1991), p. 77-82

<http://www.numdam.org/item?id=AST_1991__198-199-200__77_0>

LE PROBLEME DE WARING POUR LES CORPS DE FONCTIONS

Mireille CAR

Soit F_q le corps fini à q éléments. L'analogie entre l'anneau Z et l'anneau $F_q[X]$ a conduit à l'étude de nombreux problèmes additifs dans $F_q[X]$ et notemment à l'étude du problème de Waring. Sous sa forme la plus générale, le problème de Waring peut être posé dans un anneau A quelconque. Il s'énonce ainsi. Soit un entier $k \geq 2$. Soit $W(k, A)$ le plus petit entier m, s'il existe, tel que pour tout $a \in A$, l'équation

$$a = a_1^k + \cdots + a_m^k$$

admette une solution $(a_1, \cdots, a_m) \in A^m$. Récemment, L.N. VASERSTEIN a donné une majoration des nombres $W(k, A)$ pour différents anneaux A et pour des algèbres A sur un corps fini F_q, [6], [7]. Cette majoration est de l'ordre de k^3 pour un entier k non divisible par la caractéristique du corps F_q lorsque A est une algèbre sur F_q. Cette majoration est valable lorsque A est l'anneau $F_q[X]$ ou lorsque A est l'anneau des S-entiers d'un corps de fonctions algébriques sur F_q, objet de ce travail.

Toutefois, les problèmes qui m'intéressent sont d'une nature différente comme le montre le cas simple où $A = F_q[X]$.

1 Le problème de Waring pour $F_q[X]$

Pour $A \in F_q[X]$, on s'intéresse aux solutions $(A_1, \cdots, A_m) \in F_q[X]^m$ de l'équation

$$(I.1) \quad A = A_1^k + \cdots + A_m^k$$

réalisant les conditions de degré les plus restrictives possibles, c'est à dire telles que

$$(I.2) \quad degA_i \leq n \qquad \text{si} \qquad k(n-1) < degA \leq kn.$$

On désigne par $g(k)$, resp. $G(k)$, le plus petit entier m s'il existe, tel que pour tout $A \in F_q[X]$, l'équation (I.1) ait une solution vérifiant (I.2), resp. tel que pour tout $A \in F_q[X]$ de degré assez grand, (I.1) ait une solution vérifiant (I.2).

Par une méthode analogue à la méthode du cercle on établit une estimation asymptotique du nombre $r_m(A)$ de solutions de l'équation (I.1) assujetties aux conditions (I.2) valable pour des entiers $k < p$, p désignant la caractéristique du corps F_q. On obtient alors pour $k < p$:

$$(I.3) \quad G(k) \leq k2^{k-1} + 1 \quad , cf \cdot [1], [3],$$

$$(I.4) \quad G(2) \leq 4 \qquad et \qquad G(2) = 3 \quad \text{si} \quad q \geq 53, cf \cdot [2] \cdot$$

On a peu de renseignements sur $g(k)$. Jean-Pierre SERRE a établi que $g(2) = 3$ pour $q \geq 5$. Ce résultat n'a pas été publié.

2 Le problème de Waring pour les anneaux d'entiers des corps de fonctions algébriques sur F_q.

Soit L une extension algébrique finie séparable du corps $F_q(X)$.

L'analogie entre corps de nombres et corps de fonctions algébriques sur F_q laissait espérer que les méthodes introduites par C.L. SIEGEL, cf.[4], [5], pour l'étude du problème de Waring dans les corps de nombres pouvaient être adaptées à l'anneau B fermeture intégrale de $F_q[X]$ dans L. Cet espoir était raisonnable. La seule difficulté, en dehors des difficultés techniques, était de bien poser le problème. Bien poser le problème consiste à avoir des conditions faisant intervenir tous les prolongements à L de la valuation à l'infini v de $F_q(X)$ définie par $v(A/B) = degB - degA$ si A et B sont des polynômes non nuls.

Pour exploiter l'analogie entre L et les corps de nombres, on fait une distrinction entre valuations P-adiques de L et valuations prolongeant la valuation à l'infini v. Cette distinction est artificielle. En effet, soit S un ensemble fini non vide de valuations de L, soit O_S l'ensemble des S-entiers de L, i.e. l'ensemble des $a \in L$ tels que $w(a) \geq 0$ pour toute valuation $w \notin S$. Les résultats établis pour l'anneau B se généralisent à l'anneau O_S.

On s'intéresse aux représentations de $b \in O_S$ comme somme

$$(II.1) \qquad b = b_1^k + \cdots + b_m^k,$$

telles que

$$(II.2) \qquad w(b_j) \geq [w(b)/k]$$

pour tout $j \in \{1, \cdots, m\}$, tout $w \in S$.

On note $r_m(b)$ le nombre de ces représentations et on désigne par $G(k)$ le plus petit entier m, s'il existe tel que $r_m(b) > 0$ pour tout les $b \in O_S$ pour lesquels la somme

$$(II.3) \qquad h(b) = \sum_{w \in S} f_w w(b)$$

est assez petite, f_w désignant le degré de la place w.

Dans le cas où $L = F_q(X)$ et S est réduit à la seule valuation à l'infini v, $O_S = F_q[X]$, la condition (II.2) se réduit à la condition (I.2) et $h(b) = -deg(b)$. On retrouve le problème de Waring posé au paragraphe I. Dans le cas où S est l'ensemble $\{w_1, \cdots, w_r\}$ de tous les prolongements de w à L, $O_S = B$, et, pour $b \in B$, la condition (II.2) s'écrit aussi

$$(II.2)' \qquad -w_i(b_j) \leq N_i \quad \text{si} \quad k(N_i - 1) < -w_i(b) \leq kN_i,$$

ce qui est une généralisation de la condition (I.2).

On a le théorème suivant :

Théorème 2.1 *Pour $2 \leq k < p$, on a*

$$(II.4) \qquad G(k) \leq 1 + k2^{k-1} Card(S) \ .$$

La démonstration de ce théorème est basée sur la méthode du cercle. Elle est très longue. J'indique seulement les étapes importantes. Tout d'abord on démontre qu'il existe $y \in L$ possédant la propriété suivante : $F_q[y]$ est inclus dans l'anneau de valuation de w si et seulement si $w \notin S$, ce qui prouve que y est transcendant sur F_q, que L est une extension algébrique de $F_q(y)$ nécessairement finie et que O_S est la clôture entière de l'anneau $F_q[y]$. Il suffit donc de faire la démonstration lorsque $S = \{w_1, \cdots, w_r\}$ et que $O_S = B$.

On se place dans le cas où $O_S = B$. Si $\vec{N} = (N_1, \cdots, N_r) \in Z^r$, si $A \in B$, on désigne par $R(m, \vec{N}, A)$ le nombre de solutions $(A_1, \cdots, A_m) \in B^m$ de l'équation

$$A = A_1^k + \cdots + A_m^k,$$

telles que

$$-w_i(A_j) \leq N_i,$$

pour tout $i = 1, \cdots, r$, tout $j = 1, \cdots, m$. Si $\vec{N} \in Z^r$ et $A \in B$ vérifient

$$(II.5) \qquad k(N_i - 1) < -w_i(A) \leq kN_i,$$

on a

$$r_m(A) = R(m, \vec{N}, A).$$

Pour $\vec{N} \in Z^r$, soit

$$(II.6) \qquad s(\vec{N}) = \sum_{i=1}^{r} f_{w_i} N_i.$$

On note que lorsque $A \in B$ et $\vec{N} \in Z^r$ sont liés par (II.5) $s(\vec{N})$ tend vers $+\infty$ si et seulement si $h(A)$ tend vers $-\infty$. Pour démontrer le théorème on fixe un entier $m \geq 1 + k2^{k-1}Card(S)$ et on montre que pour tous les $A \in B$ pour lesquels la somme $s(\vec{N})$ est assez grande, on a $R(m, \vec{N}, A) > 0, \vec{N}$ et A étant toujours liés par (II.5). On ne sait pas obtenir d'estimation asymptotique des nombres $R(m, \vec{N}, A)$ pour tous les éléments A de B, mais seulement pour les éléments A vérifiant la condition supplémentaire

$$|f_{w_i} N_i - \frac{1}{r} s(\vec{N})|$$

borné pour tout i lorsque $s(\vec{N})$ tend vers $+\infty$. Pour de tels éléments, on obtient l'estimation suivante, valable pour tout nombre réel $a > 0$,

$$(II.7) \quad R(m,\vec{N},A) = C_m(A)q^{(m-k)s(\vec{N})} + 0(q^{s(\vec{N})(1+m-k-m/2k)} + q^{ms(\vec{N})(1+a-2^{1-k}r^{-1})}),$$

où $C_m(A)$ définie par une série singulière est uniformément minorée par une constante strictement positive, les constantes impliquées par le symbole O dépendant de a.

De cette estimation, on déduit que $R(m,\vec{N},A) > 0$ lorsque $s(\vec{N})$ est assez grand et que A vérifie la condition supplémentaire exigée.

A l'aide du théorème de unités, on montre qu'il existe des constantes $a_1,\cdots,a_r$ ne dépendant que du corps L telles que pour tout $b \in B$ il existe une unité U de B possédant la propriété suivante : si $\vec{Y} \in Z^r$ et bU^k sont liés par la relation (II.5) , on a

$$|f_{w_i}Y_i - \frac{1}{r}s(\vec{Y})| \leq f_{w_i}a_i.$$

La relation (II.7) s'applique à bU^k et $\vec{Y}$. Mais si B et $\vec{N}$ sont aussi liés par (II.5), la formule du produit donne l'égalité

$$s(\vec{Y}) = s(\vec{N}),$$

on a aussi

$$R(m,\vec{N},b) = R(m,\vec{Y},bU^k)$$

et on a $R(m,\vec{N},b) > 0$ dès que $s(\vec{N}) = s(\vec{Y})$ est assez grand, d'où le résultat annoncé.

Pour obtenir l'estimation (II.7) on majore des sommes de caractères par la méthode de Weyl. Cette méthode fait appraitre un facteur $k!$ qui conduit à la majoration triviale lorsque $k \geq p$, d'où la restriction $k < p$.

Références

[1] M.CAR. Le problème de Waring pour l'anneau des polynômes sur un corps fini. C.R.A.S., Paris, t. 273, 19 juillet 1971, p. 141-144.

[2] M.CAR. Sommes de carrés dans $F_q[X]$. Dissertationes Mathematicae, 215, VARSOVIE, (1983).

[3] R.M.KUBOTA. Waring's problem for $F_q[X]$. Dissertationes Mathematicae, 117, VARSOVIE, (1974).

[4] C.L.SIEGEL. Generalization of Waring's problem to algebraic number fields. Amer. J. Math. 66, (1944), p. 122-136.

[5] C.L.SIEGEL. Sums of mth. powers of algebraic integers. Ann. of Math. 46, (1945), p. 313-339.

[6] L.N.VASERSTEIN. Waring's problem for commutative rings. J. Number theory 26, (1987), p. 299-307.

[7] L.N.VASERSTEIN. Waring's problem for algebras over fields. J. Number Theory 26, (1987), p. 286-298.

Mireille CAR
URA – 225
Faculté de St-Jérôme
Av. Normandie Niemen
13013 MARSEILLE

(reçu le 1er novembre 1989)

Astérisque

JØRGEN CHERLY

Sommes d'exponentielles cubiques dans l'anneau des polynomes en une variable sur le corps à 2 éléments, et application au problème de Waring

Astérisque, tome 198-199-200 (1991), p. 83-96

<http://www.numdam.org/item?id=AST_1991__198-199-200__83_0>

SOMMES D'EXPONENTIELLES CUBIQUES DANS L'ANNEAU DES POLYNOMES EN UNE VARIABLE SUR LE CORPS A 2 ELEMENTS, ET APPLICATION AU PROBLEME DE WARING

par

Jørgen CHERLY

En 1770, Waring a énoncé que tout nombre entier (positif) est somme de 4 carrés, 9 cubes, 19 bicarrés. Quelques années plus tard, il a étendu son affirmation au cas des puissances supérieures ; c'était le début d'une longue succession de variations sur le thème.

Bien que la touche finale du problème original ait été donnée - encore est-ce tout récemment en 1986, par les efforts conjoints de Balasubramanian, Deshouillers et Dress que le problème de Waring pour les bicarrés a été résolu - de nombreuses questions restent encore en suspens.

L'une des variantes consiste à étudier l'ensemble des sommes de puissances k-ièmes dans l'anneau $\mathbb{F}_q[X]$ des polynômes en une indéterminée sur le corps fini $\mathbb{F}_q$, anneau qui partage de nombreuses propriétés arithmétiques avec $\mathbb{Z}$. Les travaux de Matthews (1966), Kubota (1971) et Car (1971) conduisent à des résultats dont nous citons le dernier en date, qui est le meilleur possible concernant les restrictions imposées aux degrés des termes.

Tout élément M de $\mathbb{F}_q[X]$ de degré suffisamment grand peut s'écrire sous la forme

$$M = M_1^k + \cdots + M_s^k$$

où $s = \min(k2^{k-1} + 1, 2[k(k-1)\log 2] + 2k + 3)$ *et* $\deg M_i < \frac{1}{k}\deg M + 1$, *à la condition que k soit inférieur à la caractéristique de $\mathbb{F}_q$.*

Ce travail a pour but d'apporter une première pierre à l'étude du cas où le degré est supérieur à la caractéristique de $\mathbb{F}_q$. Nous montrons le résultat suivant :

THÉORÈME I : *Tout élément M de $\mathbb{F}_2[X]$ de degré assez grand qui est congru à 0 ou 1 modulo $1+X+X^2$ est somme d'au plus 18 cubes de polynômes de degré inférieur à $\frac{1}{3}\deg M + 1$.*

On remarque que la condition de congruence est indispensable, car toute somme de cubes dans $\mathbb{F}_2[X]$ est congrue à 0 ou 1 modulo $1+X+X^2$. Le résultat a surtout une importance qualitative (nombre de termes finis) la valeur 18 n'est sûrement pas la meilleure possible.

La démonstration s'effectue en deux étapes ; la première partie, qui nous semble avoir un intérêt intrinsèque est l'estimation de sommes trigonométriques. La seconde partie est plus standard. On y met en oeuvre la "méthode du cercle" adaptée à l'anneau $\mathbb{F}_q[X]$ en suivant Carlitz. Pour cela, on introduit un caractère E sur le complété $\mathbb{F}_q((\frac{1}{X}))$ de $\mathbb{F}_q[X]$; le nombre de représentations de M en somme de s cubes prend une expression intégrale

$$R_s(M) = \int \Big(\sum_{\deg B \leq n} E(B^3 t) \Big)^s E(-Mt) dt$$

étendue à la boule unité de $\mathbb{F}_q((\frac{1}{X}))$.

Le traitement traditionnel des "arcs mineurs" par la méthode de Weyl s'avère inefficace, car il repose sur des différentiations successives et introduit un facteur 3 ! qui est nul dans $\mathbb{F}_2$. On a recours au traitement suggéré par Vaughan en 1977 dans le cas archimédien. La difficulté que l'on rencontre dans le cas présent est l'impossibilité d'utiliser une quelconque variété de la méthode de la phase stationnaire ; en effet, les termes résiduels qui interviennent dans la formule sommatoire de Poisson, loin d'être négligeable, peuvent avoir un ordre de grandeur maximal, comme nous le montrons. Dans la première partie nous prouvons également que peu de ces termes sont en fait non nuls. On obtient ainsi l'équivalent du lemme de Weyl.

THÉORÈME II : *Il existe un réel K tel que, pour tout couple de polynômes G et H premiers entre eux ($H \neq 0$), pour tout entier n et tout $u \in \mathbb{F}_2((\frac{1}{X}))$ vérifiant $n + \deg H < v(u) \leq 2n + \deg H$ on ait*

$$\left| \sum_{B \in \mathbb{F}_2[X], \deg B \leq n} E(B^3(\frac{G}{H} + u)) \right| \leq K.2^{\frac{19}{20}n}$$

où $v(u)$ désigne la valuation de u.

Commentaire.

La constante K peut être explicitée : $K = 2^{2^{540}}$ convient. La méthode utilisée ne permet pas d'obtenir l'exposant $\frac{3}{4}$ du cas archimédien au lieu de $\frac{19}{20}$; sa limite théorique, atteinte dans plusieurs cas, est $\frac{5}{6}$.

Remarque : L'intérêt du résultat provient de ce que tout élément t de $\mathbb{F}_2((\frac{1}{X}))$ peut s'écrire sous la forme

$$(1) \qquad \begin{cases} t = \frac{G}{H} + u. \text{ avec } (G, H) = 1, 0 \leq \deg H \leq n \\ (\text{et } v(u) > n + \deg H) \end{cases}$$

et que la somme

$$\sum_{B \in \mathbb{F}_2[X], \deg B \leq n} E(B^3(\frac{G}{H} + u))$$

notée $S_n(t)$ peut être calculée explicitement si $v(u) > 2n + \deg H$.

PREMIERE PARTIE : Une inégalité du type de celle de Weyl pour les sommes trigonométriques cubiques dans $\mathbb{F}_2((\frac{1}{X}))$

a) Notation

On note $F_2((\frac{1}{X}))$ le complété du corps $F_2(X)$ des fractions rationnelles en une indéterminée sur F_2, pour la valuation 0-adique v telle que $v(\frac{A}{B}) =$

$\deg B - \deg A$ lorsque A et B sont des polynômes non nuls. Un élément non nul u de $F_2((\frac{1}{X}))$ peut être représenté comme un série de Laurent

$$\sum_{m=-\infty}^{-v(u)} u_m X^m \ , \text{ où } u_m \in F_2.$$

A la valuation v est associée la valeur absolue $|.|$ telle que pour tout u dans $F_2((\frac{1}{X}))$, on ait $|u| = 2^{-v(u)}$.

On note E le caractère du groupe additif $F_2((\frac{1}{X}))$, défini par

$$E(\sum u_m X^m) = \begin{cases} 1 & \text{si } u_{-1} = 0 \\ -1 & \text{si } u_{-1} = 1. \end{cases}$$

Pour tout entier n, on note $\mathcal{P}_n$ le groupe additif compact des éléments de $\mathbb{F}_2((\frac{1}{X}))$ de valuation supérieure à n.
On note dt la mesure de Haar normalisée sur la boule unité $\mathcal{P}_0$; que l'on notera également $\mathcal{P}$.

b)Un lemme sur les sommes trigonométriques cubiques dans $\mathbb{F}_2((\frac{1}{X}))$

Pour un entier positif k, notons g_k l'ensemble des polynômes de degré au plus égal à k.

LEMME 1 : *Soient* $\alpha, \alpha_1, \alpha_2, \alpha_3 \in \mathbb{F}_2((\frac{1}{X}))$ *et* $\phi(y) = \alpha y^3 + \alpha_1 y^2 + \alpha_2 y + \alpha_3$, $y \in \mathbb{F}_2((\frac{1}{X}))$ *nous obtenons la relation*

$$\left| \sum_{B \in g_k} E(\phi(B)) \right|^4 = \left| \sum_{B \in g_k} E(\phi(B)) \right|^2 \sum_{R \in g_k} \sum_{Q \in g_k} E(\alpha(R^2 Q + R Q^2)).$$

c)Formule sommatoire de Poisson et sommes de Gauss

Soit $t = \frac{G}{H} + u$ un élément de $\mathbb{F}_2((\frac{1}{X}))$ satisfaisant **(1)** et la condition **(2)** suivante

(2) $$v(u) \leq 2n + \deg H \ .$$

On définit la fonction f par la relation

(3) $$f(\eta) = \begin{cases} E(\eta^3 H^3 u) & \text{si } v(\eta) \geq \deg H - n \\ 0 & \text{sinon.} \end{cases}$$

La formule sommatoire de Poisson implique que l'on a

$$S_n(t) = \sum_{K \in \mathbb{F}_2[X]} \widehat{f}(K) S(G,H,K) \tag{4}$$

où $\widehat{f}(K)$ désigne la transformée de Fourier de f en K et où la somme de Gauss $S(G,H,K)$ est définie par

$$S(G,H,K) = \sum_{R(\mathrm{mod}\ H)} E\left[\frac{GR^3 + KR}{H}\right].$$

Il résulte du lemme 1 que si une somme de Gauss est non nulle, le carré de son module est égal à la somme double

$$\sum_{R(\mathrm{mod}\ H)} \sum_{Q(\mathrm{mod}\ H)} E\left(\frac{G(R^2Q + RQ^2)}{H}\right)$$

que nous noterons $T(G,H)$. Il résulte alors de (4) que l'on a

$$|S_n(t)| \leq T(G,H)^{\frac{1}{2}} \sum_{K \in \mathbb{F}_2[X]} |\widehat{f}(K)| \,. \tag{5}$$

Nous terminerons cette section en mentionnant la majoration suivante pour les sommes de Gauss ; on a

$$T(G,H) \leq 2^{\frac{14}{3}} |H|^{\frac{4}{3}} \tag{6}$$

où l'exposant de $|H|$, ainsi que la constante sont les meilleurs possibles. Cette majoration s'obtient en remarquant que l'on a

$$T(G, H_1H_2) = T(GH_2^2, H_1)T(GH_1^2, H_2)$$

dès que H_1 et H_2 sont premiers entre eux ; on calcule alors explicitement $T(G, P^\ell)$, où P est irréductible et ℓ entier.

d)Evaluation d'une transformée de Fourier

PROPOSITION 1 : *La fonction f étant définie par la relation* (3), *on a pour tout K dans $\mathbb{F}_2[X]$:*

$$|\widehat{f}(K)| \in \left\{0, 2^{[(v(H^3u)+2)/3]}\right\} \,. \tag{7}$$

Démonstration : A seule fin de simplifier les calculs, on se placera dans le cas où $v(u)$ est divisible par 3. Soit $\{w_j\}_{j\in J}$ un système de représentants de

$$\mathcal{P}_{\deg H-n-1}/\mathcal{P}_{\deg H-v(u)/3}.$$

On peut alors écrire :

$$\widehat{f}(K)=\sum_{j\in J} a_j I_j \quad \text{où} \quad a_j = E(w_j^3 H^3 u + K w_j) \text{ et}$$
$$I_j = \int_{v(\eta)\geq 1-\frac{v(u)}{3}+\deg H} E((\eta^2 w_j + \eta w_j^2)H^3 u + K\eta)d\eta$$

L'intégrale I_j vaut 0 ou $2^{v(H^3u)/3}$ et si $\widehat{f}(K)$ est non nul, il existe un et un seul indice $k \in J$ tel que pour tout $j \in J$

on a

$$I_j = \begin{cases} 2^{v(H^3u)/3} & \text{si } j = k \\ 0 & \text{si } j \neq k \end{cases}$$

d'où la proposition.

e) Démonstration du théorème II dans le cas où $v(u) > 3\deg H$

On indique comment établir une version forte du théorème, dans le cas où l'élément $t = \dfrac{G}{H} + u$ est tel que l'on ait :

$$\max(n+\deg H, 3\deg H) < v(u) \leq 2n + \deg H \quad (G,H) = 1, 0 \leq \deg H \leq n\ .$$

THEOREME A : *Sous les conditions précisées ci-dessus, on a :*

$$\left|S_n\left(\frac{G}{H}+u\right)\right| \leq 2^4 . 2^{\frac{5n}{6}}\ .$$

Démonstration : D'après les relations **(5) (6)**, et **(7)** nous avons :

$$|S_n(t)| \leq 2^{\frac{7}{3}} |H|^{\frac{2}{3}} \sum_{\substack{K\in \mathbb{F}[X] \\ \widehat{f}(K)\neq 0}} 2^{[(v(H^3u)+2)/3]}\ .$$

Il ne nous reste plus qu'à majorer le cardinal des K tels que $\widehat{f}(K) \neq 0$.
Les ensembles $B + \mathcal{P}$ où $B \in \mathbb{F}_2[X]$, $\deg B \leq n - \deg H$ forment une partition

de $\mathcal{P}_{\deg H-n-1}$.
Nous avons donc d'après la condition $v(u) > 3\deg H$:

$$\widehat{f}(K) = \int_{v(\eta)\geq \deg H-n} E(\eta^3 H^3 u)E(K\eta)d\eta = \sum_{\deg B\leq n-\deg H} E(B^3H^3u)\int_{\mathcal{P}} E((\eta^2 B+\eta B^2)H^3u+K\eta)d\eta\ .$$

On peut donc majorer le cardinal des K tel que $\widehat{f}(K)$ soit non nul par le nombre des polynômes K tel qu'il existe

$$B\in \mathbb{F}_2[X],\ \deg B\leq n-\deg H \text{ avec } \int_{\mathcal{P}} E((\eta^2B+\eta B^2)H^3u+K\eta)d\eta$$

non nulle.

Or ce nombre peut être évalué explicitement. Il vaut $2^{n-\deg H+1-[(v(H^3u)+1)/2]}$.
Le théorème A en résulte.

f) Démonstration du théorème II dans le cas où $v(u)\leq 3\deg H$

On considère dans toute cette section un élément $t=\dfrac{G}{H}+u$ de $\mathbb{F}_2((\dfrac{1}{X}))$ tel que l'on ait

$$\text{(8)}\qquad \begin{cases} n+\deg H < v(u)\leq 3\deg H \\ (G,H)=1\ ,\ 0\leq \deg H\leq n \end{cases}$$

Introduisons maintenant la fonction arithmétique multiplicative Φ de $\mathbb{F}_2[X]$ dans lui-même, tel que, pour P irréductible, on ait

$$\text{(9)}\qquad \Phi(P^\ell)=\begin{cases} P^{[(\ell+1)/3]} & \text{si } \ell\neq 2 \\ P^2 & \text{si } \ell=2 \end{cases}$$

Cette fonction s'introduira de façon naturelle dans notre étude (cf. Proposition 3). Notre but dans cette section est d'établir le résultat suivant :
THÉORÈME B : *Sous les conditions* (8), *on a pour*

$$n\geq 2^{541}\qquad |S_n(t)|\leq 2^3\ .2^{\frac{19}{20}n}\ .$$

Démonstration : Nous allons distinguer deux cas :

1er cas : $|\Phi(H)| \leq |H|^{\frac{1}{5}}$

et

2ème cas : $|\Phi(H)| > |H|^{\frac{1}{5}}$

Démonstration du 1er cas :

Nous partons de la relation **(5)**. D'après la condition $v(u) \leq 3 \deg H$ il découle du théorème de Plancherel

$$\sum_{K \in \mathbb{F}_2[X]} |\widehat{f}(K)|^2 = 2^{n+1-\deg H} .$$

D'où

$$|S_n(t)| \leq T(G,H)^{\frac{1}{2}} \cdot 2^{n+1-[(v(u)+2)/3]} \tag{10}$$

Pour majorer $T(G,H)$ dans la relation **(10)** nous avons besoin du résultat suivant dû à Georges Rhin.

LEMME 2 : *Soit $Q \in \mathbb{F}_2[X]$ de degré $\chi \geq 2$. Le nombre $r = r(Q)$ de polynômes irréductibles qui divisent Q, vérifie l'inégalité*

$$r \leq \frac{3\chi \log 2}{\log \chi} . \tag{11}$$

Par des méthodes purement arithmétiques, en appliquant :

* d'une part, la définition de $\Phi(H)$ et les résultats concernant le module des sommes de Gauss $S(G,H,K)$,
* d'autre part, le résultat **(11)** de Georges Rhin,

nous obtenons la proposition suivante :

PROPOSITION 2 : *Soient $H \in \mathbb{F}_2[X]$ et $|\Phi(H)| \leq |H|^{1/5}$ alors :*

$$T(G,H) \leq 2^{\frac{14}{3}} |H|^{\frac{11}{9} + \frac{6 \log 2}{\log \deg H}} .$$

Ainsi, pour $|\Phi(H)| \leq |H|^{\frac{1}{5}}$ le théorème B résulte de la relation **(10)** et de la proposition 2.

Démonstration du 2ème cas :

La somme $S_n(t)$ peut s'écrire

$$(12)\quad S_n(t) = \sum_{\deg L \le n - \deg H} E(L^3 H^3 u) \sum_{\deg R < \deg H} E\left(R^3\left(\frac{G}{H} + u\right)\right) E(R^2 L H u) E(R L^2 H^2 u)$$

D'après le lemme 1 nous avons la majoration suivante :

$$(13)\quad |S_n(t)| \le 2^{n+1-\deg H} T(G,H,u)^{\frac{1}{2}}$$

où

$$(14)\quad T(G,H,u) = \sum_{\deg R < \deg H} \sum_{\deg Q < \deg H} E\left(\left(\frac{G}{H} + u\right)(R^2 Q + R Q^2)\right) .$$

Nous allons majorer $T(G,H,u)$ en considérant séparément les trois cas suivants. En fait nous avons divisé l'intervalle $n + \deg H < v(u) \le 3 \deg H$ en trois intervalles distincts qui varient en fonction du degré de $\Phi(H)$. Les intervalles considérés peuvent être vides.

cas (a) $\quad n + \deg H < v(u) \le 3 \deg \Phi(H)$

cas (b) $\quad 3 \deg \Phi(H) + 1 \le v(u) \le 2 \deg H + \deg \Phi(H) - 2$

cas (c) $\quad 2 \deg H + \deg \Phi(H) - 2 < v(u) \le 3 \deg H$

on obtient :

$$(15)\quad T(G,H,u) \le \begin{cases} \dfrac{|H|^3}{2^{2[(v(u)+2)/3]}} & \text{si } (a) \\ \dfrac{|H|^3}{2^{[(v(u)+\deg \Phi(H)+1)/2]}} & \text{si } (b) \\ \dfrac{|H|^2}{|\Phi(H)|} & \text{si } (c) \end{cases}$$

La relation **(15)** se démontre à l'aide de la proposition suivante :

PROPOSITION 3 : *Soient* $(G,H) = 1$ *et* R *un polynôme de* $\mathbb{F}_2[X]$ *alors :*

$$\sum_{Q (\mathrm{mod}\ H)} E\left(\frac{G(R^2 Q + R Q^2)}{H}\right) = |H| \Longrightarrow \Phi(H) \mid R$$

où Φ désigne la fonction arithmétique multiplicative définie par la relation **(9)**.

Il résulte alors de **(13)** et **(15)** que l'on a

$$(16) \qquad |S_n(t)| \leq \begin{cases} 2^{n+1}\dfrac{|H|^{1/2}}{2^{2[(v(u)+2)/3]}} & \text{si (a)} \\ 2^{n+1}\dfrac{|H|^{1/2}}{2^{[(v(u)+\deg\Phi(H)+1)/2]/2}} & \text{si (b)} \\ 2^{n+1}\dfrac{1}{2^{\deg\Phi(H)/2}} & \text{si (c)} \end{cases}$$

Ainsi, pour $|\Phi(H)| > |H|^{\frac{1}{5}}$, le théorème B résulte de la relation **(16)**.

DEUXIEME PARTIE : Méthode du cercle dans $\mathbb{F}_2[X]$ (Application au problème de Waring)

a) Méthode du cercle dans $\mathbb{F}_2[X]$

Soit M un polynôme de $\mathbb{F}_2[X]$ de degré $\deg M \in]3(n-1), 3n]$. Alors le nombre de représentations de M, noté $R_s(M)$, comme somme $M = M_1^3 + M_2^3 + \cdots + M_s^3$ où pour $i = 1, 2, \ldots s, M_i \in \mathbb{F}_2[X]$ avec $\deg M_i \leq n$ est égale à l'intégrale

$$\int_{\mathcal{P}} S_n^s(t)E(Mt)dt \text{ où } S_n(t) = \sum_{\substack{\deg B \leq n \\ B \in \mathbb{F}_2[X]}} E(B^3 t) \ .$$

On a une partition de $\mathcal{P}$ analogue à une dissection de Farey du segment $[0,1]$.

$$\mathcal{P} = \bigcup_{\substack{H \in \mathbb{F}_2[X] \\ 0 \leq \deg H \leq n}} \bigcup_{\substack{G \in \mathbb{F}_2[X] \\ \deg G < \deg H \\ (G,H)=1}} \mathcal{M}_{G/H} \qquad \text{où}$$

$$\mathcal{M}_{G/H} = \left\{ t \in \mathcal{P} \mid v(t - \frac{G}{H}) > n + \deg H \right\} \ .$$

Notons qu'il n'y a que des arcs majeurs.

Posons

$$m = \bigcup_{\substack{H \in \mathbb{F}_2[X] \\ \deg H = 0}}^{n} \left(\bigcup_{\substack{(G,H)=1 \\ \deg G < \deg H}} \left\{ t \in P | t = \frac{G}{H} + u, n + \deg H < v(u) \leq 2n + \deg H \right\} \right)$$

$$\mathcal{M} = \mathcal{P} \setminus m$$

On obtient :

$$R_s(M) = \int_{\mathcal{M}} S_n^s(t)E(Mt)dt + \int_m S_n^s(t)E(Mt)dt \ .$$

b) Un équivalent de l'intégrale $\int_{\mathcal{M}}$ sur l'ensemble $\mathcal{M}$

L'intégrale $\int_{\mathcal{M}}$ sur l'ensemble $\mathcal{M}$ se calcule à l'aide du résultat suivant :

LEMME 3 : *Pour* $t = \dfrac{G}{H} + u \in \mathcal{M}$ *on a :*

$$S_n(\frac{G}{H}+u) = \begin{cases} S(G,H).2^{v(u)/3-\deg H} & \text{si } v(u) \equiv 0(3) \text{ et } v(u) \leq 3n+1 \\ 0 & \text{si } v(u) \equiv 1(3) \text{ et } v(u) \leq 3n+1 \\ S(G,H).2^{(v(u)+1)/3-\deg H} & \text{si } v(u) \equiv 2(3) \text{ et } v(u) \leq 3n+1 \end{cases}$$

$$S_n(\frac{G}{H}+u) = S(G,H).2^{n+1-\deg H} \ \textit{si} \ v(u) \geq 3n+2$$

où

$$S(G,H) = \sum_{R(\mathrm{mod}\ H)} E(\frac{G}{H}R^3) \ .$$

On a :

$$\int_{\mathcal{M}} S_n^s(t)E(Mt)dt = 2^{n(s-3)}(2^{s-1}-\varepsilon) \sum_{0\leq \deg H\leq n} \sum_{\substack{(G,H)=1 \\ \deg G<\deg H}} E(M\frac{G}{H})\frac{S(G,H)^s}{|H|^s}$$

$$\text{où } \varepsilon = \begin{cases} 0 & \text{si } \deg M = 3n \\ 1 & \text{si } \deg M = 3n-1 \text{ ou } \deg M = 3n-2. \end{cases}$$

L'intégrale $\int_{\mathcal{M}}$ fait apparaître les premiers termes d'une série singulière notée $G_s(M)$. On montrera le lemme suivant :

LEMME 4 : *Soit pour* $s \in \mathbb{N}$, *pour* $M \in \mathbb{F}_2[X]$:

$$G_s(M) = \sum_{\substack{H\in\mathbb{F}_2[X] \\ H\neq 0}} |H|^{-s} \sum_{\substack{G\in\mathbb{F}_2[X] \\ \deg G<\deg H \\ (G,H)=1}} [S(G,H)]^s E(M\frac{G}{H}).$$

Pour $s \geq 7$, pour M un polynôme congru à 0 ou 1 modulo $1 + X + X^2$ on a :

$$a_1(s) \leq G_s(M) \leq a_2(s) \text{ avec } \begin{cases} a_1(s) &= 2(1-2^{4-s})^3(1-2^{2-s/3}) \\ a_2(s) &= 2(1+2^{4-s})^3(1-2^{3-2s/3})/1-2^{2-s/3} \end{cases}$$

A l'aide du lemme 4 on démontre pour $s \geq 7$, pour M congru à 0 ou 1 modulo $1 + X + X^2$

$$\textbf{(17)} \qquad \int_{\mathcal{M}} S_n^s(t)E(Mt)dt = 2^{n(s-3)}(2^{s-1}-\varepsilon)G_s(M) + O_s(2^{n(s-3-\frac{s-6}{3})}).$$

c) Majoration de l'intégrale sur m

L'intégrale $\int_m$ sur l'ensemble m est majorée à l'aide du théorème II, l'équivalent du lemme de Weyl et l'identité de Parseval.

On a :

$$\textbf{(18)} \qquad \left|\int_m S_n^s(t)E(Mt)dt\right| \leq \max_{t\in m}\left|S_n^{s-2}(t)\right| \int_{\mathcal{P}} S_n^2(t)dt = O_s(2^{n(s-3-\frac{s-42}{20})})$$

d) Un équivalent de $R_s(M)$

On obtient ainsi d'après **(17)** et **(18)** un équivalent de $R_s(M)$ pour $s \geq 43$ et M congru à 0 ou 1 modulo $1 + X + X^2$

$$R_s(M) = 2^{n(s-3)}(2^{s-1}-\varepsilon)G_s(M) + O_s(2^{n(s-3-\frac{s-42}{20})}).$$

Démonstration du Théorème I :

On désigne par $K_{\ell,n-1}$ l'ensemble des polynômes $\mathcal{U} \in \mathbb{F}_2[X]$ du degré $(\leq 3(n-1))$ de la forme

$$\mathcal{U} = A_1^3 + \cdots + A_\ell^3, \deg A_i \leq n-1, i = 1, 2, \ldots \ell\ .$$

On a la minoration

$$\text{card } \mathcal{K}_{\ell,n-1} \geq b(\ell).2^{3n(1-(\frac{2}{3})^\ell)}$$

où

$$b(\ell) = 2^{3-2\ell-2(\frac{2}{3})^{\ell-1}}.$$

Soient $M \in \mathbb{F}_2[X]$ tel que $3(n-1) < \deg M \leq 3n$ et congru à 0 ou 1 modulo $1 + X + X^2$,

$$R_{\ell,n-1}(t) = \sum_{\mathcal{U}\in\mathcal{K}_{\ell,n-1}} E(t\,\mathcal{U}) \text{ et } J_{s,\ell}(M) = \int_{\mathcal{P}} S_n^s(t)R_{\ell,n-1}^2(t)E(Mt)dt\ .$$

L'intégrale $J_{s,\ell}(M)$ est égale au nombre de représentations de M sous la forme

$$M = M_1^3 + \cdots + M_s^3 + A_1^3 + \cdots + A_\ell^3 + B_1^3 + \cdots B_\ell^3$$

avec $\deg M_i \leq n$ pour $i = 1, 2, \ldots s$ $\deg A_k \leq n-1$ pour $k = 1, 2, \ldots \ell$ $\deg B_j \leq n-1$ pour $j = 1, 2, \ldots \ell$.

Le nombre de cubes dans cette présentation de M est inférieur ou égal à $s + 2\ell$.
Il suffit donc de minimaliser $s + 2\ell$ sous la condition : $J_{s,\ell}(M)$ strictement positive.
Les calculs se font de la même manière que pour obtenir un équivalent de $R_s(M)$.
On obtient la condition supplémentaire $s > \sup(6, 10.2^{\ell+1}/2^{\ell-1})$. Il ne nous reste qu'à minimaliser $s + 2\ell$ sous cette condition, ce qui donne pour résultat 18. D'où le théorème.

Je tiens à remercier Monsieur Jean-Marc Deshouillers de l'Université de Bordeaux I qui par ses nombreux conseils et encouragements m'a permis de mener à bien ce travail.

REFERENCES

[1] BALASUBRAMANIAN R., DESHOUILLERS J.M., DRESS F., Problème de Waring pour les bicarrés, *CRAS Paris*, série I, n°4 et n°5, **303** (1986).

[2] CAR M., Le problème de Waring pour l'anneau des polynômes sur un corps fini, *CRAS Paris*, Série A, **273** (1971), 141-144.

[3] CHERLY J., *Sommes d'exponentielles cubiques dans l'anneau des polynômes en une variable sur le corps à 2 éléments, et application au problème de Waring*, Thèse soutenue à l'Université de Bordeaux I le 27/10/89.

[4] KUBOTA R.M., Waring's problem for $\mathbb{F}_q[X]$, *Dissertationes Math.* **117** (1974).

[5] MATTHEWS K.R., *Waring's theorem for polynomials over a finite field*, Thèse soutenue à l'Université du Queensland, (1966).

[6] RHIN G., Répartition modulo I dans un corps de séries formelles sur un corps fini, *Dissertationes Math.* **95** (1972).

[7] VAUGHAN R.C., *The Hardy-Littlewood Method*, Cambridge tracts in Mathematics **80** (1981).

Jørgen CHERLY
Université de Bretagne Occidentale
Département de Mathématiques
et Informatique
6, avenue le Gorgeu
29287 BREST CEDEX

Astérisque

PAULA COHEN
JÜRGEN WOLFART

Monodromie des fonctions d'Appell, variétés abéliennes et plongement modulaire

Astérisque, tome 198-199-200 (1991), p. 97-105
<http://www.numdam.org/item?id=AST_1991__198-199-200__97_0>

MONODROMIE DES FONCTIONS D'APPELL, VARIETES ABELIENNES ET PLONGEMENT MODULAIRE

par

Paula COHEN et Jürgen WOLFART

1. Les groupes de Picard-Terada-Mostow-Deligne

Soient $0 < \mu_0, \ldots, \mu_4 < 1$ des nombres rationnels avec le dénominateur plus petit commun $d > 2$ satisfaisant à la condition

$$\sum_j \mu_j = 2 \tag{1}$$

Alors pour tout $x \neq y$, $x, y \in \mathbb{C} - \{0, 1\}$,

$$\omega := u^{-\mu_0}(u-1)^{-\mu_1}(u-x)^{-\mu_2}(u-y)^{-\mu_3}du = \frac{du}{w} .$$

définit une différentielle holomorphe sur une courbe projective non-singulière $X(x, y)$ dont un modèle affine s'écrit

$$w^d = u^{d\mu_0}(u-1)^{d\mu_1}(u-x)^{d\mu_2}(u-y)^{d\mu_3}. \tag{2}$$

Comme fonction de x et y, chaque période de ω satisfait à un système d'équations différentielles partielles linéaires dont on peut choisir les trois solutions de base comme des périodes de ω, par exemple

$$\int_{\gamma_0} \omega \ , \ \int_{\gamma_1} \omega \ , \ \int_{\gamma_2} \omega \ ,$$

où les γ_i sont des cycles sur $X(x, y)$, décrits par leurs projections sous $(u, w) \mapsto u$ (ramifié en $0, 1, x, y, \infty$) comme des cycles de Pochhammer autour des paires 1 et ∞, 1 et 0, 1 et x respectivement, en évitant des points de ramification. En

effet, à un facteur cyclotomique et un dénominateur $B(1-\mu_1, 1-\mu_4)$ près, $\int_{\gamma_0} \omega$ est une fonction hypergéométrique $F_1(x,y)$ d'APPELL [AK]. Le système d'EDP a ses singularités (régulières, voir e.g. [Y]) dans les *surfaces caractéristiques* $x = y$ et $x, y = 0, 1, \infty$. Le prolongement analytique suivant les cycles dans l'espace des points réguliers définit par représentation du groupe fondamental sur l'espace des solutions *le groupe de monodromie affine* $\Delta_0 \subset GL_3\mathbf{C}$ et *projectif* $\Delta \subset PGL_3\mathbf{C}$. Sous ces hypothèses on obtient le

THÉORÈME ([P], [TE 1,2],[DM],[M], [Y]). *L'application*

$$\Psi : \begin{cases} \mathbf{P}^1 \times \mathbf{P}^1 - \{(x,y) \mid x = y \text{ ou } x, y = 0, 1, \infty\} \longrightarrow \mathbf{P}_2 \\ (x,y) \longmapsto (\int_{\gamma_0} \omega, \int_{\gamma_1} \omega, \int_{\gamma_2} \omega) \end{cases}$$

définit une application localement biholomorphe et $PGL_3\mathbf{C}$*-multivalente sur une partie dense d'une boule projective* $B \subset \mathbf{P}_2$*, donnée par* $|\alpha_1 z_1|^2 + |\alpha_2 z_2|^2 < |z_0|^2$ *avec des constantes algébriques* $\alpha_1, \alpha_2 \neq 0$*. Le groupe de monodromie* Δ *opère sur* B*, et si l'on a pour tout* $i \neq j \in \{0,1,2,3,4\}$

$$(3) \qquad (1 - \mu_i - \mu_j)^{-1} \begin{cases} \in & \frac{1}{2}\mathbf{Z} \cup \{\infty\} & \text{si } \mu_i = \mu_j \\ \in & \mathbf{Z} & \text{sinon,} \end{cases}$$

Δ *opère comme groupe discontinu sur* B.

A des permutations des μ_j près, on obtient comme cela 49 groupes discontinus Δ que nous appelons *les groupes de Picard-Terada-Deligne-Mostow (PTDM)* en tenant compte du fait qu'une version faible du Théorème déjà formulée par PICARD est démontrée sous cette forme faible par TERADA et en cette version-ci par DELIGNE-MOSTOW et MOSTOW. Une autre démonstration -utilisant des travaux de HIRZEBRUCH et HÖFER sur les revêtements des surfaces algébriques, sous une condition plus restrictive que (3)- est donnée par YOSHIDA. Parmi ces 49 groupes, il y en a 15 qui ne sont pas arithmétiquement définis. Il existe une extension du Théorème à la situation en plus de deux variables (les fonctions de LAURICELLA), mais nous nous bornons ici aux groupes de *PTDM* $\Delta \subset PGL_3\mathbf{C}$.

Par continuité, Ψ s'étend sur les surfaces caractéristiques hors de leurs intersections ; cette extension contracte e.g. la surface $x = 0$ (pour $y \neq 0$) en des points de la boule si $\mu_0 + \mu_2 > 1$ et en des points au bord de la boule (des pointes de Δ) si $\mu_0 + \mu_2 = 1$. Mais Ψ ne s'étend pas e.g. au point $x = y = 0$

si $\mu_0 + \mu_2 + \mu_3 > 1$, donc l'espace naturel pour la définition de Ψ n'est pas $\mathbb{P}^1 \times \mathbb{P}^1$. D'autre part, on peut traiter les points de ramification $0,1,x,y,\infty$ de façon équivalente en les remplaçant par $x_0, x_1, x_2, x_3, x_4 \in \mathbb{C}$, la différentielle ω par

$$\prod_{j=0}^{4}(u - x_j)^{-\mu_j} du =: \omega'.$$

Finalement, le bon espace de définition pour Ψ sera donc l'espace des *points stables* [DM]

$$\begin{aligned} Q_{st} = \{&(x_0, x_1, x_2, x_3, x_4) \in (\mathbb{P}^1)^5\} \\ &- \{(x_0, \ldots, x_4) \mid \exists i \neq j \text{ avec } x_i = x_j \text{ et } \mu_i + \mu_j \geq 1\} \\ &- \{(x_0, \ldots, x_4) \mid \exists i, j, k \text{ deux à deux distincts} \\ &\qquad\qquad \text{avec } x_i = x_j = x_k \text{ et } \mu_i + \mu_j + \mu_k \geq 1\} \\ &- \{(x_0, \ldots, x_4) \mid \text{quatre coordonnées coïncident}\} \\ &\text{modulo l'action diagonale de } PSL_2\mathbb{C} \text{ sur } (\mathbb{P}^1)^5. \end{aligned}$$

L'espace Q_{st} porte une structure complexe naturelle, et même après l'adjonction d'un nombre fini de points *semi-stables* correspondant aux pointes de Δ, la structure d'une variété algébrique projective (plus précisément, d'un $\mathbb{P}_2$ éclaté en au plus quatre points en position générale). Localement, on peut normaliser Q_{st} par l'action de $PSL_2\mathbb{C}$ de telle façon que trois des x_j prennent les valeurs $0,1,\infty$; si l'on désigne les deux autres par x et y, on retrouve donc les définitions données au début. Mais globalement, on considère maintenant dix surfaces caractéristiques $S(ij)$ données par $x_i = x_j$; si $\mu_i + \mu_j < 1$, nous désignons par $S_{st}(ij)$ la partie stable $S(ij) \cap Q_{st}$, tandis que $S_{st}(ijk)$ désigne le point $x_i = x_j = x_k$ de Q_{st} si $\mu_i + \mu_j + \mu_k < 1$. Dans tous les cas, Ψ s'étend par continuité comme application $PGL_3\mathbb{C}$-multivalente de Q_{st} *sur* B. L'extension sera appelée encore Ψ.

Remarquons enfin que la restriction de Ψ à une surface caractéristique stable $S_{st}(ij)$ est essentiellement composée de deux solutions de l'équation différentielle hypergéométrique de Gauss en une variable pour les périodes de $\omega'|_{x_i=x_j}$, dont le quotient est une application triangulaire. Le groupe de monodromie Δ_{ij} de cette application triangulaire est déterminé, comme Δ, par les périodes de ω : il ne faut que remplacer le quintuplet $(\mu_j)_{j=0,\ldots,4}$ par un quadruplet en remplaçant la paire μ_i, μ_j par la somme $\mu_i + \mu_j$. Ce procédé cadre avec les formules classiques pour la restriction des fonctions d'Appell $F_1(x, y)$ aux surfaces caractéristiques.

2. Le plongement modulaire dans les points réguliers

Le résultat principal de ce travail-ci dit que même les groupes de *PTDM* non-arithmétiques sont étroitement liés à certains groupes arithmétiques :

THÉORÈME 1. *Soit Δ un groupe de PTDM. Alors il existe un groupe arithmétique Γ agissant sur une puissance B^m de la boule et un plongement modulaire qui consiste en une injection analytique*

$$F : B \hookrightarrow B^m$$

compatible à une injection de groupes

$$h : \Delta \hookrightarrow \Gamma$$

tel que $F(\gamma\tau) = h(\gamma)F(\tau)$ pour tout $\gamma \in \Delta$ et $\tau \in B$. Si l'on munit les espaces quotients compactifiés de leur structure naturelle de variétés projectives définis sur $\overline{\mathbb{Q}}$, l'application induite par F

$$\overline{\Delta \setminus B} \to \overline{\Gamma \setminus B^m}$$

est un morphisme défini sur $\overline{\mathbb{Q}}$.

Nous publierons les détails de la démonstration ailleurs, mais nous indiquons ici les idées principales pour expliquer le lien avec les variétés abéliennes et pour expliciter la construction de F. Pour les Ψ-images des points réguliers dans B, c'est une extension de la troisième construction dans [CoWo,§3]. Naturellement, pour les Δ arithmétiques on obtient $m = 1$ et des identités respectives pour F et h (e.g. dans le cas traité par [Ho]).

A chaque point régulier $(x, y) \in Q_{st} - \bigcup S(ij)$ on associe une variété abélienne $T(x, y)$ principalement polarisée contenue dans la Jacobienne $J(X(x, y))$. Les morphismes naturels de $X(x, y)$ sur des courbes $X_f(x, y)$ avec des modèles

$$w^f = u^{d\mu_0}(u-1)^{d\mu_1}(u-x)^{d\mu_2}(u-y)^{d\mu_3},$$

f un diviseur propre de d, induisent des morphismes m_f de $J(X(x, y))$ sur $J(X_f(x, y))$, et on prend pour $T(x, y)$ la composante connexe de 0 du noyau commun de ces m_f.

L'automorphisme $\chi : (u, w) \longmapsto (\zeta_d^{-1}u, w)$, $\zeta_d = e^{2i\pi/d}$, de $X(x, y)$ entraîne $\mathbb{K} = \mathbb{Q}(\zeta_d) \subset \mathrm{End}_0\, T(x, y) = \mathbb{Q} \otimes \mathrm{End}\, T(x, y)$, donc $T(x, y)$ admet des multiplications complexes par $\mathbb{K}$ avec un type de CM généralisé

$$\sum_{n \in (\mathbb{Z}/d\mathbb{Z})^*} r_n \sigma_n \ , \ \sigma_n \text{ les plongements } \mathbb{K} \hookrightarrow \mathbb{C} \text{ avec } \zeta_d \longmapsto \zeta_d^n \ ,$$

qui contient des informations sur l'action induite par $\mathbb{K}$ sur l'espace $H^0(T(x, y), \Omega)$ des différentielles de première espèce : $r_n = \dim V_n$ pour l'espace

$\mathbb{K}$-propre V_n des $\omega \in H^0(T(x,y),\Omega)$ sur lesquels $\mathbb{K}$ agit comme multiplication par $\sigma_n\mathbb{K}$. Autrement dit, r_n est la multiplicité de la valeur propre ζ_d^n pour l'automorphisme χ^* de $H^0(X(x,y),\Omega)$ induit par χ ; une formule classique de CHEVALLEY et WEIL [CW] permet de le calculer (soit $< a >$ la partie fractionnaire $a - [a]$ du nombre $a \in \mathbb{R}$) sous la forme

$$r_n = -1 + \sum_j < n\mu_j > , \tag{4}$$

d'où résulte $r_n + r_{-n} = 3$ pour tout n, donc $\dim T(x,y) = \frac{3}{2}\Phi(d)$ avec la fonction d'Euler Φ. En particulier, la différentielle $\omega = \dfrac{du}{w}$ se trouve dans V_1 et (1) entraîne $r_1 = 1$.

Or, d'après les travaux de SIEGEL [SIE] et SHIMURA [SHI 1], la famille de toutes les variétés abéliennes T avec multiplication complexe par $\mathbb{K}$ et du même type de CM que cette sous-famille des $T(x,y)$ est paramétrisée par le domaine symétrique complexe B^m, où l'exposant m est le nombre de sous-espaces propres V_n avec $r_n = 1$, et les points de B^m qui correspondent à T sont donnés par des m-tuplets

$$\left(\int_{\gamma_0}\omega_n \ , \ \int_{\gamma_1}\omega_n \ , \ \int_{\gamma_2}\omega_n\right)_{n\in(\mathbb{Z}/d\mathbb{Z})^* \text{ avec } r_n=1} \tag{5}$$

de triplets (à des facteurs algébriques près) $\in B \subset \mathbb{P}_2$, où les γ_i sont des générateurs du $\mathbb{Z}[\zeta_d]$-module des cycles $H_1(T,\mathbb{Z})$ et les ω_n sont certains générateurs de V_n. Pour $T = T(x,y)$ on peut choisir

$$\omega_n = u^{-<n\mu_0>}(u-1)^{-<n\mu_1>}(u-x)^{-<n\mu_2>}(u-y)^{-<n\mu_3>}du \tag{6}$$

(donc $\omega_1 = \omega = \dfrac{du}{w}$) et les cycles de Pochhammer γ_i du §1 s'identifient à des $\mathbb{Z}[\zeta_d]$-générateurs de $H_1(T(x,y),\mathbb{Z})$. Dans (5), tout triplet définit une application localement biholomorphe de l'espace des points réguliers (x,y) dans B, donc hors des singularités et à des facteurs algébriques près,

$$F : \left\{ \begin{array}{c} B \hookrightarrow B^m \\ \left(\int_{\gamma_0}\omega \ , \ \int_{\gamma_1}\omega \ , \ \int_{\gamma_2}\omega\right) \longmapsto \left(\int_{\gamma_0}\omega_n \ , \ \int_{\gamma_1}\omega_n \ , \ \int_{\gamma_2}\omega_n\right)_{n\in(\mathbb{Z}/d\mathbb{Z})^* \text{ avec } r_n=1} \end{array} \right.$$

est une injection analytique.

Quant à la compatibilité avec les actions de Δ et Γ, on remarque que le prolongement analytique des $\int_{\gamma_j}\omega_n$ le long des cycles dans l'espace des points

réguliers change les cycles d'intégration γ_j en une autre base du $\mathbb{Z}[\zeta_d]$-module $H_1(T,\mathbb{Z})$, mais ne change ni la courbe ni les différentielles. Comme cela, tout $\gamma \in \Delta$ définit un élément $h(\gamma)$ du groupe modulaire associé à cette famille des variétés abéliennes T. En effet, h est une injection de groupes.

3. Singularités et points CM

Pour compléter la démonstration du Théorème 1 il faut 1°) étendre F dans les Ψ-images des singularités stables et 2°) prouver la rationalité de l'application quotient. Ces deux points reposent sur une extension de la famille $T(x,y)$ aux surfaces caractéristiques stables dont nous résumons ici quelques résultats.

Soit $i \neq j$ et $\mu_i + \mu_j < 1$, donc $S_{st}(ij) \neq \emptyset$. Alors la famille $T(x,y)$ s'étend continûment sur $S_{st}(ij)$ comme somme directe

- d'une variété abélienne A_{ij} avec multiplication complexe par $\mathbb{K}$ au sens strict de SHIMURA-TANIYAMA [ST], de dimension $\frac{1}{2}\Phi(d)$ et avec le type

$$\sum_{n\in(\mathbb{Z}/d\mathbb{Z})^*} (< n\mu_i > + < n\mu_j > - < n(\mu_i+\mu_j) >)\sigma_n \ ,$$

  uniquement caractérisé à isogénie près [WW] par sa période de

$$\left\{ \begin{array}{ll} \text{première espèce} & B(\mu_i,\mu_j) \\ \text{deuxième espèce} & B(1-\mu_i,1-\mu_j) \end{array} \right\}$$

- et une variété abélienne de dimension $\Phi(d)$ avec multiplication complexe par $\mathbb{K}$ et un type de CM généralisé

$$\sum_{n\in(\mathbb{Z}/d\mathbb{Z})^*} (r_n - (< n\mu_i > + < n\mu_j > - < n(\mu_i+\mu_j) >))\sigma_n \ ,$$

  qui dépend d'un seul paramètre complexe.

Si par exemple $i = 0$, $j = 2$, $S(ij)$ est donné par $x = 0$, et sur $S_{st}(ij)$ la famille $T(x,y)$ prend la forme $A_{02} \oplus T(y)$, où $T(y)$ désigne la famille de variétés abéliennes introduite et étudiée dans [CoWo], §3 sous le nom de $\mathcal{T}$; là, cette famille joue le même rôle pour une construction d'un plongement modulaire du groupe triangulaire Δ_{02} (introduit à la fin du §1) que la famille $T(x,y)$ pour Δ ici. Comme on sait bien que ce $T(y)$ même se casse en deux facteurs avec multiplication complexe pour $y = 0, 1$ et ∞ dont on connaît les types, on obtient un certain nombre de *points CM* : Ce sont des points dans soit Q_{st}

soit B soit B^m auxquels correspondent des variétés abéliennes $T(x,y)$ isogènes à un produit de facteurs de type CM. Si l'on note par "$\sim$" une égalité dans $\mathbb{C}^* \bmod \overline{\mathbb{Q}}^*$, et si $\{i,j,k,l,s\} = \{0,1,2,3,4\}$, on a le

THÉORÈME 2. *Sur chaque surface caractéristique stable $S_{st}(ij)(\mu_i+\mu_j<1)$ on a au moins trois points CM, soit de la forme $S_{st}(ijk)$ avec $\mu_i+\mu_j+\mu_k<1$ dont la variété abélienne se casse en un facteur avec période $B(1-\mu_l, 1-\mu_s)$ et deux facteurs isogènes à $A_{ij} \widehat{=} A_{ik} \widehat{=} A_{jk}$ avec des périodes $B(\mu_i,\mu_j) \sim B(\mu_i,\mu_k) \sim B(\mu_j,\mu_k)$, soit de la forme $S_{st}(ij) \cap S_{st}(kl)$ dont les trois facteurs ont les périodes respectives $B(\mu_i,\mu_j), B(\mu_k,\mu_l)$ et $B(1-\mu_i-\mu_j, 1-\mu_k-\mu_l)$.*

Dans ces points CM, on peut choisir les cycles d'intégration γ_ν pour les solutions fondamentales $\int_{\gamma_\nu} \omega$ du système d'EDP de telle manière que ces solutions ont des développements dans $\overline{\mathbb{Q}}[[\xi,\eta]]$ pour des variables locales ξ,η convenables fois des puissances rationnelles de ξ et η et des facteurs c_ν qui sont simplement les périodes $B(\alpha_\nu,\beta_\nu)$ mentionnées dans le Théorème 2 ou bien les périodes de deuxième espèce $\dfrac{\pi}{B(\alpha_\nu,\beta_\nu)}$ correspondantes. Ceci entraîne un résultat sur la nature arithmétique des coefficients de Taylor des fonctions Δ-automorphes dans les points CM de B :

THÉORÈME 3. *Supposons que le point CM*
$$\left.\begin{array}{ll} a) & S_{st}(ijk) \\ b) & S_{st}(ij) \cap S_{st}(kl) \end{array}\right\} \in Q_{st} \text{ soit appliqué par } \Psi \text{ dans le point } (1,0,0) \in B.$$
Alors les composantes (Δ-automorphes) du revêtement $B \to \Delta \setminus B$ ont des développements dans $\overline{\mathbb{Q}}\left[\left[\dfrac{c_0 z_1}{c_1 z_0}, \dfrac{c_0 z_2}{c_2 z_0}\right]\right]$ avec des "rayons" transcendants $\dfrac{c_1}{c_0}$ et $\dfrac{c_2}{c_0}$ qui sont des quotients de

a) $c_0 \sim B(1-\mu_l, 1-\mu_s)$, $c_1 \sim c_2 \sim B(1-\mu_i, 1-\mu_j)$ *et*
b) $c_0 \sim B(1-\mu_i-\mu_j, 1-\mu_k-\mu_l)$, $c_1 \sim B(1-\mu_i, 1-\mu_j)$, $c_2 \sim B(1-\mu_k, 1-\mu_l)$ *respectivement.*

Ces quotients sont la généralisation naturelle aux surfaces Q_{st} du rayon de revêtement de certaines courbes comme dans la discussion de [CoWo] et [WW]. Leur transcendance résulte de [WW]. Pour les Δ arithmétiques, le Théorème 3 résulte aussi bien du travail de SHIMURA [Shi 2] ; pour les Δ non-arithmétiques, la comparaison avec ces résultats de SHIMURA (sur Γ, cette fois !) est possible à l'aide du plongement modulaire du Théorème 1.

REFERENCES

[AK] P.APPELL et M.J. KAMPÉ DE FÉRIET, *Fonctions hypergéométriques et hypersphériques. Polynômes d'Hermite.* Gauthier-Villars 1926.

[CW] CL.CHEVALLEY et A.WEIL, Über das Verhalten der Integrale 1. Gattung bei Automorphismen des Funktionenkörpers, *Abh. Hamburger Math. Sem.*, **10** (1934), 358-361.

[CoWo] P.COHEN et J.WOLFART, Modular Embeddings for some Non-arithmetic Fuchsian Groups, to appear in *Acta Arithmetica,* **56**, preprint IHES/M/88/57.

[DM] P.DELIGNE et G.D.MOSTOW, Monodromy of Hypergeometric Functions and Non-Lattice Integral Monodromy, *Publ. IHES*, **63** (1986), 5-89.

[Ho] R.P. HOLZAPFEL, *Geometry and Arithmetic around Euler Partial Differential Equations,* DVW Berlin 1986.

[M] G.D.MOSTOW, Generalized Picard Lattices arising from Half-Integral Conditions, *Publ. IHES*, **63** (1986), 91-106.

[P] E.PICARD, Sur les fonctions hyperfuchsiennes provenant des séries hypergéométriques de deux variables, *Ann. ENS III*, **2** (1885), 357-384.

[SHI 1] G.SHIMURA , On analytic families of polarized abelian varieties and automorphic functions, *Ann. Math.*, **78** (1963), 149-192.

[SHI 2] G.SHIMURA , Automorphic forms and the periods of abelian varieties, *J. Math. Soc. Japan*, **31** (1979), 561-592.

[ST] G.SHIMURA et Y.TANIYAMA Complex multiplication of abelian varieties ans its applications to number theory, *Publ. Math. Soc. Japan*, **6** (1961).

[SIE] C.L. SIEGEL, *Lectures on Riemann Matrices.* Tata Institute, Bombay 1963.

[TE 1] T.TERADA, Problème de Riemann et fonctions automorphes provenant des fonctions hypergéométriques de plusieurs variables, *J. Math. Kyoto Univ.*, **13** (1973), 557-578.

[TE 2] T.TERADA, Fonctions hypergéométriques F_1 et fonctions automorphes I, II, *J. Math. Soc. Japan*, **35-3** (1983), 451-475 et **37-2** (1985), 173-185.

[WW] J.WOLFART et G.WÜSTHOLZ, Der Überlagerungsradius gewisser algebraischer Kurven und die Werte der Betafunktion an rationalen Stellen, *Math. Ann.*, **273** (1985), 1-15.

[Y] M.YOSHIDA, *Fuchsian Differential Equations.* Aspects of Mathematics E11, Vieweg 1987.

Paula COHEN
Laboratoire de Math. Fondamentales
UER 48, Univ. P. et M. Curie
4, place Jussieu
F 75230 PARIS Cédex 05

et

Jürgen WOLFART
Math. Seminar der Univ.
Robert-Mayer-Str.10
D 6000 Frankfurt a.M.1

Astérisque

E. DUBOIS
R. PAYSANT-LE ROUX

Sur la longueur du développement en fraction continue de $\sqrt{f(n)}$

Astérisque, tome 198-199-200 (1991), p. 107-119
<http://www.numdam.org/item?id=AST_1991__198-199-200__107_0>

SUR LA LONGUEUR DU DEVELOPPEMENT EN FRACTION CONTINUE DE $\sqrt{f}(n)$

par

E. DUBOIS ET R. PAYSANT-LE ROUX

Introduction

On considère un polynôme $f(X)$ de degré pair à coefficients entiers dont le terme de plus haut degré est un carré et l'on s'intéresse à la longueur $\ell p(\sqrt{f}(n))$ de la période du développement en fraction continue de $\sqrt{f}(n)$ lorsque n est un entier rendant $f(n)$ positif non carré. SCHMIDT [1948] a considéré le cas $f(x) = X^2 + h$; SCHINZEL [1961] pour $f(X) = a^2X^2 + bX + c$, a introduit l'ensemble

$$E = \{n \in \mathbf{Z} \mid (b^2 - 4ac) \textit{ ne divise pas } 4(2a^2n + b)\}$$

et a montré que :

(1) Pour les entiers n n'appartenant pas à E, la longueur de la période de $\sqrt{f}(n)$ est bornée ;

(2) Pour les entiers n de E, la limite de $\ell p(\sqrt{f}(n)$ tend vers l'infini avec n.

SCHINZEL [1962] a généralisé ce résultat pour un polynôme à coefficients entiers dont le terme de plus haut degré est un carré. LOUBOUTIN [1987] a donné une version effective de (2). Nous nous proposons de généraliser ce résultat à un polynôme $f(X)$ du type précédent et nous pourrons en déduire si le développement en fraction continue formelle de $\sqrt{f}(X)$ est périodique. Signalons que dans le cas d'un polynôme $f(X) = aX^d + \ldots$ avec d impair et a positif ou avec d pair et a positif non carré, SCHINZEL [1961] a montré que la limite supérieure de $\ell p(\sqrt{f}(n)$ est infinie. Dans une autre direction, on peut citer les résultats de COHN [1977] : pour m entier non carré on a avec une constante effective :

$$\ell p(\sqrt{m}) \ll \sqrt{m}\ log\ m.$$

1. Le cadre des meilleures approximations

1.1. les fractions continues formelles

Un élément $\alpha = \sum_{-h}^{\infty} a_i X^{-i}$ du corps des séries de Laurent $\mathbf{Q}((1/X))$ se décompose en $E(\alpha) + F(\alpha)$ où $E(\alpha) = a_{-h}X^h + ... + a_{-1}X + a_0$ joue le rôle de la partie entière, ou partie polynômiale ; on pose deg $\alpha = h$ si a_{-h} est non nul. A partir de $\alpha_0 = \alpha$ on détermine la suite (α_k) par $\alpha_k = F(\alpha_{k-1})^{-1}$. En posant $u_k = E(\alpha_k)$ on obtient le développement en fraction continue formelle $[u_0, u_1, ..., u_k, ...]$ de α auquel on associe les réduites A_k/B_k par les formules de récurrences habituelles provenant de $A_k/B_k = [u_0, u_1, \ldots, u_k]$.

PROPOSITION 1. — *Soit $W \in \mathbf{Q}((1/X))$ avec $W^2 \in \mathbf{Z}[X]$. Si le développement en fraction continue formelle de W est périodique, la prépériode est de longueur 1 et la période possède une symétrie. Si*

$$W = [u_0, \overline{u}_1, \ldots, u_\ell],$$

on a

$$u_\ell(X) = 2u_0(X), u_j(X) = u_{\ell-j}(X) \text{ pour } 1 \leq j \leq \frac{\ell}{2}.$$

Cette proposition semble classique mais tous les résultats bien connus du cas réel ne se prolongent pas toujours au cas formel. Par exemple on sait que le développement d'un nombre quadratique n'est pas toujours périodique.

Démonstration (schéma). Si

$$\beta = (A(X) + B(X)W)D(X)^{-1} = c_d X^d + c_{d-1}X^{d-1} + \ldots$$

dans $\mathbf{Q}((1/X))$ avec $c_d \neq 0$ on pose

$$d = deg\beta, \beta' = (A(X) - B(X)W)D(X)^{-1}.$$

On dit que β est spécial si deg $(\beta) \geq 1$ et deg $(\beta') \leq 0$. On montre facilement les points suivants :

- si la fraction continue formelle de β est purement périodique alors β est spécial ;
- le successeur d'un nombre spécial est spécial ;

- parmi les prédécesseurs possibles d'un nombre spécial, il y a un seul nombre spécial ;
- si la fraction continue de W, avec $W^2 = f(X)$, est périodique, alors le développement de $\alpha = W + E(W)$ est purement périodique.

Soit maintenant $W = [u_0, u_1, \ldots]$ périodique ; alors

$$\alpha = [2u_0, u_1, ..., \overline{u_k, u_{k+1}, ..., u_{k+\ell-1}}]$$

est aussi périodique. Posons $\beta = [\overline{u_k, u_{k+1}, ..., u_{k+\ell-1}}]$. Le nombre α étant spécial tous ses successeurs le sont. Pour $k > 1$ les nombres $\gamma = u_{k-1}\beta^{-1}$ sont deux prédécesseurs spéciaux de β. Il sont donc égaux et on a $u_{k-1} = U_{k+\ell-1}$. De proche en proche on obtient $\alpha = [2u_0, u_1, \ldots, u_{\ell-1}]$. En remarquant que

$$-1/\alpha' = \alpha_1 = [\overline{u_1, u_2, ..., u_{\ell-1}, 2u_0}],$$

on obtient la symétrie annoncée et la proposition.

1.2. Meilleures approximations et fractions continues

Soit $f(X) = a^2X^{2d} + ... \in \mathbf{Z}[X]$ avec a entier positif. On considère $W = aX^d + ... \in \mathbf{Q}((1/X))$ vérifiant $W^2 = f(X)$. Pour tout entier n rendant $f(n)$ positif non carré, on pose $w = \sqrt{f}(n)$. On note $\mathbf{O}_x$ l'anneau $\mathbf{Q}[X]+\mathbf{Q}[X]W$ et $\mathbf{O}_n$ l'anneau $\mathbf{Z} + \mathbf{Z}w$.

Nous définissons ici les meilleures approximations de w et de W et nous donnons rapidement, le lien avec les fractions continues réelles ou formelles, et la manière de lire les propriétés classiques des fractions continues (voir [2] et [7]).

Traitons d'abord le cas réel. Pour $\zeta = p - qw$, avec $(p, q) \in \mathbf{Z}^2$, on pose $|\ \zeta\ |_1 = |\ \zeta\ |$ et $|\ \zeta\ |_2 = |\ p + qw\ |$. On dit que ζ est *une meilleure approximation* de w si et seulement si pour tout $\delta \in \mathbf{O}_n = \mathbf{Z} + \mathbf{Z}w$, vérifiant $|\ \delta\ |_1 < |\ \zeta\ |_1$ et $|\ \delta\ |_2 < |\ \xi\ |_2$ on a $\delta = 0$. Ces meilleures approximations sont définies au signe près. L'ensemble des meilleures approximations de w dans $]0, 1]$ forment une suite $1, \zeta_1, \zeta_2, ...$ ordonnée par $|\ \zeta\ |$ décroissant et tendant vers 0. Cette suite est en bijection avec la suite des réduites p_k/q_k du développement en fraction continue de w par la relation $\zeta_{k+1} = |\ p_k - q_k w\ |$ pour $k \geq 0$. De même les meilleures approximations supérieures a 1 sont rangées par $|\ \zeta\ |_1$ croissant : $1, \zeta_{-1}, \zeta_{-2}, ...$

On note ε l'unité fondamentale dans $]0,1[$ de l'ordre $\mathbf{O}_n$. La périodicité du développement en fraction continue s'exprime par $\zeta_{k+\ell} = \pm\varepsilon\zeta_k$ pour tout $k \in \mathbf{Z}$. D'autre part, la définition montre que si $\zeta = p - qw$ est une meilleure approximation de w, son conjugué $\zeta' = p + qw$ l'est aussi. On obtient alors la suite des meilleures approximations positives :

$$\ldots \mid \zeta'_\ell \mid, \mid \zeta'_{\ell-1} \mid, \ldots, \mid \zeta'_1 \mid, 1, \zeta_1, \zeta_2, \ldots, \zeta_{\ell-1}, \zeta_\ell = \varepsilon, \ldots$$

Pour tout entier k,on a $\mid \zeta'_k \mid = \zeta_{\zeta-k}$ et avec la périodicité on a $\zeta_j = \varepsilon \mid \zeta'_{\ell-j} \mid$ pour $j = 1, 2, \ldots, \ell$. Ceci exprime la propriété de symétrie de la période du développement $w = [a_0, \overline{a_1, a_2, \ldots a_2, a_1, 2a_0}]$. Si la longueur ℓ est paire, il y a un terme médiant a'_h avec $h = \frac{\mathbf{l}}{2}$, et on a $\zeta_h = \pm\zeta'_h$. En résumé :

PROPOSITION 2. — *Avec les définitions et notations précédentes, les meilleures approximations positives de w forment une suite (ζ_k) vérifiant $\zeta_0 = 1, \zeta_\ell = \varepsilon$ et $\zeta_{k+\ell} = \varepsilon\zeta_k$; on a $\zeta_j = \varepsilon \mid \zeta'_{\ell-j} \mid$ pour $j = 1, 2, \ldots, \ell$. Le lien avec les réduites s'exprime par $\zeta_{k+1} = \mid p_k - q_k w \mid$ pour $k \geq 0$.*

Revenons au cas formel. Pour $\beta = A(X) + B(X)W \in \mathbf{O}_x$ on définit les deux valeurs absolues $\mid \beta \mid_1 = e^{deg\beta}$ et $\mid \beta \mid_2 = \mid \beta' \mid_1$. On peut prendre la même définition que dans le cas réel : β est une meilleure approximation de W si et seulement si pour tout γ de $\mathbf{O}_x$ tel que $\mid \gamma \mid_1 < \mid \beta \mid_1$ et $\mid \gamma \mid_2 < \mid \beta \mid_2$ on a $\gamma = 0$. Ces meilleures approximations sont définies à un facteur multiplicatif rationnel non nul près. Les meilleures approximations de W de degré négatif forment une suite $1, \beta_1, \beta_2, \ldots$ qui est en bijection avec la suite des réduites de W par la relation $\beta_{k+1} = A_k - B_k W$ modulo $\mathbf{Q}*$. La périodicité (de longueur ℓ) du développement en fraction continue de W se traduit par l'existence d'une unité ε de $\mathbf{O}_x$ telle que

$$\beta_{k+\ell} = \varepsilon\beta_k \ (modulo\ \mathbf{Q}*)$$

pour tout $k \geq 0$, mais contrairement au cas réel ε n'est pas toujours l'unité fondamentale de $\mathbf{O}_x$, même si ℓ est minimale. Nous précisons cette particularité au paragraphe suivant.

Signalons que toute unité ε de $\mathbf{O}_x$ est une meilleure approximation, que si ζ est une meilleure approximation, il en va de même pour $\varepsilon\zeta$, et que comme dans le cas réel la notion de meilleure approximation ainsi exprimée donne une démonstration élégante de la propriété de symétrie de la période de W et de la

propriété de conjugaison

$$(\beta_j = \varepsilon\beta'_{\ell-j} modulo \mathbf{Q}*, 1 \leq j \leq \ell).$$

1.3. Groupes d'unités de $\mathbf{O}_x$

Un élément $\eta \in \mathbf{O}_x$ est une unité si et seulement si sa norme $N(\eta) = \eta\eta'$ est un nombre rationnel non nul. Si η est une unité de $\mathbf{O}_x$, $\lambda\eta$ l'est aussi pour tout $\lambda \in \mathbf{Q}*$. On considère donc le groupe G des unités modulo $\mathbf{Q}^*$. On sait [3] que le rang de ce groupe est soit 0 soit 1. Il est de rang 1 si est seulement si la fraction continue de W est périodique. Puisque nous supposons le développement en fraction continue de

$$W = [u_0, \overline{u_1, \ldots, u_{\ell-1}, 2u_0}]$$

périodique de longueur ℓ minimale, nous savons que $\varepsilon = A_{l-1}(X) - B_{l-1}(X)W$ est une unité de G de norme ± 1. Le groupe G_1 des unités de norme ± 1 sera donc aussi de rang 1.

Nous établissons maintenant le lien entre ε et les générateurs de G et de G_1 que nous notons respectivement φ et ψ. Montrons d'abord que la première unité dans la suite des meilleures approximations, de degré négatif, est située soit à la fin de la période du développement en fraction continue de W, soit au milieu et dans ce cas $\ell \equiv 2 \bmod 4$. Si parmi les $\ell - 1$ premières meilleures approximations de degré négatif de $W, \beta_1, \beta_2, \ldots, \beta_{\ell-1}$, il y a une unité $\beta_h = A_{h-1} - B_{h-1}W$ de G écrivons, pour $k \geq 0$:

$$W_k = [u_k, u_{k+1}, \ldots] = (P_k + W)C_1^{-1};$$

alors

$$C_h = (-1)^h(A_{h-1}^2 - B_{h-1}^2 f(X))$$

est de degré nul. De l'égalité

$$W_h = (P_h + E(W))C_h^{-1} + (W - E(W))C_h^{-1}$$

on déduit $W_{h+1} = C_h W_1$ puis $W_{h+2} = W_2 C_h^{-1}$, etc. Si h est impair on a $W_{2h} = C_h W_h = P_h + W, W_{2h+1} = W_1$ et donc $\ell = 2h$. Si h est pair $W_{2h} = W_h W_h^{-1}, W_{3h} = W_h C_h^{-2}, \ldots$, ce qui conduit à une infinité de quotients partiels distincts et le développement de W ne serait pas périodique contrairement l'hypothèse. Si ℓ est impair on peut prendre $\varphi = \Psi = \varepsilon = (A_{\ell-1} - B_{\ell-1}W)$

comme générateur de G et de G_1. Si maintenant ℓ est pair, notons $h = \ell/2$, considérons $\beta_h = A_{h-1} - B_{h-1}W$ et notons $C = N(\beta_h) = A_{h-1}^2 - B_{h-1}^2 f(X)$. Il faut ensuite discuter suivant C. Si C est de degré non nul, β_h n'est pas dans G et on peut prendre ε comme générateur de G modulo $\mathbf{Q}*$ et de G_1 au signe prs. Si $C = \pm c^2$ avec c rationel, β_h est dans G et $\beta_h c^{-1}$ est dans G_1. Dans les autres cas, β_h est dans G et $\beta_h^2 C^{-1}$ est dans G_1. En résumé on a :

PROPOSITION 3. — *Avec les notations précédentes, soit ℓ la longueur de la période du développement en fraction continue de $\sqrt{f}(X)$ et notons $\varepsilon = \beta_\ell = A_{\ell-1} - B_{\ell-1}W$.*

1. *Si ℓ est impair, ε est un générateur de G modulo $\mathbf{Q}^*$ et de G_1.*
2. *Si ℓ est pair, notons $h = \ell/2$ et $C = N(\beta_h)$; alors :*
   a. *Si $deg(C)$ est non nul, ε est un générateur de G modulo $\mathbf{Q}^*$ et de G_1.*
   b. *Si $deg(C) = 0$ avec $C = \pm c^2$ et c rationnel, β_h est un générateur de G modulo $\mathbf{Q}^*$ et $\beta_h c^{-1}$ est un générateur de G_1.*
   c. *Si $deg(C) = 0$ avec $\mid C \mid$ non carré dans $\mathbf{Q}$, β_h est un générateur de G modulo $\mathbf{Q}^*$ et $\varepsilon = \beta_\ell$ est un générateur de G_1.*

2 - Le résultat principal

2.2. Enoncé

THÉORÈME — *Soit $f(X) = a^2X^{2d} + \ldots$ un polynôme non carré dans $\mathbf{Z}[X]$ tel que le développement en fraction continue d'un élément $W = aX^d + \ldots$ vérifiant $W^2 = f(X)$, soit périodique. Notons $W = [u_0, \overline{u_1, \ldots, u_\ell}]$ et A_k/B_k les réduites du développement en fraction continue de W et considérons l'ensemble :*

$$E = \{n \in \mathbf{Z} \mid 2A_{\ell-1}(n) \notin \mathbf{Z}, f(n) \text{ positif non carré } \}.$$

Alors il existe une constante C ne dépendant que de f telle que pour tout $n \in E$, la longueur de la période du développement en fraction continue de $\sqrt{f(n)}$ soit minorée par $1 + 2[\log \sqrt{f(n)}/\log C]$ où $[z]$ désigne la partie entière de z.

L'idée de la démonstration est la suivante : on considère un générateur $\varphi(X)$ du groupe des unités G et on montre que pour $n \in E$ et pour $k = 1, 2, \ldots, k_0 = [\log \sqrt{f(n)}/\log C]$ on peut associer aux $\varphi^k(n)$ des meilleures approximations de $\sqrt{f(n)}$ non congrues modulo les unités. La longueur de la

période sera alors minorée par k_0. On précise la minoration en utilisant les propriétés particulières des meilleures approximations de la racine carrée d'un entier (positif non carré).

LEMME 1 — *Soit $\varphi = T + UW$ une unité fondamentale de G vérifiant $|\varphi|_1 < 1$. Il existe une partition des entiers rationnels $\mathbf{Z}$ en un nombre fini de classes F_j, $j = 1, \ldots, s$ et des polynômes $T^{(j)}, U^{(j)} \in \mathbf{Q}[X]$ à valeurs entières sur F_j tels que pour tout $j \in \{1, 2, \ldots, s\}$:*

a) le polynôme $T^{(j)}(n)$ est premier à $U^{(j)}(n)$ pour tout $n \in E_j$;

b) la série $\varphi_j = T^{(j)} + U^{(j)}W$ est équivalente à φ (i.e. $\varphi_j \varphi^{-1} \in \mathbf{Q}^*$) ;

c) En posant $C_j = N_{[\mathbf{Q}(X,W):\mathbf{Q}(X)]}(\varphi_j)$ on a $C_{j_1} \neq C_{j_2}$ dès que $j_1 \neq j_2$.

Démonstration. On se ramène à un représentant de φ tel que T et U soient à valeurs entières sur $\mathbf{Z}$ en multipliant éventuellement par un rationnel. Soit $C = T^2(X) - U^2(X)f(X)$. Le nombre C est un entier non nul et pour tout entier n le pgcd de $T(n)$ et de $U(n)$ divise C. On obtient le lemme en considérant les diviseurs d_j de C (en nombre fini) tels que

$$F_j = \{n \in \mathbf{Z} \text{ t.q pgcd } (T(n), U(n)) = d_j\}$$

soit non vide, en posant $(T^{(j)}, U^{(j)}) = (T, U)d_j^{-1}$ et en remarquant que $C = C_j d_j^2$.

On peut montrer que les classes F_j sont en fait des réunions de progressions arithmétiques. Elles sont donc infinies.

Dans la suite, nous omettons l'indice j pour alléger l'écriture.

LEMME 2 — *Soient (F, T, U, φ, C) l'une des classes du lemme 1 avec $\varphi(n) = T(n) + U(n)w$ $(w^2 = f(n))$ et $C = T^2(n) - U^2(n)f(n)$.*
Pour tout $n \in F \cap E$ il existe un nombre premier p divisant C tel que

$$2v_p(2T(n)) < v_p(C) \tag{3}$$

où v_p désigne la valuation p-adique. En notant $\varphi^k(X) = T_k(X) + U_k(X)W$ les puissances de φ on a :

$$v_p(f(n)) = v_p(T^2(n)) \tag{4}$$

$$v_p(T_k(n)) = (k-1)v_p(2T(n)) + v_p(T(n)) \quad \text{pour } k \geq 1 \tag{5}$$

$$v_p(U_k(n)) = (k-1)v_p(2T(n)) \quad \text{pour } k \geq 1\ . \tag{6}$$

Démonstration : D'après le lien mis en évidence dans la proposition 3 entre l'unité formelle génératrice de G et l'unité $\varepsilon = A_{\ell-1} - B_{\ell-1}W$ provenant de la fraction continue formelle, nous avons deux cas à considérer suivant que ε est ou non un générateur de G. Si ε engendre G on a $\varphi = a\varepsilon$ avec a entier et donc $2A_{\ell-1}(n) = \pm 2T(n)$ et $C = \pm a^2$. Mais pour $n \in E$, $2A_{\ell-1}(n)$ n'est entier et il existe donc p vérifiant (3). Dans l'autre cas $\varepsilon = \pm\varphi^2 C^{-1} = \pm(T^2 + U^2 f + 2TUW)C^{-1}$ et on a $2A_{\ell-1} = \pm 2(T^2 + U^2 f)C^{-1}$. Pour $n \in E$, le nombre $2(T^2(n) + U^2(n)f(n))C^{-1}$ n'est pas entier et en tenant compte de $T^2 - U^2 f = C$ on en déduit que $4T^2(n)C^{-1}$ n'est pas entier et il existe p tel que $2v_p(2T(n)) < v_p(C)$. On peut considérer que p est indépendant de n dans F. En effet, comme il n'y a qu'un nombre fini de p possibles, il suffit de partitionner F.

Pour la deuxième partie du lemme, on écrit :

$$T^2(n) - U^2(n)f(n) = C \ ; \tag{7}$$

d'après (3), on a $v_p(U^2(n)f(n)) = v_p(T^2(n) - C) = v_p(T^2(n))$ mais $T(n)$ est premier avec $U(n)$ et donc $v_p(f(n)) = v_p(T^2(n))$. Pour prouver (5) et (6) on remarque que les entiers $T_k(n)$ et $U_k(n)$ vérifient les relations de récurrence linéaire

$$\begin{cases} T_{k+2}(n) = & 2T_{k+1}(n)T(n) - CT_k(n) \\ U_{k+2}(n) = & 2U_{k+1}(n)T(n) - CU_k(n), \quad k \geq 1 \ . \end{cases} \tag{8}$$

En effet, à partir de $\varphi^{k+1} = \varphi^k\varphi$ on tire

$$\begin{pmatrix} T_{k+1} \\ U_{k+1} \end{pmatrix} = \begin{pmatrix} T & Uf \\ U & T \end{pmatrix} \begin{pmatrix} T_k \\ U_k \end{pmatrix}$$

et en écrivant que $M = \begin{pmatrix} T & Uf \\ U & T \end{pmatrix}$ est racine de son polynôme caractéristique $M^2 - 2TM - CI = 0$ on obtient la relation (8). On peut alors montrer (5) et (6) par récurrence. En tenant compte de (7) on a $T_1(n) = T(n)$ et $T_2(n) = T^2(n) + U^2(n)f(n) = 2T^2(n) - C$. Ce qui montre (5) pour $k = 1$ et $k = 2$. D'autre part, $U_1(n) = U(n)$ et on veut $v_p(U(n)) = 0$. Si $v_p(T(n)) > 0$ on a $v_p(U(n)) = 0$ car $T(n)$ et $U(n)$ sont des entiers premiers entre eux. Si maintenant $v_p(T(n)) = 0$ la relation (7)et $v_p(C) > 0$ entraîne $v_p(U(n)) = 0$. Puisque $U_2(n) = 2T(n)U(n)$ on a donc (6) pour $k = 1$ et $k = 2$. Pour $k > 2$ les relations (5) et (6) se vérifient facilement par récurrence à partir de (8).

LEMME 3 — *Avec les notations du lemme 2, considérons pour $n \in F \cap E$ le pgcd $d_{k,n}$ des entiers $T_k(n), U_k(n)$ et posons*

$$T_{k,n} = T_k(n)/d_{k,n}, U_{k,n} = U_k(n)/d_{k,n} \ .$$

Les entiers algébriques $\varphi_{k,n} = T_{k,n} + U_{k,n}w$ du corps quadratique $\mathbf{Q}(w)$ ont des normes distinctes et sont donc non congrus deux à deux modulo les unités du corps pour tout $k \geq 1$.

Démonstration : Soit $n \in F \cap E$ et p un nombre premier divisant la norme C de $\varphi(n)$ tel que (n,p) vérifie (3). Il résulte de (5) et (6) que $v_p(d_{k,n}) = (k-1)v_p(2T(n))$ et donc la norme C'_k de $\varphi_{k,n}$ vérifie

$$v_p(C'_k) = kv_p(C) - 2(k-1)v_p(2T(n)) \ .$$

$v_p(C'_{k_1}) = v_p(C'_{k_2})$ entraîne $(k_1 - k_2)(v_p(C) - 2v_p(2T(n))) = 0$ et donc $k_1 = k_2$. Ce qui prouve le lemme 3.

LEMME 4 — *Avec les notations des lemmes 2 et 3, soient $\varphi = T + UW$ et n un entier de $F \cap E$. Si k est un entier vérifiant $w > |C^k|$, la fraction $T_{k,n}U_{k,n}^{-1} = T_k(n)U_k^{-1}(n)$ est une réduite du développement en fraction continue de W. De plus, en notant $\varphi'_{k,n} = T_{k,n} - U_{k,n}w$ le conjugué de $\varphi_{k,n}$, le nombre $\varphi'_{k,n}\varphi_{k_1,n}^{-1}$ n'est pas une unité du corps $K_n = \mathbf{Q}(w)$ quels que soient les entiers k, k_1 et n dans $F \cap E$.*

Démonstration : La première partie résulte directement de la proposition 2 et du chapitre 10 de HUA [1982] affirmant que si t et u sont des entiers tels que $|t^2 - wu^2| < w$ alors t/u est une réduite de w. La seconde partie pour $k \neq k_1$ résulte du lemme 3. Soient maintenant $n \in F \cap E$ et p un premier divisant $C = N(\varphi(n))$ tel que (n,p) vérifie (3). Posons $2\alpha = 2v_p(2T(n))$ et supposons $p \neq 2$. Il résulte du lemme 2 que $p^{2\alpha}$ divise exactement $T^2(n)$ et $f(n)$ et que $p^{2\alpha+1}$ divise C. L'égalité $T^2(n)p^{-2\alpha} - f(n)p^{-2\alpha}U^2(n) = Cp^{-2\alpha}$ montre que $f(n)p^{-2\alpha}$ est un carré modulo p. Si on note $\mathbf{O}_{K_n}$ l'anneau des entiers du corps $K_n = \mathbf{Q}(w)$, l'idéal $(p\mathbf{O}_{K_n})$ est donc décomposé. On en déduit les égalités :

$$(T + Uw)\mathbf{O}_{K_n} = p^\alpha P^{\gamma-2\alpha}Q,$$
$$(T - Uw)\mathbf{O}_{K_n} = p^\alpha P'^{\gamma-2\alpha}Q',$$

où $\gamma = v_p(C)$, où P, P' sont les idéaux premiers distincts au-dessus de p et où Q est un idéal étranger à P.

Dans le cas $p = 2$, le lemme 2 entraîne que $2^{2(\alpha-1)}$ divise exactement $T^2(n)$ et $f(n)$. D'autre part, $v_2(C) > 2v_2(2T(n)) = 2\alpha$ et donc 8 divise $C2^{-2(\alpha-1)}$. L'égalité

$$T^2(n)2^{2-2\alpha} - f(n)2^{2-2\alpha}U^2(n) = C2^{2-2\alpha}$$

montre que l'idéal $2\mathbf{O}_{K_n}$ est encore décomposé. On en déduit

$$(T + Uw)\mathbf{O}_{K_n} = 2^{\alpha-1}P^{\gamma-2(\alpha-1)}Q,$$
$$(T - Uw)\mathbf{O}_{K_n} = 2^{\alpha-1}P'^{\gamma-2(\alpha-1)}Q';$$

Il en résulte que les idéaux $\varphi'_{k,n}\mathbf{O}_{K_n}$ et $\varphi_{k,n}\mathbf{O}_{K_n}$ sont distincts, ce qui équivaut à dire $\varphi'_{k,n}\varphi_{k,n}^{-1}$ n'est pas une unité de $\mathbf{O}_{K_n}$.

Démonstration du théorème : Considérons l'un des ensembles F_j définis au lemme 1. Posons $F = F_j, C = C_j$ et pour $n \in F \cap E$, considérons l'entier

$$k_0 = [\log\left(\sqrt{f(n)}\right) / \log c] \ .$$

Avec les notations des lemmes précédents, il résulte des lemmes 3 et 4 que les nombres

$$\varphi_{1,n}, \varphi_{2,n}, \ldots, \varphi_{k_0 n}, \varphi'_{1,n}, \varphi'_{2,n}, \ldots, \varphi'_{k_0 n} \tag{9}$$

sont des meilleures approximations de w et qu'elles sont non congrues deux à deux modulo les unités de l'anneau $\mathbf{O}_{K_n}$, on a donc $\ell p(w) \geq 2k_0$. Si $\ell p(w)$ est impair, on en déduit immédiatement $\ell p(w) \geq 2k + 1$. Si $\ell p(w)$ est pair, on va montrer que : $\ell p(w) \geq 2k_0 + 2$. En effet, la proposition 2 nous dit que la meilleure approximation $\zeta_h = |p_{h-1} - q_{h-1}w|$ avec $h = \dfrac{\ell p(w)}{2}$, qui se trouve au milieu de la période, vérifie $\zeta_h = \pm\zeta'_h\varepsilon$ (ε unité de $\mathbf{O}_{K_n}$). Or, d'après le lemme 4, les meilleures approximations $(\varphi_{i,n})_{1\leq i\leq k_0}$ $(\varphi'_{i,n})_{1\leq i\leq k_0}$ que l'on considère ne peuvent être associées modulo les unités de $\mathbf{O}_{K_n}$ à ζ_h. Alors $\ell p(w) \geq 2k_0 + 1$ et comme $\ell p(w)$ est pair on a $\ell p(w) \geq 2k_0 + 2$.

2.2. Un exemple

Dans le cas $f(X) = a^2X^2 + bX + c$ le développement en fraction continue formelle est toujours périodique de longueur 1 ou 2. On a :

$$\sqrt{f(X)} = \left[aX + \frac{b}{2a}\ , \overline{\frac{8a^3X + 4ab}{4a^2c - b^2}},\ 2aX + \frac{b}{a}\right]$$

L'exemple $F(X) = X^2 + 9X + 16$ avec $n = 17^m$ donné par LOUBOUTIN [1989] montre que la minoration obtenue est optimale puisque $\ell p(\sqrt{f(17^m)}) = 1 + 2m$ et que $m = k_0$.

Nous donnons ci-dessous un exemple explicite, avec $\deg(f) = 4$, dans lequel la longueur du développement formel est $\ell = 10$. Si

$$f(X) = X^4 + 4X^3 - 6X^2 + 4X + 1, \ \textit{et}\ W(X) = X^2 + 2X - 5 + \ldots,$$

on obtient facilement le développement en écrivant les quotients complets W_k sous la forme $(B_k + W)C_k^{-1}$ car on a les formules de récurrence classiques :

$$u_k(X) = E(B_k + W)C_k^{-1},\ B_{k+1} = u_kC_k - B_k,\ C_{k+1} = (f(X) - B_{k+1}^2)C_k^{-1}.$$

La suite des quotients partiels est :

$u_0(X) = X^2 + 2X - 5$, $u_1(X) = (X+3)/12$, $u_2(X) = -6(X+2)$,
$u_3(X) = (X+2)/18$, $u_4(X) = -9(X+3)$, $u_5(X) = -(X^2+2X-5)/54$,
$u_6 = u_4 \ldots \quad u_{10}(X) = 2u_0(X)$.

La suite des normes de la suite des meilleures approximations
$\beta_k = A_{k-1} - B_{k-1}W$, $k \geq 1$, est :

$N(\beta_0) = 1$, $N(\beta_1) = -24(X-1)$, $N(\beta_2) = -X/3$, $N(\beta_3) = -36X$,
$N(\beta_4) = -2(X-1)/9$, $N(\beta_5) = 108$, $N(\beta_6) = N(\beta_4), \ldots, N(\beta_10) = 1$.

L'élément suivant :

$$\varphi(X) = 4\beta_5 = (X^6 + 12X^5 + 45X^4 - 33X^2 - 43) - (X^4 + 10X^3 + 30X^2 + 22X - 11)W$$

est un générateur de G ; nous posons $\varphi(X) = T(X) + U(X)W$.

Déterminons l'ensemble E : Puisque $C = N(\varphi) = 16.108$ n'est pas un carré, on a d'après le paragraphe I.3 :

$$\varepsilon = \beta_{10} = \beta_5^2 C^{-1} = A_9 - B_9 W$$

et donc $2A_9(n) = \pm 2(T^2 + U^2 f)C^{-1}$.

Pour tout entier n, $2A_9(n)$ n'est jamais entier car $n \equiv 0$ ou $1 (\mathrm{mod}\ 3)$ implique $T^2 + U^2 f \equiv 2$ ou $1 \pmod 3$ et que $n \equiv 2 \pmod 3$ implique $T^2 + U^2 f$ divisible par 9 mais non par 27. D'autre part, $f(0)$ et $f(1)$ sont carrés et $f(n)$ est négatif pour $n = -1, -2,$
$-3, -4, -5$. On a donc

$$E = \mathbf{Z} \setminus \{0, 1, -1, -2, -3, -4, -5\}.$$

En explicitant les résultats du lemme 1 pour ce générateur φ et en utilisant les notations de ce lemme on a la partition suivante de E :

$$F_1 = \{n \in E \mid n \equiv 0 \bmod 2 \text{ et } n \equiv 0 \text{ ou } 1 \bmod 3\}$$
avec $T^{(1)} = T$, $U^{(1)} = U$, $C_1 = 2^6.3^3$

$$F_2 = \{n \in E \mid n \equiv 0 \bmod 2 \text{ et } n \equiv 2 \bmod 3\}$$
avec $T^{(2)} = T/3$, $U^{(2)} = U/3$, $C_2 = 2^6.3$

$$F_3 = \{n \in E \mid n \equiv 1 \bmod 2 \text{ et } n \equiv 0 \text{ ou } 1 \bmod 3\}$$
avec $T^{(3)} = T/2$, $U^{(2)} = U/2$, $C_3 = 2^4.3^3$

$$F_4 = \{n \in E \mid n \equiv 0 \bmod 2 \text{ et } n \equiv 2 \bmod 3\}$$
avec $T^{(4)} = T/6$, $U^{(4)} = U/6$, $C_4 = 2^4.3$

Le théorème donne la minoration :

$$\ell p(\sqrt{f(n)}) \geq 1 + 2[\log \sqrt{f(n)} / \log C],$$

avec $C = \max C_j = 2^6 3^3$ mais la démonstration permet de l'améliorer suivant que n appartient à F_2, F_3 ou à F_4 en remplaçant C par C_2, C_3 ou C_4.

REFERENCES

[1] COHN J.H.E. *The length of the period of the simple continued fraction of* $d^{1/2}$. Pacific J.Math.Vol. 71 n° 1, 1977,pp.31-32.

[2] DUBOIS E. *Approximations diophantiennes simultanées de nombres algébriques.* Thèse, Paris VI, 1980.

[3] HELLEGOUARCH Y., MC QUILLAN D.L., PAYSANT-LE ROUX R. *Unités de certains sous anneaux de corps de fonctions algébriques.* Acta Arith. (1987), p. 9-47.

[4] HUA L.K. *Introduction to number theory.* Springer-Verlag, 1982.

[5] LOUBOUTIN S. *Une version effective d'un théorème de A. Schinzel sur les longueurs des périodes de certains développements en fractions continues.* C.R.A.S. Paris t.308, série I, p. 511-513, 1987.

[6] NEUBRAND M. *Einheiten in algebraischen Funktionen und Zahlhörpen.* J. Reine Angew. Math. 303/304 (1978) p.170-204.

[7] PAYSANT-LE ROUX R. *Calibre d'un corps arithmétique et unités.* Thèse, Caen 1987.

[8] PAYSANT-LE ROUX R. et DUBOIS E. *Meilleures approximations formelles ou réelles.* Colloque de théorie des Nombres. Alger 1989.

[9] SCHINZEL A. *On some problems of the arithmetical theory of continued fractions.* Acta Arith. 6 (1961) p.393-413.

[10] SCHINZEL A. *On some problems of the arithmetical theory of continued fractions.* Acta Arith. 7 (1962) p.287-298.

[11] SCHMIDT H. *Zur Approximation und Kettenbruchentwicklung quadratischer Zahlen.* Math.Z. (1948) p.168-192.

DUBOIS E.
ISMA & Département de Mathématiques
Université de Caen
14032 CAEN

et

PAYSANT-LE ROUX R.
Département de Mathématiques
Université de Caen
14032 CAEN

Astérisque

W. DUKE
H. IWANIEC

Sums over primes of the Fourier coefficients of half-integral weight cusp forms

Astérisque, tome 198-199-200 (1991), p. 121-125
<http://www.numdam.org/item?id=AST_1991__198-199-200__121_0>

SUMS OVER PRIMES OF THE FOURIER COEFFICIENTS OF HALF-INTEGRAL WEIGHT CUSP FORMS

W. DUKE* and H. IWANIEC

The following is a brief summary of work presented in detail in [1]. Our intention is to expose main ideas and to compare and contrast our methods with more traditional ones used in similar contexts.

We are concerned with certain properties of the Fourier coefficients of half-integral weight cusp forms. More specifically we give non-trivial estimates for various bilinear forms in these coefficients. These are then applied in Vinogradov's method to give an estimate for their sum over primes.

In general, given an arithmetic function f_n one is often interested in the sum over primes

$$S(X) = \sum_{p \leq X} f_p \quad .$$

If f_n is normalized so that

$$\sum_{n \leq X} |f_n|^2 \ll X$$

then Cauchy's inequality gives the trivial bound

$$S(X) \ll \frac{X}{\log^{\frac{1}{2}} X} \quad .$$

For most randomly oscillating f_n essentially the best bound one could hope for would be

$$S(X) \ll_\epsilon X^{\frac{1}{2}+\epsilon} \quad .$$

For multiplicative functions f_n one traditionally considers the Dirichlet series

$$F(s) = \sum_{n=1}^{\infty} f_n n^{-s} = \prod_{p \text{ prime}} \left(\sum_{m=0}^{\infty} f_{p^m} p^{-ms} \right)$$

for $\mathrm{Re}(s) > 1$. If $F(s)$ may be continued to an entire function, satisfies a standard type of functional equation relating $F(s)$ to $F(1-s)$, and if $F(s) \neq 0$ for $\mathrm{Re}(s) > \theta \geq \frac{1}{2}$ then we may deduce classically that

$$S(X) \ll_\epsilon X^{\theta+\epsilon} \quad .$$

* Research supported by NSF Grant No. DMS-8705939.

Of course, this last condition is not known for $\theta < 1$ for any interesting $F(s)$. If, for example, $f_n = \chi(n)$ is a non-trivial Dirichlet character or if $n^{\frac{k-1}{2}} f_n$ is the n^{th} Fourier coefficient of a cuspidal eigenform of weight k then the method of Hadamard and de la Vallée Poussin gives only

$$S(X) \ll X \exp\left(-c \log^{\frac{1}{2}} X\right)$$

for some $c > 0$ depending on the "conductor" of f_n.

For non-multiplicative f_n Vinogradov's method may be applicable. This was first applied by him in 1937 to $f_n = e(n\alpha)$. We apply it to the Fourier coefficients of certain half-integral weight cusp forms. To define these, let χ be a Dirichlet character modulo N, where $N \equiv 0 \pmod 4$, and $k = \frac{1}{2} + l$ where $l \in \mathbf{Z}$, $l \geq 2$. H is the upper half-plane acted on by

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{R}) \quad \text{where} \quad \gamma z = \frac{az+b}{cz+d} \quad .$$

$S_k(N, \chi)$ is the finite-dimensional Hilbert space of holomorphic functions on H which satisfy

$$f(\gamma z) = \nu(\gamma)(cz+d)^k f(z) \quad \text{for } \gamma \in \Gamma = \Gamma_0(N)$$

and are such that $y^{\frac{k}{2}} |f(z)|$ is uniformly bounded on H. Here $\nu(\gamma) = \chi(d)\left(\frac{c}{d}\right)\overline{\epsilon}_d$ where $\left(\frac{c}{d}\right)$ is the extended quadratic residue symbol (see [6]) and

$$\epsilon_d = \begin{cases} 1, & \text{if } d \equiv 1 \pmod 4, \\ i^{2k}, & \text{if } d \equiv -1 \pmod 4. \end{cases}$$

The inner product on $S_k(N, \chi)$ is defined by

$$\langle f, g \rangle = \int_{\Gamma \backslash H} f(z)\overline{g}(z) y^k \frac{dxdy}{y^2} \quad .$$

Any $f \in S_k(N, \chi)$ has a Fourier expansion

$$f(z) = \sum_{n=1}^{\infty} \hat{f}_n e(nz) \quad .$$

Define $f_n = n^{-\frac{k-1}{2}} \hat{f}_n$. It is expected that for all $\epsilon > 0$, $f_n \ll_\epsilon n^\epsilon$, the best known estimate being $f_n \ll_\epsilon n^{\frac{3}{14}+\epsilon}$ which follows from [3]. By the Rankin-Selberg method

$$\sum_{n \leq X} |f_n|^2 \ll_f X$$

so the trivial bound for $S(X)$ is, as before,

$$S(X) \ll_f \frac{X}{\log^{\frac{1}{2}} X} \quad .$$

We prove in [1] the following

THEOREM : *For all* $\epsilon > 0$

$$S(X) = \sum_{p \leq X} f_p \ll X^{\frac{155}{156}+\epsilon} \quad as \quad X \to \infty \ ,$$

where the summation is over p prime and the implied constant depends only on ϵ *and* f.

Vinogradov's method reduces the estimation of $S(X)$ to that of certain bilinear forms in f_{mn} for various ranges of m and n. We actually use a variant of this method given by Vaughan in [7] which, among other things, simplifies the arguments. We shall consider here only one of the required estimates, namely

$$\sum_{n \leq X} \sum_{m \leq Y}{}' a_m b_n f_{mn} \ll_{\epsilon,f} (X^{\frac{1}{2}} + X^{\frac{1}{4}}Y)(XY)^{\epsilon}\|a\| \, \|b\| \tag{1}$$

where the prime restricts the variable of summation to squarefree values, a_m and b_n are any complex numbers, and $\|a\|^2 = \sum_{m \leq Y} |a_m|^2$.

The trivial bound for the left-hand side of (1) is $(XY)^{\frac{1}{2}+\epsilon}\|a\|\|b\|$ and this would generally be best possible if f_n were multiplicative. In this case we see that f_n is not multiplicative since (1) is non-trivial if $X \gg Y^{2+\epsilon} \gg 1$.

By Cauchy's inequality the proof of (1) is reduced to

$$\sum_{n \leq X} \left| \sum_{m \leq Y}{}' a_m f_{mn} \right|^2 \ll_{\epsilon,f} (X + X^{\frac{1}{2}}Y^2)(XY)^{\epsilon}\|a\|^2 \ . \tag{2}$$

We conjecture that the following self-dual form in fact holds :

$$\sum_{n \leq X}{}' \left| \sum_{m \leq Y}{}' a_m f_{mn} \right|^2 \ll_{\epsilon,f} (X + Y)(XY)^{\epsilon}\|a\|^2 \ . \tag{3}$$

This would be somewhat analogous to the self-dual inequality

$$\sum_{n \leq X}{}'' \left| \sum_{m \leq Y}{}'' a_m \left(\frac{m}{n}\right) \right|^2 \ll_{\epsilon} (X + Y)(XY)^{\epsilon}\|a\|^2 \tag{4}$$

where the double prime restricts the summation to squarefree integers congruent to 1 modulo 4. The possibility that an inequality of this type might hold was suggested orally by Montgomery to the second author in 1984. Jutila has given results related to (4) (see [4] and [5]) but (4) itself is unknown.

For the proof of (2) we require the following estimate :

$$\sum_{n\geq 1} f_{nr}\overline{f}_{ns}\exp\left(-\frac{n}{X}\right) \ll_{\epsilon,f} \delta_{rs}X + (rsX)^{\frac{1}{2}+\epsilon} \tag{5}$$

where r, s are squarefree integers congruent modulo 4 and prime to a number depending only on f. Here δ_{rs} denotes the Kronecker delta. It is important to realize that the uniformity of this estimate in r and s is its key feature. For its proof we may assume that $f(z)$ is a Poincaré series and then f_{ns} may be evaluated as a sum of Kloosterman sums. We substitute this evaluation of f_{ns} into (5). Then we apply Poisson's summation for f_{nr} twisted by an additive character (resulting from the Kloosterman sum) to obtain Gauss-Ramanujan sums. These are estimated to give (5).

Our approach shares some features with the Rankin-Selberg method. However, we avoided this because we had difficulty in establishing the required uniformity in r and s through the functional equation of the Eisenstein series.

The estimate in our theorem should be compared with that of Heath-Brown and Patterson for sums of cubic Gauss sums over prime moduli [**2**]. Their technique is, however, rather different from ours since they use a kind of twisted multiplicativity of cubic Gauss sums to estimate the relevant bilinear forms. Such multiplicativity does not exist in the case of half-integral weight cusp forms.

REFERENCES

[**1**]. W. Duke and H. Iwaniec., Bilinear forms in the Fourier coefficients of half-integral weight cusp forms and sums over primes, *Math. Ann.,* 286 (1990), 783-802.

[**2**]. D.R. Heath-Brown and S.J. Patterson., The distribution of Kummer sums at prime arguments, *J. Reine Angew. Math.,* 310 (1979), 111-130.

[**3**]. H. Iwaniec., Fourier coefficients of modular forms of half-integral weight, *Invent. Math.,* 87 (1987), 385-401.

[**4**]. M. Jutila., On character sums and class numbers, *J. Number Theory,* 5 (1973), 203-214.

[**5**]. M. Jutila., On mean values of Dirichlet polynomials with real characters, *Acta Arith.,* 27 (1975), 191-198.

[6]. G. Shimura., On modular forms of half–integral weight, *Ann. Math.*, 97 (1973), 440-481.

[7]. R.C. Vaughan., Mean value theorems in prime number theory, *J. London Math. Soc.*, 10 (1975), 153-162.

William Duke

Dept. of Mathematics

Rutgers University

New Brunswick, NJ 08903

USA

Henryk Iwaniec

Dept. of Mathematics

Rutgers University

New Brunswick, NJ 08903

USA

Astérisque

NOAM D. ELKIES

Distribution of supersingular primes

Astérisque, tome 198-199-200 (1991), p. 127-132

<http://www.numdam.org/item?id=AST_1991__198-199-200__127_0>

Distribution of supersingular primes

Noam D. Elkies

Let E be a fixed elliptic curve over $\mathbf{Q}$ without complex multiplication, and let j_E be its j-invariant. A *supersingular prime* for E is a rational prime p such that (i) E has good reduction mod p, and (ii) the reduced curve $E_p = E \bmod p$ is supersingular; observe that condition (i) excludes only finitely many primes (those dividing the discriminant of E), and condition (ii) depends only on j_E. Following [7] we define $\pi_0(x)$ to be the number of supersingular $p < x$, and ask for the asymptotic behavior of $\pi_0(x)$ as $x \to \infty$. A naïve heuristic suggests that, since (for $p \geq 5$) E_p is supersingular if and only if it has $p+1$ points over $\mathbf{F}_p$, while in general its number of $\mathbf{F}_p$-points could differ from $p+1$ by as much as $\pm 2p^{1/2}$, each p is supersingular with "probability" roughly $p^{-1/2}$, and so (summing over $p < x$) the expected value of $\pi_0(x)$ should be roughly $x^{1/2}/\log x$. Refinements of this heuristic, together with numerical evidence gathered for several curves E, led Lang and Trotter to make the

CONJECTURE[7]: $\pi_0(x) = (C + o(1))x^{1/2}/\log x$, *for some explicit* $C > 0$ *depending on* j_E.

But it is not even immediately obvious that either $\pi_0(x) = o(\pi(x))$ (that is, that the supersingular primes have density zero) or that $\pi_0(x) \neq O(1)$ (i.e. that there are infinitely many such primes). The former was proved by Serre in 1968 [8] by applying the Čebotarev Density Theorem to the number fields generated by the coordinates of the torsion points of E; later [9] he combined this idea with sieve techniques to obtain the upper bound

$\pi_0(x) \ll x/\log^{3/2-\epsilon}$ (the exponent $3/2-\epsilon$ was recently improved by D. Wan [10] to $2-\epsilon$), and further proved that under the Generalized Riemann Hypothesis (GRH) for these number fields the same method would yield $\pi_0(x) \ll x^{3/4}$. The infinitude of supersingular primes was proved by me in 1986, and generalized in my thesis to curves defined over an arbitrary number field with a real embedding [2, 3]. The main purpose of this report is to describe recent progress on an upper bound for $\pi_0(x)$. We start, however, with a few remarks on the lower bounds that can be obtained from the methods of [2], both to put the upper bounds in context and to introduce some ideas that also figure prominently in these new upper bounds.

For positive $D \equiv 0$ or $3 \bmod 4$, let $P_D(X)$ be the minimal polynomial of the algebraic integer $j((D+\sqrt{-D})/2)$. In [2] it was shown that, if $\{p_1, p_2, \ldots, p_n\}$ is a finite set of primes containing all of E's primes of bad reduction, and $l \equiv 3 \bmod 4$ a sufficiently large prime of which all the p_i are quadratic residues (the existence of such l is guaranteed by Dirichlet's theorem on primes in arithmetic progressions), then one of $P_l(j_E)$ and $P_{4l}(j_E)$ is divisible by a prime p_{n+1}, distinct from each of $p_1, \ldots, p_n$, which is a new supersingular prime for E. Iterating this procedure we not only obtain the infinitude of supersingular primes, but also an implicit upper bound on p_n, and thus equivalently a lower bound on $\pi_0(x)$: Dirichlet's theorem gives an effective bound on the least admissible l, and the absolute value of the numerator of $P_D(j_E)$ (and thus also its factor p_{n+1}) is easily bounded above by $O(\exp C \cdot D^{1/2} \log^2 D)$. Unfortunately this bound on p_n is astronomical—an n-fold iterated exponential!—unless we assume the GRH for real Dirichlet characters. Applying the standard explicit formulas for the number of primes in an arithmetic progression, we then find that $\pi_0(x) \gg \log\log\log x$; this bound, since independently discovered by Brown [1], has been improved

by R. Murty to $\pi_0(x) \gg (\log\log x)^{1/2}$. A better method is to assume that the $p_i (1 \leq i \leq n)$ already comprise all the supersingular primes less than x, and then use not only the first but all admissible primes $l \ll x^{1/2}$, obtaining many new supersingular primes between x and $x' \ll \exp(Cx^{1/4}\log^2 x)$, all distinct by [4]. Assuming again the GRH, we find that either $\pi_0(x) \gg \log x$ or there are enough admissible $l \ll x^{1/2}$ to ensure $\pi_0(x') \gg \log x'$; either way we obtain the bound (Theorem 2 in my thesis):

THEOREM A: *Under GRH for real Dirichlet characters,* $\pi_0(x) \gg \log\log x$.

It occurred to me in 1987 that these ideas might be useful for getting an upper bound on $\pi_0(x)$; one version of this idea, mentioned in my thesis, is the

OBSERVATION (with R. Murty): *If, for some positive* θ, *each supersingular prime* p *of* E *divides* $P_D(j_E)$ *for some* $D \ll p^\theta$, *then* $\pi_0(x) \ll x^{3\theta/2}\log x$.

Indeed, by the above estimate on the size of $P_D(j_E)$, the product of all of E's supersingular primes less than x would divide the product of the numerators of $P_D(j_E)$ over $D \ll x^\theta$, which is bounded by

$$\prod_{D \ll x^\theta} \exp(C \cdot D^{1/2}\log^2 D) \ll \exp O(x^{3\theta/2}\log^2 x);$$

so the sum of these primes' logarithms would be $\ll x^{3\theta/2}\log^2 x$, and their number $O(x^{3\theta/2}\log x)$. [Several remarks are in order here: First, that for this Observation to be of any use we must have θ strictly less than 2/3; second, that this proof fails only when E has complex multiplication, because that's exactly when one of the $P_D(j_E)$ vanishes (and fail it must in that case, since for a CM curve $\pi_0(x) \sim \pi(x)/2$); third, that the bound $\pi_0(x) \ll x^{3\theta/2}\log x$ would be unconditional, not depending on GRH or other unproved hypotheses, provided the same was true of the proof of $D \ll p^\theta$; and last,

that we can save a factor of $\log x$ by more carefully estimating the size of $\prod_{D \ll x^\theta} P_D(j_E)$, obtaining $D \ll p^\theta \Rightarrow \pi_0(x) \ll x^{3\theta/2}$.]

Thus the problem of estimating θ, which I raised in [2] in the context of computing large supersingular primes, assumes a new theoretical significance. Now p divides $P_D(j_E)$ if and only if the supersingular curve E_p has complex multiplication by $(D + \sqrt{-D})/2$, that is, if the quadratic order $\mathbf{Z}[\frac{1}{2}(D + \sqrt{-D})]$ imbeds into the endomorphism ring A of E_p, or equivalently if A contains an endomorphism α whose discriminant $(\alpha - \bar{\alpha})^2 = \mathrm{Tr}^2(\alpha) - 4\deg(\alpha)$ is $-D$. Thus the least D such that p divides $P_D(j_E)$ is the smallest nonzero value attained by the positive-definite quadratic form $(4\deg - \mathrm{Tr}^2)$ on the rank-3 lattice $A_1 = A/\mathbf{Z}$. In [2] I used a simple geometry-of-numbers argument to estimate this value: A_1 has covolume $2p$ (this follows from Deuring's theorem that A has reduced discriminant p), so it must contain a nonzero vector of norm at most $2p^{2/3}$. Unfortunately this gives only $\theta = 2/3$, the smallest useless value of θ.

But computations suggested that this bound might not be best possible. Indeed, recently Kaneko obtained [6]:

THEOREM: *E_p has an endomorphism of discriminant $(-D)$ for some positive $D \leq 4\sqrt{p/3}$.*

Sketch of proof: Note that while in general a supersingular j-invariant in characteristic p need only lie in $\mathbf{F}_{p^2}$, the j-invariant of E_p is necessarily in $\mathbf{F}_p$ (though most of its endomorphisms can only be defined once we extend scalars to $\mathbf{F}_{p^2}$). Thus A contains a square root ϕ of $-p$, namely the Frobenius endomorphism. Kaneko now uses Ibukiyama's classification [5] of such quaternion algebras A to show that $A/\mathbf{Z}$ contains a rank-2 sublattice of determinant $4p$, whence the Theorem follows. This sublattice consists of the lattice vectors orthogonal to the image of the Frobenius endomorphism ϕ

in A_1. When Serre read this he remarked that the order of magnitude of the determinant of the sublattice, and thus the bound $D \ll \sqrt{p}$, could be easily obtained by "pure thought" without invoking the explicit classification in [5]: the Galois involution of $\mathbf{F}_{p^2}$ induces an involution ι of A (conjugation by ϕ) whose invariant subring A^+ is either $\mathbf{Z}[\phi]$ or possibly $\mathbf{Z}[\frac{1}{2}(1+\phi)]$ if $p \equiv 3 \bmod 4$; let $A^- \subset A$ be the anti-invariant sublattice $\{\alpha : \iota\alpha = -\alpha\}$ of rank 2. Then $A^+ \oplus A^-$ is of bounded index in A (the quotient is an elementary abelian 2-group of rank at most 4), so since A has determinant p^2 and A^+ has determinant at least p, the determinant of A^- with the quadratic form $\deg(\cdot)$ is $\ll p$. Also A^- is orthogonal to A^+ and so in particular to 1, whence any $\alpha \in A^-$ has trace zero and determinant $-4\deg(\alpha)$. Therefore the image of A^- in $A/\mathbf{Z}$ is again a rank-2 lattice of determinant $\ll p$ and we are done.

Either way we thus have $\theta = 1/2$ and conclude:

THEOREM B: $\pi_0(x) \ll x^{3/4}$.

Note that this is exactly the bound obtained by Serre under GRH; it is unclear what if any significance this coincidence has.

Details of the analytic estimates used in the proofs of Theorems A and B will appear elsewhere.

References

[1] Brown, M.L.: Note on supersingular primes of elliptic curves over $\mathbb{Q}$. *Bull. London Math. Soc.* **20** (1988), 293–296.

[2] Elkies, N.D.: The existence of infinitely many supersingular primes for every elliptic curve over $\mathbb{Q}$. *Invent. Math.* **89** (1987), 561–567.

[3] Elkies, N.D.: Supersingular primes for elliptic curves over real number fields. *Compositio Math.* **72** (1989), 165–172.

[4] Gross, B. H., Zagier, D.: On singular moduli, *Jour. für die reine und angew. Math.* **335** (1985), 191–220.

[5] Ibukiyama, T.: On maximal orders of division quaternion algebra of the rational number field with certain optimal embeddings. *Nagoya Math. J.* **88** (1982), 181–195.

[6] Kaneko, M.: Supersingular j-invariants as singular moduli mod p. *Osaka J. Math.* **26** (1989), 849–855.

[7] Lang, S., Trotter, H.: *Frobenius distributions in* GL_2*-extensions.* Lect. Notes Math. 504, 1976.

[8] Serre, J.-P.: *Abelian l-adic representations and elliptic curves.* New York: Benjamin 1968.

[9] Serre, J.-P.: Quelques applications du théorème de densité de Chebotarev. *IHES Publ. Math.* **54** (1981), 123–201.

[10] Wan, D.: On the Lang-Trotter Conjecture. *J. Number Th.* **35** (1990), 247–268.

Noam D. Elkies
Department of Mathematics
Harvard University
Cambridge, MA 02138 USA

Astérisque

BOAS EREZ

A survey of recent work on the square root of the inverse different

Astérisque, tome 198-199-200 (1991), p. 133-152

<http://www.numdam.org/item?id=AST_1991__198-199-200__133_0>

A SURVEY OF RECENT WORK ON THE SQUARE ROOT OF THE INVERSE DIFFERENT

by

Boas EREZ

We will give a survey of recent work done by several authors on the Galois-hermitian module obtained by restricting the trace form of a Galois extension K/F to the ideal in K which -when it exists- is the square root of the inverse different of K/F. This is the only additive Galois module, apart from the ring of integers, whose structure is now fairly well known.

Although the work exposed here has benefitted enormously by the techniques developed by A. FRÖHLICH, M.J. TAYLOR *et alia* to study the structure of the ring of integers, we will not suppose here that the reader is acquainted with them, so that this paper can also serve as an introduction to their work.

We shall begin by fixing the notations which will be in force throughout the paper and then we will define the object of our interest. Next an example is given to try to motivate our subsequent discussion. In Section 2 we analyze the situation for weakly ramified extensions, while in Section 3 we drop the restrictions on ramification but consider only abelian extensions. We also give some details concerning the proofs of several results discussed in Section 3 which are not to be published elsewhere. These are to be found in two appendices due to D. BURNS.

Acknowledgements

I heartily thank C. BACHOC and D. BURNS for their assistance in preparing this paper and J. QUEYRUT for very helpful discussions at an earlier stage of my work, in particular he suggested the use of the Adams operation for Theorem 2.7.

1. The square root of the inverse different

Notations.

The arithmetic side. Let us denote by : K/F a finite Galois extension of either number fields or finite extensions of a p-adic field $\mathbb{Q}_p$, $G = \mathrm{Gal}(K/F)$ its Galois group, $\mathrm{Tr}_{K/F}$ the bilinear trace form of K/F, $\mathbb{Z}_L$ the ring of integers in L, $D(K/F)^{-1}$ the inverse different of K/F.

The algebraic side. We will have to consider : FG (resp. $\mathbb{Z}_F G$) the group algebra of G over F (resp. $\mathbb{Z}_F$), m_G the multiplication form on FG for which the elements in G form an orthonormal basis.

Recall that by a formula due to Hilbert (see e.g.[S1] Chap. IV.1, Prop.4) we can compute the order of the different $D(K/F)$ at any prime P in K by means of the sequence $\{G_i = G_i(P, K/F)\}$ of ramification sub-groups of G :

$$\mathrm{ord}_P(D(K/F)) = \sum_{i>-1} (\mathrm{ord}(G_i) - 1) \ . \tag{1.1}$$

As a consequence we have that for instance in an odd degree Galois extension K/F there exists a unique ideal $A(K/F)$ such that

$$A(K/F)^2 = D(K/F)^{-1} \ . \tag{1.2}$$

We will call the ideal A satisfying (1.2) the *square root of the inverse different* (of K/F).

Since G acts on K as a group of isometries of the trace form $\mathrm{Tr}_{K/F}$ and since the dual with respect to the trace form of an ideal B in K is the ideal $B^{-1}D(K/F)^{-1}$, we see that by restricting the trace form to the square root of the inverse different we get a self-dual integral $\mathbb{Z}_F G$-hermitian form $(A(K/F), \mathrm{Tr}_{K/F})$. One would like to have a description of this form up to equivariant isometry (see [C-P] Question (V.4.3)). It is the aim of this survey to summarize what is known on this problem.

1.1. Example

We show how one can use the results on the hermitian module $(A(K/F), \mathrm{Tr}_{K/F})$ to describe the structure of the module $(\mathbb{Z}_K, \mathrm{Tr}_{K/F})$.
Observe that $\mathbb{Z}_K \leq A(K/F) \leq D(K/F)^{-1}$. Suppose that K/F is tamely ramified, that is all its first ramification groups are trivial. To ensure the existence of $A(K/F)$ suppose K/F is Abelian of odd degree and for simplicity let $F = \mathbb{Q}$.

Since the degree of the extension $K/\mathbb{Q}$ is odd, we know that there is a $\mathbb{Q}G$-equivariant isometry between $(K, \mathrm{Tr}_{K/\mathbb{Q}})$ and $(\mathbb{Q}G, m_G)$ (see [B-L] for a proof under more general hypothesis). So $(\mathbb{Z}_K, \mathrm{Tr}_{K/F})$ is isometric to a $\mathbb{Z}G$-ideal M in $\mathbb{Q}G$ which is locally free because we are supposing that $K/\mathbb{Q}$ is tame. We shall now define one such ideal $M = M(K/\mathbb{Q})$ by defining its localizations $M_p = \mathbb{Z}_p \otimes M$ for all primes p of $\mathbb{Q}$. So fix a prime number p and a prime P in K above p, then choose a uniformizing parameter π in K_P. Let $\theta_p := \theta_{0,p}$ be the *injective* character of the inertia group $I(p) := G_0(P, K/F)$ defined by

$$\theta_p(g) = g(\pi)/\pi \bmod P$$

(see [S1] Chap.IV.2 Prop.7). θ_p generates the (cyclic) group of characters of $I(p)$ and to each integer i between 0 and $e(p) := \mathrm{ord}(I(p))$ we can associate in $\mathbb{Z}_pG$ the idempotent $e_{i,p} = (1/e(p)) \sum_{I(p)} \theta_p^i(g) g^{-1}$.

Now form the sum $E_p = e_{0,p} + e_{1,p} + \cdots + e_{m,p}$ where $m = (e(p) - 1)/2$. Then we define M_p to be $M_p := (p, E_p)\mathbb{Z}_pG$. Of course if p doesn't ramify in K/F (i.e $I(p) = \{1\}$), then $M_p = \mathbb{Z}_pG$ so M is well defined. The interest of M stems from the following result -which is shown in [E-M].

THEOREM 1.3. *Under the restrictions introduced above we have*

(i) $M(K/\mathbb{Q})A(K/\mathbb{Q}) = \mathbb{Z}_K$.

(ii) *The following conditions are equivalent*

(a) $(\mathbb{Z}_K, \mathrm{Tr}_{K/\mathbb{Q}})$ *is* $\mathbb{Z}G$*-isometric to* $(M(K/\mathbb{Q}), m_G)$

(b) $(A(K/\mathbb{Q}), \mathrm{Tr}_{K/\mathbb{Q}})$ *is* $\mathbb{Z}G$*-isometric to* $(\mathbb{Z}G, m_G)$.

Now, under the hypothesis of this example one can show that (ii-b) is true (see Theorem 2.9 and Remark 2.10 below), so that -in this particular case- we have a more precise description of $(\mathbb{Z}_K, \mathrm{Tr}_{K/\mathbb{Q}})$ than in [T1] (see [E-M] for more details).

2. Weakly ramified extensions

Our next result will give necessary and sufficient conditions for the square root of the inverse different $A(K/F)$ to be locally isomorphic to $\mathbb{Z}_FG$, in a way completely analogous to what is known as E. NOETHER's characterization of tame extensions (see e.g. [F1] Theorem 3, p.26).

DEFINITION 2.1. The Galois extension K/F is *weakly ramified* if all its second ramification groups (in lower numbering) are reduced to the identity.

Instances of weakly ramified extensions are

(a) all tamely ramified extensions

(b) absolute Galois extensions of odd prime degree.

(c) the dihedral extension obtained as the compositum of $\mathbb{Q}((-3)^{1/2})$ and the (non-Galois) cubic field $\mathbb{Q}((2)^{1/3})$ (see e.g.[C](16.29) and (17.31)).

Observe that (Galois) sub-extensions of weakly ramified extensions are weakly ramified, but that the compositum of weakly ramified extensions is not necessarily weakly ramified : indeed if p is an odd prime, then the cyclotomic field $\mathbb{Q}(p^2)$ of p^2-th roots of unity is not even weakly ramified over $\mathbb{Q}(p)$ although it is the compositum of $\mathbb{Q}(p)$ and the unique subfield of degree p over $\mathbb{Q}$ which it contains.

THEOREM 2.2. *Suppose* ord(G) *is odd. Then* $A(K/F)$ *is locally free over* $\mathbb{Z}_F G$ *if and only if* K/F *is weakly ramified.*

The necessity of a condition on the second ramification groups for *any* ambiguous ideal to be locally free over $\mathbb{Z}_F G$ has been shown by S.ULLOM in [U1], 2.1. The converse is shown in [E2] by using the results of [U2].

Remark. The computations in [Mi1] et [Mi2] show that the characterization of the first ramification group as "vertex of the ring of integers" has no analog even for the second ramification group -as one would hope in light of Theorem 2.2. (see also [F1] Note 3 to Chapter 1).

H1. HYPOTHESIS. In the rest of this section we will always suppose that the order of G is odd and that K/F is weakly ramified.

To get more precise results in this situation - i.e., to investigate when $A(K/F)$ is globally free over $\mathbb{Z}_F G$ - we are led to describe the class defined by $A(K/F)$ in the group $Cl(\mathbb{Z}G)$ of stable isomorphism classes of locally free $\mathbb{Z}G$-modules (we will eventually have to restrict scalars from $\mathbb{Z}_F$ to $\mathbb{Z}$). Recall that since the order of G is assumed to be odd, the stable isomorphism class defined by $A(K/F)$ completely determines its isomorphism class. We now recall the description of $Cl(\mathbb{Z}_F G)$ in terms of Galois homomorphisms (see (2.3) below). This description will allow us to express the class defined by $A(K/F)$ in a way relating it to the arithmetic of the extension K/F. For ease of notation let $R = \mathbb{Z}_F$, $\Lambda = \mathbb{Z}_F G$, $A = FG$ and $C = \text{center}(FG)$. If M is a rank one locally free module over Λ, then for every (finite) prime p in R there exists m_p in M and m_0 such that $\Lambda_p m_p = R_p \otimes_R M$ and $Am_0 = F \otimes_R M$. So for every (finite) prime

p there exists b_p in $(A_p)^x$ such that $m_p = b_p m_0$. Note that since $(\Lambda m_0)_p$ and M_p coincide for almost all p, b_p is a unit in Λ_p for almost all p. It follows that M is isomorphic over Λ to the ideal Λb in A defined at each local completion by $R_p \otimes \Lambda b = \Lambda_p b_p$. These considerations lead to the idelic description of $Cl(\Lambda)$, which generalizes the idelic description of class groups of number fields. Sending b to the class (Λb) gives a surjective homomorphism from the ideles $J(A)$ to $Cl(\Lambda)$ whose kernel can be computed (see [C-R]Vol.II (49.22)). By taking the reduced norm to the center $\mathrm{nrd} = \mathrm{nrd}_{A/C}$ (and taking into account the infinite places) one obtains the isomorphism

$$Cl(\Lambda) \cong J(C)/C^x \mathrm{nrd}(U(\Lambda))$$

where $U(\Lambda)$ are the unit ideles of Λ (see[C-R]Vol.II(49.23)). Under this isomorphism the class defined by M corresponds to the class of the reduced norm of b. The final step in the description consists in the following. Choose E to be a "big enough" (finite) extension of F-at least Galois over F and splitting A and write R_G for the group of virtual characters of G. Recall that $C = \Pi F(\chi_i)$, product over a set of representatives of the orbits of absolutely irreducible characters of G. We have an isomorphism $f : C^x \cong \mathrm{Hom}_{\Omega(F)}(R_G, E^x)$ defined by $f(\Pi c_i)(\chi) = \Pi f(c_i)(\chi)$ and $f(c_i)(\chi) = 1$ unless $\chi = \chi_i^\omega$ is in the orbit of χ_i, in which case $f(c_i)(\chi) = c_i^\omega$. This isomorphism then extends to the idele groups and we only have to interpret the image of the reduced norm as so-called determinant homomorphisms to obtain FRÖHLICH's Hom-description :

$$Cl(\Lambda) \cong \mathrm{Hom}_{\Omega(F)}(R_G, J(E))/\mathrm{Hom}_{\Omega(F)}(R_G, E^x)\mathrm{Det}\ (U(\Lambda)) \qquad (2.3)$$

(see[C-R] Vol.II (52.11), [F1] II.1). Here the class defined by M corresponds to the Ω-invariant homomorphism f which on an irreducible character χ takes the idelic value $(f_p(\chi))_p$, where -in $E_p^x = (F_p \otimes E)^x$)-

$$f_p(\chi) = \det_\chi(b_p) \qquad (2.4)$$

is the determinant of the matrix in $GL(E_p)$ obtained by evaluating any extension of an E-representation $T = T_\chi$ with character χ on the (invertible) group algebra element b_p.

Remark. Of course all this goes through for more general orders Λ than group rings.

We will now proceed to give a representative homomorphism for the class defined by $A(K/F)$ in $Cl(\mathbb{Z}_F G)$. Here E will also have to contain K and the

values of arithmetic functions needed. So fix local normal generators m_p of $A(K/F)_p$ over $\mathbb{Z}_{F,p}G$ and a normal generator m_0 of K over FG. Let b_p be such that $b_p m_0 = m_p$. Define the idelic resolvent $(m|\chi)$ by letting its p-component be $(m|\chi)_p = (m_p|\chi) = \det(\sum_G T(g^{-1})g(m_p))$ with $T = T_\chi$ as after (2.4). Then $\mathrm{Det}_\chi(b) = (m|\chi)/(m_0|\chi)$ (see [F1] I.4.1). Observe this is immediate for abelian characters, for which we get the classical Lagrange resolvents. Already because $\mathbb{Z}_F$ need not be a principal ring we will restrict scalars from $\mathbb{Z}_F$ to $\mathbb{Z}$ and consider $A(K/F)$ as a $\mathbb{Z}G$-module; this forces us to replace the above resolvents with norm-resolvents $\mathcal{N}_{F/\mathbb{Q}}(m|\chi)$ -which we will not define (see [F1] Theorem 2 and (2.16)). We will make a full use of the Hom-description in that we will need the (second) Adams operation $\Psi = \Psi_2$ on R_G : this is the endomorphism of R_G defined by $\Psi(\chi)(g) = \chi(g^2)$ (see e.g. [C-R] Vol. I, 12B, [K]). Let $\tau(K/F, \Phi)$ be the Galois-Gauss sum attached to the field extension K/F and the character Φ of G (= $\mathrm{Gal}(K/F)$) (as in say [F1] I.5 or [Ma]). We now change the representative homomorphism above with the aid of the Gauss sum and Ψ.

PROPOSITION 2.5. ([E2] Theorem 3.6). *Suppose* (H1) *is fulfilled, then the class defined by* $A(K/F)$ *in* $Cl(\mathbb{Z}_F G)$ *is represented by the Galois homomorphism* $v_{K/F}$ *which on the character* χ *of* R_G *takes the idelic value* $v_{K/F}(\chi) = \mathcal{N}_{F/\mathbb{Q}}(m|\chi)\tau(K/F, \Psi(\chi) - \chi)^{-1}$.

The proof of this proposition follows -as in the study of rings of integers- from the fact that $\mathcal{N}_{F/\mathbb{Q}}(m_0|\chi)$ and $\tau(K/F, \Psi(\chi) - \chi)$ behave in the same way under Galois action (see[F1] III.3).

Remark 2.6. One is led to consider the representative homomorphism given in the proposition after having noticed the decomposition in terms of the Jacobi sums $\tau(\chi)^2/\tau(\chi^2)$ as given in [E1] for absolute Galois extensions of odd prime degree.

Now that we have a nice representative homomorphism we can try to show it lies in the denominator of the right hand side of (2.3). We have not yet succeeded in doing this in general although it is true for tame extensions (see Theorem 2.8 below), howewer in general we can prove the following. Let $\mathcal{M}$ be any maximal order in $\mathbb{Q}G$ containing $\mathbb{Z}G$ and let $D(\mathbb{Z}G)$ denote the kernel of the (surjective) homomorphism from $Cl(\mathbb{Z}G)$ to $Cl(\mathcal{M})$ obtained by extending scalars from $\mathbb{Z}G$ to $\mathcal{M}$. We know that $D(\mathbb{Z}G)$ does not depend on $\mathcal{M}$.

THEOREM 2.7. ([E2] Theorem 2.) *Suppose* (H1) *is fulfilled, then* $v_{K/F}$ *lies in* $D(\mathbb{Z}G)$, *that is* $\mathcal{M} \otimes_{\mathbb{Z}G} A(K/F)$ *is free over* $\mathcal{M}$.

As with FRÖHLICH in his proof of the Martinet Conjecture for tame extensions (see [F1] Theorems 5 and 23), we show that the components of the ideles $\mathcal{N}_{F/\mathbb{Q}}(m|\chi)$ and $\tau(K/F, \Psi(\chi) - \chi)$ are the same up to units, so that $v_{K/F}$ actually lies in $\mathrm{Hom}_\Omega(R_G, U(E))$ and hence is zero in $Cl(\mathcal{M})$ (see [F1] I.2.19). By using the functorial properties of the ideal $A(K/F)$ and of the homomorphisms involved this amounts to a computation in local totally ramified extensions analogous to the one in [F1], III.7 for the tame case, but involving non-abelian local characters in the wild case (see [E2]).

THEOREM 2.8. ([E2] Theorem 3.) *Suppose* (H1) *is fulfilled, but assume also that* K/F *is at most tamely ramified, then* $A(K/F)$ *is free over* $\mathbb{Z}G$.

Given Theorem 2.7 above and its proof (!), this is an almost formal consequence of M.J. TAYLOR's work on Galois-Gauss sums and on groups of determinant homomorphisms together with his joint work with Ph. CASSOU-NOGUÈS on Adams operations (see [F1] Theorems 30, 31 and 10, [CN-T] Théorème 1′ and (2.7) or [T2] Theorems 8.1.2 and 9.1.2, [E2]). In the absolute abelian case we have a complete picture for the hermitian structure as well.

THEOREM 2.9. ([E3] or [E-M] Theorem 4.1.) *Suppose that* $F = \mathbb{Q}$ *and that* $G = \mathrm{Gal}(K/\mathbb{Q})$ *is abelian of odd order. Then the following are equivalent :*

(a) K/F *is weakly ramified*

(b) *for every prime* p *in* $\mathbb{Z}$ *the order of the inertia group* $G_0(K/\mathbb{Q}, p)$ *is either equal to* p *or prime to* p

(c) $(A(K/\mathbb{Q}), \mathrm{Tr}_{K/\mathbb{Q}})$ *is isometric to* $(\mathbb{Z}G, m_G)$

(d) $A(K/\mathbb{Q})$ *is free over* $\mathbb{Z}G$.

This is less involved than the previous results, the hardest part being the proof that (b) implies (c). We exhibit explicit self-dual normal bases - taken from [E1]- for special extensions $K(p)$, one for each prime p ramified in $K/\mathbb{Q}$, so that : K is contained in the compositum $L = \Pi_p K(p)$, the $K(p)$ are arithmetically disjoint in pairs -hence $(A(L/\mathbb{Q}), \mathrm{Tr}_{L/\mathbb{Q}})$ is the tensor product of the $(A(K(p)/\mathbb{Q}), \mathrm{Tr}_{K(p)/\mathbb{Q}})$ -, and also $A(K/\mathbb{Q}) = \mathrm{Tr}_{L/K}(A(L/\mathbb{Q}))$. (Of course $K(p)$ can be chosen to be the field corresponding to the group X_p of p-parts of the Dirichlet characters associated to K (see [E-M]).)

Recall that by Section 1.1 this theorem gives the structure of the hermitian pair $(\mathbb{Z}_K, \mathrm{Tr}_{K/\mathbb{Q}})$ in this special situation.

Remark 2.10. The recent paper [E-T] deals with the hermitian structure of both the ring of integers $\mathbb{Z}_K$ and the square root of the inverse different $A(K/F)$ in arbitrary odd degree tamely ramified Galois extensions K/F. It contains a generalization of the results of [E-M]. In particular it generalizes the definition of the "comparison" module $M(K/F)$ of Example 1.1 above and it shows how to use Theorem 2.8 to get a description of the class that $A(K/F)$ defines in the Grothendieck group of (locally free) hermitian modules over $\mathbb{Z}G$.

3. Very wildly ramified extensions

Unless explicitly stated, in this section we will always assume.

H2 - HYPOTHESIS. $F = \mathbb{Q}$, $G = \mathrm{Gal}(K/F)$ is abelian and K/F is such that the square root of the inverse different $A(K/F)$ exists.

According to the results above, if K/F is not weakly ramified then on the one hand $A(K/F)$ cannot even be locally isomorphic to $\mathbb{Z}G$ (Theorem 2.2) and on the other hand the trace form on $A(K/F)$ cannot be the standard one (Theorem 2.9). To encompass these difficulties one compares $A(K/F)$ to its associated order Λ, that is the order $\Lambda(A(K/F))$ in FG of elements stabilizing $A(K/F)$. The local problem was considered by D. BURNS who showed

THEOREM 3.1. *Under* (H2) $A(K/F)$ *is locally free over its associated order* $\Lambda(A(K/F))$.

A proof of this theorem is given in Appendix A below.

Remark 3.2. There exist local cyclic extensions $K/F/\mathbb{Q}_p$ in which no fractional ideal is locally free over its associated order; for example if F is absolutely unramified, then this is so for any totally ramified cyclic extension K/F of degree rp^2 with $r > p^2$ (see [Bu2]).

BURNS predicted that the local isometry class would only depend on the group structure of G together with its inertia subgroups. By using Theorem 3.5 below, he and the author were able to show

THEOREM 3.3. *Let* p *be an odd prime and let* $K/\mathbb{Q}_p$ *and* $K'/\mathbb{Q}_p$ *be abelian extensions in which the inverse different has a square root. Suppose* $K/\mathbb{Q}_p$ *and* $K'/\mathbb{Q}_p$ *are such that there exists an isomorphism between their Galois groups which restricts to one between their inertia groups, then there is an equivariant isometry between* $(A(K/\mathbb{Q}_p), \mathrm{Tr}_{K/\mathbb{Q}_p})$ *and* $(A(K'/\mathbb{Q}_p), \mathrm{Tr}_{K'/\mathbb{Q}_p})$.

Proof. We refer to the notation introduced in Appendix A for the proof of Theorem 3.1. By (A.2) the A decompose as

$$A = \bigoplus_{\chi} e(\chi)A = e(1)A \oplus \bigoplus_{\chi \neq 1} (e(\chi) + e(\overline{\chi}))A \ .$$

These are orthogonal sums with respect to the trace form. The summand corresponding to the identity character is dealt with by Theorem 3.5 below : it corresponds to a cyclic p-extension. We then observe that on the summands of the form $(e(\chi)+e(\overline{\chi}))A$ the trace form is even, hyperbolic and self-dual. By [Bas] (4.4), there is only one such form on a projective module over a commutative ring, so we are done by Theorem 3.1.

∎

Remark 3.4. It is shown in [E-M] that for two $\mathbb{Z}G$-projective ideals in $\mathbb{Q}G$, say L and M, the *forms* (L, m_G) and (M, m_G) are locally isometric everywhere if and only if the "discriminant *modules*" $L^\sharp/L$ and $M^\sharp/M$ are isomorphic (here $L^\sharp$ is the dual of L with respect to m_G). Theorem 3.3 would also be a consequence of a result of this kind with $\mathbb{Z}G$ replaced by the associated order of the square root of the inverse different.

The local structure is thus fairly well known, so let us consider global extensions.

THEOREM 3.5. *Suppose* (H2) *holds, and assume the order of G to be odd. If for every prime p of $\mathbb{Q}$ either $G_0(K/\mathbb{Q}, p)$ is a p-group or has order prime to p, then there exists an equivariant isometry between $(A(K/\mathbb{Q}), \mathrm{Tr}_{K/\mathbb{Q}})$ and $(\Lambda(A(K/\mathbb{Q})), n_G)$ where n_G is a form on $\mathbb{Q}G$ not depending on K.*

The proof of this theorem was obtained in two steps. First in [B-E] the Hermitian pair $(A(K/\mathbb{Q}), \mathrm{Tr}_{K/\mathbb{Q}})$ was studied in detail in the special case of cyclic p-extensions totally ramified at p. For instance if the order of G is p^n with $p \neq 3$ and n even, we have that $(A(K/\mathbb{Q}), \mathrm{Tr}_{K/\mathbb{Q}})$ is $\mathbb{Z}G$-isometric to an orthogonal sum $< 1 > \oplus B_2 \oplus B_4 \oplus \ldots \oplus B_n$ where the $B_i = B_i(p)$ are indecomposable, even bilinear forms independent of K with a nice description ; their root system is $(p^{i-2} + p^{i-1})\mathbb{A}_{p-1}$ (standard notation). Later C. BACHOC observed that the results of [B-E] together with an explicit description of the associated order $\Lambda(A(K/\mathbb{Q}))$ were sufficient -via a construction like that given for Theorem 2.9 above- to prove the theorem in the general case under the stated restrictions. Details can be found in [Ba], where a description of n_G is also given.

Remark. We observe that in all the situations so far considered the form

$(A(K/F), \mathrm{Tr}_{K/F})$ always turned out to have a very "symmetric" system of minimal vectors.

In light of Remark 3.2 one couldn't hope for such a precise description in the relative case ($F \neq \mathbb{Q}$), but even for absolute extensions -and quite unexpectedly- D. BURNS was able to prove the following

THEOREM 3.6. *Given any integer n, there exist infinitely many abelian extensions $K = K_n/\mathbb{Q}$ with a square root of the inverse different satisfying the following : let $G_K = \mathrm{Gal}(K/\mathbb{Q})$ and let $\mathcal{M} = \mathcal{M}_K$ denote the maximal order in $\mathbb{Q}G_K$. Write $\mathcal{M}A(K/\mathbb{Q})$ for the smallest $\mathcal{M}$-module in K containing $A(K/\mathbb{Q})$. Then the order of the class of $\mathcal{M}A(K/\mathbb{Q})$ in the locally free class group of $\mathcal{M}$ is greater than n. Moreover, given any odd prime p, one can even choose the extensions $K/\mathbb{Q}$ to be of p-power conductor (and hence cyclic).*

This theorem shows that the analog of LEOPOLDT's Hauptsatz in [L] is false for the square root of the inverse different. In Appendix B the reader will find a complete proof - by BURNS - of the fact that the unique extension of absolute degree 39 and conductor 13^2 is the smallest example of an extension $K/\mathbb{Q}$ for which $\mathcal{M}A(K/\mathbb{Q})$ is not free over $\mathcal{M}$.

In conclusion we can say that, although many results on the square root of the inverse different we have discussed have perfect analogues concerning the ring of integers, some have not and we hope that the parallels that can be drawn will help to throw a different light on this area of research.

Appendix A. Sketch proof of Theorem 3.1

We follow D. BURNS. For the proof it will be sufficient to consider local extensions and by functoriality properties (see e.g. [Be], 2.1) we can even restrict our attention to totally ramified extensions. So let K/F be a local totally ramified Galois extension over $\mathbb{Q}_p$ with Galois group $G = Gal(K/F)$. Let $A = A(K/F)$ and let Λ be its associated order in FG. The strategy of the proof is the following : we show that Λ is weakly self-dual, that is we show that Λ is isomorphic to its linear dual $\Lambda^* = Hom(\Lambda, \mathbb{Z}_F)$. By [F2] Theorem 10 on page 211, this will imply that A is isomorphic to Λ. To show the self-duality of Λ we shall use Theorem 2 of [Bu1] which relates local isomorphism to two other equivalence relations on lattices : factor equivalence (also discussed in [F3]) and G-o-equivalence. (To use this theorem we need to know that F is absolutely unramified). To check these equivalence relations we will need a precise description of the maximal order $\mathcal{M}$ in FG and of Λ.

To begin with, G decomposes into a direct product $G = P \times C$, where P is the p-Sylow subgroup in G. Let r (resp. p^n) be the order of C (resp. P). It is well known that r divides $p-1$.

Case I : p odd. Here G is cyclic and by Hypothesis (H2) r is odd. For i between 0 and n, let $H(i)$ be the subgroup of order p^i in P and let $e(i)$ be the corresponding "trace" idempotent defined by

$$p^i e(i) = \Sigma_{H(i)} h.$$

(A.1) We record the fact that if $k > l$ then $e(k)e(l) = e(k)$. Let also $P = < g >$ and $f = g - 1$.

(A.2) For any character χ of C let :

$$e(\chi) = (\Sigma_C \chi(c^{-1})c)/r.$$

Observe that $e(\chi)$ is in $\mathbb{Z}_L C$ so any G-module M decomposes into $M = \oplus e(\chi)M$, with the sum taken over all characters χ of C. In particular the maximal order $\mathcal{M}$ decomposes in this way and by work of A.-M. BERGÉ a basis of $e(\chi)\mathcal{M}$ is given by the set

$$\{e(\chi)e(i)f^{j(i)}\} \tag{A.3}$$

where $0 \leq i \leq n$ and $j(i)$ runs over a suitable range (see [Bu2]). Let us now check that $\Lambda \cong \Lambda^*$. Since G is cyclic in this case, Λ is factor equivalent to Λ^* and so by Theorem 2 of [Bu1] it is sufficient to check G-o-equivalence. More precisely, for all "trace" idempotents e corresponding to subgroups of G, we must show that both $(\Lambda^*)^e$ and Λ^e have the same associated orders in FGe (see [Bu1] Section 2). But, for any lattice M, the associated order of M equals the associated order of its linear dual M^* and there is also a natural identification $(M^*)^e = (eM)^*$, and hence we must only check that for each "trace" idempotent e :

$$e\Lambda \text{ equals the associated order of } \Lambda^e \text{ in } FGe. \tag{A.4}$$

Now, if e belongs to Λ, then (A.4) is easily verified ; so (A.4) certainly holds for all idempotents e corresponding to subgroups of C, since these are sums of the idempotents $e(\chi)$ and $e(\chi)A \leq A$ by the above observation. Moreover, a simple computation shows (or see [B-E] Proposition 2.3.4) that :

(A.5) for even i, the idempotents $e(i)$ are in Λ,

(A.6) for all i, $fe(i)$ is in Λ.

So we are left to check (A.4) for $e = e(i)$ with odd i. In view of the description (A.3) and of (A.6) it suffices to consider elements m (in $\mathcal{M}$) of the form $m = \Sigma_{k \geq i+1} m_k e(\chi) e(k)$, but since $m = e(i+1)m$ by (A.1), m belongs to the l.h.s. of (A.4) if and only if it belongs to the r.h.s. of (A.4).

Case II : $p = 2$. There really are two subcases here depending on whether G is cyclic or not, but if G is cyclic, then we can argue as in Case I. So let G be non-cyclic. Then G is a 2-group of type $(2^{n-1}, 2)$: $G = < a > \times < b >$ where a is of order 2^{n-1} and b of order 2. We can compute the valuation of the different by means of Hilbert's formula and results on the ramification sequence (see e.g. [Le], page 147). We find that :

(A.7) if n is even, then A is $\mathbb{Z}_F G$-isomorphic to $\mathbb{Z}_K$ and so the result follows from (4.2.7) of [Bu2] ;

(A.8) if n is odd, then A is isomorphic to $X = P_K^{(\text{ord } G)/2}$ where P_K denotes the maximal ideal in $\mathbb{Z}_K$.

Again we must consider G-o-equivalence : here, between X and its associated order Λ, this is easy so we will not go into it. In view of [Bu2] it suffices to prove that the so-called factorisable quotient function is trivial on the character group $G^\circ = \text{Hom}\,(G, \mathbb{C}^x)$ of G. By definition this means we have to check the equality

$$[\Lambda : i(X)] = \Pi_D f(\Lambda, X)(D) \tag{A.9}$$

where here i is any injective homomorphism from X into Λ with finite cokernel, D runs over all divisions in the character group G° , and $f(\Lambda, X)(D)$ is the ideal of F defined by Möbius inversion from the ideal $f(\Lambda, X)(C) = [\Lambda^{e_H} : (iX)^{e_H}]$, with C the cyclic subgroup $(G/H)^\circ$ of G° (i.e. if $f = f(\Lambda, X)$ and if $\mu(D/C)$ denotes the Möbius function of the order of $< D > /C$, then by definition $f(D) = \Pi_{C<D} f(C)^{\mu(D/C)}$). Since we already know about G-o-equivalence, Lemma (2.11) of [Bu1] tells us that $[\Lambda : i(X)]$ divides $\Pi_D f(\Lambda, X)(D)$. Also by the (general) Theorem 7 in [F3], page 64, we know that $\mathbb{Z}_K$ is *always* factor equivalent to $\mathbb{Z}_F G$, so $[\mathbb{Z}_F G : \mathbb{Z}_K] = \Pi_D f(\mathbb{Z}_F G, \mathbb{Z}_K)(D)$.

Hence we are left to check that

$$[\Lambda : \mathbb{Z}_F G] = (\Pi_D f(\Lambda, \mathbb{Z}_F G)(D)) P_F^{-1} \tag{A.10}$$

(the P_F^{-1} comes from the factorisable quotient function $f(\mathbb{Z}_K, X)$). But the product over divisions in (A.10) equals $2^{\text{ord } G}$, and one can show that here (n odd) Λ contains the order $\{\mathcal{M}(FG(2)), ((1-a)/2)e_{<a^2,b>}\}\mathbb{Z}_F G$ where $G(2) = < a >$ and $\mathcal{M}(FG(2))$ is the maximal order in $FG(2)$. So (A.10) follows since $[\mathcal{M}(FG(2)) : \mathbb{Z}_F G] = 2^{\text{ord } G(2)-1}$.

Appendix B, by D. Burns : A surprising example

Let K be an abelian extension of $\mathbb{Q}$ such that in K there exists the square root of the inverse different $A(K) = A(K/\mathbb{Q})$. In Section 3, it was noted that whilst $A(K)$ is always locally free over its associated order (Theorem 3.1) its global structure depends critically upon the ramification of the extension $K/\mathbb{Q}$. In particular, setting $G_K = \text{Gal}(K/\mathbb{Q})$ with $\mathcal{M}_K$ the maximal $\mathbb{Z}$-order in the $\mathbb{Q}$-algebra $\mathbb{Q}G_K$ it was claimed - in Theorem 3.6 - that even the lattice $\mathcal{M}_K A(K)$ may have a non-trivial structure in the very wildly ramified case. In this appendix, rather than giving a proof of the full Theorem 3.6 we reduce technicalities to a minimum by discussing an explicit example in which $\mathcal{M}_K A(K)$ can be shown to have a non-trivial $\mathcal{M}_K$-structure. In fact, it is not difficult to verify that amongst extensions in which $\mathcal{M}_K A(K)$ has a non-trivial structure the example given here has the minimum possible absolute degree.

For simplicity we shall only consider extensions $K/\mathbb{Q}$ which possess a unique ramified prime (which is therefore totally ramified in the extension $K/\mathbb{Q}$). For p an odd prime, n a positive integer and r an odd divisor of $p-1$ there exists a unique abelian extension $K = K(p,n,r)$ of $\mathbb{Q}$ of degree $p^n r$ in which p is the only ramifying prime. Furthermore, since the degree of any such extension K is odd, we know that the square root of the inverse different $A(K)$ exists. Now, by the Hom-description of the locally free class group $Cl(\mathcal{M}_K)$ of $\mathcal{M}_K$ (see (2.3)), the global structure of a locally free $\mathcal{M}_K$-module X is determined by a function $g = g_X$ defined on the character group $G_K^\circ = Hom(G_K, \mathbb{C}^x)$ and satisfying at each character θ in G_K°

$$g_X(\theta) \text{ is an element of the ideal class group } Cl(\mathbb{Q}(\theta)) \text{ of } \mathbb{Q}(\theta) \tag{B.1}$$

with for each ω in $\text{Gal}(\mathbb{Q}(\theta)/\mathbb{Q})$

$$g_X(\theta)^\omega = g_X(\theta^\omega). \tag{B.2}$$

Now, if $K = K(p,n,r)$ is such that $\mathcal{M}_K A(K)$ is not free, then by Theorem 3.5 we shall certainly require that $r \neq 1$. Since we also want $Cl(\mathbb{Q}(\theta)) \neq 0$ checking

a table of class numbers now reveals that the smallest possible degree of such an extension occurs with $p = 13$, $n = 1$, and $r = 3$. Indeed we know that $Cl(\mathbb{Q}(39))$ has order 2 whereas $Cl(\mathbb{Q}(3))$ and $Cl(\mathbb{Q}(13))$ are both trivial. In this appendix we shall prove the

THEOREM B.3 : *For $K = K(13,1,3)$ the class $(\mathcal{M}_K A(K))_{\mathcal{M}_K}$ has order 2.*

Henceforth we shall write $K = K(13,1,3)$ with $O = \mathbb{Z}_K$, $G = G_K$, $\mathcal{M} = \mathcal{M}_K$ and $A = A(K)$. Now, by the above remarks one knows that if X is any locally-free $\mathcal{M}$-module and θ is an element of G°, then $g_X(\theta)$ is trivial if the order of θ is not 39. On the other hand, any two elements of G° of exact order 39 are conjugate under the action of $\mathrm{Gal}(\mathbb{Q}(39)/\mathbb{Q})$ and hence (by condition (B.2)) give the same evaluation of g_X. In this case we shall therefore refer to the class $(X)_{\mathcal{M}}$ as being represented by (the class of) a suitable fractional ideal of $\mathbb{Q}(39)$. Set $E = \mathbb{Q}(3)$. In E the rational prime ideal (13) splits as a product $(13)\mathbb{Z}_E = p_1 p_2$ and we let P_1 (respectively P_2) denote the unique prime of $\mathbb{Q}(39)$ lying above p_1 (respectively p_2). The numbering is to be understood as follows. Let F denote the local completion of K at the unique prime of residue characteristic 13. We can and do identify G with the local Galois group $\mathrm{Gal}(F/\mathbb{Q}_{13})$. Fix a character θ of G° of exact order 39. Let t be an embedding of $\mathbb{Q}(39)$ into an algebraic closure $\mathbb{Q}_{13}^c$ of $\mathbb{Q}_{13}$. Composing θ with t gives a 13-adic character which we denote by $\theta(t)$. Decompose G as $G = S \times C$ where S is the subgroup of G of order 13 and C is the complementary subgroup of order 3. Accordingly the character $\theta(t)$ decomposes as $\theta(t) = \Psi \times \Phi$. Let π be any element in F generating the maximal ideal of $\mathbb{Z}_F$. The map sending g in G to $g(\pi)/\pi$ gives an isomorphism θ_0 (independent of the choice of π) from C to a subgroup of the units of the residue field of $\mathbb{Q}_{13}$. Let $\chi = \chi(F)$ denote the element of the group of 13-adic characters C° that induces by passage to the residue field the isomorphism θ_0. Since χ generates C° we can define an integer $u(\Phi) = 1$ or 2 by $\Phi = \chi^{u(\Phi)}$. Then we choose our numbering in such a way that, if the embedding t_1 (respectively t_2) corresponds to the prime ideal P_1 (respectively P_2) and $\theta(t_i) = \Psi_i \times \Phi_i$, then $\Phi_i = \chi(F)^i$ for $i = 1$ or 2. The following lemma reduces the proof of Theorem B.3 to an exercise in explicit class field theory.

LEMMA B.4 : *The class $(\mathcal{M}A)_{\mathcal{M}}$ is represented by the ideal P_1.*

To prove the result of the lemma we first note that if we denote by $A^{\mathcal{M}}$ the largest $\mathcal{M}$-lattice in K contained in A, then

$$(\mathcal{M}A)_{\mathcal{M}} = (A^{\mathcal{M}})_{\mathcal{M}} \,. \tag{B.5}$$

Indeed by definition A is a self dual lattice from which it follows that $\mathcal{M}A$ is a lattice dual to $A^{\mathcal{M}}$. But now, equation (B.5) follows as a consequence of the general theory of the Hom-description (see for example [F1] Section 1.2, Example 1) together with the fact that $Cl(\mathbb{Q}(39))$ admits no non-trivial automorphism. On the other hand, Theorem 2 and Lemma (2.3) of [Bu3] together imply that

$$O^{\mathcal{M}} \cong \mathcal{M} \tag{B.6}$$

since O is known to be locally free over its associated order in $\mathbb{Q}G$. Now, from (B.5) and (B.6) the explicit Hom-description of $Cl(\mathcal{M})$ implies that the class $(\mathcal{M}A)_{\mathcal{M}}$ is represented by the ideal

$$h(\theta) := h_{(\mathcal{M}A)}(\theta) = ([(\mathbb{Z}[\theta] \otimes_{\mathbb{Z}} A)^{\theta} : (\mathbb{Z}[\theta] \otimes_{\mathbb{Z}} O)^{\theta}]_{\mathbb{Z}[\theta]})^{-1}. \tag{B.7}$$

It is immediate that $h(\theta)$ has support only above the rational prime (13). However, to compute expression (B.7) precisely, we go over to the local extension $F/\mathbb{Q}_{13}$. Let $A' = A(F/\mathbb{Q}_{13})$ and $O' = \mathbb{Z}_F$. Write $\mathbb{Z}'_{13}$ for the valuation ring of the local field obtained by adjoining a primitive 13th root of unity η to $\mathbb{Q}_{13}$. For any embedding t of $\mathbb{Q}(39)$ into $\mathbb{Q}_{13}^c$ one has

$$h^t(\theta(t)) := h(\theta)^t = ([(\mathbb{Z}'_{13} \otimes_{\mathbb{Z}_{13}} A')^{\theta(t)} : (\mathbb{Z}'_{13} \otimes_{\mathbb{Z}_{13}} O')^{\theta(t)}]_{\mathbb{Z}'_{13}})^{-1}.$$

If now $\theta(t)$ decomposes as $\theta(t) = \Psi \times \Phi$ and if $e(\theta(t))$, $e(\Psi)$ and $e(\Phi)$ denote the corresponding idempotents of $\mathbb{Q}_{13}(\eta)[G]$, $\mathbb{Q}_{13}(\eta)[S]$ and $\mathbb{Z}_{13}C$ respectively, then of course $e(\theta(t)) = e(\Psi)e(\Phi)$ in $\mathbb{Q}_{13}(\eta)[G]$. Since Φ is non-trivial, one checks that both $(\mathbb{Z}'_{13} \otimes_{\mathbb{Z}_{13}} A')^{\theta(t)} = e(\theta(t))(\mathbb{Z}'_{13} \otimes_{\mathbb{Z}_{13}} A')$ and $(\mathbb{Z}'_{13} \otimes_{\mathbb{Z}_{13}} O')^{\theta(t)} = e(\theta(t))(\mathbb{Z}'_{13} \otimes_{\mathbb{Z}_{13}} O')$. But, if ε is the identity character of S, then

$$(1 - e(\varepsilon))e(\Phi) = \sum_{\omega} e(\theta(t))^{\omega} \text{ sum over } \omega \text{ in } \mathrm{Gal}\,(\mathbb{Q}_{13}(\eta)/\mathbb{Q}_{13})$$

and hence for the norm N from $\mathbb{Q}_{13}(\eta)$ to $\mathbb{Q}_{13}$ we have the expression in terms of $\mathbb{Z}_{13}$-indices

$$N(h(\theta)^t) = \prod_{\omega} h^t(\theta(t)^{\omega}) = [e(\varepsilon)e(\Phi)O' : e(\varepsilon)e(\Phi)A']/[e(\Phi)O' : e(\Phi)A']. \tag{B.8}$$

To evaluate the expression (B.8) we recall that to every 13-character Φ of C we have associated an integer $u(\Phi)$ (= 1 or 2). Let x be a non-zero element in F.

Of course, since $e(\Phi)$ is in $\mathbb{Z}_{13}C$, one has for the valuation $v_F(x)$ of x

$$v_F(e(\Phi)x) \geq v_F(x). \tag{B.9}$$

The importance of the integer $u(\Phi)$ is that one has

$$v_F(e(\Phi)x) = v_F(x) \text{ if and only if } v_F(x) = u(\Phi) \text{ modulo } (3). \tag{B.10}$$

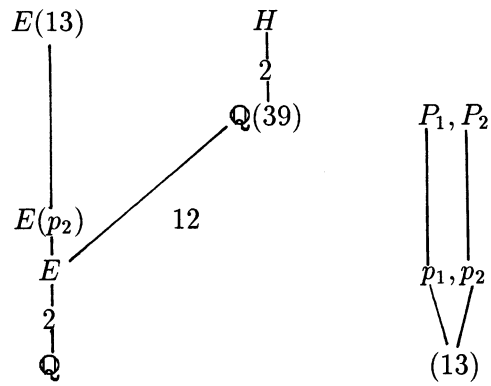
Let now F'' denote the subfield of F of degree 3 over $\mathbb{Q}_{13}$, let O'' denote its valuation ring and P'' the unique maximal ideal of O''. By Hilbert's formula one computes that $A' = (13)^{-1}P'^2$ so that $e(\Phi)A' = e(\Phi)(13)^{-1}P'^2$ and hence $e(\varepsilon)e(\Phi)A' = e(\Phi)(13)^{-1}P'' = e(\Phi)(13)^{-1}P''^{u(\Phi)}$, where for the last equality we have used (B.9) and (B.10). Similarly, one has $e(\varepsilon)e(\Phi)O' = e(\Phi)O'' = e(\Phi)P''^{u(\Phi)}$ and hence $[e(\varepsilon)e(\Phi)O' : e(\varepsilon)e(\Phi)A']_{\mathbb{Z}_{13}} = (13)^{-1}\mathbb{Z}_{13}$. Using the same type of argument one has $e(\Phi)(13)A' = e(\Phi)O' = e(\Phi)P'^2$ if $u(\Phi) = 2$, and $e(\Phi)(13)A' = e(\Phi)P'^4$ and $e(\Phi)O' = e(\Phi)P'$ if $u(\Phi) = 1$. So $[e(\Phi)O' : e(\Phi)A']_{\mathbb{Z}_{13}} = (13^{-13})\mathbb{Z}_{13}$ or $(13^{-12})\mathbb{Z}_{13}$ according as $u(\Phi)$ is 2 or 1. Finally therefore (B.8) becomes

$$\begin{aligned} N(h(\theta)^t) &= (13^{12})\mathbb{Z}_{13} \quad \text{if } u(\Phi) = 2 \text{ and} \\ &= (13^{11})\mathbb{Z}_{13} \quad \text{if } u(\Phi) = 1\,. \end{aligned} \tag{B.11}$$

With the convention of the numbering of primes introduced before the statement of the lemma, (B.11) implies that $h(\theta) = (P_1P_2)^{-12}P_1$. Now P_1P_2 is inflated from $\mathbb{Q}(13)$ and hence is a principal ideal so that in fact the class $(\mathcal{M}A)_{\mathcal{M}}$ is represented by the ideal P_1. But this is precisely the statement of Lemma B.4.

■

Having proved Lemma B.4 we are reduced to a problem of explicit global class field theory - namely to verify that P_1 is not a principal ideal of $\mathbb{Q}(39)$. In general of course, such problems are very difficult but in this case we are saved by reinterpreting the Hilbert class field of $\mathbb{Q}(39)$ as a ray class field of an imaginary quadratic subfield of class number one. To be more precise we write, for each integral ideal J or E, $E(J)$ for the ray class field of E modulo the ideal J. Writing H for the Hilbert class field of $\mathbb{Q}(39)$, one has a diagram of fields and degrees



The key to our computation is the observation that

$$E(13) = H. \tag{B.12}$$

But $\mathbb{Q}(39)$ is the compositum of E and $\mathbb{Q}(13)$ and so is included in $E(13)$ and hence to prove (B.12) we need only to demonstrate that the extension $E(13)/\mathbb{Q}(39)$ is unramified of degree at least two. Of course, one knows *a priori* that $E(13)/\mathbb{Q}(39)$ can be ramified only at either P_1 or P_2. We shall show that there is no ramification above P_1 (with an exactly similar argument proving the same for P_2). Well, p_1 is unramified in the extension $E(p_2)/E$ and totally ramified in the extension $\mathbb{Q}(39)/E$ which is of degree twelve. To conclude, we shall merely compute the degrees $|E(p_2) : E|$ and $|E(13) : E|$. But E has class number one and hence, for any integral $\mathbb{Z}_E$-ideal P, one has an exact sequence

$$\mu_E \longrightarrow (\mathbb{Z}_E/P)^x \longrightarrow \mathrm{Gal}\,(E(P)/E) \longrightarrow 0 \tag{B.13}$$

where here $\mu_E = (\mathbb{Z}_E)^x$ and the second map is derived from the Artin reciprocity law (by choosing a generator of each ideal of $\mathbb{Z}_E$ that is coprime to P). In particular, therefore one has

$$\begin{aligned} |E(P) : E| &= \text{card (cokernel } (\mu_E \longrightarrow (\mathbb{Z}_E/P)^x) \\ &= \text{card } ((\mathbb{Z}_E/P)^x) \text{ card } (\mu_E(P))/ \text{ card } (\mu_E) \end{aligned}$$

where we have used the notation $\mu_E(P)$ for the set of elements in μ_E which are congruent to one modulo P. From here one computes that $|E(p_2) : E| = 2$ and $|E(13) : E| = 24$ and it now follows that $E(13)/\mathbb{Q}(39)$ is an extension of degree

two in which P_1 is unramified. A similar argument dealing with P_2 allows us to deduce equality (B.12). We note that this argument also proves that any prime ideal of $E(P_2)$ lying above p_1 is totally ramified in the extension $E(13)/E(P_2)$.

Now by (B.12) together with the prime decomposition law of class field theory we have the equivalence of the following statements :

- P_1 is a principal ideal of $\mathbb{Q}(39)$
- P_1 is split in the extension $E(13)/\mathbb{Q}(39)$
- p_1 is split in the extension $E(p_2)/E$
- if $p_1 = (\pi)\mathbb{Z}_E$, then π is in the kernel of the Artin map (for $P = p_2$)
- π is congruent modulo p_2 to an element in μ_E (B.14)

where for the last equivalence we have used the exact sequence (B.13) with $P = p_2$. Setting now $z = -(1 + (-3)^{1/2})/2$ we can take $\pi = 1 - 3z$ so that $p_2 = (\pi - 5)\mathbb{Z}_E$. But card $(\mu_E) = 6$ and modulo p_2 we have $\pi^6 = 5^6 = (-1)^3 = -1$ so that condition (B.14) cannot be satisfied. Finally therefore one deduces that P_1 is not principal in $\mathbb{Q}(39)$ as was to be proved.

REFERENCES

[Ba] BACHOC C., *Sur les réseaux unimodulaires pour la forme Trace(x^2)*, to appear in the proceedings of the Séminaire de Théorie des Nombres de Paris, (1988-1989).

[B-E] BACHOC C., EREZ B., Forme trace et ramification sauvage, *Proc. London Math. Soc.* (3) **61** (1990), 209-226.

[Bas] BASS H., Unitary algebraic K-theory, 57-265, in *Algebraic K-theory III*, Proceedings of Batelle Institute Conference (1972), Springer Lecture Notes **343**, Berlin, Springer (1973).

[B-L] BAYER E., LENSTRA H.W., Forms in odd degree extensions and self-dual normal bases, *American J. of Math.*, **112** (1990), 359-373.

[Be] BERGÉ A.-M., Extensions galoisiennes a groupe d'inertie cyclique,*Ann. Inst. Fourier*, **28** (1978), 17-44.

[Bu1] BURNS D., Factorisability, group lattices and Galois module structure, *J. of Algebra*, **134** (1990), 257-270.

[Bu2] BURNS D., Factorisability and wildly ramified Galois extensions, to appear in *Ann. Inst. Fourier.*

[Bu3] BURNS D., Canonical factorisability and a variant of Martinet's conjecture, to appear in *J. of the London Math. Soc.*.

[C] COHN H., *A classical invitation to algebraic numbers and class fields*, Universitext. New-York, Springer (1978).

[CN-T] CASSOU-NOGUÈS PH., TAYLOR M.J., Opérations d'Adams et groupes de classes d'algèbres de groupe, *J. of Algebra* (1), **95** (1985), 125-152.

[C-P] CONNER P., PERLIS R., *A survey of trace forms in algebraic number fields*, Singapore, World Scientific (1984).

[C-R] CURTIS C., REINER I., *Methods of representation theory*, 2 volumes, New-York, John Wiley and Sons (1981-1987).

[E1] EREZ B., The Galois structure of the trace form in extensions of odd prime degree, *J. of Algebra*, **118** (1988), 438-446.

[E2] EREZ B., The Galois structure of the square root of the inverse different, to appear in *Math. Z.*.

[E3] EREZ B., *Structure galoisienne et forme trace*, Genève, Thèse (1987).

[E-M] EREZ B., MORALES J., The hermitian structure of rings of integers in odd degree abelian extensions, to appear in *J. of Number Theory.*

[E-T] EREZ B., TAYLOR M.J., *Hermitian modules in Galois extensions of number fields and Adams operations*, Preprint (1990).

[F1] FRÖHLICH A., *Galois module structure of algebraic integers*, Ergebnisse der Mathematik, 3, Folge, Bd. 1, Berlin, Springer (1983).

[F2] FRÖHLICH A., Invariants for modules over commutative separable orders, *Quart. J. Math. Oxford*, **16** (1965), 193-232.

[F3] FRÖHLICH A., L-values at zero and multiplicative Galois module structure (also Galois-Gauss sums and additive Galois module structure), *J. Reine und Angew. Math.*, **397** (1989), 42-99.

[K] KERVAIRE M., Opérations d'Adams en théorie des représentations linéaires des groupes finis, *l'Ens. Math.*, T. XXII, 1-28 (1976).

[L] LEOPOLDT H.W., Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers, *J. Reine und Angew, Math.*, **201** (1959), 119-149.

[Ma] MARTINET J., Character theory and Artin L-functions, 1-87, in *Algebraic Number Fields*, Proceedings of the Durham Symposium 1975, London, Academic Press (1977).

[Mi1] MIYATA Y., Vertices of ideals of a p-adic number field, *Illinois J. of Math.* (2), **31** (1987), 185-199.

[Mi2] MIYATA Y., Vertices of ideals of a p-adic number field II, Nagoya Math. J., **107**, 49-62 (1987).

[S1] SERRE J.-P., Corps locaux, 3rd edition, Paris, Hermann (1968).

[T1] TAYLOR M.J., Rings of integers and trace forms, Math. Z, **202**, 313-341 (1989).

[T2] TAYLOR M.J., Classgroups of group rings, London Mathematical Society Lecture Note Series 91, Cambridge, Cambridge University Press (1984).

[U1] ULLOM S., Normal bases in Galois extensions of number fields, Nagoya Math. J., **34**, 153-167.

[U2] ULLOM S., Galois cohomology of ambiguous ideals, J. Number Th., **1**, 11-15 (1969).

Boas EREZ
Section de Mathématiques
Université de Genève
2-4, rue du Lièvre
C.P. 240
CH - 1211 GENEVE 24
SUISSE

Astérisque

D. R. HEATH-BROWN

The Number of Abelian Groups of Order at Most x

Astérisque, tome 198-199-200 (1991), p. 153-163

<http://www.numdam.org/item?id=AST_1991__198-199-200__153_0>

THE NUMBER OF ABELIAN GROUPS OF ORDER AT MOST x

by

D.R. HEATH-BROWN

1. Introduction

Let $a(n)$ denote the number of isomorphism classes of Abelian groups of order n. The arithmetic function $a(n)$ is multiplicative, and has a generating series

$$\sum_{n=1}^{\infty} a(n)n^{-s} = \zeta(s)\zeta(2s)\zeta(3s)\cdots .$$

We shall be concerned here with the counting function

$$A(x) = \sum_{n \leq x} a(n) ,$$

first considered by ERDŐS and SZEKERES [2]. One expects that $A(x)$ will be approximated by $\sum c_j x^{1/j}$, where

$$c_j = \prod_{\substack{k=1 \\ k \neq j}}^{\infty} \zeta(\frac{k}{j}).$$

Indeed, if we write

$$A(x) = \sum_{j=1}^{5} c_j x^{1/j} + \Delta(x), \tag{1.1}$$

then it is known on the one hand that

$$\Delta(x) \ll x^{97/381}(\log x)^{35}$$

(KOLESNIK [8]), and on the other, that

$$\int_1^X \Delta(x)^2 dx = \Omega(X^{4/3} \log X) \tag{1.2}$$

(IVIĆ [7]; see also BALASUBRAMANIAN and RAMACHANDRA [1]). Thus

$$\Delta(x) = \Omega(x^{1/6}(\log x)^{1/2}),$$

so that the extra terms in the sum (1.1) that would correspond to $j \geq 6$, cannot be relevent. Note that

$$\frac{97}{381} = 0.25459\cdots > 0.16666\cdots = \frac{1}{6}\cdot$$

Our aim is to prove an upper bound corresponding to (1.2).

THEOREM 1. *We have*

$$\int_1^X \Delta(x)^2 dx \ll X^{4/3}(\log X)^{89}$$

for $X \geq 2$.

Apart from the exponent of $\log X$ this is, of course, best possible. IVIĆ [6] has given a weaker estimate with exponent $\frac{39}{29}$ in place of $\frac{4}{3}$. A result similar to Theorem 1 was stated by BALASUBRAMANIAN and RAMACHANDRA [1], but it appears that their claim cannot be substantiated. We have made no attempt to obtain a good exponent for the power of $\log X$ in Theorem 1.

Our method is an elaboration of that used by the author [4] to estimate

$$\int_0^T \left|\zeta(\tfrac{5}{8} + it)\right|^8 dt\ .$$

We take this opportunity to point out that exactly the same technique yields :

THEOREM 2. *We have*

$$\int_0^T \left|\zeta(\tfrac{11}{20} + it)\right|^{10} dt \ll T^{3/2}(\log T)^{52}$$

and

$$\int_0^T \left|\zeta(\tfrac{9}{20} + it)\right|^{10} dt \ll T^2(\log T)^{52}$$

for $T \geq 2$. *Hence, in the generalized divisor problem, one has* $\beta_5 \leq \frac{9}{20}$.

These results (with the exponent 52 replaced by 50) have been given without proof by ZHANG [11].

Finally we observe that our method for proving Theorem 1 has a little to spare. An examination of the proof shows that the key estimate (3.1) can be obtained with a saving of a power of T, except when M and N differ only by a factor of a small power of T. In this latter case further arguments are available covering all possibilities except that in which M and N are both small powers of T. This argument suggests that one might actually hope to obtain an asymptotic formula for the integral in (1.2).

2. Mean-Value Bounds

To estimate the average of $\Delta(x)^2$ we shall use the analysis of IVIĆ [6; pp.19-21]. After suitable modifications, this leads to

$$\int_{X/2}^{X} \Delta(x)^2 dx \ll X^{4/3}(\log X)^8 \max_{1\le T\le X} T^{-1} I_T , \tag{2.1}$$

where

$$I_T = \int_{T/2}^{T} |\zeta(1-\sigma+it)\zeta(1-2\sigma+2it)\zeta(3\sigma+3it)\zeta(4\sigma+4it)\zeta(5\sigma+5it)|^2 dt ,$$

and

$$\sigma = \frac{1}{6} + \frac{1}{\log X}.$$

In view of the inequality $2|ab| \le a^2 + b^2$, we have

$$I_T \le \max(J_T, J_T') , \tag{2.2}$$

where

$$J_T = \int_{T/2}^{T} |\zeta(3\sigma+3it)^2\zeta(4\sigma+4it)^4\zeta(5\sigma+5it)^4| dt \tag{2.3}$$

and

$$J_T' = \int_{T/2}^{T} |\zeta(3\sigma+3it)^2\zeta(1-\sigma+it)^4\zeta(1-2\sigma+2it)^4| dt .$$

Since the estimation of J_T and J_T' is similar, we shall henceforth restrict our attention to J_T.

We replace the integral in (2.3) by a sum over well-spaced points $t_n \in [T/2, T]$ for which

$$|t_m - t_n| \ge 1 \quad (m \ne n) . \tag{2.4}$$

Since

$$\zeta(s) = \sum_{n\le K} n^{-s} + 0(1) \quad (T \le K \le 2T)$$

for

$$|\mathrm{Im}\,(s)| \leq 5T\ , \quad \frac{1}{2} \leq \mathrm{Re}\,(s) \leq \frac{7}{8}\ ,$$

by TITCHMARSH **[10, Theorem 4.11]**, we have, for example

$$\zeta(3\sigma + 3it) \ll (\log T) \max_{L \leq T} |S_3(L, 3t)|\ , \tag{2.5}$$

where L runs over powers of 2, and

$$S_3(L, 3t) = \sum_{L < n \leq 2L} n^{-3\sigma - 3it}\ .$$

Of course, for the value of L giving the maximum in (2.5) we will clearly have

$$|S_3(L, 3t)| \geq |S_3(1, 3t)| \gg 1\ .$$

Similarly

$$\zeta(4\sigma + 4it) \ll (\log T) \max_{M \leq T} M^{-1/6} |S_4(M, 4t)|$$

with

$$S_4(M, 4t) = \sum_{M < n \leq 2M} M^{1/6} n^{-4\sigma - 4it}\ , \tag{2.6}$$

and

$$\zeta(5\sigma + 5it) \ll (\log T) \max_{N \leq T} N^{-1/3} |S_5(N, 5t)|\ ,$$

with

$$S_5(N, 5t) = \sum_{N < n \leq 2N} N^{1/3} n^{-5\sigma - 5it}\ . \tag{2.7}$$

It follows that

$$J_T \ll (\log T)^{13} M^{-2/3} N^{-4/3} \sum_n |S_3(L, 3t_n)^2 S_4(M, 4t_n)^4 S_5(N, 5t_n)^4|$$

for certain fixed L, M, N with

$$|S_3(L, 3t_n)|, |S_4(M, 4t_n)|, |S_5(N, 5t_n)| \gg 1\ .$$

We proceed to classify the points t_n according to the ranges

$$U < |S_3| \leq 2U\ , \quad V < |S_4| \leq 2V$$

and

$$W < |S_5| \leq 2W$$

in which the relevent sums lie. Here U, V and W run over powers of 2 with

$$1 \ll U \ll L^{\frac{1}{2}} \quad , \quad 1 \ll V \ll M^{\frac{1}{2}} \quad , \quad \text{and} \quad 1 \ll W \ll N^{\frac{1}{2}} \; . \tag{2.8}$$

If there are $N(U,V,W)$ such points t_n for each triple (U,V,W) it follows that

$$\begin{aligned} J_T &\ll (\log T)^{13} M^{-2/3} N^{-4/3} \sum_{U,V,W} U^2 V^4 W^4 N(U,V,W) \\ &\ll (\log T)^{16} M^{-2/3} N^{-4/3} U^2 V^4 W^4 N(U,V,W) \; , \end{aligned} \tag{2.9}$$

for some particular triple (U,V,W).

In estimating $N(U,V,W)$ we shall illustrate our methods by examining S_3. We begin by using the mean-value theorem for Dirichlet polynomials due to MONTGOMERY [**9** ; Theorem 7.3], with $Q = 1, \chi = 1, \delta = 1$. When applied to $S_3(L,t)^k$ this yields

$$\begin{aligned} U^{2k} N(U,V,W) &\ll (L^k + T)(\log T) \sum_{L^k < n \leq (2L)^k} d_k(n)^2 n^{-6\sigma} \\ &\ll (L^k + T)(\log T)^{1+k^2} . \end{aligned}$$

Similarly we have

$$V^{2k} N(U,V,W) \ll (M^k + T)(\log T)^{1+k^2} \tag{2.10}$$

and

$$W^{2k} N(U,V,W) \ll (N^k + T)(\log T)^{1+k^2} \; . \tag{2.11}$$

Notice that our purpose in making the somewhat peculiar definitions (2.6) and (2.7) was to produce bounds for $N(U,V,W)$ which are symmetric in S_3, S_4 and S_5. Our second estimate uses the Halász method, in the form due to HUXLEY [**5** ; p.171] (with a trivial modification to allow for the weaker spacing condition (2.4)). When applied to $S_3(L,t)^2$ this yields

$$\begin{aligned} N(U,V,W) &\ll L^2 U^{-4} \left(\sum_{L^2 < n \leq 4L^2} d(n)^2 n^{-6\sigma} \right) (\log T) \\ &\qquad + T L^2 U^{-12} \left(\sum_{L^2 < n \leq 4L^2} d(n)^2 n^{-6\sigma} \right)^3 (\log T)^5 \\ &\ll (L^2 U^{-4} + T L^2 U^{-12})(\log T)^{17} \; . \end{aligned}$$

Similarly one finds

$$N(U,V,W) \ll (M^2V^{-4} + TM^2V^{-12})(\log T)^{17} \tag{2.12}$$

and

$$N(U,V,W) \ll (N^2W^{-4} + TN^2W^{-12})(\log T)^{17} .$$

For our remaining estimates we start from Perron's formula (see TITCHMARSH [**10**; Lemma 3.19]), which yields

$$\begin{aligned} S_3(L,3t) &= \frac{1}{2\pi i}\int_{\frac{1}{2}-4iT}^{\frac{1}{2}+4iT} \zeta(s+3\sigma+3it)\,\frac{(2L)^s - L^s}{s}\,ds + 0(\log X) \\ &= \frac{1}{2\pi i}\int_{\frac{1}{2}-3\sigma-4iT}^{\frac{1}{2}-3\sigma+4iT} \zeta(s+3\sigma+3it)\,\frac{(2L)^s - L^s}{s}\,ds + 0(\log X) \\ &\ll \int_{-7T}^{7T} \left|\zeta(\frac{1}{2}+i\tau)\right| \,\frac{d\tau}{\frac{1}{\log X} + |\tau - 3t|} + \log X . \end{aligned}$$

Thus

$$\begin{aligned} U^4N(U,V,W) &\le \sum_n |S_3(L,3t_n)|^4 \\ &\ll (\log X)^4 \sum_n \left(1 + \left\{\int_{-7T}^{7T} \left|\zeta(\frac{1}{2}+i\tau)\right| \,\frac{d\tau}{1+|\tau-3t_n|}\right\}^4\right) \\ &\ll (\log X)^4 \left(T + \sum_n \int_{-7T}^{7T} \left\{\frac{d\tau}{1+|\tau-3t_n|}\right\}^3 \right. \\ &\qquad \left. \left\{\int_{-7T}^{7T} \left|\zeta(\frac{1}{2}+i\tau)\right|^4 \,\frac{d\tau}{1+|\tau-3t_n|}\right\}\right) \\ &\ll (\log X)^7 \left(T + \int_{-7T}^{7T} \left|\zeta(\frac{1}{2}+i\tau)\right|^4 \left\{\sum_n \frac{1}{1+|\tau-3t_n|}\right\} d\tau\right) \\ &\ll (\log X)^8 \int_{-7T}^{7T} \left|\zeta(\frac{1}{2}+i\tau)\right|^4 d\tau + T(\log X)^7 . \end{aligned}$$

In the final step above we have used the spacing condition (2.4). We can now apply the fourth power moment estimate for the Riemann Zeta-function (see TITCHMARSH [**10**; (7.6.1)] for example) to give

$$U^4N(U,V,W) \ll T(\log X)^{12} . \tag{2.13}$$

An entirely analogous argument based on twelfth power moments, and using the bound

$$\int_0^T \left|\zeta(\frac{1}{2}+it)\right|^{12} dt \ll T^2(\log T)^{17}$$

of HEATH-BROWN [3], produces

$$U^{12}N(U,V,W) \ll T^2(\log X)^{41} . \tag{2.14}$$

Similarly we obtain

$$V^4N(U,V,W) \ll T(\log X)^{12} , \tag{2.15}$$
$$V^{12}N(U,V,W) \ll T^2(\log X)^{41} , \tag{2.16}$$
$$W^4N(U,V,W) \ll T(\log X)^{12} ,$$

and

$$W^{12}N(U,V,W) \ll T^2(\log X)^{41} .$$

3. Proof of Theorem 1

We now use our bounds for $N(U,V,W)$ to show that

$$U^2V^4W^4N(U,V,W) \ll TM^{2/3}N^{4/3}(\log X)^{65} . \tag{3.1}$$

From (2.9) we will conclude that $J_T \ll T(\log X)^{81}$, and similarly for J_T'. The theorem will then follow from (2.1) and (2.2). Because of the symmetry in our bounds for $N(U,V,W)$ it will suffice to prove (3.1) when $N \leq M$, since otherwise

$$M^{4/3}N^{2/3} \leq M^{2/3}N^{4/3} .$$

We shall therefore consider the following cases :

$$\text{Case 1} \quad N \leq M \leq T^{1/8} ,$$
$$\text{Case 2} \quad N \leq M^{1/4} ,$$
$$\text{Case 3} \quad M^4N^8 \geq T^3 ,$$

and

$$\text{Case 4} \quad T^{1/32} \leq N \leq T^{1/4} .$$

These are readily seen to exhaust all possibilities when $N \leq M$. In what follows we shall repeatedly use the principle that

$$\min(A_1,\ldots,A_k) \leq A_1^{\alpha_1}\cdots A_k^{\alpha_k}$$

for $A_i \geq 0$, $\alpha_i \geq 0$ and $\sum \alpha_i = 1$.

Case 1 : Here we use (2.10) and (2.11) with $k = 8$, together with (2.13). Thus

$$\begin{aligned} N(U,V,W) &\ll (\log X)^{65} \min((M^8+T)V^{-16}, (N^8+T)W^{-16}, TU^{-4}) \\ &\ll (\log X)^{65} \min(TV^{-16}, TW^{-16}, TU^{-4}) \\ &\ll (\log X)^{65} (TV^{-16})^{1/4} (TW^{-16})^{1/4} (TU^{-4})^{1/2} \\ &= TU^{-2}V^{-4}W^{-4}(\log X)^{65} \\ &\ll TM^{2/3}N^{4/3}U^{-2}V^{-4}W^{-4}(\log X)^{65} . \end{aligned}$$

The bound (3.1) follows.

Case 2 : Here it is convenient to consider two subcases, in which $V \geq T^{1/8}$ and $V \leq T^{1/8}$. If $V \geq T^{1/8}$ then (2.12) yields

$$N(U,V,W) \ll M^2V^{-4}(\log X)^{17} . \tag{3.2}$$

From (2.15), (2.16) and (2.14) we therefore have

$$\begin{aligned} N(U,V,W) &\ll (\log X)^{41} \min(M^2V^{-4}, TV^{-4}, T^2V^{-12}, T^2U^{-12}) \\ &\ll (\log X)^{41} (M^2V^{-4})^{1/4} (TV^{-4})^{1/2} (T^2V^{-12})^{1/12} (T^2U^{-12})^{1/6} \\ &= (\log X)^{41} TM^{1/2}U^{-2}V^{-4} . \end{aligned}$$

On the other hand, if $V \leq T^{1/8}$, we deduce from (2.12) that

$$N(U,V,W) \ll (\log X)^{17} TM^2V^{-12} . \tag{3.3}$$

Now (2.15) and (2.13) yield

$$\begin{aligned} N(U,V,W) &\ll (\log X)^{17} \min(TM^2V^{-12}, TV^{-4}, TU^{-4}) \\ &\ll (\log X)^{17} (TM^2V^{-12})^{1/4} (TV^{-4})^{1/4} (TU^{-4})^{1/2} \\ &= (\log X)^{17} TM^{1/2}U^{-2}V^{-4} . \end{aligned}$$

In either case we conclude that

$$\begin{aligned} U^2V^4W^4N(U,V,W) &\ll (\log X)^{41} TM^{1/2}W^4 \\ &\ll (\log X)^{41} TM^{1/2}N^2 \\ &\ll (\log X)^{41} TM^{2/3}N^{4/3} , \end{aligned}$$

as required. Here we have used (2.8) together with the condition $N \leq M^{1/4}$.

Case 3 : Here we use (2.11) with $k = 4$, together with (2.14) and (2.16). Then

$$\begin{aligned} N(U,V,W) &\ll (\log X)^{41} \min(\max(T, N^4)W^{-8}, T^2U^{-12}, T^2V^{-12}) \\ &\ll (\log X)^{41} (\max(T, N^4)W^{-8})^{1/2} (T^2U^{-12})^{1/6} (T^2V^{-12})^{1/3} \\ &= (\log X)^{41} \max(T^{3/2}, TN^2) U^{-2}V^{-4}W^{-4} \ . \end{aligned}$$

However $T^{3/2} \leq TM^{2/3}N^{4/3}$ providing that $M^4N^8 \geq T^3$, and $TN^2 \leq TM^{2/3}N^{4/3}$, since $N \leq M$. The bound (3.1) therefore follows in this case.

Case 4 : Again we shall consider seperately the cases $V \geq T^{1/8}$ and $V \leq T^{1/8}$. If $V \geq T^{1/8}$ we have (3.2) just as in Case 2. Then (2.11), with $k = 8$, together with (2.14), (2.15) and (2.16), yield

$$\begin{aligned} N(U,V,W) &\ll (\log X)^{65} \min(M^2V^{-4}, \max(T, N^8)W^{-16}, \\ &\qquad T^2U^{-12}, TV^{-4}, T^2V^{-12}) \\ &\ll (\log X)^{65} (M^2V^{-4})^{1/3} (\max(T, N^8)W^{-16})^{1/4} (T^2U^{-12})^{1/6} \\ &\qquad \times (TV^{-4})^{1/24} (T^2V^{-12})^{5/24} \\ &= (\log X)^{65} M^{2/3} \max(T^{25/24}, T^{19/24}N^2) U^{-2}V^{-4}W^{-4} \ . \end{aligned}$$

On the other hand, if $V \leq T^{1/8}$, then (3.3) holds, as in Case 2. The bound (2.11), with $k = 8$, in conjunction with (2.13) and (2.14) now produces

$$\begin{aligned} N(U,V,W) &\ll (\log X)^{65} \min(TM^2V^{-12}, \max(T, N^8)W^{-16}, TU^{-4}, T^2U^{-12}) \\ &\ll (\log X)^{65} (TM^2V^{-12})^{1/3} (\max(T, N^8)W^{-16})^{1/4} (TU^{-4})^{3/8} \\ &\qquad \times (T^2U^{-12})^{1/24} \\ &= (\log X)^{65} M^{2/3} \max(T^{25/24}, T^{19/24}N^2) U^{-2}V^{-4}W^{-4} \ . \end{aligned}$$

We therefore get the same estimate whether $V \geq T^{1/8}$ or not. To prove (3.1) it remains to observe that

$$\max(T^{25/24}, T^{19/24}N^2) \ \leq TN^{4/3}$$

when $T^{1/32} \leq N \leq T^{1/4}$.

We have now proved (3.1) in each of the four cases. This completes the treatment of Theorem 1.

4. Proof of Theorem 2

To prove Theorem 2 we adopt the procedure of Section 2, using the sum

$$S(t) = \sum_{M<m\leq 2M} M^{1/20} m^{-11/20-it}, \quad (1 \ll M \ll T).$$

We deduce that

$$\int_{T/2}^{T} \left|\zeta(\frac{11}{20}+it)\right|^{10} dt \ll (\log T)^{11} M^{-1/2} N(V) V^{10} \tag{4.1}$$

for some V in the range $1 \ll V \ll M^{\frac{1}{2}}$, where $N(V)$ is the number of well spaced points $t_n \in [T/2, T]$ at which

$$V < |S(t)| \leq 2V.$$

If $V \geq T^{1/8}$ then (2.12) yields

$$N(V) \ll M^2 V^{-4} (\log T)^{17}.$$

From (2.16), adjusted by replacing $\log X$ by $\log T$, we therefore deduce that

$$\begin{aligned} N(V) &\ll (\log T)^{41} \min(M^2 V^{-4}, T^2 V^{-12}) \\ &\ll (\log T)^{41} (M^2 V^{-4})^{1/4} (T^2 V^{-12})^{3/4} \\ &= (\log T)^{41} T^{3/2} M^{1/2} V^{-10}. \end{aligned} \tag{4.2}$$

Similarly, if $V \leq T^{1/8}$ then (2.12) produces

$$N(V) \ll TM^2 V^{-12} (\log T)^{17}.$$

Hence (2.15) and (2.16) yield

$$\begin{aligned} N(V) &\ll (\log T)^{41} \min(TM^2 V^{-12}, TV^{-4}, T^2 V^{-12}) \\ &\ll (\log T)^{41} (TM^2 V^{-12})^{1/4} (TV^{-4})^{1/4} (T^2 V^{-12})^{1/2} \\ &= (\log T)^{41} T^{3/2} M^{1/2} V^{-10}. \end{aligned} \tag{4.3}$$

The bounds (4.1), (4.2) and (4.3) lead to

$$\int_{T/2}^{T} \left|\zeta(\frac{11}{20}+it)\right|^{10} dt \ll T^{3/2} (\log T)^{52},$$

which gives the first statement of Theorem 2. The second part needs only an application of the functional equation, and the remark about β_5 follows from TITCHMARSH [**10** ; Theorem 12.5].

REFERENCES

[1] R. BALASUBRAMANIAN and K. RAMACHANDRA, Some problems of analytic number theory III, *Hardy-Ramanujan J.*, **4** (1981), 13-40.

[2] P. ERDŐS and G. SZEKERES, Über die Anzahl Abelscher Gruppen gegebener Ordnung und über ein verwandtes zahlentheoretisches Problem, *Acta Sci. Math. (Szeged)*, **7** (1935), 95-102.

[3] D.R. HEATH-BROWN, The twelfth power moment of the Riemann zeta-function, *Quart. J. Math. Oxford Ser.* (2), **29** (1978), 443-462.

[4] D.R. HEATH-BROWN, Mean values of the zeta-function and divisor problems, *Recent progress in analytic number theory,* 115-119, (Academic Press, London, 1981).

[5] M.N. HUXLEY, *The distribution of prime numbers*, (Oxford, 1972).

[6] A. IVIĆ, The number of finite non-isomorphic Abelian groups in mean square, *Hardy-Ramanujan J.*, **9** (1986), 17-23.

[7] A. IVIĆ, The general divisor problem, *J. Number Theory*, **26** (1987), 73-91.

[8] G. KOLESNIK, On the number of Abelian groups of a given order, *J. Reine Angew. Math.*, **329** (1981), 164-175.

[9] H.L. MONTGOMERY, *Topics in multiplicative number theory*, (Springer, Berlin, 1971).

[10] E.C. TITCHMARSH, *The theory of the Riemann zeta-function*, 2nd Edition (Oxford, 1986).

[11] W.-P. ZHANG, On the divisor problem, *Kexue Tongbao*, **33** (1988), 1484-1485.

Roger HEATH-BROWN
Magdalen College
Oxford OX1 4AU

Astérisque

M. N. HUXLEY

Exponential sums after Bombieri and Iwaniec

Astérisque, tome 198-199-200 (1991), p. 165-175

<http://www.numdam.org/item?id=AST_1991__198-199-200__165_0>

EXPONENTIAL SUMS AFTER BOMBIERI AND IWANIEC

by

M.N. HUXLEY

BOMBIERI and IWANIEC [BI1, BI2] obtained $\theta = 9/56$ for the Lindelöf exponent (the least θ for which the Riemann zeta function satisfies $\zeta(1/2 + it) = O(t^{\theta+\epsilon})$ as $t \to \infty$.)

They remarked that their method might not be special to the Lindelöf problem ; in fact, as the saying goes, "they wrought [worked] better than they knew".

To show that one property is uniformly distributed with respect to another property, one forms exponential sums

$$S = \sum_{M}^{2M-1} e(f(m)) \,, \tag{1}$$

where

$$e(x) = \exp 2\pi i x, \qquad f(m) = TF(m/M)$$

with $F(x)$ in the function class $C^n[1 - \delta, 2 + \delta]$ for some $\delta > 0$ and $n \geq 4$. The case $F(x) = \log x$ gives Dirichlet series. If $F(x)$ is a polynomial of degree d with rational coefficients, denominator q, and if $T = M^d$, then the sum S is approximately

$$MS_q/q \,,$$

where S_q is a complete exponential sum with denominator q. One imposes conditions to prevent $F(x)$ from being well approximated by a polynomial for a long interval of values of m. A sufficient condition is that $F(x)$ be holomorphic on a neighbourhood of the segment $1 \leq x \leq 2$ of the real axis, and satisfies there

$$F'(x) = (1 + o(1))x^{-s}$$

for some real $s > 0$. This condition is called the "virial" or "monomial" condition. It holds in many applications.

There are three useful ideas for treating exponential sums :

O. Subdivide the range for m,

A. Cauchy's inequality,

B. Poisson summation.

The name "Step A" is usually given to Weyl's differencing lemma, which may be analysed as subdivision, followed by Cauchy, followed by averaging. Van der Corput's method [see GK, I or K]consists of iterating these steps. The simplest form of Van der Corput's method, applying steps O, A, B (read from left to right) gives

$$S = O(M^{1/2}T^{1/6}) .$$

The method can be applied to exponential sums in several variables, and it becomes extremely complicated.

Bombieri and Iwaniec obtained

$$S = O(M^{1/2}T^{9/56+\varepsilon})$$

by taking the steps in the order O, B, A. The method is arithmetic, and is essentially limited to one variable. Their subdivisions correspond to approximations to $f(m)$ by quadratic polynomials with rational coefficients. If the denominator q of the leading coefficient is small, the short interval is a "major arc", length N say, and the sum over the short interval is approximately

$$NS_q/q .$$

If q is large, the short interval is a "minor arc", and one expects the sum over the short interval to be small. This behaviour is seen in computer studies of exponential sums, notably those of DESHOUILLERS [D]. The Cauchy inequality is employed to show that the minor arc contribution is small in L_p norm (for some suitable p). In some ways the treatment resembles applying Hardy and Littlewood's Farey dissection to

$$\int_0^1 \sum_{n=1}^{N} e(f(n + \alpha M))d\alpha . \tag{2}$$

If all arcs are treated as major (steps O,B alone), one gets

$$S = O(M^{1/2}T^{1/6+\varepsilon}).$$

This method is no worse than that of Van der Corput.

At the same time JUTILA [J1-8] has been considering sums

$$\sum_{M}^{2M-1} \tau(m)e(f(m)) \,, \tag{3}$$

where $\tau(m)$ is the divisor function or the Fourier coefficient of a modular form, beginning with steps O, B where O is subdivision according to the rational approximation to the first derivative, B is Voronoi or Wilton summation. In this context the numbers $\tau(m)\, e(-am/q)$ are the coefficients of the modular form twisted by the matrix $\begin{bmatrix} q & -a \\ 0 & q \end{bmatrix}$, and the Wilton summation formula is still available. These ideas could extend to any motivic L-series characterised by the three conditions :

D. An ordinary Dirichlet series with denominators n^{-s},
E. An Euler product,
F. Functional equations for the L-series and its twists.

One may fit Bombieri and Iwaniec's ideas into this frame by taking $\tau(m)$ to be the theta-function coefficients, 2 if m is a perfect square, 0 if not, and by considering $F(x)$ as a function of x^2. This change of variable explains why the derivatives do not correspond.

There are two successful applications of the Bombieri-Iwaniec method to sums with an extra variable. The Weyl step O, A replaces the sum S of (1) with double sums of the form

$$\sum_{h=H}^{2H-1} \sum_{m=M}^{2M-1} e(f(m+h) - f(m)). \tag{4}$$

This sum suggests the simpler sum

$$\sum_{h=H}^{2H-1} \sum_{m=M}^{2M-1} e(hf'(m)). \tag{5}$$

The sum (5) was estimated by IWANIEC and MOZZOCHI [IM] using the same method. The rational polynomial approximation to $hf'(x)$ is found by multiplying the approximation to $f'(x)$ by h, so h must not be too large. HEATH-BROWN and HUXLEY [HBH] estimated (4) - actually in the form

$$\sum_{h=H}^{2H-1} \sum_{m=M}^{2M-1} e(f(m+h) - f(m-h)). \tag{6}$$

This in turn gives estimates for

$$\int_{-U}^{U} |S(T_o + T)|^2 dT, \tag{7}$$

where $S(T)$ is the sum (1) considered as a function of T, if H goes up to T_o/U in size.

More general multiple exponential sums have not been treated, since one cannot find a good approximation by a rational polynomial.

The Iwaniec-Mozzochi sum (5) is connected with numerical integration. The prettiest case is the discrepancy for a circle (or more generally a smooth closed curve), the number of integer points minus the area. For a circle radius R, approximating the circle by a polygon whose sides lie along lattice lines $x =$ integer, $y =$ integer shows that the discrepancy is $O(R)$. Voronoi's method, applied by Sierpiński, approximates the circle by a polygon with rational gradients. Sierpiński obtained a discrepancy $O(R^{2/3})$ if the centre of the circle is at an integer point. The method can be modified [H2] to give $O(R^{2/3}(\log R)^{4/3})$ in general.

Exponential sums are introduced by way of the row-of-teeth function

$$\rho(t) = [t] - t + 1/2 \cong \sum_{h \neq 0} \frac{e(ht)}{2\pi i h} .$$

Thus

$$\sum_m \rho(\sqrt{(R^2 - m^2)})$$

can be expressed in terms of terms of the sums (5). The subdivision in step O corresponds to the sides of the Sierpiński polygon, with q as the denominator of the rational gradient a/q.

Minor arc contributions can be classified as follows.

E1. The "main term", estimated in L_p norm,
E2. Edge effects from ends of ranges of summation,
E3. Approximation errors in each summand in each Poisson summation.

The O, B, A sequence is dangerous because the errors of types (E2) and (E3) from each short sum in the subdivision must be added. For the sum S of (1) there is a finite Poisson summation modulo q, followed by a Poisson summation in m, giving an Airy integral. For the double sums (5) and (6)

Poisson summation in m is followed by Poisson summation in h. The second Poisson summation gives the Bessel function

$$Hi_{-1/2}(t) = \sqrt{\left[\frac{2}{\pi t}\right]}\, e^{-it} ,$$

with an (E3) error term because the Bessel function is given by an integral from 0 to ∞ , and one only integrates over a bounded range.

The main term on a minor arc is a sum over vectors $\underset{\sim}{x}$ of an exponential $e(x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)$.

For the sum (5)

$$\underset{\sim}{x} = (k\ell, \ell, \ell\sqrt{k}, \ell/\sqrt{k})$$

summed over a range (depending on the minor arc) of the form

$$L_1 \le \ell \le L_2, \quad \max(K_1, c_1\ell^2) \le k \le \min(K_2, c_2\ell^2).$$

The exponent is really a power series in $1/\sqrt{k}$, but the further terms can be treated as type (E3) errors. The vector $\underset{\sim}{y}$ is $\underset{\sim}{y}(a/q)$ indexed by the gradient a/q of the Sierpiński polygon :

$$\underset{\sim}{y} = \left[\frac{\overline{a}}{q}, \frac{\overline{a}b}{q} - \frac{\nu}{q}, \frac{1}{\sqrt{(\mu q^3)}}, \frac{\kappa}{\sqrt{(\mu q^3)}}\right] ,$$

where a, b and q are integers, $\overline{a}$ being the inverse modulo q, and κ, μ and ν are real, all depending on the minor arc. The obvious technical difficulty, that the ranges for k and ℓ are not independent and vary with the minor arc, can be overcome. For this and other technical reasons the sum is squared, and the $\underset{\sim}{x}$ vectors are replaced by differences

$$\underset{\sim}{x}^{(k_1,k_2,\ell_1,\ell_2)} = (k_1\ell_1 - k_2\ell_2, \ldots).$$

The treatment of the sum (6) is analogous but more complicated. The Bessel integral is perturbed, with larger (E3) errors, and the third entry of the vector is

$$k\sqrt{\ell}(1 + \ell^2/48k^2).$$

The simpler sum (1) gives a very similar $\underset{\sim}{y}$ vector and an $\underset{\sim}{x}$ vector

$$\underset{\sim}{x}^{(h)} = (h^2, h, h^{3/2}, h^{1/2}).$$

One raises the sum to the r-th power and uses

$$\underset{\sim}{x}^{(h_1,\dots,h_r)} = \underset{\sim}{x}(h_1) + \cdots + \underset{\sim}{x}(h_r).$$

Cauchy's inequality takes the form of the Large Sieve [B], generalised to be symmetric between the "integer" $\underset{\sim}{x}$ and the "rational" $\underset{\sim}{y}$ vectors.
Moreover vectors of each type may coincide with one another, so that instead of the number of vectors, one counts the number of coincident pairs. For the $\underset{\sim}{x}$ vectors, this is like the Hilbert-Kamke problem. BOMBIERI and IWANIEC [BI2] gave a bound for $r = 4$ using ingenious exponential sum arguments. WATT [W1] gave an elementary argument based on the fact that the variety

$$h_1^2 + \cdots + h_r^2 = h_{r+1}^2 + \cdots h_{2r}^2 ,$$
$$h_1 + \cdots + h_r = h_{r+1} + \cdots h_{2r}$$

is an affine cylinder. One wants to show that most coincidences are the trivial ones when h_{r+1} to h_{2r} are h_1 to h_r permuted. This is easy for $r = 3$, but false for $r \geq 7$. WATT [W3] has a weaker result for $r = 5$, combining elementary and exponential sum methods. HUXLEY and KOLESNIK [HK] have essentially settled the case $r = 5$. IWANIEC and MOZZOCHI [IM] treated the corresponding k_r, ℓ_r coincidence problem elementarily; see also [W2]. For the sum (6) Heath-Brown noticed that the perturbing factor $(1 + \ell^2/48k^2)$ can be neglected in a range of h in which the h^3 term in (6) cannot be neglected.

Bombieri and Iwaniec gave a bound for the number of coincident $\underset{\sim}{y}$ vectors in the case $F(x) = \log x$ only. HUXLEY and WATT [HW1] gave the same bound for general $F(x)$. KOLESNIK [GK] later found a simpler idea which leads to the same bound. All five authors only assume that the entries y_1 and y_3 coincide; this uses f'' (as a/q) and the residual term in $f^{(3)}$. The entries y_2 and y_4 involve f' also, and are harder to use. The coincidence of $\underset{\sim}{y}$ vectors may be regarded as resonance between different arcs of the curve. The possible resonances correspond to matrices in the modular group $SL(2, Z)$. One would like to show that most matrices of $SL(2, Z)$ give no resonance. Further progress may entail the use of "Kloostermania", the Fourier theory of $SL(2, Z)$.

The various sums (1) to (7) may be averaged over a family of related functions $f_i(x)$. This is important in many of JUTILA's applications [J3-8]. In some cases [HW1,W4] one uses the second and fourth entries of the minor arc vector $\underset{\sim}{y}$.

The latest results for the sum S of (1) are

$$S = O[M^{1/2}T^{89/560+\varepsilon}]$$

by WATT [W3], giving $\theta = 89/560$ in the Lindelöf problem, and a corresponding bound for sums with an exponential and a Dirichlet character [W4], and

$$S = O[M^{1/2}T^{11/70+\varepsilon}]$$

for M near $T^{1/2}$ by HUXLEY and KOLESNIK [HK]. The latter result gives only $\theta = 17/108$ in the Lindelöf problem ($11/70 = 0.1571\ldots < 17/108 = 0.1574\ldots < 89/560 = 0.1589\ldots < 9/56 = 0.1607\ldots$).

For the sum (5) IWANIEC and MOZZOCHI [IM] and HUXLEY [H3] get

$$O\left[HT^{1/4+\varepsilon}\left[\frac{HT}{M}\right]^{1/10}\right],$$

which becomes $O(M)$ for

$$H = O(MT^{-7/22-\varepsilon}),$$

and gives the discrepancy estimate $O(R^{7/11+\varepsilon})$ for the circle [IM] or a more general smooth closed curve [H3]. The same bound for the sum (6) in [HBH] estimates the integral (7) as $O(MU)$ for

$$U \geq T^{7/22+\varepsilon}.$$

It leads indirectly to

$$\int_0^T |\zeta(1/2+it)|^2 = T(\log T/2\pi + 2\gamma - 1) + O(T^{7/22+\varepsilon}).$$

This implies $\theta = 7/44$ in the Lindelöf problem, but $7/44 = 0.1590\ldots$ is worse than WATT's 89/560 [W3].

JUTILA [J1-8] has many bounds for the sum (3). Two applications are

$$\sum_{\chi \bmod D} \int_T^{T+T^{2/3}} \left|L\left[\frac{1}{2}+it,\chi\right]\right|^4 dt = O(DT^{2/3}(DT)^{\varepsilon})$$

where $\tau(n)$ is the divisor function and

$$\sum_{\chi \bmod D} \int_T^{T+T^{2/3}} \left|\varphi\left[\frac{1}{2}+it,\chi\right]\right|^2 dt = O(DT^{2/3}(DT)^{\varepsilon})$$

where $\tau(n)$ is the Fourier coefficient of a modular form, and $\varphi(s, \chi)$ is its Hecke L-series, normalised to have critical line Re $s = 1/2$.

FOUVRY and IWANIEC [FI1] have also considered using steps B and A without subdivision, but in several variables, provided that the monomial condition holds in each variable. This idea should give new exponents in some classical problems.

Finally, in the spirit of the Journées, some problems. If

$$y = f(x), \quad M \leq x \leq 2M$$

is a smooth curve, then there are connections between

a) the exponential sum S of (1) over the interval M to $2M - 1$,
b) the rounding error sum $\sum \rho(f(m))$ over the same interval,
c) the number of integer points within a distance δ of the curve,
d) the number of integer points on the curve.

BOMBIERI and PILA [BP] have an upper bound $O(T^{\epsilon})$ for problem (d). For (a) there is the classical Van der Corput iteration, whilst for (c) there is an analogous elementary iteration [H5], in which Step A is differencing, and Step B is interchanging the variables x and y. Is there an iteration for the rounding error (b) ?

What conditions ensure that the Diophantine approximations to f, f' and f'' at integer values of x are independent ? A quantitative result could allow one to count coincidences among minor arc $\underset{\sim}{y}$ vectors properly, or even to avoid putting moduli round the minor arc sums.

Are there any counterexamples of curves which are not rational algebraic curves of genus zero and of low degree, but for which the sums (a), (b) or (c) are unexpectedly large ?

REFERENCES

[B] E. BOMBIERI, *Le grand Crible dans la Théorie analytique des Nombres*, 2de édn. (Astérisque, Paris 1987).

[BI1] E. BOMBIERI and H. IWANIEC, On the order of $\zeta(1/2 + it)$, *Ann. Scuola Norm. Sup. Pisa Cl. Sci.* (4), **13** (1986), 449-472.

[BI2] E. BOMBIERI and H. IWANIEC, Some mean value theorems for exponential sums, *Ann. Scuola Norm. Sup. Pisa Cl. Sci.* (4), **13** (1986), 473-486.

[BP] E. BOMBIERI and J. PILA, The Number of Integral Points on Arcs and Ovals, *Duke Math. J.*, **59** (1989), 337-357.

[D] J.M. DESHOUILLERS, Geometric aspect of Weyl sums, *Elementary and Analytic Theory of Numbers, Banach Centre Pub.*, **17** (Polish Sci. Pub. Warszawa 1985), 75-82.

[FI1] E. FOUVRY and H. IWANIEC, Exponential sums with monomials, *J. Number Theory.*

[GK] S.W. GRAHAM and G. KOLESNIK, *Van der Corput's Method for Exponential Sums*, London Math. Soc. Lecture Notes, to appear.

[HBH] D.R. HEATH-BROWN and M.N. HUXLEY, Exponential sums with a difference, *Proc. London Math. Soc.*, (3), **61** (1990) to appear.

[H1] M.N. HUXLEY, Exponential sums and the Riemann zeta function, *Théorie des Nombres, C.R.C.I.T.N. Laval 1987* (de Gruyter, Berlin 1989), 417-423.

[H2] M.N. HUXLEY, The area within a curve, *Proc. Indian Acad. Sci. (Math. Sci.)*, **97** (1987), 111-116.

[H3] M.N. HUXLEY, Exponential sums and lattice points, *Proc. London Math. Soc.* (3), **60**, 471-502.

[H4] M.N. HUXLEY, The fractional parts of a smooth sequence, *Mathematika*, **35** (1988), 292-296.

[H5] M.N. HUXLEY, The integer points close to a curve, *Mathematika*, **36** (1989), 198-215.

[H6] M.N. HUXLEY, Exponential sums and rounding error, *J. London Math. Soc.*, to appear.

[H7] M.N. HUXLEY, *Fractional parts as pseudo-random numbers,*preprint 1989.

[HK] M.N. HUXLEY and G. KOLESNIK, Exponential sums and the Riemann zeta function III, *Proc. London Math. Soc*, to appear.

[HW1] M.N. HUXLEY and N. WATT, Exponential sums and the Riemann zeta function, *Coll. Math. Soc. János Bolyai*, **51** (Number Theory, Budapest 1987) (North Holland 1990), 173-191.

[HW2] M.N. HUXLEY and N. WATT, Exponential sums and the Riemann zeta function, *Proc. London Math. Soc.* (3), **57** (1988), 1-24.

[HW3] M.N. HUXLEY and N. WATT, Exponential sums with a parameter, *Proc. London Math. Soc.* (3), **59** (1989), 233-252.

[I] A. IVIĆ, *The Riemann Zeta function*, (Wiley, New-York 1985).

[IM] H. IWANIEC and C.J. MOZZOCHI, On the divisor and circle problems, *J. Number Theory*, **29** (1988), 60-93.

[J1] M. JUTILA, On exponential sums involving the divisor function, *J. Reine Angew. Math.*, **355** (1985), 173-190.

[J2] M. JUTILA, *Lectures on a Method in the Theory of Exponential Sums,* Tata Institute Lectures in Maths. and Physics, 80 (Springer, Bombay 1987).

[J3] M. JUTILA, The fourth power moment of the Riemann zeta function over a short interval, *Coll. Math. Soc. János Bolyai*, **51** (Number Theory, Budapest 1987) (North Holland 1990).

[J4] M. JUTILA, Mean value estimates for exponential sums, *C.R. Journées Arithmétiques Ulm*, 1987, to appear.

[J5] M. JUTILA, On exponential sums involving the Ramanujan function, *Proc. Indian Acad. Sci. (Math. Sci.)*, **97** (1987), 157-166.

[J6] M. JUTILA, Exponential sums related to quadratic forms, *Proc. Canadian Number Theory Conference Banff* 1988, (de Gruyter, Berlin) to appear.

[J7] M. JUTILA, Mean value estimates for exponential sums with applications to L-functions, *Acta Arith.*, to appear.

[J8] M. JUTILA, *Mean value estimates for exponential sums II,* to appear.

[K] E. KRÄTZEL, *Lattice Points*, (D.V.W., Berlin 1988).

[M1] T. MEURMAN, On exponential sums involving the Fourier coefficients of Maass wave forms, *J. Reine Angew. Math.*, **384** (1988), 192-207.

[M2] T. MEURMAN, *On the order of the Maass L-functions on the critical line,* to appear.

[W1] N. WATT, A problem on semicubical powers, *Acta Arith.*, **52** (1988), 119-140.

[W2] N. WATT, *A problem on square roots of integers*, to appear.

[W3] N. WATT, Exponential sums and the Riemann zeta function II, *J. London Math. Soc.*, **39** (1989), 385-404.

[W4] N. WATT, *Exponential sums with a character*, to appear.

[W5] N. WATT, An elementary treatment of a general Diophantine problem, *Ann. Scuola Norm. Sup. Pisa Cl. Sci.* (4), **15**, 603-614.

HUXLEY, Martin Neil
School of Mathematics
University of Wales College of Cardiff
Senghenydd Road
Cardiff CF2 4AG
Grande Bretagne

Astérisque

DAVID-OLIVIER JAQUET

Classification des réseaux dans $\mathbb{R}^7$ (via la notion de formes parfaites)

Astérisque, tome 198-199-200 (1991), p. 177-185

<http://www.numdam.org/item?id=AST_1991__198-199-200__177_0>

CLASSIFICATION DES RESEAUX DANS $\mathbb{R}^7$
(via la notion de formes parfaites)

par

David-Olivier JAQUET

1. Introduction

On part d'une forme quadratique réelle à n variables, définie positive. On peut écrire cette forme de la façon suivante :

$Q(x) = x^t Ax$ où A est une matrice symétrique réelle définie positive.

Nous allons étudier la restriction de $Q(x)$ à $x \in \mathbb{Z}^n$. Tout d'abord, remarquons que A peut être considérée comme la matrice des produits scalaires d'une base de $\mathbb{R}^n$. On montre facilement que cette base est unique à isométrie près. Restreindre $Q(x)$ à $x \in \mathbb{Z}^n$ revient à ne considérer que les combinaisons linéaires entières des vecteurs de cette base, c'est-à-dire les points du *réseau* engendré par les vecteurs de cette base. $Q(x)$ nous donne alors le carré de la distance euclidienne entre le point x du réseau et l'origine.

On appelle *minimum* de A, noté $\min A$, le minimum sur $\mathbb{Z}^n \backslash \{O\}$ de $Q(x)$. C'est donc le carré de la distance euclidienne à l'origine, du point du réseau le plus proche de O.

Les paires de vecteurs $\pm v_k \in \mathbb{Z}^n$ $(k = 1, \ldots, s)$, qui vérifient

$$v_k{}^t A v_k = \min A$$

s'appellent les *vecteurs minimaux* de A.

Dans le but de donner une classification des réseaux de $\mathbb{R}^n$, on introduit des relations "naturelles" d'équivalence entre réseaux :

- les isométries (pas d'influence sur A),

- les changements de base dans $GL_n(\mathbb{Z})$,
- les homothéties.

Un invariant important de cette classification est l'invariant d'Hermite μ :

$$\mu(A) = \frac{\min A}{\sqrt[n]{\det A}}$$

Cet invariant est borné pour n fixé. On rencontre, dans la littérature, diverses inégalités relatives à la fonction μ. Je ne citerai que celle de MINKOWSKI, liée à la géométrie des nombres, $\mu(A) < n$ si $n \geq 2$. D'autre part, μ atteint ses maxima ; les formes correspondant à ces maxima sont dites *extrêmes*. On montre que, modulo les homothéties, les maxima sont isolés et, qu'à équivalence près, il n'existe qu'un nombre fini de formes extrêmes. Le maximum absolu est appelé γ_n.

On connait les valeurs de γ_n pour $n \leq 8$:

$$\gamma_1 = 1 \quad \gamma_2 = \sqrt{\frac{4}{3}} \quad \gamma_3 = \sqrt[3]{2} \quad \gamma_4 = \sqrt{2}$$

$$\gamma_5 = \sqrt[5]{8} \quad \gamma_6 = \sqrt[6]{\frac{64}{3}} \quad \gamma_7 = \sqrt[7]{64} \quad \gamma_8 = 2 \ .$$

VORONOÏ, essentiellement à l'aide des notions de formes parfaites et de domaines associés aux formes parfaites, donne une méthode de réduction des formes quadratiques définies positives, de même qu'un algorithme permettant de calculer les maxima de la fonction μ, donc en particulier γ_n. VORONOÏ donne aussi un critère, maintenant classique, pour les formes extrêmes et montre qu'il n'existe qu'un nombre fini de formes parfaites inéquivalentes en dimension n.

2. Formes parfaites

Pour comprendre ce qu'est une forme parfaite, il faut en quelque sorte inverser le procédé de départ. Connaissant A, on a, tout d'abord, calculé les vecteurs minimaux $\pm v_k \in \mathbb{Z}^n$ associés à A. Maintenant, connaissant les v_k et ayant effacé A, peut-on retrouver A ? Ou encore, A est-elle l'unique solution du système d'équations linéaires ${}^t v_k B v_k = \min A$, $(k = 1, \ldots, s)$? Si oui, on dit que A est *parfaite*.

Donc une forme est dite parfaite si la connaissance des coordonnées entières de ses vecteurs minimaux dans une base du réseau permet de retrouver la matrice des produits scalaires de cette base, c'est-à-dire A.

Par contre, la connaissance des vecteurs minimaux considérés comme points d'un réseau plongé dans $\mathbb{R}^n$ ne caractérise pas la forme, ni même le réseau. On connaît, en effet, des exemples de formes parfaites, non équivalentes, pour lesquelles les vecteurs minimaux plongés dans $\mathbb{R}^n$ coïncident.

On peut tout de même faire la remarque évidente suivante : lorsqu'on plonge un réseau dans $\mathbb{R}^n$, les points correspondant aux vecteurs minimaux sont sur une sphère centrée à l'origine. Les formes associées à ce réseau sont parfaites si et seulement si le seul ellipsoïde dans $\mathbb{R}^n$ qui passe par ces points est la sphère.

3. Domaine associé à une forme parfaite

Plaçons-nous, maintenant, dans l'espace des matrices symétriques réelles $n \times n$, qui est de dimension $N = \dfrac{n(n+1)}{2}$; on identifie cet espace à $\mathbb{R}^N$ qu'on rend euclidien via le produit scalaire $A \cdot B = \text{Trace } AB$.

A chaque vecteur minimal v_k, on peut faire correspondre un point ${\lambda_k}^2$ dans cet espace : on pose ${\lambda_k}^2 = v_k {v_k}^t$. (On remarque, au passage, que ${\lambda_k}^2 \cdot A = \min A$.)

A chaque ${\lambda_k}^2$, on associe alors la demi-droite qui part de l'origine et contient ${\lambda_k}^2$. L'enveloppe convexe de ces demi-droites est appelée *domaine* associé à A.

On peut montrer que A est parfaite si et seulement si son domaine est de dimension maximale.

On appelle *faces* de dimension $N-1$ du domaine, les intersections de ce domaine avec ses hyperplans d'appui.

Une face de dimension d ($d < N-1$) est une variété de dimension d obtenue en intersectant des faces de dimension $N-1$.

Définissons, maintenant, une action de $GL_n(\mathbb{Z})$ sur l'ensemble des formes quadratiques (définies ou non), en considérant tout élément de $GL_n(\mathbb{Z})$ comme une matrice de changement de base. Cette action induit une action de $GL_n(\mathbb{Z})$ sur l'ensemble des domaines de VORONOÏ. On dira que deux domaines sont équivalents s'ils appartiennent à la même orbite.

On montre facilement que deux domaines sont équivalents si et seulement si les formes parfaites correspondantes sont équivalentes.

4. Quelques résultats dus à Voronoï

4.1 Deux domaines ne peuvent être en contact que par leurs bords (faces de dimension $d \leq N-1$).

4.2 Soit une face F de dimension $N-1$ appartenant à un domaine. Alors F appartient également à un autre domaine. Géométriquement, ces deux domaines se situent de part et d'autre de F. Ces deux domaines sont dits *voisins* ou *contigus.*

4.3 Toute forme quadratique définie positive appartient au moins à un domaine.

4.4 Soient deux domaines quelconques. Il existe un chemin reliant ces deux domaines qui, à chaque pas, ne fait que passer d'un domaine à un domaine voisin.

4.5 A équivalence près, il n'existe qu'un nombre fini de formes parfaites en dimension n, donc qu'un nombre fini de domaines inéquivalents.

Le problème actuel est d'obtenir la liste exhaustive des domaines inéquivalents en dimension N, ainsi que leurs faces. Il est judicieux d'injecter, dans la théorie comme dans la pratique, le groupe des automorphismes de chacune des formes. Il faut comprendre automorphisme dans le sens d'isométrie de la forme à coefficients entiers.

Tout automorphisme de la forme induit de manière canonique une application linéaire de $\mathbb{R}^N \to \mathbb{R}^N$, qui laisse le domaine de la forme globalement invariant.

5. Problème en dimension n=7 (N=28)

Pourquoi s'intéresser particulièrement à la dimension $n = 7$? La raison est historique :

$n = 3$ Le problème a été résolu par GAUSS en 1831. GAUSS a montré que $A_3 = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}$ représente la seule forme parfaite à équivalence près. Par conséquent, le réseau cubique à faces centrées qui correspond à cette forme est le seul réseau absolument extrême en dimension $n = 3$.

$n = 4$,

$n = 5$ Ces deux dimensions ont été traitées en 1877 par KORKINE et ZOLOTAREFF.

$n = 6$ Il a fallu attendre 1957 pour que BARNES donne la liste exhaustive des formes parfaites à 6 variables, toujours à équivalence près.

$n = 7$ Jusqu'en 1971, on ne connaissait que 22 formes parfaites non équivalentes en dimension $n = 7$. STACEY amena cette liste à 33 en employant des méthodes dues à WATSON.

Dans le cadre de la thèse de doctorat que je fais sous la direction du Professeur François SIGRIST, je cherche à montrer que cette liste de 33 formes en dimension $n = 7$ est exhaustive. Il suffit pour cela, d'après l'algorithme de VORONOÏ, de montrer que chacune des formes contiguës à l'une de ces 33 formes est équivalente justement à une de ces 33 formes.

La connaissance de la liste exhaustive des formes parfaites en dimension $n = 7$ permettrait de calculer directement γ_7. Bien que la valeur de γ_7 soit connue, les démonstrations de $\gamma_7 = \sqrt[7]{64}$ restent très longues. La première est due à BLICHFELD en 1929. Plus récemment, en 1980, VETCHINKIN a confirmé ce résultat. (Pour les références, voir la bibliographie de [1]).

Pour traiter une forme, il faut calculer l'ensemble des faces de son domaine, les formes voisines correspondantes et, finalement, exhiber les changements de base qui permettent d'identifier ces formes voisines avec une des 33 formes de la liste.

Il faut remarquer que si l'on aborde le calcul des faces du point de vue combinatoire, le problème explose rapidement. Certes, le cas où la forme possède 28 vecteurs minimaux est trivial : on obtient 28 faces en éliminant à tour de rôle chacun des $v_k v_k{}^t$; ceux qui restent déterminent une face ! L'algorithme que j'ai développé trouve son intérêt quand le nombre s de vecteurs minimaux est supérieur à $N = \dfrac{n(n+1)}{2}$.

Je construis tout d'abord un cône de dimension maximale dans un espace de dimension s, cône qui se projette dans un sous-espace de dimension N, exactement sur le domaine de la forme.

En projetant ce cône successivement dans un sous-espace de dimension $s-1$, puis $s-2$, etc... jusqu'à $N = \dfrac{n(n+1)}{2}$, le temps de calcul est considé-

rablement réduit.

L'identification des voisines, dans la phase finale, est une recherche en arbre avec une très forte heuristique (très peu de "backtracking"). L'heuristique se base principalement sur le spectre des vecteurs minimaux, c'est-à-dire sur leur position relative.

Mon programme utilise, à plusieurs endroits, les données précieuses contenues dans l'article de CONWAY et SLOANE [1], en particulier le recensement des 33 formes connues ainsi que la description détaillée de leurs groupes d'automorphismes. J'ai développé ce programme en LISP. Le calcul d'une matrice de changement de base dans $GL_n(\mathbb{Z})$ qui identifie une forme à une des 33 formes connues demande, en moyenne, environ une dizaine de secondes.

CONWAY et SLOANE dans leur article [1] écrivent : "... the (sometimes putative) lists of neighbours given by STACEY (1973), P.R. SCOTT (quoted in STACEY 1973) and SHUSHBAEV (1985), who together have studied the VORONOÏ neighbours for 27 of the seven-dimensional perfect lattices...". Actuellement, j'ai réussi à énumérer les listes de toutes les voisines pour 32 des 33 formes connues. Pour chacune de ces formes, j'ai regroupé ses voisines en orbites sous l'action de son groupe d'automorphismes.

Plus précisément, 31 formes ont pu être entièrement traitées à l'aide de mon programme.

Pour $D_7(x) = (x_1-x_2)^2+x_3{}^2+\cdots+x_7{}^2+(x_1+\cdots+x_7)^2$ (la notation indique que les vecteurs minimaux forment le système de racines correspondant), j'ai utilisé, d'une part, l'article de VORONOÏ [3] qui donne une liste suffisante de faces pour D_n [2] et, d'autre part, mon programme pour engendrer les orbites correspondantes, les voisines associées et pour faire finalement les identifications nécessaires.

Pour $E_7(x) = (x_1 - x_2)^2 + (x_1 - x_3)^2 + x_4{}^2 + \cdots + x_7{}^2 + (x_1 + \cdots + x_7)^2$, qui possède 63 vecteurs minimaux (formant le système de racines de E_7), il faut renoncer à énumérer *explicitement* toutes les faces. La forme E_7 possède 77965804 voisines équivalentes à une des 32 autres formes. Je suis en train d'élaborer un algorithme qui, se basant sur les résultats actuels, devrait éviter cette énumération tout en caractérisant complètement les orbites des faces de E_7 sous l'action du groupe des automorphismes de cette forme.

Prenons, pour conclure, l'exemple de P_7^3 (la notation est de CONWAY et SLOANE dans [1]). P_7^3 possède 36 vecteurs minimaux. Lorsqu'on normalise son

minimum à 2, son déterminant vaut $\frac{243}{64}$. Le nombre de faces possibles du point de vue combinatoire vaut $\binom{36}{27} = 94143280$. Avec mon programme, il a fallu moins de cinq heures pour énumérer les 3906 faces de P_7^3, les regrouper en 23 orbites sous l'action du groupe des automorphismes dont l'ordre est 2592, calculer les formes voisines et finalement les identifier aux formes déjà connues. On obtient ainsi pour les voisines de P_7^3 :

6 orbites de voisines équivalentes à P_7^1,

3 orbites de voisines équivalentes à P_7^3,

1 orbite de voisines équivalentes à P_7^4,

3 orbites de voisines équivalentes à P_7^6,

3 orbites de voisines équivalentes à P_7^7,

2 orbites de voisines équivalentes à P_7^8,

1 orbite de voisines équivalentes à P_7^9,

1 orbite de voisines équivalentes à P_7^{17},

1 orbite de voisines équivalentes à P_7^{22},

1 orbite de voisines équivalentes à P_7^{26},

1 orbite de voisines équivalentes à P_7^{29} .

Le tableau annexé résume les liens de voisinages entre les 33 classes de formes parfaites.

Actuellement, je peux donc déjà affirmer que, s'il existe une nouvelle forme parfaite en dimension $n = 7$, elle n'est reliée que par E_7 à la liste des formes déjà connues.

REFERENCES

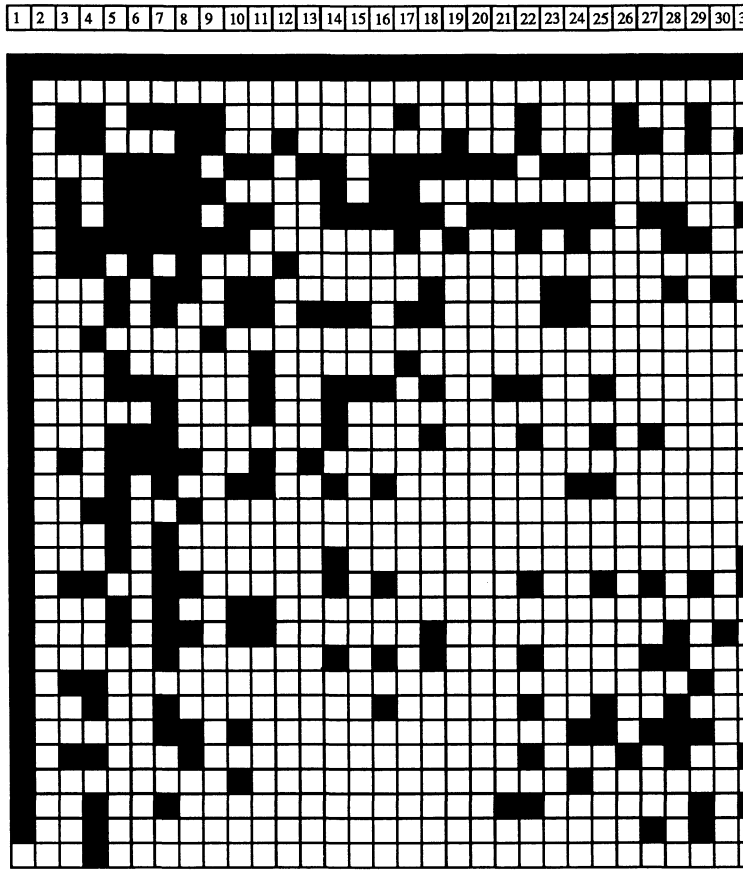
[1] J.H. CONWAY et N.J.A. SLOANE, Low-dimensional lattices III, Perfect forms, *Proc. R. Soc. Lond. A*, **418** (1988), 43-80.

[2] D.-O. JAQUET et F. SIGRIST, Formes quadratiques contiguës à D_7, *C.R. Acad. Sci. Paris*, Série I, **309** (1989), 641-644.

[3] G. VORONOÏ, Sur quelques propriétés des formes quadratiques positives parfaites, *J. Reine Angew. Math.*, **133** (1908), 97-178.

David-Olivier JAQUET
Institut de Mathématiques
et d'Informatique (IMI)
Chantemerle 20 - Case postale 2
2007 NEUCHÂTEL
SUISSE

déterminant (min = 2)	s *
2	63
8192 / 2187	28
243 / 64	36
4	42
4	36
1024 / 243	32
135 / 32	34
9 / 2	32
71344 / 15625	28
147 / 32	32
1120 / 243	30
10240 / 2187	28
4805 / 1024	28
10336 / 2187	29
38809 / 8192	28
128 / 27	30
10528 / 2187	28
2465 / 512	28
392 / 81	28
10658 / 2187	28
3584 / 729	28
315 / 64	30
10780 / 2187	28
10808 / 2187	28
11008 / 2187	28
81 / 16	30
81 / 16	30
81 / 16	30
171 / 32	29
343 / 64	28
45 / 8	28
189 / 32	28
8	28



* s = nombre de vecteurs minimaux.

Astérisque

JEAN-FRANÇOIS JAULENT

Noyau universel et valeurs absolues

Astérisque, tome 198-199-200 (1991), p. 187-208

<http://www.numdam.org/item?id=AST_1991__198-199-200__187_0>

à la mémoire de Georges POITOU

NOYAU UNIVERSEL ET VALEURS ABSOLUES

par

Jean-François JAULENT

L'objet de l'exposé est de présenter quelques unes des relations entre la ℓ−partie du noyau universel de la K-théorie pour un corps de nombres K contenant les racines ℓ-ièmes de l'unité, et le noyau des valeurs absolues principales définies sur le ℓ- adifié du groupe des idèles de K, et ce à la lumière des conjectures de Leopold et de Gross généralisées.

En fait, cette note trouve sa motivation dans de récents travaux de M. Kolster (cf. [10]) et de K. Kramer (cf. [11]), qui recoupent des résultats antérieurs de l'auteur (cf. [9]) et de T. Nguyen Quang Do (cf. [13]) obtenus par d'autres voies, et mettent plus particulièrement en valeur le rôle non explicité jusqu'ici d'un noyau remarquable que l'on peut construire très facilement en s'aidant des valeurs absolues ℓ-adiques principales (c'est à dire des valeurs absolues à valeurs ℓ-adiques) attachées aux places non complexes d'un corps de nombres quelconque.

Notre point de départ sera donc la théorie ℓ-adique du corps de classes, élaborée dans [9], et que nous allons brièvement rappeler :

1 - Le ℓ-adifié du groupe des idèles d'un corps de nombres.

Fixons une fois pour toutes un nombre premier ℓ, et considérons un corps de nombres K arbitraire (mais de degré fini sur $\mathbb{Q}$).

Le groupe des idèles classique de K est défini depuis Chevalley comme le produit restreint

$$J_K = \prod_{\mathfrak{p}\in Pl(K)}^{res} K_{\mathfrak{p}}^{\times}$$

des groupes multiplicatifs des complétés respectifs de K en ses diverses places. Le facteur $K_{\mathfrak{p}}^{\times}$ désigne donc soit le groupe divisible $\mathbb{C}^{\times}$ si $\mathfrak{p}$ est complexe ; soit le groupe $\mathbb{R}^{\times} = \{\pm 1\} \times \mathbb{R}_{+}^{\times}$, si $\mathfrak{p}$ est réelle ; soit, si $\mathfrak{p}$ est ultramétrique au-dessus d'un premier p, le produit

$$K_{\mathfrak{p}}^{\times} = \mu_{\mathfrak{p}}^{\circ}.U_{\mathfrak{p}}^{1}.\pi_{\mathfrak{p}}^{\mathbb{Z}}$$

du groupe fini $\mu_{\mathfrak{p}}^{\circ}$ des racines de l'unité dans $K_{\mathfrak{p}}$ d'ordre étranger à $\mathfrak{p}$, du sous groupe $U_{\mathfrak{p}}^{1}$ des unités principales de $K_{\mathfrak{p}}$, et du $\mathbb{Z}$-module libre engendré par une uniformisante arbitraire $\pi_{\mathfrak{p}}$.

Dans aucun des cas $K_{\mathfrak{p}}^{\times}$ n'est donc un $\mathbb{Z}_{\ell}$-module. Aussi, pour construire un $\mathbb{Z}_{\ell}$-module à partir de $K_{\mathfrak{p}}^{\times}$, la solution la plus économique consiste-t-elle à former la limite projective

$$\mathcal{K}_{\mathfrak{p}}^{\times} = \varprojlim_{n} K_{\mathfrak{p}}^{\times} K_{\mathfrak{p}}^{\times \ell^{n}}$$

des quotients ℓ-primaires de $K_{\mathfrak{p}}^{\times}$. Cela étant, le passage au quotient ayant pour effet de tuer la partie ℓ-divisible de $K_{\mathfrak{p}}^{\times}$, le groupe obtenu est évidemment trivial lorsque $\mathfrak{p}$ est complexe, et égal à $(-1)^{\mathbb{Z}_{\ell}/2\mathbb{Z}_{\ell}}$ lorsque $\mathfrak{p}$ est réelle, donc encore trivial sauf pour $\ell = 2$ auquel cas il est isomorphe à $\mathbb{Z}/2\mathbb{Z}$. Enfin, si $\mathfrak{p}$ est ultramétrique, deux cas se présentent :

- ou bien $\mathfrak{p}$ est modérée (i.e. étrangère à ℓ) et

$$\mathcal{K}_{\mathfrak{p}}^{\times} = \mu_{\mathfrak{p}}.\pi_{\mathfrak{p}}^{\mathbb{Z}_{\ell}}$$

s'identifie au produit du ℓ-sous-groupe de Sylow $\mu_{\mathfrak{p}}$ de $\mu_{\mathfrak{p}}^{\circ}$ et du $\mathbb{Z}_{\ell}$-module libre engendré par l'image de l'uniformisante $\pi_{\mathfrak{p}}$ (image que nous continuerons par abus à noter $\pi_{\mathfrak{p}}$)

- ou bien $\mathfrak{p}$ est sauvage (i.e. au-dessus de ℓ) et

$$\mathcal{K}_{\mathfrak{p}}^{\times} = U_{\mathfrak{p}}^{1}\pi_{\mathfrak{p}}^{\mathbb{Z}_{\ell}}$$

est le produit du sous-groupe $U_{\mathfrak{p}}^{1}$ des unités principales de $\mathcal{K}_{\mathfrak{p}}^{\times}$ et du $\mathbb{Z}_{\ell}$-module libre engendré par l'image de $\pi_{\mathfrak{p}}$ (que nous écrirons encore $\pi_{\mathfrak{p}}$).

Dans tous les cas, $\mathcal{K}_{\mathfrak{p}}^{\times}$ est ainsi un $\mathbb{Z}_{\ell}$-module noethérien (donc compact pour sa topologie naturelle de $\mathbb{Z}_{\ell}$-module) et il est commode d'écrire

$$\mathcal{K}_{\mathfrak{p}}^{\times} = \mathcal{U}_{\mathfrak{p}}.\pi_{\mathfrak{p}}^{\mathbb{Z}_{\ell}}$$

en convenant de prendre $\pi_{\mathfrak{p}} = -1$, si $\mathfrak{p}$ est réelle, lorsque ℓ vaut 2.

Il est alors naturel de définir le ℓ-adifié $\mathcal{J}_K$ du groupe des idèles J_K comme le produit restreint

$$\mathcal{J}_K = \prod_{\mathfrak{p}\in Pl(K)}^{\text{res}} K_{\mathfrak{p}}^{\times}$$

c'est-à-dire comme la réunion pour tous les ensembles finis S de places de K

$$\mathcal{J}_K = \bigcup_{S\subset Pl(K)} \mathcal{U}_K^S, \quad \text{avec} \quad \mathcal{U}_K^S = \prod_{\mathfrak{p}\in S} K_{\mathfrak{p}}^{\times} . \prod_{\mathfrak{p}\notin S} \mathcal{U}_{\mathfrak{p}};$$

et d'équiper $\mathcal{J}_K$ de la topologie limite inductive des topologies des $\mathcal{U}_K^S$, ces derniers étant regardés comme compacts en tant que produits de modules compacts (de sorte que la topologie de $\mathcal{J}_K$ n'est pas la restriction à $\mathcal{J}_K$ du produit des topologies des $K_{\mathfrak{p}}^{\times}$, mais fait cependant de $\mathcal{J}_K$ une réunion dénombrable de modules compacts).

Si maintenant on prend comme ℓ-adifié du groupe des idèles principaux le tensorisé ℓ-adique

$$\mathcal{R}_K = \mathbb{Z}_\ell \otimes_{\mathbb{Z}} K^{\times}$$

du groupe multiplicatif de K (qui joue donc le rôle du rayon dans la théorie), et qu'on envoie $\mathcal{R}_K$ dans $\mathcal{J}_K$ en s'aidant du plongement diagonal de $K^{\times}$ dans J_K, le résultat fondamental du corps de classes ℓ-adique est le suivant (cf. [9], th. I.1.13) :

THÉORÈME 1. - *Isomorphisme ℓ-adique du corps de classes - Le groupe $\mathcal{R}_K$ des idèles principaux s'identifie canoniquement à un sous-groupe fermé du groupe des idèles $\mathcal{J}_K$, et le quotient topologique*

$$\mathcal{C}_K = \mathcal{J}_K/\mathcal{R}_K$$

est un groupe compact, isomorphe comme tel au groupe de Galois $G_K = Gal(\overline{K}^{ab}/K)$ de la pro-ℓ-extension abélienne maximale de K.

Sans doute n'est-il pas inutile de rappeler, puisqu'elle intervient plus loin, comment s'exprime dans ce contexte la conjecture de Leopoldt. Désignons par μ_K le ℓ-groupe des racines de l'unité dans K (i.e. le ℓ-sous-groupe de Sylow de $K^{\times}$), puis, pour toute place non complexe $\mathfrak{p}$ de K, écrivons $\mu_{\mathfrak{p}}$ son homologue dans $K_{\mathfrak{p}}$. Cela posé, nous avons (cf. [9], Ch. I) :

CONJECTURE DE LEOPOLD GÉNÉRALISÉE.- *Les idèles principaux (i.e. les éléments de $\mathcal{R}_K$), qui sont localement partout des racines de l'unité (dans $\mathcal{J}_K$) sont les racines globales de l'unité ; ce qui s'écrit :*

$$\mathcal{R}_K \cap \prod_{\mathfrak{p} \in Pl(K)} \mu_{\mathfrak{p}} = \mu_K.$$

Bien entendu, les idèles concernés étant trivialement des unités (i.e. des éléments du tensorisé ℓ-adique $\mathcal{E}_K = \mathbb{Z}_\ell \otimes_{\mathbb{Z}} E_K$ du sous-groupe des unités de $K^\times$), la conjecture précédente revient à affirmer que le rang ℓ-adique des unités de K est égal au nombre de Dirichlet, ce qui, lorsque K est totalement réel, est exactement le postulat initial de H.W. Leopoldt.

2 - Définition des valeurs absolues ℓ-adiques principales.

On sait que les valeurs absolues réelles (c'est-à-dire à valeurs dans $\mathbb{R}^\times$) attachées aux diverses places du corps K, définies sur le groupe des idèles J_K, sont telles que leurs restrictions à $K^\times$ satisfont la formule du produit :

$$\prod_{\mathfrak{p} \in Pl(K)} |x|_{\mathfrak{p}} = 1, \quad \forall x \in K^\times.$$

Pour obtenir un analogue dans $\mathcal{J}_K$, il est nécessaire de définir des valeurs absolues à valeurs non plus dans $\mathbb{R}_+^\times$, mais dans le groupe multiplicatif $\mathbb{Z}_\ell^\times$, en fait dans son sous-groupe principal $U = 1 + \ell\mathbb{Z}_\ell$. Pour cela, on peut procéder comme suit : soit

$$< \ > |\mathbb{Z}_\ell^\times \longrightarrow U = 1 + \ell\mathbb{Z}_\ell$$

la surjection canonique de $\mathbb{Z}_\ell^\times$ dans U, qui a pour noyau le sous-groupe des racines $(\ell - 1)$-ièmes de l'unité dans $\mathbb{Z}_\ell$.

DÉFINITION 2. - *Pour chaque place $\mathfrak{p}$ de K, on définit sur $\mathcal{J}_K$ une valeur absolue $|\ |_{\mathfrak{p}}$ à valeurs dans $U = 1 + \ell\mathbb{Z}_\ell$, qui se factorise via le complété profini $K_{\mathfrak{p}}^\times$, en posant pour tout $\mathfrak{x} = (x_{\mathfrak{p}})_{\mathfrak{p}}$ de $\mathcal{J}_K$:*

(i) $|\mathfrak{x}|_{\mathfrak{p}} = 1$, *si $\mathfrak{p}$ est complexe ;*

(ii) $|\mathfrak{x}|_{\mathfrak{p}} =< sg(x_{\mathfrak{p}}) >$, *si $\mathfrak{p}$ est réelle ;*

(iii) $|\mathfrak{x}|_{\mathfrak{p}} =< N\mathfrak{p}^{-v_{\mathfrak{p}}(x_{\mathfrak{p}})} >$, *si $\mathfrak{p}$ est ultramétrique, mais étrangère à ℓ ;*

(iv) $|\mathfrak{x}|_{\mathfrak{p}} =< N_{K_{\mathfrak{p}}/\mathbb{Q}_\ell}(x_{\mathfrak{p}}) N\mathfrak{p}^{-v_{\mathfrak{p}}(x_{\mathfrak{p}})} >$, *enfin, si $\mathfrak{p}$ divise ℓ.*

Nous disons que $|\ |_{\mathfrak{p}}$ *est la valeur absolue* ℓ*-adique principale attachée à la place* $\mathfrak{p}$.

Remarque : La valeur absolue ainsi définie ne coïncide pas exactement avec celle donnée par J. Tate (cf. [15], Ch VI, déf. 1.1). Plus précisément elle est égale au crochet $<\ >$ de la valeur absolue de Tate.

Dans les trois premiers cas ((i) à (iii)) la définition donnée est la transposition de la définition réelle, le choix de la norme absolue $N\mathfrak{p}$ correspondant à une normalisation naturelle. La condition (iv) est alors dictée par la formule du produit. En effet, avec les conventions précédentes, on a immédiatement (cf. [9], prop. I.1.8):

$$\prod_{\mathfrak{p}\in Pl(K)} |x|_{\mathfrak{p}} = \prod_{\mathfrak{p}\in Pl(\mathbb{Q})} |N_{K/\mathbb{Q}}(x)|_{\mathfrak{p}} = 1,\ \forall x \in \mathcal{R}_K,$$

comme attendu.

D'un autre côté, pour chaque place finie $\mathfrak{p}$, l'image $|\mathcal{K}_{\mathfrak{p}}^{\times}|$ est évidemment un sous-module d'indice fini de U. En particulier, sauf peut-être pour $\ell = 2$, c'est un $\mathbb{Z}_\ell$-module libre de rang 1, et, dans ce cas, le noyau $\mathcal{K}_{\mathfrak{p}}^{*}$ de $|\ |_{\mathfrak{p}}$ alors un sous-module pur de $\mathcal{K}_{\mathfrak{p}}^{\times}$. De fait :

PROPOSITION 3. - *Le noyau* $\mathcal{K}_{\mathfrak{p}}^{*}$ *dans* $\mathcal{K}_{\mathfrak{p}}^{\times}$ *de la valeur absolue* ℓ*-adique principale* $|\ |_{\mathfrak{p}}$ *est donné par les deux formules suivantes :*

(i) $\mathcal{K}_{\mathfrak{p}}^{*} = \mathcal{U}_{\mathfrak{p}}$, *pour* $\mathfrak{p} \nmid \ell$. *Autrement dit,* $\mathcal{K}_{\mathfrak{p}}^{*}$ *est trivial si* $\mathfrak{p}$ *est réelle ; et égal au sous-groupe de torsion* $\mu_{\mathfrak{p}}$ *de* $\mathcal{K}_{\mathfrak{p}}^{\times}$, *si* $\mathfrak{p}$ *est ultramétrique mais modérée.*

(ii) $\mathcal{K}_{\mathfrak{p}}^{*} = Ker(Log_{Iw} \circ N_{K_{\mathfrak{p}}/\mathbb{Q}_\ell})$, *où* Log_{Iw} *est le logarithme d'Iwasawa dans* $\mathbb{Q}_\ell^{\times}$, *pour* $\mathfrak{p} \mid \ell$, *sous réserve d'imparité de* ℓ. *Dans ce dernier cas,* $\mathcal{K}_{\mathfrak{p}}^{\times}$ *est le produit direct du sous-module de torsion* $\mu_{\mathfrak{p}}$ *de* $\mathcal{K}_{\mathfrak{p}}^{\times}$ *et d'un* $\mathbb{Z}_\ell$*-module libre de dimension* $[K_{\mathfrak{p}} : \mathbb{Q}_\ell]$ *; et c'est encore un sous-module pur de* $\mathcal{K}_{\mathfrak{p}}^{\times}$.

Démonstration. Le cas (i) étant immédiat, examinons plus attentivement le cas (ii). Si $\mathfrak{p}$ divise ℓ, la condition $|x_{\mathfrak{p}}|_{\mathfrak{p}} = 1$ pour un $x_{\mathfrak{p}}$ de $\mathcal{K}_{\mathfrak{p}}^{\times}$ s'écrit :

$$< N_{K_{\mathfrak{p}}/\mathbb{Q}_\ell}(x_{\mathfrak{p}}) N\mathfrak{p}^{-v_{\mathfrak{p}}(x_{\mathfrak{p}})} >= 1.$$

Elle affirme donc que la norme de $x_{\mathfrak{p}}$ s'écrit comme produit d'une puissance de ℓ (qui est nécessairement $N\mathfrak{p}^{v_{\mathfrak{p}}(x_{\mathfrak{p}})}$) et d'une racine de l'unité. Mais cette

propriété caractérise précisément le noyau du logarithme d'Iwasawa dans $\mathbb{Q}_\ell$, ce qui conduit à l'égalité annoncée.

Nota : Lorsque ℓ vaut 2, la condition $|x_\mathfrak{p}|_\mathfrak{p} = 1$ pour $\mathfrak{p} \mid \ell$ s'écrit :

$$N_{K_\mathfrak{p}/\mathbb{Q}_2}(x_\mathfrak{p}) \in 2^{\mathbb{Z}_2}.$$

Elle définit donc un sous-groupe d'indice 1 ou 2 du noyau de l'application composée de la norme locale et du logarithme d'Iwasawa dans $\mathbb{Q}_2^\times$. Cet indice s'interprète d'ailleurs très simplement par la théorie locale du corps de classes.

Considérons, en effet, l'extension abélienne, disons $L_\mathfrak{p}$, de $K_\mathfrak{p}$ qui est associée à $\mathcal{K}_\mathfrak{p}^*$ par le corps de classes local : le groupe de Galois $G_\mathfrak{p} = Gal(\overline{K}_\mathfrak{p}^{ab}/K_\mathfrak{p})$ de la pro-ℓ-extension abélienne maximale de $K_\mathfrak{p}$ s'identifiant au groupe profini $\mathcal{K}_\mathfrak{p}^\times = \varprojlim_n K_\mathfrak{p}^\times/K_\mathfrak{p}^{\times \ell^n}$, le corps $L_\mathfrak{p}$ est tout simplement la sous-extension de $\overline{K}_\mathfrak{p}^{ab}$ qui est fixée par $\mathcal{K}_\mathfrak{p}^*$,

- si $\mathfrak{p}$ est réelle (i.e. si $K_\mathfrak{p} = \mathbb{R}$), c'est $\mathbb{R}$ si ℓ est impair, et $\mathbb{C}$ si ℓ vaut 2, et dans les deux cas c'est la ℓ-extension cyclotomique de $\mathbb{R}$;

- si $\mathfrak{p}$ est modérée, $\mathcal{K}_\mathfrak{p}^*$ s'identifie au sous-groupe d'inertie de $G_\mathfrak{p}$, et $L_\mathfrak{p}$ est donc la pro-ℓ-extension abélienne maximale non ramifiée de $K_\mathfrak{p}$; c'est-à-dire sa $\mathbb{Z}_\ell$-extension cyclotomique.

- si $\mathfrak{p}$ est sauvage et ℓ impair, $\mathcal{K}_\mathfrak{p}^*$ est l'image réciproque par la norme locale $N_{K_\mathfrak{p}}/\mathbb{Q}_\ell$ du noyau dans $\mathbb{Q}_\ell^\times$ du logarithme d'Iwasawa, noyau qui est précisément constitué des normes cyclotomiques. De sorte que dans ce cas encore $L_\mathfrak{p}$ est exactement la $\mathbb{Z}_\ell$-extension cyclotomique de $K_\mathfrak{p}$;

- enfin, si $\mathfrak{p}$ est sauvage et ℓ vaut 2, la même description normique montre que $L_\mathfrak{p}$ est la 2-tour cyclotomique de $K_\mathfrak{p}$, c'est-à-dire que c'est une extension au plus quadratique de la $\mathbb{Z}_2$-extension cyclotomique de $K_\mathfrak{p}$.

3.- Le groupe des classes de valeurs absolues.

Nous avons vu dans la section précédente que les idèles principaux (i.e. les éléments de $\mathcal{R}_K$) satisfont la formule du produit pour les valeurs absolues ℓ-adiques :

$$\|x\| =_{\text{déf}} \prod_{\mathfrak{p} \in Pl(K)} |x|_\mathfrak{p} = 1$$

Désignons par $\tilde{\mathcal{J}}_K$ le sous-groupe fermé de $\mathcal{J}_K$ constitué de tous les idèles qui vérifient la formule du produit :

$$\tilde{\mathcal{J}}_K = \widetilde{\prod}_{\mathfrak{p}\in Pl(K)} \mathcal{K}_\mathfrak{p}^\times = \{(x_\mathfrak{p})_{\mathfrak{p}\in Pl(K)} |\ \|(x_\mathfrak{p})_\mathfrak{p}\| = \prod_{\mathfrak{p}\in Pl(K)} |x_\mathfrak{p}|_\mathfrak{p} = 1\}.$$

C'est un sous-module fermé de $\mathcal{J}_K$ qui contient $\mathcal{R}_K$, et il lui correspond donc, par la théorie ℓ-adique du corps de classes une extension abélienne, disons K_∞, de K. Pour la déterminer, il suffit de remarquer que $\tilde{\mathcal{J}}_K$ est l'image réciproque par la norme arithmétique $N_{K/\mathbb{Q}}$ de son analogue $\tilde{\mathcal{J}}_\mathbb{Q}$ dans $\mathcal{J}_\mathbb{Q}$. Maintenant, un calcul immédiat montre que $\tilde{\mathcal{J}}_\mathbb{Q}$ est engendré par $\mathcal{R}_\mathbb{Q}$ et le produit $\prod_{p\neq\ell} \mathcal{U}_p$. La pro-$\ell$-extension abélienne de $\mathbb{Q}$ associée à $\tilde{\mathcal{J}}_\mathbb{Q}$ est donc celle ℓ-ramifiée maximale, c'est-à-dire, tout simplement la ℓ-tour cyclotomique $\mathbb{Q}_\infty$ de $\mathbb{Q}$; et celle associée à $\tilde{\mathcal{J}}_K$ est ainsi la ℓ-tour cyclotomique $K_\infty = \mathbb{Q}_\infty K$ de K.

DÉFINITION 4. - *Soit, comme plus haut* $\tilde{\mathcal{J}}_K = \widetilde{\prod}_{\mathfrak{p}\in Pl(K)} \mathcal{K}_\mathfrak{p}^\times$ *le noyau dans* J_K *de la formule du produit, et* $J_K^* = \prod_{\mathfrak{p}\in Pl(K)} \mathcal{K}_\mathfrak{p}^*$ *le noyau des valeurs absolues. Nous disons que le quotient*

$$\widetilde{Cl}_K = \tilde{J}_K / J_K^* \mathcal{R}_K$$

est le ℓ-groupe des classes logarithmiques du corps K.

L'appellation de classes logarithmiques se comprend comme suit : aux places finies modérées, l'application composée de la valeur absolue ℓ-adique principale $|\ |_\mathfrak{p}$ sur $\mathcal{K}_\mathfrak{p}^\times$ et de l'opposé du logarithme ℓ-adique Log_ℓ (défini sur le groupe multiplicatif $1+\ell\mathbb{Z}_\ell$ par son développement en série $-\mathrm{Log}_\ell(1+x) = \sum_{n=1}^{\infty} (-1)^k x^k$) induit un isomorphisme du quotient $\mathcal{K}_\mathfrak{p}^\times / \mathcal{K}_\mathfrak{p}^*$ sur le sous-module de $\mathbb{Z}_\ell$ engendrée par le logarithme ℓ-adique de la norme absolue de l'idéal $\mathfrak{p}$:

$$\mathcal{K}_\mathfrak{p}^\times / \mathcal{K}_\mathfrak{p}^* \simeq \mathbb{Z}_\ell \ \mathrm{Log}_\ell N\mathfrak{p}.$$

Comme un résultat semblable (bien que plus compliqué) vaut pour les places sauvages, le quotient $\tilde{\mathcal{J}}_K / \mathcal{J}_K^*$ représente en quelque sorte le ℓ-groupe des diviseurs logarithmiques du corps K ; et son quotient par le sous groupe principal $\mathcal{R}_K \mathcal{J}_K^* / \mathcal{J}_K^*$ est bien le ℓ-groupe des classes logarithmiques de K.

Cela posé, nous avons :

CONJECTURE DE GROSS GÉNÉRALISÉE. - *Le groupe* $\widetilde{Cl}_K$ *est fini.*

Pour retrouver la conjecture initiale de Gross dans cette formulation, considérons la suite exacte canonique (où le tilde signifie que l'on se restreint aux familles qui vérifient la formule du produit) :

$$\mathcal{E}'_K \longrightarrow \widetilde{\prod}_{\mathfrak{p}|\ell} |K_{\mathfrak{p}}^{\times}|_{\mathfrak{p}} \longrightarrow \widetilde{Cl}_K \longrightarrow Cl'_K$$

$$\mathcal{E}'_K \longrightarrow \widetilde{\prod}_{\mathfrak{p}|\ell} K_{\mathfrak{p}}^{\times}/K_{\mathfrak{p}}^{*} \longrightarrow \tilde{\mathcal{J}}_K/\mathcal{J}_K^{*}\mathcal{R}_K \longrightarrow \mathcal{J}_K/\prod_{\mathfrak{p}|\ell\infty} K_{\mathfrak{p}}^{\times}.\prod_{\mathfrak{p}\nmid\ell} \mathcal{U}_{\mathfrak{p}}.\mathcal{R}_K$$

Dans celle-ci le terme de gauche $\mathcal{E}'_K = \mathbb{Z}_\ell \otimes_{\mathbb{Z}} E'_K$ est le tensorisé ℓ-adique du groupe des ℓ-unités de K ; le terme de droite Cl'_K n'est rien d'autre que le ℓ-groupe des ℓ-classes d'idéaux du corps K (i.e. le quotient du ℓ-groupe des classes d'idéaux au sens ordinaire par le sous-groupe engendré par les idéaux premiers au-desus de ℓ) ; le terme en $\tilde{\prod}$ est un $\mathbb{Z}_\ell$-module noethérien de dimension $l_K - 1$, si l_K est le nombre de places de K au-dessus de ℓ (qui est libre si ℓ est impair) ; et le terme de gauche $\mathcal{E}'_K$ est simplement le tensorisé ℓ-adique du groupe des ℓ-unités de K. Cela étant, affirmer la finitude de $\widetilde{Cl}_K$ équivaut donc à affirmer que le sous-module de $\tilde{\prod}_{\mathfrak{p}|\ell} |K_{\mathfrak{p}}^{\times}|_{\mathfrak{p}}$ qui est engendré par les valeurs absolues ℓ-adiques des ℓ-unités de K est encore de dimension $l_K - 1$; ce qui, appliqué aux seules composantes imaginaires pour un corps à conjugaison complexe (i.e. extension quadratique totalement imaginaire d'un sous-corps totalement réel), est bien la première conjecture de B.H. Gross.

Pour relier maintenant la conjecture de Gross à ses interprétations cyclotomiques, il est commode de réinterpréter le groupe $\widetilde{Cl}_K$ à l'aide de la théorie ℓ-adique du corps de classes : Nous avons vu plus haut que le numérateur $\tilde{\mathcal{J}}_K$ est associé à la ℓ-extension cyclotomique K_∞ de K. D'un autre côté, nous savons par le corps de classes local que le facteur $K_{\mathfrak{p}}^{*}$ de $\mathcal{J}_K^{*}$ est le sous-groupe de normes de $K_{\mathfrak{p}}^{\times}$ qui correspond à la ℓ-extension cyclotomique locale $L_{\mathfrak{p}}$ de $K_{\mathfrak{p}}$. L'extension globale associée au produit $\mathcal{J}_K^{*}\mathcal{R}_K$ est donc la plus grande ℓ-extension abélienne de K, qui est localement cyclotomique en chacune des places de K, autrement dit la pro-ℓ-extension

maximale L_∞ de K_∞ qui est abélienne sur K et complètement décomposée partout sur K_∞. Naturellement, aux places modérées, la montée dans la ℓ-tour cyclotomique K_∞/K ayant épuisé les possibilités d'inertie, la condition de complète décomposition est simplement une condition de non ramification. Le corps L_∞ est donc aussi la pro-ℓ-extension abélienne maximale de K qui est non ramifiée et ℓ-décomposée sur K_∞ : c'est ce qu'il est convenu d'appeler le ℓ-corps des ℓ-genres de l'extension profinie K_∞/K. Par suite, lorsque K_∞ est procyclique sur K (ce qui est toujours le cas lorsque ℓ est impair), disons $K_\infty = \bigcup_{n\in\mathbb{N}} K_n$, avec K_n cyclique de degré ℓ^n sur K, le groupe $\widetilde{C\ell}_K$ s'identifie au quotient des genres

$$\widetilde{C\ell}_K \simeq \mathcal{C}'_{K_\infty}/\mathcal{C}'^{(\gamma-1)}_{K_\infty},$$

où $\mathcal{C}'_{K_\infty} = \varprojlim_n Cl'_{K_n}$ est le groupe de Galois de la ℓ-extension abélienne non ramifiée ℓ- décomposée maximale de K_∞, et γ un générateur topologique du groupe profini $\Gamma = Gal(K_\infty/K)$. On retrouve ainsi l'interprétation classique de la conjecture de Gross, qui consiste à postuler que le polynôme caractéristique $P \in \mathbb{Z}_\ell[\gamma - 1]$ du $\mathbb{Z}_\ell[[\gamma - 1]]$-module $\mathcal{C}'_{K_\infty}$ n'est pas un multiple de $(\gamma - 1)$ (cf. [9]; p. 317).

4.- Le noyau des valeurs absolues.

Supposons, pour simplifier l'exposé, que la ℓ-tour cyclotomique K_∞/K soit procyclique (ce qui est automatique lorsque ℓ est impair, mais peut être en défaut si ℓ vaut 2). Dans ce cas, lorsque ℓ vaut 2, le corps K est nécessairement totalement imaginaire, de sorte que l'hypothèse faite implique en particulier que les valeurs absolues ℓ-adiques attachées aux places réelles n'interviennent plus (parce qu'elles sont triviales pour ℓ impair, parce qu'il n'y en a plus pour $\ell = 2$). Plus généralement, l'image $|\mathcal{K}_\mathfrak{p}^\times|_\mathfrak{p} \simeq \mathcal{K}_\mathfrak{p}^\times/\mathcal{K}_\mathfrak{p}^*$ du complété profini $\mathcal{K}_\mathfrak{p}^\times$ par la valeur absolue correspondante $|\ |_\mathfrak{p}$ est alors un $\mathbb{Z}_\ell$-module libre quelle que soit la place $\mathfrak{p}$ (de rang 0 si $\mathfrak{p}$ est réelle, 1 sinon), et le noyau $\mathcal{N}_K = \mathcal{R}_K \cap \mathcal{J}_K^*$ des valeurs absolues dans $\mathcal{R}_K$ contenu dans le tensorisé $\mathcal{E}_K = \mathbb{Z}_\ell \otimes_\mathbb{Z} E'_K$ du groupe des ℓ-unités de K.

Plus précisément, dans la suite exacte déjà rencontrée :

$$1 \longrightarrow \mathcal{N}_K \longrightarrow \mathcal{E}'_K \longrightarrow \tilde{\prod}_{\mathfrak{p}|\ell} |\mathcal{K}_\mathfrak{p}^\times|_\mathfrak{p} \longrightarrow \widetilde{C\ell}_K \longrightarrow Cl'_K,$$

le terme médian $\tilde{\prod}_{\mathfrak{p}|\ell} |\mathcal{K}_\mathfrak{p}^\times|_\mathfrak{p}$ est alors un $\mathbb{Z}_\ell$-module libre de rang $l_K - 1$ (où l_K désigne le nombre de places sauvages de K), et $\mathcal{E}'_K$ le produit du

sous-module de torsion μ_K de $\mathcal{R}_K$ (le ℓ-groupe des racines de l'unité dans K) par un $\mathbf{Z}_\ell$-module libre de dimension $r_K + c_K + l_K - 1$ (où r_K et c_K désignent respectivement les nombres de places réelles et complexes de K).

Nous pouvons donc énoncer :

PROPOSITION 5. - *Le noyau $\mathcal{N}_K = \mathcal{R}_K \cap \mathcal{J}_K^*$ dans $\mathcal{R}_K$ des valeurs absolues ℓ-adiques principales est un $\mathbf{Z}_\ell$-module noethérien de dimension*

$$r_K + c_K + \delta_K$$

où r_K est le nombre de places réelles de K, c_K le nombre de places complexes, et $\delta_K = dim_{\mathbf{Z}_\ell} \widetilde{Cl}_K$ mesure le défaut de la conjecture de Gross dans K.

C'est un sous-module pur de $\mathcal{R}_K$ (contenu dans le groupe des ℓ-unités $\mathcal{E}'_K$) dès que la ℓ-tour cyclotomique K_∞/K est procyclique (ce qui est toujours le cas lorsque ℓ est impair).

SCOLIE 6. - *Le groupe dual $\mathfrak{N}_K = (\mathbf{Q}_\ell/\mathbf{Z}_\ell) \otimes_{\mathbf{Z}_\ell} \mathcal{N}_K$ est, lui, un $\mathbf{Z}_\ell$-module divisible de codimension $r_K + c_K + \delta_K$.*

On notera, en effet, que le produit tensoriel par $\mathbf{Q}_\ell/\mathbf{Z}_\ell$ a pour conséquence de tuer le sous-groupe de torsion μ_K de $\mathcal{N}_K$.

Ce point acquis, le théorème principal de [10] (th. 1.12) peut s'énoncer comme suit : Désignons par $\mathfrak{H}_K$ le radical hilbertien attaché au corps K, défini par

$$\mathfrak{H}_K = \{\ell^{-k} \otimes x \in (\mathbf{Q}_\ell/\mathbf{Z}_\ell) \otimes_{\mathbf{Z}_\ell} \mathcal{R}_K |\ \ x \ \in \mathcal{J}_K^{\ell^k} \mathcal{J}_K^*\}.$$

Nous avons :

THÉORÈME 7. - *Lorsque l'extension cyclotomique K_∞/K est procyclique, il existe une suite exacte naturelle scindée*

$$1 \longrightarrow \mathfrak{N}_K \longrightarrow \mathfrak{H}_K \longrightarrow \widetilde{Cl}_K^{\text{tor}} \longrightarrow 1,$$

où $\widetilde{Cl}_K^{\text{tor}}$ est le sous-module de torsion du groupe des classes de valeurs absolues $\widetilde{Cl}_K$ (autrement dit $\widetilde{Cl}_K$ lui-même, sous la conjecture de Gross).

En particulier, $\mathfrak{N}_K$ est le sous-module divisible maximal de $\mathfrak{H}_K$.

Démonstration du théorème : Remarquons d'abord que $\mathcal{N}_K$ étant un sous-module pur de $\mathcal{R}_K$ (comme expliqué à la proposition 5), son dual $\mathfrak{N}_K$

est un sous-module de celui $\mathfrak{R}_K = (\mathbb{Q}_\ell/\mathbb{Z}_\ell) \otimes_{\mathbb{Z}_\ell} \mathcal{R}_K \simeq (\mathbb{Q}_\ell/\mathbb{Z}_\ell) \otimes_{\mathbb{Z}} K^\times$ de $\mathcal{R}_K$, et il est trivialement contenu dans $\mathfrak{H}$. Tout le problème est donc d'interpréter le quotient $\mathfrak{H}_K/\mathfrak{N}_K$.

Pour cela, considérons un élément $\ell^{-k} \otimes x$ de $\mathfrak{H}_K$. Par définition, nous pouvons écrire $x = \mathfrak{y}^{\ell^k}\mathfrak{z}$, avec $\mathfrak{z} \in \mathcal{J}_K^*$ et $\mathfrak{y} \in \mathcal{J}_K$, en fait $\mathfrak{y} \in \tilde{\mathcal{J}}_K$, (puisque x et $\mathfrak{z}$ sont tous deux contenus dans le noyau de la formule du produit). En associant à l'élément $\ell^{-k} \otimes x$ la classe $c\ell(\mathfrak{y})$ de $\mathfrak{y}$ dans $\widetilde{C\ell}_K = \tilde{J}_K/\mathcal{J}_K^*\mathcal{R}_K$, nous définissons ainsi un morphisme de $\mathfrak{H}_K$ dans $\widetilde{C\ell}_K$ dont l'image est exactement le sous-groupe de torsion de $\widetilde{C\ell}_K$. Quel est son noyau ? Supposons $c\ell(\mathfrak{y}) = 1$, i.e. $\mathfrak{y} = \mathfrak{z}'x'$ avec $\mathfrak{z}' \in \mathcal{J}_K^*$ et $x' \in \mathcal{R}_K$. Nous avons alors $\ell^{-k} \otimes x = \ell^{-k} \otimes (x/x'^{\ell^k})$, et $x/x'^{\ell^k} \in \mathcal{R}_K \cap \mathcal{J}_K^* = \mathcal{N}_K$; ce qui établit l'exactitude de la suite.

Interprétation du noyau hilbertien : Considérons l'image, disons $\mathfrak{H}'_K$, du radical hilbertien $\mathfrak{H}_K$ dans le dualisé $\mathfrak{J}_K = (\mathbb{Q}_\ell/\mathbb{Z}_\ell) \otimes_{\mathbb{Z}} \mathcal{J}_K$ du groupe des idèles. Par définition les éléments de $\mathfrak{H}'_K$ sont ceux construits à partir des éléments de $\mathcal{J}_K^*$ c'est-à-dire, comme on l'a vu, à partir des normes cyclotomiques locales. Maintenant, dans l'extension procyclique K_∞/K le fait d'être norme ou non se lit localement, en vertu du principe de Hasse. Les éléments de $\mathfrak{H}_K$ sont donc tout simplement les éléments du radical $\mathfrak{R}_K \simeq (\mathbb{Q}_\ell/\mathbb{Z}_\ell) \otimes_{\mathbb{Z}} K^\times$ qui sont représentés par les normes cyclotomiques :

$$\mathfrak{H}_K = \{\ell^{-k} \otimes x \in \mathfrak{R}_K |\ \forall n \in \mathbb{N}\ \ x \in K_n^{\times \ell^k} N_n(K^\times)\},$$

si l'on désigne par N_n la norme arithmétique dans la sous-extension K_n/K de degré ℓ^n de l'extension cyclotomique K_∞/K.

L'introduction du groupe $\mathfrak{H}_K$ dans la théorie cyclotomique, sous une forme naturellement très différente, remonte en fait à F. Bertrandias et J.-J. Payan qui l'ont utilisé dans [1] pour étudier une condition suffisante de la conjecture de Leopoldt. Enfin l'appellation radical hilbertien que nous préférons s'explique aisément : du point de vue de la K-théorie des corps de nombres, les normes cyclotomiques sont caractérisées comme noyau des symboles de Hilbert construits sur les racines de l'unité (cf. [9], Ch. I.2).

5 - Noyau universel et radical des $\mathbb{Z}_\ell$-extensions.

Nous supposerons dans cette section que le corps K contient les racines 2ℓ-ièmes de l'unité (de sorte que la condition restrictive introduite au début de

la section 4 sera en particulier remplie). Disons cependant que lorsque cette hypothèse n'est pas vérifiée, il est toujours possible de pallier cette difficulté (au moins pour ℓ impair), en raisonnant sur le sur-corps $K' = K[\zeta_\ell]$, puis en redescendant certains résultats sur K en s'aidant de la décomposition semi-locale de l'algèbre $\mathbf{Z}_\ell[Gal(K'/K)]$ donnée par les idempotents primitifs associés aux caractère ℓ-adiques irréductibles du groupe $Gal(K'/K)$.

Commençons par fixer quelques notations : pour chaque naturel n écrivons K_n l'extension $K[\zeta_{\ell^n}]$ engendrée sur K par les racines ℓ^n-ièmes de l'unité (de sorte que nous avons $K = K_0 = ... = K_m$ jusqu'à un certain rang m, puis $[K_{n+1} : K_n] = \ell$ pour $n \geq m$) ; notons Γ le groupe de Galois $Gal(K_\infty/K)$ identifié à $\mathbf{Z}_\ell$ par le choix d'un générateur topologique γ, puis $\Lambda = \mathbf{Z}_\ell[[\gamma - 1]]$ l'algèbre d'Iwasawa associée, et $\Gamma_n = \Gamma^{\ell^{n-m}}$ (pour $n \geq m$) le sous-groupe $Gal(K_\infty/K_n)$. Introduisons enfin le module de Tate :

$$\mathbf{T}_\ell = \varprojlim_n \mu_{\ell^n}$$

limite projective des sous-groupes finis de μ_{ℓ^∞} (qui est isomorphe à $\mathbf{Z}_\ell$ comme groupe abstrait), et

$$\overline{\mathbf{T}}_\ell = Hom(\mu_{\ell^\infty},\ \mathbf{Q}_\ell/\mathbf{Z}_\ell)$$

le module opposé, défini comme dual de Pontrjagin de la limite inductive des μ_{ℓ^n} (qui est encore $\mathbf{Z}_\ell$ comme groupe abstrait, mais avec une action galoisienne différente).

Cela posé, les résultats de [9] montrent que les radicaux respectifs

$$\mathfrak{R}_{K_n} = (\mathbf{Q}_\ell/\mathbf{Z}_\ell) \otimes_{\mathbf{Z}} K^\times \simeq (\mathbf{Q}_\ell/\mathbf{Z}_\ell) \otimes_{\mathbf{Z}_\ell} \mathcal{R}_{K_n},$$

associés aux corps K_{K_n}, vérifient la théorie de Galois dans K_∞/K ; c'est à dire que l'on a :

$$\mathfrak{R}_{K_n} \subset \mathfrak{R}_{K_\infty} = (\mathbf{Q}_\ell/\mathbf{Z}_\ell) \otimes_{\mathbf{Z}} K_\infty^\times, \quad \text{en fait} \quad \mathfrak{R}_{K_n} = \mathfrak{R}_{K_\infty}^{\Gamma_n}$$

(cf. [9], prop. I.2.2) ; et qu'un résultat analogue vaut pour les radicaux hilbertiens :

$$\mathfrak{H}_{K_n} = \mathfrak{H}_{K_\infty}^{\Gamma_n}, \text{ où } \mathfrak{H}_{K_n} = \{\ell^{-k} \otimes x \in \mathfrak{R}_{K_n} |\ \ x \in \mathcal{J}_{K_n}^{\ell^k} \mathcal{J}_{K_n}^*\}$$

(cf. [9], prop. I.2.18).

Nous sommes plus particulièrement intéressés ici par trois sous-groupes remarquables de $\mathfrak{H}_{K_\infty}$:

- le noyau $\mathfrak{U}_{K_\infty}$ dans $\mathfrak{R}_{K_\infty}$ des symboles $\{\ ,\ \}$ à valeurs dans le groupe universel $K_2(K_\infty)$:

$$\mathfrak{U}_{K_\infty} = \{\ell^{-k} \otimes x \in \mathfrak{R}_{K_\infty} |\ \ \{\zeta_{\ell^k}, x\} = 1, \ \text{ dans } K_2(K_\infty)\}.$$

- Le radical $\mathfrak{Z}_{K_\infty}$ attaché à la réunion $Z_\infty = \bigcup_{n\in\mathbb{N}} Z_n$ des composées Z_n des $\mathbb{Z}_\ell$–extensions des corps K_n :

$$\mathfrak{Z}_{K_\infty} = \{\ell^{-k} \otimes x \in \mathcal{R}_{K_\infty} |\ | K_\infty[\sqrt[\ell^k]{x}] \subset Z_\infty\}.$$

- Le radical $\mathfrak{N}_{K_\infty}$ construit sur le noyau $\mathcal{N}_{K_\infty}$ dans $\mathcal{R}_{K_\infty} = \mathbb{Z}_\ell \otimes_{\mathbb{Z}} K_\infty^\times$ des valeurs absolues :

$$\mathfrak{N}_{K_\infty} = \{\ell^{-k} \otimes x \in \mathcal{R}_{K_\infty} |\ \ x \in \mathcal{N}_{K_\infty} = \bigcup_{n\in\mathbb{N}} \mathcal{N}_{K_n}\}.$$

Avec ces notations, les résultats de J. Coates (cf. [2], th. 4) et de M. Koster (cf. [10], th. 2.6) peuvent être présentés synoptiquement comme suit :

THÉORÈME 8. - *En haut de la tour cyclotomique, on a les inclusions :*

(i) $\mathfrak{U}_{K_\infty} \subset \mathfrak{Z}_{K_\infty}$, *avec égalité si et seulement si le corps* K_∞ *vérifie la conjecture de Leopoldt.*

(ii) $\mathfrak{U}_{K_\infty} \subset \mathfrak{N}_{K_\infty}$, *avec égalité si et seulement si le corps* K_∞ *vérifie la conjecture de Gross.*

Démonstration. Désignons par $\mathcal{X}$ le dual de Pontrjagin de $\mathfrak{H}_{K_\infty}$. La théorie d'Iwasawa (cf. [7] §8) montre que le groupe $\mathcal{X}$ est un Λ-module noethérien qui n'a pas de sous-module fini non nul, et plus précisément qu'il existe une suite exacte de Λ-modules

$$1 \longrightarrow \mathcal{X} \longrightarrow \Lambda^c \oplus T \longrightarrow F \longrightarrow 1$$

où c est le nombre de places complexes de K, F un Λ-module fini qui sera précisé plus loin, et T une somme directe de quotients de Λ par des puissances d'idéaux premiers de hauteur 1. Les produits tensoriels par $\mathbf{T}_\ell$

et $\overline{\mathbf{T}}_\ell$ respectivement des divers termes de la suite fournissent alors deux autres suites analogues pour $\mathbf{T}_\ell \otimes_{\mathbf{Z}_\ell} \mathcal{X}$ et $\overline{\mathbf{T}}_\ell \otimes_{\mathbf{Z}_\ell} \mathcal{X}$ dans lesquelles le terme Λ^c est inchangé.

Choisissons donc n assez grand pour que le générateur $\gamma_n = \gamma^{\ell^{n-m}}$ de Γ_n opère trivialement sur F et ses tensorisés $\mathbf{T}_\ell \otimes_{\mathbf{Z}_\ell} F$ et $\overline{\mathbf{T}}_\ell \otimes_{\mathbf{Z}_\ell} F$; puis faisons agir l'élément $\omega_n = \gamma_n - 1$ sur chacun des termes des suites obtenues.

Partant par exemple de la suite courte écrite plus haut, nous obtenons par le lemme du serpent la suite exacte à quatre termes :

$$1 \longrightarrow F \longrightarrow \mathcal{X}/\mathcal{X}^{\omega_n} \longrightarrow (\Lambda/\omega_n\Lambda)^c \oplus T/\omega_n T \longrightarrow F \longrightarrow 1,$$

qui nous montre que la dimension sur $\mathbf{Z}_\ell$ du plus grand quotient de $\mathcal{X}/\mathcal{X}^{\omega_n}$ qui est un $\mathbf{Z}_\ell$-module libre (autrement dit la codimension du sous-module divisible maximal de son dual de Pontrjagin $\mathfrak{H}_n = \mathfrak{H}_{K_\infty}^{\Gamma_n}$ est égale à celle $c_n = c\ell^n$ du $\mathbf{Z}_\ell$-module libre $(\Lambda/\omega_n\Lambda)^c$
augmentée de celle du plus grand quotient de $T/\omega_n T$ qui est un $\mathbf{Z}_\ell-$ module libre. Et un résultat analogue vaut naturellement pour les suites tensorisées. Distinguons donc les trois cas :

(i) cas des valeurs absolues : le sous-module divisible maximal de $\mathfrak{H}_{K_n}$ est le groupe $\mathfrak{N}_{K_n}$ dont la codimension a été calculée au scolie 6. Cela montre que le défaut δ_n de la conjecture de Gross dans K_n est donné par la formule :

$$\delta_n = dim_{\mathbf{Z}_\ell}\, T/\omega_n\, T.$$

En d'autres termes, la conjecture de Gross dans K_∞ postule donc simplement que le polynôme caractéristique du Λ-module T n'a pas de facteur cyclotomique. Lorsqu'elle est satisfaite, le sous-groupe $\mathfrak{N}_{K_\infty}$ de $\mathfrak{H}_{K_\infty}$ est donc exactement l'orthogonal du sous-module de torsion $\mathcal{T} = \mathcal{X} \cap T$ de $\mathcal{X}$ dans la dualité de Pontrjagin ; il est strictement plus grand sinon.

(ii) cas des symboles : d'après la théorie de Tate (cf. [14]), la dimension du sous-module divisible maximal $\mathbf{T}_\ell \otimes_{\mathbf{Z}_\ell} \mathfrak{U}_\infty$ est égale au nombre de places complexes $c_n = c\ell^n$ de K_n. Il en résulte par dualité que le polynôme caractéristique du Λ-module de torsion $\overline{\mathbf{T}}_\ell \otimes_{\mathbf{Z}_\ell} T$ n'a pas de facteur cyclotomique. Le noyau universel $\mathfrak{U}_{K_\infty}$ est donc toujours l'orthogonal du sous-module de torsion $\mathcal{T}$. En particulier il est contenu dans $\mathfrak{N}_{K_\infty}$, et lui est égal sous la conjecture de Gross.

(iii) cas des $\mathbb{Z}_\ell$-extensions : d'après la théorie de Kummer (cf. [9], I.2.1§c), le radical $\overline{\mathsf{T}}_\ell \otimes_{\mathbb{Z}_\ell} \mathfrak{Z}_n$ correspondant à la composée des $\mathbb{Z}_\ell$- extensions du corps K_n est le sous-module divisible maximal du groupe des points fixes $(\overline{\mathsf{T}}_\ell \otimes_{\mathbb{Z}_\ell} \mathfrak{H}_\infty)^{\Gamma_n}$ du tensorisé $\overline{\mathsf{T}}_\ell \otimes_{\mathbb{Z}_\ell} \mathfrak{H}_\infty$. Il s'ensuit que le défaut δ_n^* de la conjecture de Leopoldt dans K_n (qui mesure le nombre des $\mathbb{Z}_\ell$-extensions en excès) est donné par la formule :

$$\delta_n^* = dim_{\mathbb{Z}_\ell}\ (\mathsf{T}_\ell \otimes_{\mathbb{Z}_\ell} T)/\omega_n(\mathsf{T}_\ell \otimes_{\mathbb{Z}_\ell} T)$$

n'a pas de facteur cyclotomique. Lorsqu'elle est vérifiée le sous-groupe $\mathfrak{Z}_\infty = \cup_{n\in\mathbb{N}}\mathfrak{Z}_n$ est donc exactement l'orthogonal de $\mathcal{T}$; il est strictement plus grand sinon.

SCOLIE 9. - *Sous les conjectures de Leopoldt et de Gross, le radical $\mathfrak{Z}_{K_n}$ des $\mathbb{Z}_\ell$-extensions de K_n, le noyau $\mathfrak{N}_{K_n}$ des valeurs absolues dans K_n, et le noyau $\mathfrak{U}_{K_n}$ des symboles universels à valeurs dans $K_2(K_n)$, sont tous trois des $\mathbb{Z}_\ell$-modules libres de dimension $c_n = c\ell^n$. En général cependant ils ne coïncident pas, car la descente galoisienne s'écrit :*

$$(\overline{\mathsf{T}}_\ell \otimes \mathfrak{Z}_{K_n}) = (\overline{\mathsf{T}}_\ell \otimes \mathfrak{Z}_{K_\infty})^{\Gamma_n}_{\mathrm{div}}\ ;\ (\mathsf{T}_\ell \otimes \mathfrak{U}_{K_n}) = (\mathsf{T}_\ell \otimes \mathfrak{U}_{K_\infty})^{\Gamma_n}_{\mathrm{div}};$$

$$\mathfrak{N}_{K_n} = (\mathfrak{N}_{K_\infty}^{\Gamma_n})_{\mathrm{div}}$$

si l'on convient de désigner par $\mathfrak{M}_{\mathrm{div}}$ le sous-groupe divisible maximal d'un $\mathbb{Z}_\ell$−module $\mathfrak{M}$.

Remarque. Sous la condition nécessaire et suffisante $\widetilde{C\ell}_K = 1$, les trois radicaux ci-dessus coïncident pour tout n avec le radical hilbertien $\mathfrak{H}_{K_n}$. On retrouve ainsi la condition suffisante des conjectures de Leopoldt et de Gross avancée dans [1] et discutée dans [8].

6 - La question de la capitulation

Conservons les hypothèses de la section 5, et supposons vérifiées en outre les deux conjectures de Leopoldt et de Gross aux divers étages finis de la tour cyclotomique K_∞/K. Dans ce cas, les résultats de R. Greenberg (cf. [6]) montrent que la seule obstruction à l'égalité des trois radicaux définis dans le scolie 9 ci-dessus réside dans le sous-quotient $C = \Lambda^c/\Lambda^c(\mathcal{X}+T)$ du groupe fini F évoqué plus haut. Avant de préciser ce point, disons un mot

sur le groupe C lui-même. Les calculs d'Iwasawa (cf. [7], §5.4, 6.3, 8.4, et 8.5) prouvent implicitement que le dual de Pontrjagin $\hat{C}$ de C s'identifie à la limite projective, disons

$$Cap'_{K_\infty} = \lim_{\leftarrow n} Cap'_{K_\infty}$$

des sous-groupes respectifs Cap'_{K_n} des ℓ-groupes de ℓ-classes des corps K_n formés des ℓ-classes de $C\ell'_{K_n}$ qui capitulent dans $C\ell'_{K_\infty}$, les groupes Cap'_{K_n} étant d'ailleurs finis et stationnaires à isomorphisme canonique près.

Pour retrouver directement ce résultat en termes de classes logarithmiques, nous pouvons procéder comme suit : Désignons par $\hat{\mathfrak{N}}_{K_\infty}$ le dual de Pontrjagin du noyau $\mathfrak{N}_{K_\infty}$, et partons de la suite exacte courte qui définit le groupe fini C :

$$1 \longrightarrow \hat{\mathfrak{N}}_{K_\infty} \longrightarrow \Lambda^c \longrightarrow C \longrightarrow 1$$

Faisant opérer Γ_n, en fixant n assez grand pour que l'élément $\omega_n = \gamma^{\ell^n} - 1$ annule C, nous obtenons la suite exacte à quatre termes

$$1 \longrightarrow C \longrightarrow \hat{\mathfrak{N}}_{K_\infty}/\hat{\mathfrak{N}}_{K_\infty}^{\omega_n} \longrightarrow (\Lambda/\omega_n\Lambda)^c \longrightarrow C \longrightarrow 1,$$

qui nous prouve, puisque le quotient $\Lambda/\omega_n\Lambda$ est un $\mathbb{Z}_\ell$ module libre, que C est exactement le sous-module fini du quotient $\hat{\mathfrak{N}}_{K_\infty}/\hat{\mathfrak{N}}_{K_\infty}^{\omega_n}$, autrement dit que son dual de Pontrjagin $\hat{C}$ s'identifie au quotient du sous groupe $\hat{\mathfrak{N}}_{K_\infty}^{\Gamma_n}$ de $\hat{\mathfrak{N}}_{K_\infty}$ par son sous-module divisible maximal.

Écrivons maintenant la suite exacte naturelle donnée par le théorème 7 :

$$1 \longrightarrow \mathfrak{N}_{K_n} \longrightarrow \mathfrak{H}_{K_n} \longrightarrow \widetilde{C\ell}_{K_n} \longrightarrow 1.$$

Passant à la limite inductive avec n, et prenant les points fixes par Γ_n, nous obtenons la suite exacte longue de cohomologie

$$1 \longrightarrow \mathfrak{N}_{K_\infty}^{\Gamma_n} \longrightarrow \mathfrak{H}_{K_\infty}^{\Gamma_n} \longrightarrow \widetilde{C\ell}_{K_\infty}^{\Gamma_n} \longrightarrow \dots$$

où le terme médian $\mathfrak{H}_{K_\infty}^{\Gamma_n}$ n'est autre que le radical hilbertien précédent $\mathfrak{H}_{K_n}$. Par le lemme du serpent, nous en concluons immédiatement que le

quotient $\mathfrak{N}_{K_\infty}^{\Gamma_n}/\mathfrak{N}_{K_n}$ s'identifie au noyau de l'application naturelle de $\widetilde{C\ell}_{K_n}$ dans $\widetilde{C\ell}_{K_\infty}$, c'est-à-dire précisément au sous-groupe $\widetilde{Cap}_{K_n}$ de $\widetilde{C\ell}_{K_n}$ formé des ℓ-classes logarithmiques qui capitulent dans l'extension K_∞/K_n.

Bien entendu les mêmes calculs conduits cette fois à partir des suites exactes tordues

$$1 \longrightarrow \bar{\mathsf{T}}_\ell \otimes_{\mathbb{Z}_\ell} \hat{\mathfrak{U}}_{K_\infty} \longrightarrow \overline{\mathsf{T}}_\ell \otimes_{\mathbb{Z}_\ell} \Lambda^c \simeq \Lambda^c \longrightarrow \overline{\mathsf{T}}_\ell \otimes_{\mathbb{Z}_\ell} C \longrightarrow 1$$

$$1 \longrightarrow \mathsf{T}_\ell \otimes_{\mathbb{Z}_\ell} \hat{\mathfrak{Z}}_{K_\infty} \longrightarrow \mathsf{T}_\ell \otimes_{\mathbb{Z}} \Lambda^c \simeq \Lambda^c \longrightarrow \mathsf{T}_\ell \otimes_{\mathbb{Z}_\ell} C \longrightarrow 1$$

conduisent à des interprétations analogues faisant intervenir soit le noyau de l'homomorphisme d'extension pour les noyaux hilbertiens $H_2(K_n)$ de la K-théorie, soit le même noyau pour les groupes $\bar{H}_2(K_n)$ (cf. [9], ch. 1.2) définis comme les duaux de Pontrjagin respectifs des sous-groupes de torsion des groupes de Galois $Gal(H_n/K_n)$ attachés aux composées H_n des ℓ-extensions cycliques des corps K_n qui sont localement $\mathbb{Z}_\ell$-plongeables (et dans ce dernier cas, la "capitulation" en question traduit le fait banal qu'une ℓ-extension cyclique d'un K_n qui est localement $\mathbb{Z}_\ell$-plongeable sur K_n peut l'être globalement sur K_m, pour m assez grand, sans l'être sur K_n).

Résumons ces résultats qui prolongent ceux de J. Coates sur le noyau régulier (cf. [2]) :

PROPOSITION 10. *Sous les conjectures de Leopoldt et de Gross, le dual de Pontrjagin du groupe fini C s'identifie comme module galoisien à chacun des quatre modules suivants :*

i) *à la limite projective Cap'_{K_∞} des sous-groupes de ℓ-classes K_n qui capitulent dans K_∞;*
ii) *à la même limite $\widetilde{Cap}_{K_\infty}$ pour les groupes de classes logarithmiques $\widetilde{C\ell}_{K_n}$;*
iii) *aux tensorisés $\overline{\mathsf{T}_\ell} \otimes_{\mathbb{Z}_\ell} Ker(H_2(K_n) \to H_2(K_\infty))$, pour tout n assez grand ;*
iv) *aux tensorisés $\mathsf{T}_\ell \otimes_{\mathbb{Z}_\ell} Ker(\bar{H}_2(K_n) \to \bar{H}_2(K_\infty))$, pour tout n assez grand.*

Il est alors possible de préciser comme suit les résultats de R. Greenberg (cf. [6]) :

THÉORÈME 11. *Choisissons n assez grand pour que le groupe fini C soit annulé par l'opérateur $\omega_n = \gamma_n - 1$ comme par ℓ^n. Dans ce cas, sous les conjectures de Leopoldt et de Gross, les trois propriétés suivantes sont équivalentes :*

(i) *le groupe C est nul (autrement dit l'homomorphisme d'extension $C\ell'_n \to C\ell'_\infty$ est injectif.*
(ii) *il y a coïncidence entre les sous-groupes de ℓ^n-torsion respectifs du noyau universel $\mathfrak{U}_{K_n}$ et du noyau des valeurs absolues $\mathfrak{N}_{K_n}$.*
(iii) *Il y a coïncidence entre les sous-groupes de ℓ^n-torsion respectifs du radical $\mathfrak{Z}_{K_n}$ des $\mathbb{Z}_\ell$-extensions de K_n et du noyau $\mathfrak{N}_{K_n}$ des valeurs absolues.*

Et, lorsque ℓ est impair, l'équivalence s'étend à la condition :
(iv) $_{\ell^n}\mathfrak{Z}_{K_n} = {}_{\ell^n}\mathfrak{N}_{K_n}$.

Remarque : L'intérêt du théorème 11 réside avant tout dans l'extrême inégalité des complexités numériques des trois radicaux concernés : lorsque le corps K_n est connu numériquement, le calcul du noyau $_{\ell^n}\mathfrak{N}_{K_n}$ est facile, les normes cyclotomiques étant définies par des formules explicites ; la détermination du radical initial des $\mathbb{Z}_\ell$-extensions $_{\ell^n}\mathfrak{Z}_{K_n}$ est moins directe : il faut utiliser par exemple le logarithme de Gras défini sur les groupes de classes (cf. [5]) ; celle de $_{\ell^n}\mathfrak{U}_{K_n}$ est beaucoup plus difficile encore en présence de symboles exotiques.

Démonstration du théorème : Les calculs qui précèdent montrent que le noyau $_{\ell^n}\mathfrak{N}_{K_n}$ est l'ensemble des éléments de ℓ^n-torsion du sous-module divisible maximal du groupe des points fixes $\mathfrak{N}_{K_\infty}^{\Gamma_n}$. Dans la dualité de Pontrjagin entre $\mathfrak{N}_{K_\infty}$ et $\hat{\mathfrak{N}}_{K_\infty} \subset \Lambda^c$, son orthogonal, disons X_n, est donc le sous-module $\omega_n\Lambda^c + \ell^n\hat{\mathfrak{N}}_{K_\infty}$ du groupe, noté additivement, $\hat{\mathfrak{N}}_{K_\infty}$: En effet, n ayant été choisi assez grand pour que ω_n annule C, nous avons bien $\omega_n\Lambda^c \subset \hat{\mathfrak{N}}_{K_\infty}$ et le quotient correspondant $\omega_n\Lambda^c/\omega_n\hat{\mathfrak{N}}_{K_\infty}$ est exactement le sous-groupe de torsion de $\hat{\mathfrak{N}}_{K_\infty}/\omega_n\hat{\mathfrak{N}}_{K_\infty}$. Considérons donc le quotient Λ^c/X_n. D'un côté, puisque c'est un quotient de $\Lambda^c/\omega_n\Lambda^c \simeq \mathbb{Z}_\ell^{c_n}$, sa décomposition comme produit de groupes cycliques fait intervenir au plus c_n facteurs. D'un autre côté, son sous module $\hat{\mathfrak{N}}_{K_\infty}/X_n$, qui est le dual de Pontrjagin de $_{\ell^n}\mathfrak{N}_{K_n}$, est lui un $\mathbb{Z}/\ell^n\mathbb{Z}$-module libre de dimension

c_n ; et il vient donc :

$$\Lambda^c/X_n \simeq \oplus_{i=1}^{c_n} \mathbf{Z}/\ell^{n+e_i}\mathbf{Z}, \quad \text{avec} \prod_{i=1}^{c_n} \ell^{e_i} = (\Lambda^c : \hat{\mathfrak{N}}_\infty) = |C|.$$

Le théorème sera donc établi si nous prouvons que chacune des quatre conditions énoncées équivaut à la nullité de tous les entiers naturels e_i. Or l'équivalence avec (i) résulte directement de la proposition 10. Celle avec (ii) ou (iii) s'établit comme suit : L'égalité de ${}_{\ell^n}\mathfrak{N}_{K_n}$ avec ${}_{\ell^n}\mathfrak{U}_{K_n}$ (respectivement avec ${}_{\ell^n}\mathfrak{Z}_{K_n}$) signifie que X_n reste inchangé lorsqu'on tord l'action de Γ_n sur Λ^c par le caractère cyclotomique (respectivement anticyclotomique), autrement dit que Γ_n agit trivialement sur

$$\mathbf{T}_\ell \otimes_{\mathbf{Z}_\ell} (\Lambda^c/X_n)$$

(respectivement $\bar{\mathbf{T}}_\ell \otimes_{\mathbf{Z}_\ell} (\Lambda^c/X_n)$). Mais le groupe Γ_n étant engendré topologiquement par l'élément γ_n défini par l'identité

$$\zeta^{\gamma_n} = \zeta^{1+\ell^n}, \forall \zeta \in \mu_{\ell^\infty},$$

cela revient à dire dans les deux cas que $1+\ell^n$ agit trivialement sur Λ^c/X_n, i.e que Λ^c/X_n est d'exposant ℓ^n. Enfin, le cas (iv) se traite de façon analogue à ceci près qu'il convient de remplacer $1+\ell^n$ par $(1+\ell^n)^2$, ce qui nécessite d'exclure le cas $\ell = 2$.

SCOLIE 12. *Sous les conjectures de Leopoldt et de Gross, il existe un entier naturel k tel qu'on ait identiquement pour tout n assez grand :*

$$\ell^{n-k}\mathfrak{U}_{K_n} = \ell^{n-k}\mathfrak{N}_{K_n} = \ell^{n-k}\mathfrak{Z}_{K_n}.$$

Preuve. Il suffit, en effet, de choisir k tel que ℓ^k annule C.

Terminons par deux exemples pour lesquels le théorème de Baker-Brumer assure la validité des conjectures de Leopoldt et de Gross (cf. [8]).

EXEMPLE 1. - Prenons $\ell = 3$ et $K = \mathbb{Q}[\sqrt{d}, \sqrt{-3d}]$ biquadratique contenant les racines cubiques de l'unité. Supposons 3 non décomposé dans le sous-corps quadratique réel $k = \mathbb{Q}[\sqrt{d}]$, et le 3-groupe de 3-classes $C\ell'_k$ trivial. Dans ce cas, la formule des classes ambiges (cf. [9], ch. III.1),

appliquée aux sous-extensions finies k_n/k de la 3-tour cyclotomique sur k, montre que l'on a identiquement $C\ell'_{k_n} = 1$, pour tout n, donc qu'il n'y a pas de 3-capitulation dans k_∞/k et, partant, dans K_∞/K. Dans ce cas, on a donc pour tout n :

$$\ell^n \mathfrak{U}_{K_n} = \ell^n \mathfrak{N}_{K_n} = \ell^n \mathfrak{Z}_{K_n}.$$

En particulier, le radical initial des $\mathbb{Z}_\ell$-extensions, pris dans K^ℓ/K^{X^ℓ}, tout comme le noyau des symboles universels, sont $\mathbb{F}_\ell$-engendrés par les classes de la racine j, du nombre 3, et de l'unité fondamentale ϵ du corps quadratique k.

Bien entendu, ce résultat est en défaut en présence de capitulation (cf. [6]).

EXEMPLE 2. - Soit ℓ un nombre premier impair satisfaisant la conjecture de Vandiver, i.e. ne divisant pas le nombre des classes du sous-corps réel maximal K^+ du ℓ-ième corps cyclotomique $K = \mathbb{Q}[\zeta]$. Dans ce cas, la formule des classes ambiges montre que la même propriété est encore vraie à chaque étage fini de la ℓ-tour cyclotomique $K_n = \mathbb{Q}[\zeta_{\ell^n}]$. Il vient alors comme plus haut :

$$\ell^n \mathfrak{U}_{K_n} = \ell^n \mathfrak{N}_{K_n} = \ell^n \mathfrak{Z}_{K_n}.$$

Et le groupe $\mathfrak{N}_{K_n}$ n'est autre que le $\mathbb{Z}_\ell$-module divisible construit sur les ℓ-unités de K_n.

RÉFÉRENCES

[1] F. BERTRANDIAS et J.-J. PAYAN - *Γ-extensions et invariants cyclotomiques*, Ann. Sci. Ec. Norm. Sup., **5** (1972), *517-543.*

[2] J. COATES - *On K_2 and some classical conjectures in algebraic number theory*, Ann. Math. **95** (1972), *99-116.*

[3] L.J.FEDERER - *The non-vanishing of Gross p-adic regulator Galois cohomologically*, Astérisque **147-148** (1987), *71-77.*

[4] L. J. FEDERER et B.H. GROSS (avec un appendice de W. SINNOT) - *Regulators and Iwasawa modules*, Inv. Math. **62** (1981), *443-457.*

[5] G. GRAS - *Plongements kummériens dans les $\mathbb{Z}_p$-extensions*, Compositio Math. **55** (1985), *383-396.*

[6] R. GREENBERG - *A note on K_2 and the theory of $\mathbb{Z}_p$-extensions*, Am. J. Math. **100** (1978), *1235-1245.*

[7] K. IWASAWA - *On $\mathbb{Z}_\ell$-extensions of algebraic number fields*, Ann. Math. **98** (1973), *246-326.*

[8] J.-F. JAULENT - *Sur les conjectures de Leopoldt et de Gross*, Astérisque **147-148** (1987), *107-120.*

[9] J.-F. JAULENT - *L'arithmétique des ℓ- extensions (Thèse)*, Pub. Math. Fac. Sci. Besançon, Théor. Nomb. **1984-85** et **1985-86**, fasc. 1 (1986), *1-349.*

[10] M. KOLSTER - *An idelic approach to the wild kernel*, Prépublication.

[11] K. KRAMER - *On the Hilbert kernel of K-theory and the Gross regulator*, Prépublication.

[12] K. KRAMER et A. CANDIOTTI - On K_2 and $\mathbb{Z}_\ell$-extensions of number fields, Am. J. Math. **100** (1978), *177-196.*

[13] T. NGUYEN QUANG DO - *Sur la torsion de certains modules galoisiens II*, Sém. Th. Nombres Paris 1986-87 ; Progress in Math. **75** (1988), *271-298.*

[14] T. NGUYEN QUANG DO - *Sur la torsion de certains modules galoisiens p-ramifiés*, Théorie des Nombres (Québec, PQ, 1987) *740-754* (1989), de Gruyter, Berlin-New York.

[15] J. TATE - *Relations between K_2 and Galois cohomology*, Inv. Math. **36** (1976), *257-274.*

[16] J. TATE - *Les conjectures de Stark sur les fonctions L d'Artin en $s = 0$*, Progress in Math. **47**, Birkhäuser (1984).

[17] J.-F. JAULENT - *La théorie de Kummer et le K_2 des corps de nombres* Sém. Th. Nombres Bordeaux Sér. 2, **2** (1990).

Jean-François JAULENT
Université Bordeaux I
U.F.R. de Mathématiques et d'Informatique
351, cours de la Libération
TALENCE Cedex

Astérisque

MICHEL LAURENT

Sur quelques résultats récents de transcendance

Astérisque, tome 198-199-200 (1991), p. 209-230

<http://www.numdam.org/item?id=AST_1991__198-199-200__209_0>

SUR QUELQUES RESULTATS RECENTS DE TRANSCENDANCE

par

Michel LAURENT

1. Introduction

Cet exposé vise un double objectif : présenter en premier lieu les principaux développements de la théorie des nombres transcendants grâce à une série d'exemples concrets et, d'autre part, illustrer une nouvelle méthode de transcendance en redémontrant de façon détaillée un résultat classique, à savoir le théorème des six exponentielles. Il est devenu maintenant habituel de formuler les résultats de transcendance en termes de groupes algébriques. Nous n'avons ici suivi ce point de vue que partiellement, nous étant surtout attaché à décrire les résultats concernant la fonction exponentielle usuelle. Aussi, commencerons nous par rappeler l'énoncé de la célèbre conjecture de SCHANUEL, qui est censé contenir tout ce qui est connu sur la transcendance de valeurs de la fonction exponentielle.

CONJECTURE : *Désignons par $x_1, \ldots, x_n$, soit des nombres complexes, soit des éléments de $\mathbf{C}_p$ situés dans le disque de convergence de l'exponentielle p-adique. On suppose que les nombres $x_1, \ldots, x_n$ sont $\mathbf{Q}$-linéairement indépendants. Alors le degré de transcendance sur $\mathbf{Q}$ du corps*

$$\mathbf{Q}(x_1, \ldots, x_n, e^{x_1}, \ldots, e^{x_n})$$

est $\geq n$.

Il s'ensuit en particulier que si $\alpha_1, \ldots, \alpha_n$ désignent des nombres algébriques non nuls et multiplicativement indépendants, les n nombres $x_i = \log \alpha_i, 1 \leq i \leq n$, sont algébriquement indépendants sur $\mathbf{Q}$.

Nous avons fait jouer au théorème des six exponentielles un rôle privilégié, l'utilisant comme fil conducteur entre les §.2, 3, 4 et 6. Le plan de l'article

est le suivant. On étudie dans le §.2 le rang de matrices dont les coefficients sont des logarithmes de nombres algébriques, et on applique les résultats obtenus à la conjecture de LEOPOLDT. Le §.3 est consacré à l'indépendance algébrique ; on y examine notamment les différents outils de nature algébrique qui ont été élaborés pour la circonstance. Dans les démonstrations modernes de transcendance, les lemmes de zéros jouent un rôle fondamental. Nous indiquons dans le §.4 l'énoncé le plus général actuellement connu en termes de groupes algébriques. Cet énoncé présente une grande analogie formelle avec une conjecture de géométrie diophantienne, due à S. LANG. On examine dans le §.5 les diverses contributions récentes à cette conjecture, ainsi que leurs relations avec certains résultats de transcendance et d'approximation diophantienne. Le §.6 est enfin consacré à la nouvelle preuve déjà mentionnée du théorème des six exponentielles.

2.1 Rang de matrices à coefficients logarithmiques

On se propose de minorer (ou si l'on est plus ambitieux de déterminer exactement) le rang sur $\mathbf{C}$ ou sur $\mathbf{C}_p$, de matrices de la forme :

$$A = \begin{bmatrix} \log \alpha_{11} & \dots, & \log \alpha_{1\ell} \\ \vdots & & \vdots \\ \log \alpha_{d1} & \dots, & \log \alpha_{d\ell} \end{bmatrix}$$

où les $\alpha_{ij}, 1 \leq i \leq d, 1 \leq j \leq \ell$, désignent des nombres algébriques non nuls. Comme exemple de résultats de ce type, citons le

THÉORÈME DES SIX EXPONENTIELLES : *Il s'agit du cas particulier* $d = 2$, $\ell = 3$. *On suppose que les deux lignes et les trois colonnes de* A *sont linéairement indépendantes sur* $\mathbf{Q}$. *Le rang de* A *est alors égal à deux.*

Signalons en passant la conjecture des quatre exponentielles, qui propose d'établir l'énoncé analogue obtenu avec $d = \ell = 2$. Dans le cas général, on dispose de minorations du rang de la matrice A sous des hypothèses du même type. D'une manière plus précise, les énoncés actuels prennent en compte les éventuelles relations $\mathbf{Q}$-linéaires entre les lignes de combinaisons $\mathbf{Q}$-linéaires de colonnes de A, relations qui ont évidemment pour effet de diminuer le rang d'une telle matrice. Il faut cependant noter que des hypothèses de cette nature, comme celles du théorème ci-dessous, sont insuffisantes pour décrire complètement le rang de la matrice A, voir [32].

Considérons le rang de A comme celui de ses vecteurs colonnes $y_j, 1 \leq j \leq \ell$, et désignons par

$$Y = \mathbf{Z}\, y_1 + \cdots + \mathbf{Z}\, y_\ell$$

le sous-groupe engendré dans $\mathbf{C}^d$ ou $\mathbf{C}_p^d$. L'énoncé suivant, dont la formulation m'a été indiquée par M. EMSALEM, se déduit du théorème 4.1 de [34]. D'un point de vue technique, on notera que les deux conditions de maximalité considérées ici impliquent la maximalité du coefficient $\mu^\sharp$ introduit dans [34].

THÉORÈME 1 : *Soit V un sous-espace vectoriel de $\mathbf{C}^d$ (resp. $\mathbf{C}_p^d$) contenant Y et soit W un sous-espace vectoriel de V. Supposons que W soit rationnel sur $\overline{\mathbf{Q}}$ (i.e. engendré par des points à coordonnées algébriques) et que l'on ait :*

$$\max_T \left[\frac{rg(Y \cap T)}{\dim T}\right] = \frac{rgY}{d} ,$$

$$\max_T \left[\frac{\dim(W \cap T)}{\dim T}\right] = \frac{\dim W}{d} ,$$

où T décrit l'ensemble des sous-espaces vectoriels $\mathbf{Q}$-rationnels non nuls de $\mathbf{C}^d$ (resp. $\mathbf{C}_p^d$). Alors

$$\dim V \geq \frac{d(rgY + \dim W)}{(rgY + d)} .$$

Lorsque $W = \{0\}$, on peut choisir pour V le $\grave{\mathbf{C}}$ (resp. $\mathbf{C}_p$)-espace vectoriel engendré par Y, et l'on obtient ainsi une minoration du rang A qui implique en particulier le théorème des six exponentielles.

A l'opposé, lorsque le sous-espace V est rationnel sur $\overline{\mathbf{Q}}$, le choix $W = V$ amène au célèbre résultat de A. BAKER : des logarithmes de nombres algébriques sont linéairement indépendants sur $\overline{\mathbf{Q}}$, si et seulement si ils le sont sur $\mathbf{Q}$.

2.2. Application à la conjecture de Leopoldt

Soit K un corps de nombres et soit p un nombre entier. La conjecture de LEOPOLDT affirme que le rang sur $\mathbf{Z}_p$ de l'adhérence p-adique du groupe des unités principales de K est égal au rang sur $\mathbf{Z}$ dudit groupe ; et cette assertion se ramène aisément au calcul du rang d'une matrice du type envisagé précédemment (voir par exemple le §.2 de [21]). Lorsque le corps K est galoisien sur $\mathbf{Q}$, de groupe de Galois G, on dispose de plus d'une action de G sur l'adhérence p-adique, et l'utilisation de certains sous-espaces $\overline{\mathbf{Q}}$-rationnels W permet d'isoler les diverses composantes isotypiques associées à cette action. On trouvera dans [20] une interprétation de cette construction en termes de tores. De façon précise, il est possible d'établir le résultat suivant.

Pour tout caractère absolument irréductible φ du groupe G, désignons par $d_\varphi = \varphi(1)$ le degré de la représentation linéaire ρ associée, et notons $r_\varphi = (\varphi(1) + \varphi(c))/2$ la multiplicité de la valeur propre $+1$ dans la matrice $\rho(c)$ représentant une conjugaison complexe $c \in G$ du corps K. On a alors le

THÉORÈME 2 (Cor.2 du th.1 de [21]) : *Supposons que pour tout caractère absolument irréductible φ du groupe G, on ait l'inégalité*

$$r_\varphi(r_\varphi - 1) < d_\varphi \ .$$

Alors le corps K vérifie la conjecture de Leopoldt pour tout nombre premier p.

On dispose ainsi de conditions suffisantes qui sont très faciles à tester dès lors que l'on connait la table des caractères du groupe G. Les inégalités ci-dessus sont notamment vérifiées lorsque le groupe G est abélien, auquel cas on retrouve le théorème de BRUMER sur les corps abéliens [5], ainsi que pour certains groupes résolubles G, comme le groupe symétrique $\mathfrak{S}_4$, ou bien le groupe $GL_2(\mathbf{F}_3) = \widetilde{\mathfrak{S}}_4$, avec des valeurs convenablement choisies de la conjugaison complexe c. On trouvera d'autres exemples dans [21].

3.1. Indépendance algébrique de valeurs de la fonction exponentielle

Soient $x_1, \ldots, x_n$ des nombres complexes $\mathbf{Q}$-linéairement indépendants, et soient $y_1, \ldots, y_n$ des nombres complexes qui sont eux aussi $\mathbf{Q}$-linéairement indépendants. On désigne par t_1, t_2, t_3 les degrés de transcendance sur $\mathbf{Q}$ des corps

$$\mathbf{Q}\ (e^{x_i y_j}; 1 \le i \le m, 1 \le j \le n)\ ,$$
$$\mathbf{Q}\ (x_i, e^{x_i y_j}; 1 \le i \le m, 1 \le j \le n)\ ,$$
$$\mathbf{Q}\ (x_i, y_j, e^{x_i y_j}; 1 \le i \le m, 1 \le j \le n)\ .$$

Plusieurs résultats classiques de transcendance se ramènent à des minorations des t_k, $1 \le k \le 3$. On vérifiera par exemple dans le §.6 que le théorème des six exponentielles équivaut à la minoration $t_1 \ge 1$ lorsque $m = 2$, $n = 3$, et que le théorème bien connu de GEL'FOND-SCHNEIDER sur la transcendance de a^b équivaut quant à lui à $t_2 \ge 1$, pour $m = 2$, $n = 1$. Un grand nombre de travaux (voir la bibliographie de [33]) ont donc été consacrés à ce problème, et le résultat suivant, extrait de [9], peut être considéré comme optimal au vu des méthodes utilisées. On notera aussi que l'on peut étendre cet énoncé au cas de vecteurs x_i et y_j de $\mathbf{C}^r$, $r \ge 1$, voir le §.12 de [35].

THÉORÈME 3 : *Sous réserve que les mesures ci-dessous d'indépendance linéaire sur* $\mathbb{Q}$ *des* x_i *et des* y_j *soient satisfaites, on a les minorations suivantes :*

i) si $m \geq 2, n \geq 3$, ou si $m \geq 3, n \geq 2$, $t_1 \geq [mn/(m+n)]$,

ii) si $m \geq 2$, $t_2 \geq [(mn+m)/(m+n)]$,

iii) $t_3 \geq mn/(m+n)$.

Les mesures d'indépendance linéaire en question sont les suivantes. Dans chacun des cas $k = 1, 2, 3$, on suppose que les x_i et les y_j vérifient des inégalités de la forme :

$$\log|\sum_{i=1}^{m} \lambda_i x_i| \gg -\max|\lambda_i| ,$$

$$\log|\sum_{j=1}^{n} \mu_j y_j| \gg -(\max|\mu_j|)^{\eta_k} ,$$

pour tout multi-entier $(\lambda_1, \ldots, \lambda_m)$ et $(\mu_1, \ldots, \mu_n)$ non nul, avec

$$\eta_1 = \frac{mn}{2m+n} \quad , \quad \eta_2 = \frac{mn+m}{2m+n} \quad , \quad \eta_3 = \frac{mn+m+n-1}{2m+n} .$$

Quelques remarques.

1) La conjecture des quatre exponentielles équivaut à l'assertion $t_1 \geq 1$, lorsque $m = n = 2$. Autrement dit, la minoration i) devrait encore être valable pour $m = n = 2$.

2) Posons

$$N_1 = mn \quad , \quad N_2 = mn + m \quad , \quad N_3 = mn + m + n \quad ,$$

de telle sorte que $N_k, 1 \leq k \leq 3$, désigne le nombre de générateurs des trois corps introduits ci-dessus. Les minorations i)-iii) du théorème 3 peuvent alors s'écrire de manière unique sous la forme

$$t_k \geq [N_k/(m+n)] \ , \ 1 \leq k \leq 3 \ ,$$

sauf lorsque $k = 3$ et que $m + n$ divise mn ; auquel cas, on obtient $t_3 \geq [N_3/(m+n)] - 1$. On peut évidemment conjecturer que cette exception n'a pas lieu d'être. Par exemple, l'inégalité $t_3 \geq 2$ pour $m = n = 2$ impliquerait entre autre chose l'indépendance algébrique des nombres π et e^{π}.

3) On peut probablement s'affranchir de toute hypothèse de mesure d'indépendance linéaire dans l'énoncé du théorème 3. Il en est notamment ainsi en degré de transcendance 0 ou 1 (i.e. $t_k \geq 1$ ou 2).

Pour apprécier la qualité du théorème 3, indiquons simplement le

COROLLAIRE : *Soit α un nombre algébrique non nul, et soit $\log \alpha$ une détermination non nulle du logarithme de α. Soit β un nombre algébrique de degré $d \geq 2$. Il existe alors au moins $[(d+1)/2]$ nombres algébriquement indépendants parmi les $d-1$ nombres $\alpha^{\beta^j} = e^{\beta^j \log \alpha}$, $1 \leq j \leq d-1$.*

On notera que l'indépendance algébrique des $d-1$ nombres ci-dessus (problème posé par GEL'FOND en 1949 et par SCHNEIDER en 1955) découle aisément de la conjecture de SCHANUEL.

3.2. Outils d'indépendance algébrique

L'obtention de grands degrés de transcendance a nécessité l'élaboration de techniques sophistiquées, issues principalement de l'algèbre commutative. On peut schématiquement classer ces outils en deux groupes : ceux qui s'appuient sur le théorème des zéros de Hilbert, et ceux qui sont des généralisations d'un critère d'indépendance algébrique dû à GEL'FOND. Les deux familles de résultats devraient pouvoir s'utiliser de manière équivalente, ce qui n'est pas encore tout à fait le cas. A la suite de travaux de W.D. BROWNAWELL sur le Nullstellensatz effectif (cf. [3] pour un historique du sujet), J. KOLLAR vient d'obtenir le résultat optimal suivant :

THÉORÈME 4 (th.1.5 de [13]) : *Soient $P_1, \ldots, P_m$ des polynômes de $\mathbb{C}[X_1, \ldots, X_n]$, sans zéros communs dans $\mathbb{C}^n$, et de degré total $\leq D$, avec $D \geq 3$. Il existe alors des polynômes $A_1, \ldots, A_m$ de $\mathbb{C}[X_1, \ldots, X_n]$ tels que :*

$$\sum_{i=1}^{m} A_i P_i = 1 \ , \quad \deg(A_i) \leq D^{\min(m,n)} \ , \ 1 \leq i \leq m \ .$$

Les critères d'indépendance algébrique ont eux aussi suscité de nombreux travaux dont on trouvera une analyse détaillée dans [3] et [33]. A titre d'exemple, voici un énoncé qui est lui aussi essentiellement optimal, corollaire du théorème principal de [28].

THÉORÈME 5 : *Soient θ un point de $\mathbb{C}^n$ et η un nombre réel $> n+1$. Il n'existe aucune suite d'idéaux*

$$I_N \subseteq \mathbb{C}[X_1, \ldots, X_n] \ , \quad N \geq N_0 \ ,$$

ayant les propriétés suivantes :

i) *I_N est engendré par des polynômes P_{Nj} , $1 \leq j \leq J_N$, de degré total $\leq N$, à coefficients entiers rationnels de valeur absolue $\leq e^N$,*

ii) *la boule de centre θ et de rayon $e^{-N^{n+1}}$ ne contient qu'un nombre fini de zéros de I_N,*

iii) $\quad 0 < \max\limits_{1 \leq j \leq J_N} (|P_{Nj}(\theta)|) < e^{-N^n}$.

4. Lemmes de zéros

Les lemmes de zéros constituent un des principaux ingrédients des démonstrations actuelles de transcendance, cf. [1]. Dans le contexte des groupes algébriques commutatifs, on dispose d'un résultat presque optimal, dû à P. PHILIPPON [25], voir aussi [26], [27], [4]. Nous en proposons ici une formulation un peu différente, qui met bien en évidence l'analogie avec la conjecture de S. LANG du §.5.

La situation est la suivante. On se donne un groupe algébrique commutatif connexe G, écrit sous forme de produit et plongé termes à termes dans un produit d'espaces projectifs :

$$G = G_1 \times \cdots \times G_P \longrightarrow \mathbf{P} = \mathbf{P}^{N_1} \times \cdots \times \mathbf{P}^{N_P} .$$

Soit Γ un sous-groupe de type fini de $G(\mathbf{C})$, et soit $W \subseteq t_G$ un sous-espace vectoriel du $\mathbf{C}$-espace vectoriel tangent à l'origine du groupe algébrique G. On identifiera (par restriction à l'origine) t_G à l'espace des champs de vecteurs tangents à $G(\mathbf{C})$ et invariants par translation. Associées à ces données, introduisons les définitions et notations suivantes.

1) Soit $\{\gamma_1, \ldots, \gamma_\ell\}$ un système générateur du groupe Γ. Pour tout entier $S \geq 0$, on désignera par $\Gamma(S)$ l'ensemble des combinaisons linéaires $\sum\limits_{i=1}^{\ell} s_i \gamma_i$, $0 \leq s_i \leq S$.

2) Soit f une fonction rationnelle sur G, et soit T un entier ≥ 1. On notera par $(f)_{0,W,T}$ le lieu des points de G où f s'annule avec une multiplicité $\geq T$ le long de W, c'est à dire l'ensemble des points γ de $G(\mathbf{C})$ tels que

$$\frac{\partial^t f}{\partial w_1 \cdots \partial w_t} (\gamma) = 0 ,$$

pour tout $0 \leq t < T$, et tout élément $w_1, \ldots, w_t$ dans W. On notera que $(f)_{0,W,T}$ est localement fermé pour la topologie de Zariski sur G.

3) Soit f une fonction rationnelle sur G. On dira que f est de multidegré $\leq D = (D_1, \ldots, D_p)$, s'il existe un système de coordonnées multiprojectives $\mathbf{X} = (X_{10}, \ldots, X_{1N_1}; \ldots; X_{p0}, \ldots, X_{pN_p})$ dans $\mathbf{P}$ et un polynôme multihomogène $F \in \mathbf{C}[\mathbf{X}]$, de multidegré D, tel que f soit la restriction à G de la fonction rationnelle sur $\mathbf{P}$ égale à $(F(\mathbf{X})/X_{10}^{D_1} \cdots X_{p0}^{D_p})$.

En d'autres termes, f se déduit de F par déshomogénéisation relative à une base multiprojective de $\mathbf{P}$.

4) Soit V une sous-variété fermée de $\mathbf{P}$, et soit $D = (D_1, \ldots, D_p)$, un p-uplet d'entiers ≥ 0. On posera :
$H(V, D) = ((\dim V)!)$ { partie homogène de plus haut degré du *polynôme de Hilbert-Samuel* multihomogène de V, évaluée en D }.
Rappelons à ce propos que si I désigne l'idéal multihomogène de $\mathbf{C}[\mathbf{X}]$ associé à V, le polynôme de Hilbert-Samuel de V, évalué en D, mesure la dimension sur $\mathbf{C}$ de la partie multihomogène de degré D de l'anneau multigradué $\mathbf{C}[\mathbf{X}]/I$, tout au moins lorsque les entiers $D_1, \ldots, D_p$ sont suffisamment grands. On notera aussi que les coefficients de $H(V, D)$, vu comme un polynôme en les variables $D_1, \ldots, D_p$ s'expriment classiquement en termes des degrés partiels de V, et que la fonction H fournit ainsi une mesure des degrés de V.

THÉORÈME 6 (th.2.1 de [25]) : *Soit f une fonction rationnelle sur G, non identiquement nulle, de multidegré $\leq D$, soit n la dimension de G, et soient T et S deux entiers ≥ 0, tels que :*

$$\Gamma(nS) \subseteq (f)_{0,W,nT+1} \cdot$$

Il existe alors un sous-groupe algébrique connexe G' de G, distinct de G et vérifiant les deux conditions suivantes :

i) $$\bigcup_{\gamma \in \Gamma(S) \bmod G'} (\gamma + G') \subseteq (f)_{0,W,T+1} \quad ,$$

ii) $$\binom{T+\alpha}{\alpha} \operatorname{card}\left(\frac{\Gamma(S)+G'}{G'}\right) H(\overline{G}', D) \leq cH(\overline{G}, D),$$

où la barre désigne l'adhérence de Zariski dans $\mathbf{P}$, c désigne une constante ne dépendant que du plongement $G \to \mathbf{P}$, et où

$$\alpha = \dim W - \dim(W \cap t_{G'}) = \dim((W + t_{G'})/t_{G'}).$$

On notera que l'inégalité ii) ci-dessus est optimale à la valeur de la constante c près : il existe en effet une constante c_1, $0 < c_1 < 1$, ne dépendant elle aussi

que du plongement $G \to \mathbf{P}$, telle que pour tout sous-groupe algébrique G' de G, connexe et distinct de G, pour tout p-uplet D d'entiers positifs suffisamment grands, et pour tout $T \geq 0$, $S \geq 0$, vérifiant l'inégalité

$$\binom{T+\alpha}{\alpha} \operatorname{card}\left(\frac{\Gamma(S)+G'}{G'}\right) H(\overline{G}', D) \leq c_1 H(\overline{G}, D) ,$$

on peut construire une fonction rationnelle non nulle $f \in \mathbb{C}(G)$, de multidegré $\leq D$, et telle que l'inclusion i) ci-dessus soit satisfaite.

Dans le cas particulier d'un groupe G linéaire, la constante c peut être choisie égale à 1, tout au moins si l'on se restreint aux plongements usuels dans $\mathbb{P}^1$ des facteurs additifs et multiplicatifs. Il serait alors intéressant (et probablement très utile) de remplacer dans l'inégalité ii) les termes $H(\overline{G}, D)$ et $H(\overline{G}', D)$ par $\dfrac{H(\overline{G}, D)}{(\dim \overline{G})!}$ et $\dfrac{H(\overline{G}', D)}{(\dim \overline{G}')!}$ respectivement (en autorisant éventuellement un terme reste additif dans le membre de droite), avec pour hypothèse initiale l'inclusion moins restrictive $\Gamma(S) \subseteq (f)_{0,W,T+1}$. Un tel résultat serait optimal, au terme reste près, et ne semble pas connu même dans les cas les plus simples.

On notera que le polynôme $H(V, D)/(\dim V)!$ fournit le terme principal de la *fonction de Hilbert-Samuel* de la variété projective V, et mesure donc le nombre de variables linéairement indépendantes disponibles, paramètre fondamental dans toute démonstration de transcendance. La remarque ci-dessus, concernant l'optimalité du théorème 6 à une constante multiplicative près, se déduit d'ailleurs aisément d'une comparaison entre la fonction de Hilbert-Samuel de V et le polynôme $H(V, D)$, cf.[6].

5. Géométrie diophantienne

Ce thème a fait l'objet de nombreux travaux récents, issus plus ou moins directement de la théorie des nombres transcendants. On peut citer notamment des questions de minoration de hauteur [8], [11], ou bien de formes linéaires de logarithmes dans les groupes algébriques [29], [30], [12] ainsi qu'une approche diophantienne du théorème de FALTINGS sur les conjectures de MORDELL-SHAFAREVITCH-TATE. [7] , [17], [23].

Nous nous proposons ici de faire le point sur une conjecture de S. LANG, qui peut être abordée par des techniques très diverses.

CONJECTURE (p.221 de [14]) : *Soit G un groupe algébrique commutatif, ne contenant aucun sous-groupe $\simeq \mathbf{G}_a$. Soit V une sous-variété algébrique de G, et soit Γ un sous-groupe de rang fini (ie. contenu dans l'ensemble des points*

de division d'un groupe de type fini) de $G(\mathbf{C})$. *Alors* $V \cap \Gamma$ *est réunion finie de sous-ensembles de la forme* $\gamma + (G' \cap \Gamma)$, *où* G' *désigne un sous-groupe algébrique de* G, *et* γ *un élément de* $V \cap \Gamma$, *tels que*

$$\gamma + G' \subseteq V.$$

Un tel groupe algébrique G est extension d'une variété abélienne A par un groupe de type multiplicatif T; autrement dit on a une suite exacte $0 \to T \to G \to A \to 0$.

Lorsque $G = T$, la conjecture a été établie dans [19], en s'appuyant essentiellement sur le théorème du sous-espace de W. SCHMIDT. On obtient ainsi d'intéressantes applications concernant les équations diophantiennes exponentielles [15] , [16]. Le cas général reste encore largement ouvert. On dispose cependant de résultats très complets dans le cas particulier où Γ est égal au groupe G_{tors} des points de torsion de G, auquel cas on peut d'ailleurs étendre la conjecture à un groupe commutatif quelconque (contenant éventuellement des sous-groupes additifs). M. RAYNAUD avait considéré le cas d'une variété abélienne (conjecture dite de Manin-Mumford) et l'avait résolue grâce à des arguments de géométrie algébrique [31]. En adaptant, entre autres choses les idées introduites dans la preuve des lemmes de zéros, M. HINDRY a pu établir le cas général et apporter de plus des informations précises sur les origines γ et les directions G' intervenant dans la conjecture ci-dessus.

Voici l'énoncé précis qu'il obtient pour un produit

$$G = \mathbf{G}_m^n \times A \longrightarrow \mathbf{P} = (\mathbf{P}^1)^n \times \mathbf{P}^N,$$

où l'on a fixé un plongement projectif de A, et où le groupe multiplicatif $\mathbf{G}_m = \mathbf{P}^1 \setminus \{0, \infty\}$ est naturellement plongé dans $\mathbf{P}^1$. La fonction H ci-dessous est alors relative à ce plongement (cf.§4). Introduisons tout d'abord quelques notations. Soit

$$m = \dim V \quad , \quad h = \left[\sum_{i=1}^{m} \frac{(2m)^i}{i!} \right].$$

On supposera que la variété abélienne A et le plongement $A \to \mathbf{P}^N$ sont définis sur un corps de nombres k. On désigne alors par q un nombre réel > 0, tel que pour tout point $P \in A_{\text{tors}}$, d'ordre exactement n dans A_{tors}, le degré d'un corps de rationalité $k(P)$ du point P soit $\gg n^{1/q}$. En fait, d'après un résultat de J-P.SERRE, tout réel > 1 convient. On a alors le

THÉORÈME 7 (th.1 de [10]) : *Supposons que la variété* V *soit définie sur* k, *et que l'adhérence de Zariski de* V *dans* $\mathbf{P}$ *soit définie par des polynômes*

de multidegré $\leq D = (D_1, \ldots, D_{n+1})$. *On peut alors choisir les couples* (γ, G') *intervenant dans la conjecture ci-dessus tels que :*

$$\begin{aligned} \text{ordre}(\gamma) &\leq c\, H(\overline{V}, D)^{q(hm+1)}, \\ H(\overline{G}', D) &\leq H(\overline{V}, 2D)^{hm}, \end{aligned}$$

où c *désigne une constante ne dépendant que de* A, k *et* q.

En ce qui concerne la constante q ci-dessus, on peut aussi utiliser des arguments diophantiens, qui ont le mérite d'être entièrement effectifs. On trouvera dans [2] un exposé des problèmes galoisiens qui peuvent être abordés par des arguments de transcendance. Voici un résultat dû à D. MASSER, qui montre en particulier que tout réel $q > \dim A$ convient.

THÉORÈME 8 (th.4 de [2]) : *Il existe une constante* c', *effectivement calculable en termes du degré* $[k : \mathbb{Q}]$ *et de la hauteur des équations de* A *dans* $\mathbb{P}^N$, *telle que pour tout point* $P \in A_{\text{tors}}$, *d'ordre exactement* n, *on ait :*

$$[k(P) : k] \geq c' n^{1/\dim A} / \log n.$$

6.1. Principe de la nouvelle preuve du théorème des six exponentielles

La plupart des démonstrations de transcendance commencent par la construction d'une fonction auxiliaire. Pour ce faire, on utilise souvent le lemme de Siegel qui permet de trouver une "petite" solution à un système d'équations linéaires. Nous allons procéder de manière différente. Au lieu de chercher une solution du système, nous considèrerons les déterminants des mineurs extraits de la matrice correspondante. Il s'agit là de *déterminants d'interpolation* que l'on peut majorer de manière tout à fait générale (§3 de [18]). De façon alternative, nous utiliserons ici un développement en série de Taylor de ces déterminants, ce qui nous amènera à étudier les *polynômes de Schur.*

Nous nous restreindrons à la version archimédienne du théorème des six exponentielles, le cas p-adique menant à des calculs similaires. Rappelons tout d'abord l'énoncé du théorème et fixons quelques notations légèrement différentes de celles du §2.

On se donne six nombres algébriques $a_1, a_2, a_3, b_1, b_2, b_3$ et on considère la matrice

$$A = \begin{pmatrix} \log a_1 & , & \log a_2 & , & \log a_3 \\ \log b_1 & , & \log b_2 & , & \log b_3 \end{pmatrix}.$$

Il s'agit de montrer que le rang de A est égal à deux lorsque les deux lignes et les trois colonnes de A sont linéairement indépendantes sur $\mathbb{Q}$. Raisonnons par l'absurde et supposons que

$$\frac{\log b_1}{\log a_1} = \frac{\log b_2}{\log a_2} = \frac{\log b_3}{\log a_3} = \theta.$$

De manière équivalente, nous disposons de deux sous-groupes

$$\begin{aligned} X &= \mathbf{Z} \oplus \mathbf{Z}\theta \ , \\ Y &= \mathbf{Z} \log a_1 \oplus \mathbf{Z} \log a_2 \oplus \mathbf{Z} \log a_3 \ , \end{aligned}$$

tels que

$$e^{XY} \subseteq \overline{\mathbb{Q}}^* .$$

On remarquera incidemment que cette formulation des hypothèses nous ramène à la situation envisagée dans le théorème 3-i) avec $m = 2$, $n = 3$.

Pour tout entier $L \geq 0$, $M \geq 0$, notons :

$$\begin{aligned} X(L) &= \{\lambda_1 + \lambda_2\theta \ ; \ 0 \leq \lambda_1, \lambda_2 \leq L\} \ , \\ Y(M) &= \{\mu_1 \log a_1 + \mu_2 \log a_2 + \mu_3 \log a_3 \ ; \ 0 \leq \mu_1, \mu_2, \mu_3 \leq M\} \ , \end{aligned}$$

et ordonnons les ensembles $X(L)$ et $Y(M)$ de manière arbitraire.

On introduit alors la matrice

$$A_{LM} = \left[\begin{array}{ccc} & \vdots & \\ \ldots & e^{xy} & \ldots \\ & \vdots & \end{array} \right]_{\substack{x \in X(L) \\ y \in Y(M)}}$$

où x désigne l'indice de ligne et y l'indice de colonne. La matrice A_{LM} comporte donc $(L+1)^2$ lignes et $(M+1)^3$ colonnes.

Le principe de la démonstration est le suivant : nous allons successivement majorer et minorer le rang de la matrice A_{LM} , et pour des valeurs convenablement choisies des paramètres L et M, nous obtiendrons des estimations incompatibles. De manière imagée, on peut dire que la petitesse du rang de A (par hypothèse égal à 1) se prolonge analytiquement aux matrices A_{LM}, tandis qu'un argument de nature algébrique (le lemme de zéros) permet de minorer le rang de A_{LM}.

6.2. Quelques calculs de déterminants

Commençons par indiquer quelques propriétés élémentaires des *polynômes de Schur*, voir par exemple le §I-3 de [22].

Soit n un entier ≥ 1, et soient $X_1, \ldots, X_n$ des indéterminées. Désignons par

$$V(X_1, \ldots, X_n) = \prod_{1 \leq i < j \leq n} (X_j - X_i)$$

le discriminant des n variables X_i . Soit

$$\mathbf{k} = (k_1, \ldots, k_n)$$

un n-uplet d'entiers ≥ 0. Le polynôme

$$\det\left(X_i^{k_j+j-1}\right)_{1 \leq i,j \leq n}$$

où i désigne l'indice de ligne et j l'indice de colonne, est antisymétrique, et est donc divisible par $V(X_1, \ldots, X_n)$. Le quotient

$$S_{\mathbf{k}}(X_1, \ldots, X_n) = \det\left(X_i^{k_j+j-1}\right) / V(X_1, \ldots, X_n)$$

s'appelle le polynôme de Schur d'indice $\mathbf{k}$. Ces polynômes de Schur sont clairement des fonctions symétriques des variables $X_1, \ldots, X_n$ et peuvent ainsi s'exprimer en termes de fonctions symétriques élémentaires. Voici un exemple d'une telle écriture, via les polynômes symétriques P_ℓ du lemme suivant :

LEMME 1 : *Pour tout n-uplet $\mathbf{k} = (k_1, \ldots, k_n)$ d'entiers ≥ 0 ,on a les formules :*

$$\begin{aligned} S_{\mathbf{k}}(X_1, \ldots, X_n) &= \det(P_{k_i+i-j})_{1 \leq i,j \leq n} \\ &= \det(Q_{ij})_{1 \leq i,j \leq n}, \end{aligned}$$

où les polynômes P_ℓ ($\ell \in \mathbb{Z}$) et Q_{ij} ($1 \leq i, j \leq n$) sont définis par

$$P_\ell = \sum_{\substack{\lambda_1 \geq 0, \ldots, \lambda_n \geq 0 \\ \lambda_1 + \cdots + \lambda_n = \ell}} X_1^{\lambda_1} \ldots X_n^{\lambda_n} \ , \ Q_{ij} = \sum_{\substack{\lambda_1 \geq 0, \ldots, \lambda_j \geq 0 \\ \lambda_1 + \cdots + \lambda_j = k_i + i - j}} X_1^{\lambda_1} \ldots X_j^{\lambda_j}.$$

(par convention, $P_\ell = 0, Q_{ij} = 0$, lorsque $\ell < 0$ ou $k_i < j - i$)

Preuve : L'égalité $S_{\mathbf{k}} = \det(P_{k_i+i-j})$ correspond à la formule 3.4 p.25 de [22]. Pour la deuxième égalité, remarquons que le polynôme Q_{ij} est égal à la

partie du polynôme P_{k_i+i-j} indépendante des variables $X_{j+1}, \ldots, X_n$. On vérifie aisément l'identité :

$$Q_{ij} = P_{k_i+i-j} - (\sum_{j<\alpha\leq n} X_\alpha)P_{k_i+i-j-1} + (\sum_{j<\alpha<\beta\leq n} X_\alpha X_\beta)P_{k_i+i-j-2} - \cdots$$

d'où s'ensuit l'égalité

$$\det(P_{k_i+i-j}) \;=\; \det(Q_{ij})$$

par combinaisons linéaires de colonnes.

Comme alternative, on peut aussi établir directement l'égalité $S_{\mathbf{k}} = \det(Q_{ij})$ par des manipulations de lignes dans la matrice $(X_i^{k_j+j-1})$ ayant pour but de faire apparaître les facteurs $(X_i - X_j)$ du discriminant exactement comme pour la formule du déterminant de Vandermonde qui correspond d'ailleurs au cas particulier $\mathbf{k} = 0$.

La *longueur* $L(P)$ d'un polynôme P à coefficients complexes désigne la somme des valeurs absolues des coefficients de P. Notons enfin $|\mathbf{k}| = k_1 + \cdots + k_n$ la *longueur* du n-uplet d'entiers naturels $\mathbf{k} = (k_1, \ldots, k_n)$. Lorsque $k_i \geq j - i$, le polynôme Q_{ij} est homogène de degré total $k_i + i - j$ et l'on a

$$L(Q_{ij}) = \binom{k_i + i - 1}{j - 1} \leq 2^{k_i+i-1}.$$

On déduit alors aisément du lemme 1 le

COROLLAIRE : *Pour tout n-uplet $\mathbf{k}$ d'entiers ≥ 0, le polynôme $S_{\mathbf{k}}$ est homogène de degré total $|\mathbf{k}|$ et de longueur $\leq (n!)2^{|\mathbf{k}|+(n^2-n)/2}$.*

Désignons par

$$\mathbf{x} = (x_1, \ldots, x_n)\ ,\ \mathbf{y} = (y_1, \ldots, y_n)$$

deux suites de n nombres complexes. On s'intéresse maintenant au déterminant

$$\Delta = \det(e^{x_i y_j})_{1\leq i,j\leq n}\ .$$

LEMME 2 : *On a les formules*

$$\begin{aligned}\Delta &= \sum_{0\leq k_1<\cdots<k_n} \frac{\det(x_i^{k_j})\det(y_j^{k_i})}{k_1!\cdots k_n!} \\ &= V(\mathbf{x})V(\mathbf{y}) \sum_{0\leq k_1\leq\cdots\leq k_n} \frac{S_{\mathbf{k}}(\mathbf{x})S_{\mathbf{k}}(\mathbf{y})}{\prod_{1\leq i\leq n}(k_i + i - 1)!}\end{aligned}$$

Preuve : On commence par développer chacun des coefficients $e^{x_i y_j}$ en série :

$$e^{x_i y_j} = \sum_{k \geq 0} \frac{x_i^k y_j^k}{k!} \ , \ 1 \leq i, j \leq n.$$

Fixant l'indice i, la formule ci-dessus peut être vue comme un développement de la i-ième ligne de la matrice $(e^{x_i y_j})_{1 \leq i,j \leq n}$ en une somme infinie de lignes. Par multilinéarité du déterminant, on obtient :

$$\Delta = \sum_{k_1 \geq 0, \ldots, k_n \geq 0} (\prod_{i=1}^{n} x_i^{k_i}/k_i!) \det(y_j^{k_i}).$$

Dans la sommation ci-dessus, il est clair que l'on peut se restreindre aux n-uplets $(k_1, \ldots, k_n)$ d'entiers deux à deux distincts. Désignons par $\mathfrak{S}_n$ le groupe symétrique à n éléments, et par $\varepsilon(\sigma)$ la *signature* de $\sigma \in \mathfrak{S}_n$. Ordonnons alors les n-uplets considérés par ordre croissant, il vient

$$\Delta = \sum_{\substack{0 \leq k_1 < \cdots < k_n \\ \sigma \in \mathfrak{S}_n}} \left(\prod_{i=1}^{n} x_i^{k_{\sigma(i)}}/k_{\sigma(i)}! \right) \det(y_j^{k_{\sigma(i)}})$$

$$= \sum_{0 \leq k_1 < \cdots < k_n} \left(\sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} (x_i^{k_{\sigma(i)}}/k_{\sigma(i)}!) \right) \det(y_j^{k_i})$$

$$= \sum_{0 \leq k_1 < \cdots < k_n} \frac{\det(x_i^{k_j}) \det(y_j^{k_i})}{k_1! \cdots k_n!} \ ,$$

d'où la première égalité. La deuxième s'en déduit immédiatement en remplaçant k_i par $k_i + i - 1$, $1 \leq i \leq n$.

6.3. Majoration du rang de A_{LM}

Comme de coutume en transcendance, on désignera dans ce qui suit par $c_1, c_2, \cdots$ des constantes > 0, indépendantes des paramètres L et M. On se propose d'établir dans ce paragraphe la

PROPOSITION 1 : *Supposons que le rang de A soit égal à 1. Alors*

$$rg(A_{LM}) \leq c_1 LM.$$

Il s'agit de montrer que pour tout entier n suffisamment grand devant LM, et pour toute suite extraite à n éléments :

$$\mathbf{x} = \{x_1, \ldots, x_n\} \subseteq X(L) \ , \ \mathbf{y} = \{y_1, \ldots, y_n\} \subseteq Y(M),$$

le déterminant

$$\Delta = \det(e^{x_i y_j})_{1 \le i,j \le n}$$

est nul. Pour cela, nous allons successivement majorer et minorer (quand $\Delta \neq 0$) la valeur absolue de Δ. Nous obtiendrons ainsi deux inégalités incompatibles lorsque $n > c_1 LM$.

LEMME 3 : *Il existe deux constantes c_2 et c_3 telles que pour toutes sous-suites $\mathbf{x} \subseteq X(L)$, $\mathbf{y} \subseteq Y(M)$ à $n > c_2 LM$ termes, on ait la majoration :*

$$|\Delta| \le e^{-c_3 n^2}.$$

Preuve : On utilise le développement de Δ fourni par le lemme 2 :

$$\Delta = V(\mathbf{x})V(\mathbf{y}) \sum_{0 \le k_1 \le \cdots \le k_n} \frac{S_{\mathbf{k}}(\mathbf{x}) S_{\mathbf{k}}(\mathbf{y})}{\prod\limits_{1 \le i \le n} (k_i + i - 1)!}$$

Remarquons tout d'abord que

$$(k_i + i - 1)! \ge k_i!(i-1)! \ , \ 1 \le i \le n.$$

Il s'ensuit que

$$|\Delta| \le \frac{|V(\mathbf{x})| \ |V(\mathbf{y})|}{\prod\limits_{1 \le \nu \le n-1} \nu!} \sum_{0 \le k_1 \le \cdots \le k_n} \frac{|S_{\mathbf{k}}(\mathbf{x})| \ |S_{\mathbf{k}}(\mathbf{y})|}{\prod\limits_{1 \le i \le n} k_i!}.$$

Posons

$$\alpha = \max(1, |x_1|, \ldots, |x_n|) \ , \ \beta = \max(1, |y_1|, \ldots, |y_n|).$$

Le corollaire du lemme 1, joint à la majoration triviale

$$|x_i - x_j| \le 2\alpha \quad , \quad |y_i - y_j| \le 2\beta$$

des facteurs des discriminants $V(\mathbf{x})$ et $V(\mathbf{y})$, implique alors l'inégalité

$$|\Delta| \le \frac{(n!)^2 (16\alpha\beta)^{(n^2-n)/2}}{\prod\limits_{1 \le \nu \le n-1} \nu!} \sum_{0 \le k_1 \le \cdots \le k_n} \frac{(4\alpha\beta)^{k_1 + \cdots + k_n}}{\prod\limits_{1 \le i \le n} k_i!}$$

$$\le \frac{(n!)^2 (16\alpha\beta)^{(n^2-n)/2} e^{4\alpha\beta n}}{\prod\limits_{1 \le \nu \le n-1} \nu!} .$$

Utilisant maintenant la minoration $\nu! \geq \nu^\nu e^{-\nu}$, valable pour tout $\nu \geq 1$, ainsi que la formule sommatoire d'Euler Mac-Laurin, il vient :

$$\log(\prod_{\nu=1}^{n-1} \nu!) \geq (\frac{n^2-n}{2}) \log n - \frac{3}{4}n^2 - 0(n) ,$$

d'où il s'ensuit que :

$$|\Delta| \leq \left(\frac{16\alpha\beta}{n}\right)^{(n^2-n)/2} e^{4\alpha\beta n + \frac{3}{4}n^2 + 0(n \log n)}.$$

Il suffit alors de remarquer que

$$\alpha \leq c_4 L \ , \ \beta \leq c_5 M.$$

LEMME 4 : *Il existe une constante c_6 telle que pour tout entier n et toutes sous-suites $\mathbf{x} \subseteq X(L)$, $\mathbf{y} \subseteq Y(M)$ à n éléments, on ait :*
ou bien $\Delta = 0$
ou bien $|\Delta| \geq e^{-c_6(LM+\log n)n}$.

Preuve : Δ est le déterminant d'une matrice carrée $n \times n$, dont les coefficients sont des nombres algébriques de la forme :

$$e^{xy} = (a_1^{\mu_1} a_2^{\mu_2} a_3^{\mu_3})^{\lambda_1} (b_1^{\mu_1} b_2^{\mu_2} b_3^{\mu_3})^{\lambda_2},$$

si $x = \lambda_1 + \lambda_2\theta$ et $y = \mu_1 \log a_1 + \mu_2 \log a_2 + \mu_3 \log a_3$.

D'après l'expression ci-dessus, il est clair que

$$\max_{1 \leq i,j \leq n} (s(e^{x_i y_j})) \leq e^{c_7 LM},$$

où l'on a noté, de façon standard, $s(\alpha)$ la *taille* d'un nombre algébrique α (voir par exemple le chapitre 1 de [36]). Il s'ensuit que

$$s(\Delta) \leq (n!) e^{c_7 LMn}.$$

Il suffit d'utiliser alors la classique *inégalité de Liouville.*

La proposition 1 se déduit alors immédiatement de la comparaison des lemmes 3 et 4. Soit n un entier ≥ 1, pour lequel il existe un déterminant extrait Δ d'ordre n et non nul. On a alors :

$$c_3 n^2 \leq c_6(LM + \log n)n,$$

d'où il s'ensuit que $n \leq c_1 LM$.

6.4. Minoration du rang de A_{LM}

Nous allons montrer que la matrice A_{LM} est de rang maximal, sauf peut-être lorsqu'elle est de forme à peu près carrée. De façon précise, on a la

PROPOSITION 2 : *Soient L et M deux entiers ≥ 0. On suppose que*

i) *ou bien* $M^3 \geq 16L^2$,

ii) *ou bien* $L^2 \geq 54M^3$,

alors

$$rg(A_{LM}) = \inf((L+1)^2 \ , \ (M+1)^3).$$

Pour minorer de manière générale le rang de la matrice A_{LM}, il suffit d'en extraire une sous-matrice du type $A_{L_1 M}$ ou A_{LM_1} vérifiant les hypothèses i) ou ii) ci-dessus. On obtient aisément le

COROLLAIRE : *Pour tout entier $L \geq 0$, $M \geq 0$, on a*

$$rg(A_{LM}) \geq \frac{1}{54} \inf(L^2, M^3).$$

Nous allons déduire la proposition 2 du lemme de zéros énoncé dans le §4. En fait, on peut remplacer essentiellement les constantes 16 et 54 par 2 et 16 respectivement ; voir pour cela les raffinements introduits dans le lemme de zéros de [24].

Preuve de la Proposition 2 : Nous allons démontrer en premier lieu que les vecteurs lignes de la matrice A_{LM} sont linéairement indépendants lorsque l'inégalité i) est satisfaite.

On raisonne par l'absurde. Soit

$$\sum_{\lambda_1=0}^{L} \sum_{\lambda_2=0}^{L} p_{\lambda_1 \lambda_2} (a_1^{\mu_1} a_2^{\mu_2} a_3^{\mu_3})^{\lambda_1} (b_1^{\mu_1} b_2^{\mu_2} b_3^{\mu_3})^{\lambda_2} \ = \ 0 \ , \ 0 \leq \mu_1, \mu_2, \mu_3 \leq M,$$

une relation non triviale entre les lignes de A_{LM}. Introduisons le polynôme non nul :

$$f(X,Y) \ = \ \sum_{\lambda_1=0}^{L} \sum_{\lambda_2=0}^{L} p_{\lambda_1 \lambda_2} X^{\lambda_1} Y^{\lambda_2},$$

vu comme une fonction sur le groupe algébrique

$$\mathbb{G}_m \times \mathbb{G}_m \longrightarrow \mathbb{P} = \mathbb{P}^1 \times \mathbb{P}^1.$$

Par construction, la fonction f s'annule en tous les points de

$$\Gamma(M) = \left\{ \begin{pmatrix} a_1^{\mu_1} a_2^{\mu_2} a_3^{\mu_3} \\ b_1^{\mu_1} b_2^{\mu_2} b_3^{\mu_3} \end{pmatrix} \ ; \ 0 \leq \mu_1, \mu_2, \mu_3 \leq M \right\}.$$

On applique alors le théorème 6 avec $S = [M/2]$. La constante c est ici égale à 1. Il existe donc un sous-groupe algébrique connexe $G' \not\subseteq \mathbb{G}_m^2$ tel que l'on ait l'inégalité :

$$\operatorname{card}\left(\frac{\Gamma(S) + G'}{G'}\right) H(\overline{G}'; L, L) \leq H(\mathbb{P}; L, L).$$

Il suffit alors de remarquer que :

$$\operatorname{card}\left(\frac{\Gamma(S) + G'}{G'}\right) = (S+1)^3 \ , \ H(\overline{G}'; L, L) \geq 1 \ , \ H(\mathbb{P}; L, L) = 2L^2,$$

pour en déduire l'inégalité voulue : $M^3 < 16L^2$.

Dans le cas ii), on procède de manière analogue avec les colonnes de la matrice A_{LM}. Les détails sont laissés au lecteur.

6.5. Preuve du théorème des six exponentielles

Sous réserve que le rang de A soit égal à 1, nous avons obtenu l'encadrement suivant du rang de la matrice A_{LM} :

$$\frac{1}{54} \inf(L^2, M^3) \leq rg(A_{LM}) \leq c_1 LM \ , \ L \geq 0, M \geq 0.$$

Il suffit alors de choisir

$$L = T^3 \ , \ M = T^2 \ , \ T \in \mathbb{N},$$

pour obtenir une contradiction lorsque T est suffisamment grand.

REFERENCES

[1] D. BERTRAND, Lemmes de zéros et nombres transcendants, Séminaire Bourbaki, 38ième année, 1985-86, exposé 652 (= *Astérisque* **146-147** (1987), 21-44).

[2] D. BERTRAND, Galois representations and transcendental numbers, *New Advances in Transcendence Theory*, Cambridge University Press (1987), 37-55.

[3] D. BROWNAWELL, Applications of Cayley-Chow forms, *Number Theory Ulm* 1987, Springer Lecture Notes 1380, 1-18.

[4] W.D. BROWNAWELL, Note on a paper of P. Philippon, *Michigan Math. J.*, **14** (1987), 461-464.

[5] A. BRUMER, On the units of an algebraic number field, *Matematika*, **14** (1967), 121-144.

[6] M. CHARDIN, Une majoration de la fonction de Hilbert et ses conséquences pour l'interpolation algébrique, *Bull. Soc. Math. France*, **117** (1989), 305-318.

[7] D.V. et G.V. CHOODNOVSKY, Padé approximations and diophantine geometry, *Proc. Nat. Acad. Sc. USA*, **82**, 2212-2216.

[8] S. DAVID, *Minorations de hauteurs sur les variétés abéliennes,* à paraître.

[9] G. DIAZ, Grands degrés de transcendance pour des familles d'exponentielles. *J. Number Theory*, **31** (1989), 1-23.

[10] M. HINDRY, Autour d'une conjecture de S. Lang, *Invent. Math.*, **94** (1988), 573-603.

[11] M. HINDRY et J. SILVERMAN, The canonical height and integral points on elliptic curves, *Invent. Math.*, **93** (1988), 419-450.

[12] N. HIRATA-KOHNO, *Formes linéaires en logarithmes sur les groupes algébriques,* à paraître.

[13] J. KOLLAR, Sharp effective Nullstellensatz, *J. Am. Math. Soc.*, **1-4** (1988), 963-975.

[14] S. LANG, *Fundamental of diophantine geometry*, Springer-Verlag (1983).

[15] M. LAURENT, Equations exponentielles-polynômes et suites récurrentes linéaires, *Astérisque*, **147-148**, 121-139.

[16] M. LAURENT, Equations exponentielles-polynômes et suites récurrentes linéaires II, *J. Number Theory*, **31** (1989), 24-53.

[17] M. LAURENT, Une nouvelle démonstration du théorème d'isogénie d'après D.V. et G.V. Choodnovsky, *Séminaire de Théorie des Nombres Paris 1985-86*, Progress in Math., **71**, 119-131 , Birkhäuser.

[18] M. LAURENT, *Déterminants d'interpolation et théorème de Gel'fond-Schneider,* à paraître.

[19] M. LAURENT, Equations diophantiennes exponentielles, *Invent. Math.*, **78** (1984), 299-327.

[20] M. LAURENT, Rang p-adique d'unités : un point de vue torique, *Séminaire de Théorie des Nombres Paris 1987-88*, Progress in Math., **81**, 131-146, Birkhäuser.

[21] M. LAURENT, Rang p-adique d'unités et action de groupes, *J. Reine Angew. Math.*, **399** (1989), 81-108.

[22] I.G. MACDONALD, *Symmetric functions and Hall polynomials*, Oxford University Press (1977).

[23] D. MASSER et G. WÜSTHOLZ, Estimating isogenies on elliptic curves, *Invent. Math.,* à paraître.

[24] M. MIGNOTTE et M. WALDSCHMIDT, Linear forms in two logarithms and Schneider's method II, *Acta Arithmetica*, **LIII** (1989), 251-287.

[25] P. PHILIPPON, Lemmes de zéros dans les groupes algébriques commutatifs, *Bull. Soc. Math. France*, **114** (1986), 355-383.

[26] P. PHILIPPON, Lemmes de zéros en caractéristique quelconque, *Problèmes diophantiens 1986-87*, Pub. de l'Univ. P. et M. Curie, **84** (1988).

[27] P. PHILIPPON, Lemmes de zéros sur les extensions, *Problèmes diophantiens 1987-88*, Pub. de l'Univ. P. et M. Curie, 88 (1989).

[28] P. PHILIPPON, Critères pour l'indépendance algébrique, *Publications IHES*, **64** (1988), 5-52.

[29] P. PHILIPPON et M. WALDSCHMIDT, Formes linéaires de logarithmes simultanées sur les groupes algébriques, *Illinois J. Math.*, **32** (1988), 281-314.

[30] P. PHILIPPON et M.WALDSCHMIDT, Formes linéaires de logarithmes simultanées sur les groupes algébriques commutatifs. *Séminaire de Théorie des Nombres Paris 1986-87*, Progress in Math., **75**, 119-131, Birkhäuser.

[31] M. RAYNAUD, Sous-variétés d'une variété abélienne et points de torsion, *Arithmetic and Geometry*, Progress in Math., **35**, 327-352, Birkhäuser.

[32] M. WALDSCHMIDT, A lower bound for the p-adic rank of units of an algebraic number field, *Topics in classical Number Theory Budapest 1981, Coll. Math. Soc. János Bolyai*, **34**, 1617-1650.

[33] M. WALDSCHMIDT, Algebraic independence of transcendental numbers, Gel'fond's method and its developments, *Perspective in Math. Anniversary of Oberwolfach 1984*, 551-571, Birkhäuser.

[34] M. WALDSCHMIDT, Transcendence method of Gel'fond, *New Advances in Transcendence Theory*, Cambridge University Press, (1988), 375-398.

[35] M. WALDSCHMIDT, Groupes algébriques et grands degrés de transcendance, *Acta Arithmetica*, **156** (1986), 253-302.

[36] M. WALDSCHMIDT, *Nombres transcendants*, Lecture Notes 402 (1974), Springer Verlag.

Michel LAURENT
Institut Henri Poincaré
11, rue P. et M. Curie
75231 PARIS Cedex 05

Astérisque

R. MASSY

Sur les bases normales d'entiers relatives

Astérisque, tome 198-199-200 (1991), p. 231-236

<http://www.numdam.org/item?id=AST_1991__198-199-200__231_0>

SUR LES BASES NORMALES D'ENTIERS RELATIVES

par

R. MASSY

Soit N/E une extension galoisienne finie de corps quelconques, de groupe de Galois $\Delta = Gal(N/E)$. On sait par le théorème de la base normale ([**1**], AV70) que N est un module libre de rang 1 sur l'algèbre du groupe Δ sur E. Lorsque N et E sont des corps de nombres, d'anneaux d'entiers respectifs O_N et O_E, on peut se poser la question de savoir si O_N est un module libre, nécessairement de rang 1, sur l'algèbre $O_E[\Delta]$ du groupe Δ sur O_E ; autrement dit, existe-t-il un entier $\vartheta \in O_N$ tel que O_N soit un O_E-module libre de base $\{\delta(\vartheta)\}_{\delta\in\Delta}$? Lorsqu'elle existe, une telle base est dite "base normale d'entiers" (BNE en abrégé) de N sur E.

Dans le cas absolu $E = \mathbf{Q}$, la question est résolue depuis peu par la théorie de Fröhlich et son école [**6**], dont le point culminant est la preuve par Taylor [**15**] de la conjecture de Fröhlich liant la structure de $\mathbf{Z}[\Delta]$-module de O_N au signe de la constante de l'équation fonctionnelle de la fonction L d'Artin associée aux caractères symplectiques de Δ.

En revanche, il n'y a pas actuellement de théorie satisfaisante dans le cas relatif $E \neq \mathbf{Q}$. La première étude systématique de ce cas est due à Brinkhuis qui démontre dans sa thèse [**2**], ainsi que dans des articles postérieurs ([**3**],[**4**]), des résultats de non-existence de BNE. A contrario, nous énonçons ici plusieurs conditions nécessaires et suffisantes d'existence de BNE relatives, avec en outre, lorsqu'elles sont vérifiées, des formules explicites permettant de calculer un générateur ϑ. Ces formules assurent la suffisance de nos conditions d'existence ; elles sont obtenues via celles de [**11**]. Quant à la nécessité de nos conditions, elle procède de la méthode de [**2**] : on ajoute une condition de module au problème de plongement classique. Plus précisément, on se donne une extension galoisienne finie de corps de nombres E/K, de groupe de Galois $Gal(E/K) = \Gamma$, et un groupe abélien Δ considéré comme Γ-module. A une classe de cohomologie $\epsilon \in H^2(\Gamma, \Delta)$ donnée, on peut alors associer les problèmes $(E/K, \epsilon)$ et $[E/K, \epsilon]$ définis comme suit.

Problème $(E/K,\epsilon)$: Existe-t-il au dessus de E un corps N, galoisien sur K, de groupe de Galois sur E s'identifiant à Δ, qui induise une extension de groupes $1 \to \Delta \hookrightarrow Gal(N/K) \to \Gamma \to 1$ de classe ϵ ? Lorsqu'elle existe, l'extension N/K est appelée "solution du problème résoluble $(E/K,\epsilon)$".

Problème $[E/K,\epsilon]$: Le problème $(E/K,\epsilon)$ est-il résoluble, et dans l'affirmative admet-il, en outre, une solution N/K telle que l'on ait une BNE de N sur E ?

Le but de cet article est de résoudre explicitement les problèmes $[E/K,\epsilon]$ sans spécifier le corps de base K comme cela se fait d'habitude (cf.[**2**] chap.8, [**7**], [**14**], [**9**], [**10**]...), ceci, pour une classe ϵ décrivant une extension cyclique d'ordre 4 ou diédrale (resp. quaternionienne) d'ordre 8. Dans toute la suite, le noyau Δ est d'ordre 2 : $\Delta = \{1,\delta\}$, et le groupe $\Gamma = Gal(E/K)$ est d'ordre 2 ou le groupe de Klein. Nos conditions d'existence de BNE sont obtenues sans rien supposer sur le corps de nombres K. Pour les conditions suffisantes, on fait l'hypothèse simplificatrice que K est de nombre de classe $h(K) = 1$, de façon à obtenir une formule de construction d'un générateur ϑ de la base existante.

Le détail des démonstrations, qui sont assez techniques, est donné en [**12**].

1. Conditions nécessaires de résolubilité des problèmes $[E/K,\epsilon]$

Dans cette section, K est un corps de nombres quelconque.

- Si $E = K(\sqrt{a})/K, a \in K$, est une extension quadratique, on note ϵ_{-1} la classe non nulle de $H^2(\Gamma,\Delta)$. Dire que le problème $[E/K,\epsilon_{-1}]$ est résoluble signifie qu'au dessus de E, il existe un corps N, extension cyclique de degré 4 de K, et admettant une BNE sur E.
- Si $E = K(\sqrt{a},\sqrt{b})/K$, $a \in K$, $b \in K$, est une extension biquadratique, soient σ,τ les générateurs de Γ définis par les égalités

$$\sigma(\sqrt{a})/\sqrt{a} = \tau(\sqrt{b})/\sqrt{b} = -1,\ \sigma(\sqrt{b})/\sqrt{b} = \tau(\sqrt{a})/\sqrt{a} = 1.$$

On note ϵ_0 (resp. ϵ_1) la classe de cohomologie d'une extension $1 \to \Delta \hookrightarrow G \to \Gamma \to 1$ de groupe G diédral d'ordre 8, d'unique sous-groupe cyclique d'ordre 4 engendré par un relèvement dans G du produit $\sigma\tau$ (resp. de groupe G quaternionien d'ordre 8). Dire que le problème $[E/K,\epsilon_0]$ (resp. $[E/K,\epsilon_1]$) est résoluble signifie qu'au dessus de E, il existe un corps N, cyclique sur $K(\sqrt{ab})$, extension galoisienne de K de groupe $Gal(N/K)$ diédral (resp. quaternionien) d'ordre 8, et admettant une BNE sur E.

Remarque. Les classes $\epsilon_{-1}, \epsilon_0, \epsilon_1$ s'expriment au moyen de cup-produits définis par a et b. Dans les notations de [**11**], on a

$$\epsilon_{-1} = ((a))_E\ ,\ \epsilon_0 = (a,b)_E\ ,\ \epsilon_1 = ((ab))_E + (a,b)_E.$$

On note $A^\times$ le groupe des inversibles d'un anneau A.

THÉORÈME 1. *(1) Pour que le problème* $[E = K(\sqrt{a})/K, \epsilon_{-1}]$ *soit résoluble, il faut que la condition* (BNE_{-1}) *suivante soit vérifiée :*
(BNE_{-1}) *Il existe une unité de* E *:* $u \in O_E^\times$*, congrue à 1 modulo 2 :* $u \equiv 1\, mod 2O_E$*, de norme* $N_{E/K}u = -1$.

La condition (BNE_{-1}) *est équivalente à la condition*
$(BNE_{-1})'$ *Il existe un entier* $t \in O_K$ *tel que* $E = K(\sqrt{1+4t^2})$.
(2) Pour que le problème $[E = K(\sqrt{a}, \sqrt{b})/K, \epsilon_n]$ *(*$n \in \{0,1\}$ *fixé) soit résoluble, il faut que la condition* (BNE_n) *suivante soit vérifiée :*
(BNE_n) *Il existe des unités* $u \in O_E^\times, v \in O_E^\times$*, de* E*, telles que l'on ait*

$$u \equiv 1\, mod 2O_E,\ u\sigma(u) = (-1)^n\ ;\ v \equiv 1\, mod 2O_E,\ v\tau(v) = (-1)^n$$
$$\tau(u)/u = -\sigma(v)/v.$$

On voit donc que ces conditions ne s'expriment qu'en termes des unités du corps E.

Idée de la démonstration. Etant donnée une extension de groupes $1 \to \Delta \hookrightarrow G \xrightarrow{\pi} \Gamma \to 1$ de classe $\epsilon \in H^2(\Gamma, \Delta)$, on se place dans "l'algèbre de groupe tordue" $\widehat{E[G]}$ de G sur E définie comme étant le E-espace vectoriel de base les éléments de G muni de la multiplication $eg \cdot e'g' = e\pi(g)(e')gg'$ $(e, e' \in E; g, g' \in G)$. Soit $O_E[\Delta]^\times G$ le sous-groupe multiplicatif de $\widehat{E[G]}^\times$ constitué des produits ηg où $\eta \in O_E[\Delta]^\times$ et $g \in G$. La démonstration consiste à traduire les propriétés des cup-produits définissant les classes $\epsilon_n (n \in \{-1, 0, 1\})$ (cf.[**11**]) au moyen de l'implication suivante : si le problème $[E/K, \epsilon]$ est résoluble, la suite exacte

$$1 \to O_E[\Delta]^\times \hookrightarrow O_E[\Delta]^\times G \xrightarrow[\eta g \mapsto \pi(g)]{\pi'} \Gamma \to 1$$

est scindée, i.e., il existe un homomorphisme $\psi : \Gamma \to O_E[\Delta]^\times G$ tel que $\pi' \circ \psi = id_\Gamma$.

Si les problèmes $(E/K, \epsilon_{-1})$ et $(E/K, \epsilon_1)$ sont résolubles et admettent une solution N/K telle que N/E soit modérément ramifiée, l'extension E/K est nécessairement modérément ramifiée (cf. [8] §39). Il n'en est pas de même en général lorsque $[E/K, \epsilon_0]$ est résoluble. Cependant, pour uniformiser et simplifier, nous supposons désormais l'extension de base E/K modérément ramifiée lorsque la condition (BNE_0) du théorème 1 est vérifiée.

On est maintenant en mesure de répondre à la question naturelle de savoir si les conditions nécessaires du théorème 1 sont aussi suffisantes. La réponse est oui sur un corps K de nombre de classe 1.

2. Formules de construction de bases normales d'entiers

Dans cette section, K est un corps de nombres de nombre de classe $h(K) = 1$. Cette hypothèse est avant tout calculatoire, et permet par exemple de choisir les éléments $a, b \in K$ de façon que l'on ait les discriminants $D(K(\sqrt{c})/K) = cO_K, c \in \{a, b\}$. On a alors le

THÉORÈME 2. *(A) Pour qu'un problème $[E/K, \epsilon_n]$ soit résoluble, il faut et il suffit que la condition (BNE_n) du théorème 1 soit vérifiée ($n \in \{-1, 0, 1\}$).*
(B) On suppose qu'il en est ainsi. Soit U le groupe multiplicatif des éléments $k \in K^\times$ tels que l'on ait $ord_\wp((k-1)/4) \geq 0$ en tout idéal premier $\wp$ de K divisant $2O_K$, où $ord_\wp$ désigne la valuation en $\wp$.
(1) Une solution du problème $[E = K(\sqrt{a})/K, \epsilon_{-1}]$ est l'extension cyclique $N = E(\sqrt{x})/K$ définie par l'entier de E

$$x = p(2t + \sqrt{1 + 4t^2})\sqrt{a}$$

obtenu comme suit. On prend pour t, un entier de K tel que $E = K(\sqrt{1+4t^2})$ (cf. condition $(BNE_{-1})'$) ; et pour p, un irréductible de O_K ne se ramifiant pas dans E (resp. une unité de K quand elle existe) vérifiant

$$\alpha(1 - 2t)/p \in U$$

où α est un entier de K tel que $\alpha^2 a = 1 + 4t^2$.
(2) Une solution du problème $[E = K(\sqrt{a}, \sqrt{b})/K, \epsilon_n]$ ($n \in \{0, 1\}$ fixé) est l'extension $N = E(\sqrt{x})/K$, diédrale si $n = 0$, quaternionienne si $n = 1$, définie par l'entier de E

$$x = p\frac{\sqrt{a}}{\lambda}\left(\frac{\sqrt{b}}{d}\right)^n \eta v$$

obtenu comme suit. On prend : pour λ, un entier de $K(\sqrt{a})$ divisant $\sqrt{a}$ tel que $\lambda/\sigma(\lambda) = u\tau(u)$; pour η, une unité de $K(\sqrt{a})$ telle que $\lambda^2 = \eta\kappa$ où κ est un entier de K divisant a ; pour d, un p.g.c.d. de a/κ et de b ; et pour p, un irréductible de O_K ne se ramifiant pas dans E (resp. une unité de K quand elle existe) vérifiant

$$d^n\kappa c/p \in U \quad avec \quad c := Tr_{E/K}\left(\theta/\left(\sqrt{a}(\sqrt{b})^n\lambda v\right)\right)$$

où $Tr_{E/K}$ est la trace de E sur K, et θ un entier de E de trace 1 sur K. (3) Dans les notations précédentes, avec $\Delta = Gal(N/E)$, on a $O_N = O_E[\Delta]\vartheta$ et $O_N = O_E[\vartheta]$ pour l'entier $\vartheta = \frac{1}{2}(1+\sqrt{x})$.

Idée de la démonstration. On montre d'abord, par les théorèmes de [**11**], que si la condition (BNE_n) est vérifiée, le problème $(E/K, \epsilon_n)$ est résoluble ($n \in \{-1, 0, 1\}$). On sait qu'un tel problème admet nécessairement une solution modérément ramifiée N'/K (cf.[**13**], Theorem(6-6)). On affine ensuite les formules de [**11**] de façon à ce qu'elles fournissent un élément $x' \in E$ tel que $N' = E(\sqrt{x'})$. Puis l'on fait varier la solution N'/K jusqu'à trouver un entier $x = ke^2x'$ de E, $k \in K^\times, e \in E^\times$, congru à $1 \bmod 4O_E$, tel que l'idéal xO_E soit un produit d'idéaux premiers distincts ou O_E lui-même. L'extension $N = E(\sqrt{x})/K$ est alors une solution du problème $[E/K, \epsilon_n]$.

Soulignons que les extensions du théorème 2 sont de "bonnes" solutions au sens de Fröhlich (cf.[**5**] Theorem 3, [**6**] p. 230) : leur ramification n'augmente que très peu celle de l'extension de base. En effet,

COROLLAIRE. *Quand $h(K) = 1$, les problèmes $[E/K, \epsilon_n](n \in \{-1, 0, 1\})$ résolubles admettent toujours une solution N/K telle que les irréductibles de O_K qui se ramifient dans N soient ceux qui se ramifient dans E, à l'exception d'au plus l'un d'entre eux.*

C'est clair par nos formules car la ramification n'augmente que si le facteur p n'est pas une unité de K. L'existence des irréductibles p se prouve par le corps de classes.

Signalons pour terminer que dans le cas particulier $K = \mathbb{Q}$, on retrouve les résultats de plusieurs auteurs : Brinkhuis, Fröhlich, M-N. Gras,... .

REFERENCES

[1] N. BOURBAKI, "Algèbre, Chapitres 4 à 7," Masson, Paris, 1981.

[2] J. BRINKHUIS, "Embedding problems and Galois modules," Doctoral Dissertation, Leiden, 1981.

[3] J. BRINKHUIS, *Normal integral bases and embedding problems*, Math. Ann. **264** (1983), 537-543.

[4] J. BRINKHUIS, *Normal integral bases and complex conjugation*, J. reine angew. Math. **375/376** (1987), 157-166.

[5] A. FRÖHLICH, *Artin-root numbers and normal integral bases for quaternion fields*, Invent. Math **17** (1972), 143-166.

[6] A. FRÖHLICH, "Galois Module Structure of Algebraic Integers," Ergebnisse der Math. 3,1,Springer-Verlag, Berlin, 1983.

[7] M.-N. GRAS, *Bases d'entiers dans les extensions cycliques de degré 4 de* $\mathbf{Q}$, Sém. Théorie des Nombres, Bordeaux (1982/83), exp. 11.

[8] E. HECKE, "Lectures on the Theory of Algebraic Numbers," Graduate Texts Math.77, Springer-Verlag, New York, 1981.

[9] F. KAWAMOTO, *On normal integral bases*, Tokyo J. Math. **7** (1984), 221-231.

[10] F. KAWAMOTO, *Remark on "On normal integral bases"*, Tokyo J. Math. **8** (1985), 275.

[11] R. MASSY, *Construction de p-extensions galoisiennes d'un corps de caractéristique différente de p*, J. Algebra **109** (1987), 508-535.

[12] R. MASSY, *Bases normales d'entiers relatives quadratiques*, J. Number Theory, à paraître.

[13] J. NEUKIRCH, *Über das Einbettungsproblem der algebraischen Zahlentheorie*, Invent. Math. **21** (1973), 59-116.

[14] K. OKUTSU, *Construction of relative integral basis of* $\mathbf{Q}(\sqrt[\ell]{a}, \zeta_\ell)$ *over* $\mathbf{Q}(\zeta_\ell)$ *(in Japanese)*, Seisūron Kenkyūshūkai hōkokushū, in Kyushu University (1982).

[15] M.J. TAYLOR, *On Fröhlich's conjecture for rings of integers of tame extensions*, Invent. Math. **63** (1981), 41-79.

Richard Massy
Département de Mathématiques
Université de Valenciennes
Le Mont Houy
F-59326 VALENCIENNES Cedex
FRANCE

(reçu le 30 octobre 1989)

Astérisque

TAPANI MATALA-AHO

On recurrences for some hypergeometric type polynomials

Astérisque, tome 198-199-200 (1991), p. 237-244

<http://www.numdam.org/item?id=AST_1991__198-199-200__237_0>

ON RECURRENCES FOR SOME HYPERGEOMETRIC TYPE POLYNOMIALS

by

TAPANI MATALA-AHO

1. Introduction

A well-known result for Legendre type polynomials $P_n = {}_2F_1\left(\begin{matrix}-n,-n\\1\end{matrix}\,\middle|\,t\right)$ is the recurrence relation $nP_n - (2n-1)(1+t)P_{n-1} + (n-1)(1-t)^2P_{n-2} = 0$. When t=-1 this implies the known sum formula $\sum_{k=0}^{2m}\binom{2m}{k}^2(-1)^k = (-1)^m\binom{2m}{m}$ $(m = 0,1,2,...)$.

There are numerous extensions of this recurrence for special values of t. ASKEY and WILSON [2] achieved three term recurrences for the sums $\sum_{k=0}^{n}\binom{n}{k}\binom{n+a+d}{k+d}\binom{n+k+b+e}{k+e}\binom{n+k+c+f}{k+f}$ $(a+d=b+c)$ by contiguous relations for hypergeometric series. PERLSTADT [6] obtained recurrences for sums $\sum_{k=0}^{n}\binom{n}{k}^r$ $(r = 2,...,6)$ by the method of telescoping series.

In the following we want to apply so called 'SISTER CELINE's method' to the following kind of hypergeometric polynomials - say ${}_3F_2\left(\begin{matrix}-n,A,B\\1,\ 1\end{matrix}\,\middle|\,t\right)$, where $(A,B) = (-n,-n),(-n,1/2)$ or $(-n,n+1)$ and ${}_4F_3\left(\begin{matrix}-n,A,B,C\\1,\ 1,\ 1\end{matrix}\,\middle|\,t\right)$, where $(A,B,C) = (-n,-n,-n)$ or $(-n,n+1,n+1)$. For the hypergeometric notation we refer to RAINVILLE [8]. These polynomials satisfy four or five order recurrences and with special values of the parameter t we shall obtain some three term recurrences like the APÉRY recurrences [1] considered in detail by VAN DEER POORTEN [7]. Also we shall get DIXON's sum formula $\sum_{k=0}^{2m}\binom{2m}{k}^3(-1)^k = (-1)^m\binom{2m}{m}\binom{3m}{m}$ $(m = 0,1,2,...)$ (MACMAHON [5]). More references can be found from ASKEY and WILSON [2] and PERLSTADT [6].

2. Sister Celine's method

From the remarks of BAILEY [3] it is clear that ${}_3F_2$-polynomials satisfy at most four term recurrences and ${}_4F_3$-polynomials satisfy at most five term recurrences. To obtain the recurrence

$$(1)\qquad a_0(n)p_n + (a_1(n)+a_2(n)t)p_{n-1} + (a_3(n)+a_4(n)t+a_5(n)t^2)p_{n-2} + ... = 0$$

for the polynomial $p_n = p_n(t)$ of degree n we shall use SISTER CELINE's method, see FASENMYER [4] or RAINVILLE [8]. Note that some of the coefficient polynomials of $p_n, p_{n-1}, ...$

may be zero e.g. in (4), (13) and (14). In these cases we shall rise the index n so that in all cases our results have the form

$$A(n,t)\ p_n\ +\ B(n,t)\ p_{n-1}\ +\ C(n,t)p_{n-2}\ +\ ...\ =\ 0.$$

Let us set $p_n(t) = \sum_{k=0}^{n} \epsilon(k,n)t^k$. In the case of the above mentioned polynomials it is easy to write polynomials $p_{n-1}, tp_{n-1}, p_{n-2}, tp_{n-2},\ t^2p_{n-2}, ...$ in the form

$$\sum_{k=0}^{n} r_i(k,n)\epsilon(k,n)t^k \qquad (i = 1,2,...)$$

(see the proof of Theorem 1), where the $r_i(k,n)$'s are certain rational expressions of k and n. Now from (1) shall we obtain the identity

$$a_0(n) + a_1(n)r_1(k,n) + a_2(n)r_2(k,n) + a_3(n)r_3(k,n) + ...\ =\ 0. \tag{2}$$

Thus it is straightforward to get enough equations to solve the unknowns $a_i(n)$ $(i = 0,1,...)$. Let the number of a_i's be m. In all our cases it sufficied to set $k = 1,...,m$ to achieve a solvable system of equations. In some cases due the symmetry it was possible to reduce significantly the number of equations (see Theorem 1).

3. Theorems

In the following theorem we shall state recurrences for

$$J_n(t)\ =\ {}_3F_2\left(\begin{matrix}-n,-n,-n\\ 1,\ 1\end{matrix}\ \middle|\ t\right)\quad\text{and}\quad H_n(t)\ =\ {}_4F_3\left(\begin{matrix}-n,-n,-n,-n\\ 1,\ 1,\ 1\end{matrix}\ \middle|\ t\right).$$

Now due the relations $J_n(1/t) = (-1/t)^n J_n(t)$ and $H_n(1/t) = (1/t)^n H_n(t)$ there are only six unknowns $a_i(n)$ in the first case and 14 in the second case.

THEOREM 1. *The recurrences for J_n and H_n are given by*

$$(3n-5)n^2J_n\ -\ (9n^3-24n^2+17n-4)(1-t)J_{n-1} \tag{3}$$

$$+\ (3n-4)(3n^2-7n+3+(21n^2-49n+24)t+(3n^2-7n+3)t^2)J_{n-2}$$

$$-\ (3n-2)(n-2)^2(1-t)^3J_{n-3}\ =\ 0$$

and

$$(b_0(n)+b_1(n)t+b_0(n)t^2)H_n\ +\ (b_2(n)+b_3(n)t+b_3(n)t^2+b_2(n)t^3)H_{n-1}\ + \tag{4}$$

$$(b_4(n)+b_5(n)t+b_6(n)t^2+b_5(n)t^3+b_4(n)t^4)H_{n-2}\ +$$

$$(b_7(n)+b_8(n)t+b_9(n)t^2+b_9(n)t^3+b_8(n)t^4+b_7(n)t^5)H_{n-3}\ +$$

$$(b_{10}(n)+b_{11}(n)t+b_{12}(n)t^2+b_{13}(n)t^3+b_{12}(n)t^4+b_{11}(n)t^5+b_{10}(n)t^6)H_{n-4} \;=\; 0,$$

where

$$\begin{aligned}
b_0(n) &= (n-1)n^3(64n^4-544n^3+1697n^2-2303n+1151),\\
b_1(n) &= (n-1)n^3(272n^4-2312n^3+7231n^2-9859n+4958),\\
b_2(n) &= -(n-1)(256n^7-2560n^6+10212n^5-20844n^4+23317n^3-\\
&\quad 14341n^2+4655n-630),\\
b_3(n) &= -(n-1)(1344n^7-13440n^6+53688n^5-109816n^4+123098n^3-\\
&\quad 75804n^2+24615n-3330),\\
b_4(n) &= 384n^8-4800n^7+25318n^6-73416n^5+127613n^4-135624n^3+\\
&\quad 85700n^2-29385n+4230,\\
b_5(n) &= -6304n^8+78800n^7-418938n^6+1237876n^5-2224383n^4+\\
&\quad 2489364n^3-1694065n^2+640890n-103320,\\
b_6(n) &= -10(3296n^8-41200n^7+218996n^6-646196n^5+1157126n^4-\\
&\quad 1286706n^3+867069n^2-323775n+51462),\\
b_7(n) &= -(n-2)(256n^7-3072n^6+15140n^5-39448n^4+58199n^3-\\
&\quad 48180n^2+20600n-3555),\\
b_8(n) &= -(n-2)(9024n^7-108288n^6+536320n^5-1412352n^4+2119776n^3-\\
&\quad 1798290n^2+793925n-142335),\\
b_9(n) &= -5(n-2)(8384n^7-100608n^6+498988n^5-1318024n^4+1987917n^3-\\
&\quad 1698342n^2+756763n-137142),\\
b_{10}(n) &= (n-2)(n-3)^3(64n^4-288n^3+449n^2-285n+65),\\
b_{11}(n) &= (n-1)(n-2)(n-3)^3(16n^3-56n^2+75n-30),\\
b_{12}(n) &= -5(n-2)(n-3)^3(128n^4-576n^3+913n^2-597n+141),\\
b_{13}(n) &= 10(n-2)(n-3)^3(112n^4-504n^3+797n^2-519n+122),
\end{aligned}$$

respectively.

PROOF: We shall shortly describe the proof of the recurrence (4). For technical reasons we shall lower the index n to $n-2$ in the formula (4). When we denote

$$H_n=\sum_{k=0}^{n}\epsilon(k,n)t^k,$$

where $\epsilon(k,n)=(-n)_k^4/(k!)^4$, then

$$t^iH_{n-j}=\sum_{k=i}^{n+i-j}\left(\frac{(k-i+1)_i(-n+k)_{j-i}}{(-n)_j}\right)^4\epsilon(k,n)t^k\quad(i\le j)$$

so that $r_3 = ((k-n)(k-n+1)/n(n-1))^4$, $r_4 = (k(k-n)/n(n-1))^4, \ldots$. Hence the left hand side of (4) can be combined into one sum

$$\sum_{k=0}^{n} \frac{N(k,n)}{(n(n-1)(n-2)(n-3)(n-4)(n-5))^4} \epsilon(k,n) t^k,$$

where

$$N(k,n) =$$

$$(n-2)^4(n-3)^4(n-4)^4(n-5)^4(((k-n)^4(k-n+1)^4+(k-1)^4k^4)b_0(n-2)+(k-n)^4k^4b_1(n-2))+\ldots$$

$$+(k-n)^4(k-n+1)^4(k-n+2)^4(k-2)^4(k-1)^4k^4b_{13}(n-2) \;=\; 0$$

identically on k and n. Counting this could have been quite tedious without the assistance of some symbolic mathematical program system like Macsyma, Musimp or Reduce. ∎

When $t = 1$ we get from (3) $J_n = \dfrac{-3(3n-4)(3n-2)}{n^2} J_{n-2}$. So we have DIXON's result $\displaystyle\sum_{k=0}^{2m} \binom{2m}{k}^3 (-1)^k = (-1)^m \binom{2m}{m}\binom{3m}{m}$ $(m = 0,1,2,\ldots)$ (MACMAHON [5]).

In the following corollary we shall state three term recurrences for $j_n = \displaystyle\sum_{k=0}^{n} \binom{n}{k}^3$, $h_n = \displaystyle\sum_{k=0}^{n} \binom{n}{k}^4$ and $g_n = \displaystyle\sum_{k=0}^{n} \binom{n}{k}^4 (-1)^k$. The recurrences for numbers j_n and h_n are results of FRANEL (PERLSTADT [6]), while the recurrence (7) for g_n is perhaps new.

COROLLARY 1. *The recurrences for j_n, h_n and g_n are given by*

$$n^2 j_n \;-\; (7n^2 - 7n + 2) j_{n-1} \;-\; 8(n-1)^2 j_{n-2} \;=\; 0, \tag{5}$$

$$n^3 h_n \;-\; 2(2n-1)(3n^2 - 3n + 1) h_{n-1} \;-4(n-1)(4n-3)(4n-5) h_{n-2} \;=\; 0 \tag{6}$$

and

$$(n-1)(12n^2 - 63n + 83) n^3 g_n \;+ \tag{7}$$

$$4(408n^6 - 3774n^5 + 13760n^4 - 25203n^3 + 24465n^2 - 11970n + 2340) g_{n-2} +$$

$$16(n-2)(12n^2 - 15n + 5)(n-3)^3 g_{n-4} \;=\; 0$$

respectively.

PROOF: We shall prove the first formula, the proof of second formula goes similarly. The third formula is an immediate consequence of (4) with $t = -1$.

Let us define the operator E by $Er_n = r_{n+1}$. As a consequence of formula (3) with $t = -1$ we get

$$(8) \qquad (3n-5)n^2 j_n - 2(9n^3 - 24n^2 + 17n - 4)j_{n-1} -$$

$$(3n-4)(15n^2 - 35n + 18)j_{n-2} - 8(3n-2)(n-2)^2 j_{n-3} = 0.$$

Then (8) is equivalent to

$$(9) \qquad P(n)j_{n-3} = ((3n-5)n^2E^3 - 2(9n^3 - 24n^2 + 17n - 4)E^2 -$$

$$(3n-4)(15n^2 - 35n + 18)E - 8(3n-2)(n-2)^2)j_{n-3} = 0,$$

where the operator $P(n)$ factors in the following way

$$P(n) = ((3n-5)E + 3n - 2)((n-1)^2E^2 - (7(n-1)(n-2) + 2)E - 8(n-2)^2).$$

Let us denote

$$(10) \qquad s_{n-3} = ((n-1)^2E^2 - (7(n-1)(n-2) + 2)E - 8(n-2)^2)j_{n-3}.$$

Thus (9) is equivalent to

$$(11) \qquad ((3n-5)E + 3n - 2)s_{n-3} = 0$$

i.e. $(3n-5)s_{n-2} = -(3n-2)s_{n-3}$. From (10) one gets $s_0 = 2^2 j_2 - (7 \cdot 2 \cdot 1 + 2)j_1 - 8j_0 = 0$, so $s_k = 0$ $(k = 0, 1, 2, ...)$ and thus (10) implies (5).

In the second case one sets $t = 1$ in (4) and gets $P(n)h_{n-4} = 0$, where the operator $P(n)$ factors in the following way

$$P(n) = ((n-1)(20n^3 - 115n^2 + 215n - 132)E + 2(2n-5)(20n^3 - 55n^2 + 45n - 12))$$

$$((n-1)^3E^2 - 2(2n-3)(3n^2 - 9n + 7)E - 4(n-2)(4n-7)(4n-9)).$$

Analogously to the first case one obtains the recurrence (6). ∎

By similar method like in Theorem 1 we can achieve recurrences for

$$F_n(t) = {}_3F_2\left(\begin{matrix}-n, -n, 1/2 \\ 1, \ 1\end{matrix} \,\middle|\, t\right), \quad B_n(t) = {}_3F_2\left(\begin{matrix}-n, -n, n+1 \\ 1, \ 1\end{matrix} \,\middle|\, t\right)$$

and

$$A_n(t) = {}_4F_3\left(\begin{matrix}-n, -n, n+1, n+1 \\ 1, \ 1, \ 1\end{matrix} \,\middle|\, t\right).$$

THEOREM 2. *The recurrences for F_n, B_n and A_n are given by*

$$(12) \qquad 4(4n-7)n^2F_n - 2(6(4n^3 - 11n^2 + 8n - 2) + (16n^3 - 44n^2 + 34n - 9)t)F_{n-1} +$$

$$(4(12n^3 - 45n^2 + 52n - 18) + 2(2n-3)t + (4n-3)(2n-3)^2t^2)F_{n-2}$$
$$- 4(4n-3)(n-2)^2(1-t)^2F_{n-3} = 0$$

and

$$(13) \qquad (b_0(n) + b_1(n)t)B_n + (b_2(n) + b_3(n)t + b_4(n)t^2)B_{n-1} +$$
$$(b_5(n) + b_6(n)t + b_7(n)t^2 + b_8(n)t^3)B_{n-2} + (b_9(n) + b_{10}(n)t + b_{11}(n)t^2)B_{n-3} = 0,$$

where

$$\begin{aligned}
b_0(n) &= 3(9n-14)n^2, & b_6(n) &= -4(159n^3 - 567n^2 + 626n - 200),\\
b_1(n) &= -4(8n-13)n^2, & b_7(n) &= 4(67n-40)(2n-3)^2,\\
b_2(n) &= -3(27n^3 - 69n^2 + 47n - 10), & b_8(n) &= -16(8n-5)(2n-3)^2,\\
b_3(n) &= -10(12n^3 - 30n^2 + 23n - 6), & b_9(n) &= -3(9n-5)(n-2)^2,\\
b_4(n) &= 8(32n^3 - 84n^2 + 62n - 15), & b_{10}(n) &= (59n-35)(n-2)^2,\\
b_5(n) &= 3(3n-5)(9n^2 - 17n + 6), & b_{11}(n) &= -4(8n-5)(n-2)^2,
\end{aligned}$$

and

$$(14) \qquad (c_0(n) + c_1(n)t)A_n + (c_2(n) + c_3(n)t + c_4(n)t^2)A_{n-1} +$$
$$(c_5(n) + c_6(n)t + c_7(n)t^2 + c_8(n)t^3)A_{n-2} + (c_9(n) + c_{10}(n)t + c_{11}(n)t^2)A_{n-3} +$$
$$(c_{12}(n) + c_{13}(n)t)A_{n-4} = 0,$$

where

$$\begin{aligned}
c_0(n) &= (n-1)(2n-3)(2n-5)^2n^3,\\
c_1(n) &= -(n-1)(2n-5)(4n-7)(4n-9)n^3,\\
c_2(n) &= -(n-1)(2n-1)(2n-5)(8n^4 - 40n^3 + 62n^2 - 33n + 6),\\
c_3(n) &= -(n-1)(2n-1)(2n-5)(4n-3)(8n^3 - 34n^2 + 41n - 18),\\
c_4(n) &= 4(n-1)(2n-1)(2n-5)(4n-9)(16n^3 - 44n^2 + 34n - 9),\\
c_5(n) &= (2n-3)(24n^6 - 216n^5 + 754n^4 - 1284n^3 + 1101n^2 - 441n + 66),\\
c_6(n) &= -(2n-3)(864n^6 - 7776n^5 + 27514n^4 - 48444n^3 + 44169n^2 -\\
&\qquad 19485n + 3270),\\
c_7(n) &= 4(2n-1)(2n-3)^3(2n-5)(64n^2 - 192n + 99),\\
c_8(n) &= -16(2n-1)(2n-3)^3(2n-5)(4n-3)(4n-9),\\
c_9(n) &= -(n-2)(2n-1)(2n-5)(8n^4 - 56n^3 + 134n^2 - 123n + 33),\\
c_{10}(n) &= -(n-2)(2n-1)(2n-5)(4n-9)(8n^3 - 38n^2 + 53n - 15),\\
c_{11}(n) &= 4(n-2)(2n-1)(2n-5)(4n-3)(16n^3 - 100n^2 + 202n - 129),\\
c_{12}(n) &= (n-2)(n-3)^3(2n-1)^2(2n-3),\\
c_{13}(n) &= -(n-2)(n-3)^3(2n-1)(4n-3)(4n-5),
\end{aligned}$$

respectively.

In the following corollary we shall state three term recurrences for $f_n = \sum_{k=0}^{n} \binom{n}{k}^2 \binom{2k}{k}$, $e_n = \sum_{k=0}^{n} \binom{n}{k}^2 \binom{2k}{k} \left(\frac{1}{4}\right)^k$, $b_n = \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}$ and $a_n = \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}^2$. The recurrence for the numbers f_n is proved in STIENSTRA and BEUKERS [9], the recurrences for the APÉRY numbers b_n and a_n can be found in APÉRY [1] and POORTEN VAN DEER A. [7].

COROLLARY 2. *The recurrences for f_n, e_n, b_n and a_n are given by*

$$n^2 f_n - (10n^2 - 10n + 3) f_{n-1} + 9(n-1)^2 f_{n-2} = 0, \tag{15}$$

$$4n^2 e_n - 2(10n^2 - 10n + 3) e_{n-1} + (4n-3)(4n-5) e_{n-2} = 0, \tag{16}$$

$$n^2 b_n - (11n^2 - 11n + 3) b_{n-1} - (n-1)^2 b_{n-2} = 0 \tag{17}$$

and

$$n^3 a_n - (2n-1)(17n^2 - 17n + 5) a_{n-1} + (n-1)^3 a_{n-2} = 0 \tag{18}$$

respectively.

For example let $a_n = A_n(1) = {}_4F_3\left(\begin{matrix} -n, -n, n+1, n+1 \\ 1, 1, 1 \end{matrix} \,\middle|\, 1\right)$ then the formula (14) gives $P(n) a_{n-4} = 0$, where

$$P(n) = ((n-2)(2n-5)E^2 - (2n-1)(2n-5)E + (n-1)(2n-1))$$
$$((n-2)^3 E^3 - (2n-5)(17(n-2)(n-3) + 5)E + (n-3)^3).$$

Again like in the proof of Corollary 1 we see that a_n satisfies (18). ∎

REFERENCES

1. APÉRY R., *Irrationalité de ζ2 et ζ3*, Astérisque **61** (1979), 11-13.

2. ASKEY R. and WILSON J.A., *A Recurrence Relation generalizing those of Apéry*, J. Austrl. Math. Soc. A **36** (1984), 267-278.

3. BAILEY W.N., *Associated Hypergeometric Series*, Quart. J. Math. Oxford **8** (1937), 115-118.

4. FASENMYER SISTER M.C., *A Note on Pure Recurrence Relations*, Am. Math. Monthly **56** (1949), 14-17.

5. MACMAHON P.A., *The Sums of Powers of the Binomial Coefficients*, Mess. Math. **33** (1902), 274-288.

6. PERLSTADT M.A., *Some Recurrences for Sums of Powers of Binomial Coefficients*, J. Number Th. **27** (1987), 304-309.

7. POORTEN VAN DEER A., *A Proof that Euler missed... Apérys Proof of the Irrationality of* $\zeta(3)$, Math Int. **1** (1979), 195-203.

8. RAINVILLE E.D., "Special Functions," Macmillian Company, New York, 1960.

9. STIENSTRA J. and BEUKERS F., *On the Picard-Fuchs Equation and the Formal Brauer Group of Certain Elliptic K3-Surfaces*, Math. Ann. **271** (1985), 296-304.

Tapani Matala-aho
University of Oulu
Department of Mathematics
90570 Oulu
Finland

Astérisque

FRANÇOIS MORAIN

Elliptic curves, primality proving and some Titanic primes

Astérisque, tome 198-199-200 (1991), p. 245-251

<http://www.numdam.org/item?id=AST_1991__198-199-200__245_0>

ELLIPTIC CURVES, PRIMALITY PROVING AND SOME TITANIC PRIMES

Abstract

We describe how to generate large primes using the primality proving algorithm of Atkin.

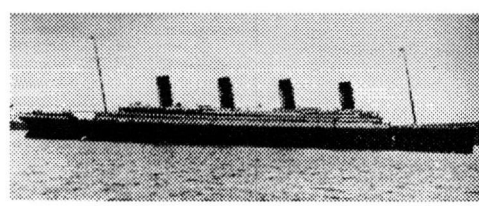


Figure 1: The Titanic*.

1. Introduction. During the last ten years, primality testing evolved at great speed. Motivated by the RSA cryptosystem [3], the first deterministic primality proving algorithm was designed by Adleman, Pomerance and Rumely [2] and made practical by Cohen, H. W. Lenstra and A. K. Lenstra (see [9, 10] and more recently [5]). It was then proved that the time needed to test an arbitrary integer N for primality is $O((\log N)^{c \log\log\log N})$ for some positive constant $c > 0$. When implemented on a huge computer, the algorithm was able to test 200 digit numbers in about 10 minutes of CPU time.

A few years ago, Goldwasser and Kilian [11], used the theory of elliptic curves over finite fields to give the first primality proving algorithm whose running time is polynomial in $\log N$ (assuming a plausible conjecture in number theory). Atkin [4] used the theory of complex multiplication to give a practical version of this algorithm.

*Taken from *Titanic, Destination disaster, The Legends and the Reality* by J. P. Eaton and C. A. Haas, W. W. Norton and Company, New York 1987.

The aim of this paper is to present some results the author has obtained using his own implementation of this algorithm in the search for large primes.

2. Elliptic curves. Let $\mathbf{K}$ be a field of characteristic prime to 6. An elliptic curve E over $\mathbf{K}$ is a non singular algebraic projective curve of genus 1. It can be shown [7, 23] that E is isomorphic to a curve with equation:

$$y^2z = x^3 + axz^2 + bz^3, \tag{1}$$

where a and b are in $\mathbf{K}$. The *discriminant* of E is $\Delta = -16(4a^3 + 27b^2)$ and the *invariant* is

$$j = 2^8 3^3 \frac{a^3}{4a^3 + 27b^2}.$$

We write $E(\mathbf{K})$ for the set of points with coordinates $(x : y : z)$ which satisfy (1) with $z = 1$, together with the point at infinity: $O_E = (0 : 1 : 0)$. We will use the well-known *tangent-and-chord* addition law on a cubic [13] over $\mathbf{Z}/N\mathbf{Z}$ (see [17] for a justification).

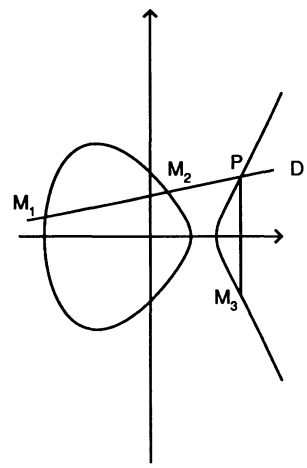


Figure 2: An elliptic curve over $\mathbf{R}$.

In order to add two points $M_1 = (x_1, y_1)$ and $M_2 = (x_2, y_2)$ on E resulting in $M_3 = (x_3, y_3)$, the equations are

$$\begin{cases} x_3 &= \lambda^2 - x_1 - x_2 \\ y_3 &= \lambda(x_1 - x_3) - y_1 \end{cases}$$

where

$$\lambda = \begin{cases} (y_2 - y_1)(x_2 - x_1)^{-1} & \text{if } x_2 \neq x_1 \\ \\ (3x_1^2 + a)(2y_1)^{-1} & \text{otherwise.} \end{cases}$$

3. Primality testing. Let us recall one of the converses of Fermat's theorem (see for example [6]).

Theorem 1 *Let a be such that $\gcd(a, N) = 1$, q a prime divisor of $N - 1$. If*

$$a^{N-1} \equiv 1 \bmod N \text{ and } \gcd(a^{(N-1)/q} - 1, N) = 1$$

then each prime divisor p of N satisfies: $p \equiv 1 \bmod q$.

Corollary 1 *Under the conditions of Theorem 1, if $q > \sqrt{N}$ then N is prime.*

A similar theorem can be stated for elliptic curves.

Theorem 2 ([11, 16]) *Let N be an integer greater than 1 and prime to 6. Let E be an elliptic curve over $\mathbf{Z}/N\mathbf{Z}$, m and s two integers such that $s \mid m$. Suppose we have found a point P on E that satisfies $m\,P = O_E$, and that for each prime factor q of s, we have verified that $\frac{m}{q}P \neq O_E$. Then if p is a prime divisor of N, $\#E(Z/pZ) \equiv 0 \bmod s$.*

Corollary 2 *Under the conditions of Theorem 2, if $s > (\sqrt[4]{N} + 1)^2$, then N is prime.*

4. Atkin's algorithm. In order to use the preceding theorem, we need to compute the number of points m. This process is far from trivial in general (see [22]). From a practical point of view, it is desirable to use deep properties of elliptic curves over finite fields. This involves the theory of complex multiplication and class fields and requires a lot of theory [18]. We can summarize the principal properties:

Theorem 3 *Let p be a rational prime number that splits as the product of two principal ideals in K (i.e. (p) splits completely in the ring class field of K): $p = \pi\pi'$ with π an integer of K. Then there exists an elliptic curve E defined over $\mathbf{Z}/p\mathbf{Z}$ having complex multiplication by the ring of integers of K, whose cardinality is $m = N_K(\pi - 1) = (\pi - 1)(\pi' - 1) = p + 1 - t$ with $|t| \leq 2\sqrt{p}$ (Hasse's Theorem) and whose invariant is a root of a fixed polynomial $H_D(X)$ (depending only upon D) modulo p.*

The computation of the polynomials H_D is dealt with in [18, 19] (see also [14, 15]).

We now explain how the preceding theorems are used in a *factor and conquer* algorithm similar to the DOWNRUN process of [24]. The first phase of the algorithm consists in finding a sequence $N_0 = N > N_1 > \cdots > N_k$ of probable primes such that: N_{i+1} prime $\Longrightarrow N_i$ prime. The second then proves that each number is prime, starting from N_k.

Procedure SearchN

1. $i := 0$; $N_0 := N$;
2. find a fundamental discriminant $-D$ such that (N_i) splits as the product of two principal ideals in $\mathbf{Q}(\sqrt{-D})$;
3. for each solution of $(N_i) = (\pi)(\pi')$, find all factors of $m_\pi = (\pi - 1)(\pi' - 1)$ less than a given bound B and let N_π be the corresponding cofactor;
4. **if** one of the N_π is a probable prime **then** set $N_{i+1} := N_\pi$, store $\{N_i, D, \pi, m\}$, $i := i + 1$, and go to step 2 **else** go to step 3.
5. **end.**

The second phase consists in proving that the numbers N_i are indeed primes: For each i, find a curve E whose invariant is a root of $H_{D_i}(X)$ modulo p and check the condition of theorem (2). For technical details, we refer to [18].

5. Implementation and some timings. I have implemented Atkin's algorithm on a SUN 3/60 (12 Mo) using the BigNum package described in [12]. For a comparison of my arithmetic with the one used by Cohen and Lenstra, see [20].

We list in Table 1 the time needed to test a number of d words of 32 bits with my program, for $d = 2(2)20$. Time are in seconds.

d	min	max	mean	st. dev.	d	min	max	mean	st. dev.
2	4.7	15.7	8.8	2.6	12	485.7	1278.7	746.4	227.3
4	14.6	40.5	25.5	7.1	14	700.5	1413.0	1037.3	153.2
6	46.8	126.6	85.9	22.2	16	1106.6	3577.1	1909.6	668.0
8	102.4	266.7	159.1	43.8	18	1578.7	5164.7	2858.4	802.4
10	191.2	609.7	357.5	97.0	20	3233.8	9025.3	5252.6	1483.0

Table 1: Time for testing a d word number for primality.

6. Titanic primes. Following Yates [25], a prime number with more than 1000 digits is called a *Titanic prime* (see also [21]). Let us explain how the author found some Titanic primes with Atkin's algorithm.

Let D be a squarefree integer congruent to 1 or 2 mod 4. Let $\alpha_0 = a+b\sqrt{-D}$ and $\alpha_1 = c+e\sqrt{-D}$ be two integers of $\mathbf{K} = \mathbf{Q}(\sqrt{-D})$ (a, b, c, e are in $\mathbf{Z}$). Let k be a positive integer. We define an *Elliptic Mersenne Number* to be a number belonging to the following sequence of integers:

$$M_E(D, a, b, c, e) = N_K(\alpha_0\alpha_1^k + 1).$$

These numbers were first introduced by D. V. and G. V. Chudnovsky in [8]. They can be seen as the analogous of the Mersenne primes when considering the $N+1$ primality testing algorithm. As a matter of fact, Atkin's algorithm works fast for N as soon as we can find a D such that $N = N_K(\pi)$ in $\mathbf{K}$ and $m = N_K(\pi - 1)$ is smooth. Here, we see that $M_E(D, a, b, c, e)$ is trivially written as $\pi\pi'$ in $\mathbf{K}$ with $\pi = \alpha_0\alpha_1^k + 1$ and moreover,

$$N_K(\pi - 1) = N_K(\alpha_0\alpha_1^k) = N_K(\alpha_0)N_K(\alpha_1)^k,$$

which is smooth, provided the α_i's are of small norm.

Using some idle time from a network of Sun workstations, the author found that the numbers given in Table 2 are primes: These are the first Titanic Elliptic Mersenne Primes.

7. Conclusions. We have seen that Atkin's algorithm is a very powerful algorithm that can test small numbers for primality in a very short time and also find some huge primes in a reasonable amount of time.

D	a	b	c	e	k	# digits	D	a	b	c	e	k	# digits
1	-1	-1	2	1	1631	1141	2	0	-1	1	1	3833	1830
1	1	1	2	1	1636	1144	1	-1	-1	2	1	2786	1948
1	-1	1	2	1	1812	1267	2	0	-1	1	1	4743	2264
1	1	-1	3	2	1179	1314 †	1	-1	1	2	1	4414	3086
1	-1	1	2	1	2062	1442							

Table 2: Some Elliptic Mersenne Primes.

References

[1] L. M. ADLEMAN, M. A. HUANG. Recognizing primes in random polynomial time. *Proc. CRYPTO 86.*

†Found on Bastille Day, 1989 !

[2] L. M. ADLEMAN, C. POMERANCE, R. S. RUMELY. On distinguishing prime numbers from composite numbers. *Annals of Math.*, **117**, 1983, pp. 173-206.

[3] L. ADLEMAN, R. L. RIVEST, A. SHAMIR. A method for obtaining digital signatures and public-key cryptosystems. *Comm. of the ACM*, **21**, 2, 1978, pp. 120-126.

[4] A. O. L. ATKIN, F. MORAIN. Elliptic curves and primality proving. *Submitted.*

[5] W. BOSMA, M.-P. VAN DER HULST. Faster primality testing. To appear in *Proc. Eurocrypt '89.*

[6] J. BRILLHART, D. H. LEHMER, J. L. SELFRIDGE. New primality criteria and factorizations of $2^m \pm 1$. *Math. of Comp.*, **29**, 130, 1975, pp. 620-647.

[7] J. W. S. CASSELS. Diophantine equations with special references to elliptic curves. *J. London Math. Soc.*, **41**, 1966, pp. 193-291.

[8] D. V. CHUDNOVSKY, G. V. CHUDNOVSKY. Sequences of numbers generated by addition in formal groups and new primality and factorization tests. Research report RC 11262, IBM, Yorktown Heights, 1985. Also appeared in *Advances in Applied Mathematics*, **7**, pp. 385–434.

[9] H. COHEN, H. W. LENSTRA, JR. Primality testing and Jacobi sums. *Math. of Comp.*, **42**, 165, 1984, pp. 297-330.

[10] H. COHEN, A. K. LENSTRA. Implementation of a new primality test. *Math. of Comp.*, **48**, 177, 1987, pp. 103-121.

[11] S. GOLDWASSER, J. KILIAN. Almost all primes can be quickly certified. *Proc. 18th STOC*, Berkeley, 1986, pp. 316-329.

[12] J.-C. HERVÉ, F. MORAIN, D. SALESIN, B. SERPETTE, J. VUILLEMIN, P. ZIMMERMANN. BigNum: A Portable and Efficient Package for Arbitrary-Precision Arithmetic. Rapport Technique INRIA, *to appear*, 1989.

[13] D. HUSEMÖLLER. *Elliptic curves.* GTM 111, Springer, 1987.

[14] E. KALTOFEN, N. YUI. Explicit construction of the Hilbert class fields of imaginary quadratic fields with class numbers 7 and 11. *Proc. EUROSAM '84*, Cambridge, England, 1984, pp. 310-320.

[15] E. KALTOFEN, N. YUI. Explicit construction of the Hilbert class fields of imaginary quadratic fields by integer lattice reduction. Renseelaer Polytechnic Institute Research Report 89-13, May 1989.

[16] H. W. LENSTRA, JR. Elliptic curves and number theoretic algorithms. Report 86-19, Math. Inst., Univ. Amsterdam, 1986.

[17] H. W. LENSTRA, JR. Factoring integers with elliptic curves. *Annals of Math.*, **126**, 1987, pp. 649-673.

[18] F. MORAIN. Implementation of the Atkin-Goldwasser-Kilian primality testing algorithm. Rapport de Recherche INRIA, 911, Octobre 1988.

[19] F. MORAIN. Construction of Hilbert class fields of imaginary quadratic fields and dihedral equations modulo p. Rapport de Recherche INRIA, 1087, Septembre 1989.

[20] F. MORAIN. Atkin's test: news from the front. To appear in *Proc. Eurocrypt '89.*

[21] P. RIBENBOIM. *The book of prime number records.* Springer, 1988.

[22] R. SCHOOF. Elliptic curves over finite fields and the computation of square roots mod$p$. *Math. of Comp.*, **44**, 1985, pp. 483-494.

[23] J. T. TATE. The arithmetic of elliptic curves. *Inventiones Math.*, **23**, 1974, pp. 179-206.

[24] M. C. WUNDERLICH. A performance analysis of a simple prime-testing algorithm. *Math. of Comp.*, **40**, 162, 1983, pp. 709-714.

[25] S. YATES. Titanic primes. *J. Recr. Math.*, **16**, 1983/84, pp. 250-260.

François Morain †
INRIA, Domaine de Voluceau, B. P. 105
78153 LE CHESNAY CEDEX (France)

Département de Mathématiques
Université Claude Bernard (Lyon I)
69622 Villeurbanne CEDEX (France)

†On leave from the French Department of Defense, Délégation Générale pour l'Armement.

Astérisque

LEO MURATA

On the magnitude of the least primitive root

Astérisque, tome 198-199-200 (1991), p. 253-257

<http://www.numdam.org/item?id=AST_1991__198-199-200__253_0>

ON THE MAGNITUDE OF THE LEAST PRIMITIVE ROOT

by

Leo MURATA

1. Let p be an odd prime number. We define

$g(p)$ = the least positive integer which is a primitive root mod p,
$G(p)$ = the least prime which is a primitive root mod p.

In most cases, $g(p)$ are very small. For example, among the 19862 odd primes ≤ 223051, $g(p) = 2$ happens for 7429 primes (37.4 %), $g(p) = 3$ happens for 4518 primes (22.8 %), and $g(p) \leq 6$ holds for about 80 % of these primes. And we can support this fact by a probabilistic argument. In fact, for a given prime p, there are $p-1$ invertible residue classes, among which $\varphi(p-1)$ residue classes are primitive modulo p, where φ denotes Euler's totient function. Therefore, on the assumption of good distribution of the primitive residue classes mod p, we can surmise that,

(1) for almost all prime $p, g(p)$ is not very far from $\dfrac{p-1}{\varphi(p-1)} + 1$.

The function $(p-1)/\varphi(p-1)$ fluctuates irregularly, but we can prove the asymptotic formula :

$$\pi(x)^{-1} \sum_{\substack{p \leq x \\ p:\text{prime}}} \frac{p-1}{\varphi(p-1)} = C + O\left(\frac{\log\log x}{\log x}\right), C = \prod_{p:\text{prime}} \left(1 + \frac{1}{(p-1)^2}\right) \doteq 2.827.$$

So, we can guess that

(2) for almost all prime p, $\dfrac{p-1}{\varphi(p-1)}$ is not very far from the constant C ,

and, combining (1) and (2), we can expect that,

(3) for almost all p, $g(p)$ is not very far from the constant $C+1$.

So, it seems very natural to conjecture that, for any monotone increasing positive function $\psi(x)$ tending to $+\infty$, we have an estimate

$$|\{p \leq x \ ; \ g(p) > \psi(p)\}| \ = \ o(\pi(x)). \tag{4}$$

In this direction, we have already a lot of results :

- BURGESS [1] : $g(p) \ll p^{(1/4)+\varepsilon}$, for any $\varepsilon > 0$,
- WANG [12] : under the assumption of the Generalized Riemann Hypothesis (G.R.H.),

$$g(p) \ll (\log p)^2 \omega(p-1)^6 \ ,$$

where $\omega(n)$ denotes the number of distinct prime divisors of n.

- If we take $\psi(x) = C$, the constant function, then we can prove, from MATTHEWS' result about ARTIN's conjecture [10] that, under G.R.H. ,

$$|\{p \leq x \ ; \ g(p) > C\}| \ = \ A_c \pi(x) + o(\pi(x)) \ ,$$

where A_c is a positive constant depending on C, with $0 < A_c \leq 1$.

The last result shows that our conjecture (4) does not hold for the constant function. So, we are interested in the problem, when $\psi(x)$ is a function tends to $+\infty$ rather slowly, is our conjecture (4) true or not ?

Our first result shows that our conjecture is true, under the assumption of G.R.H..

THEOREM 1. ([11]). *We assume G.R.H.. Let $\psi(x)$ be a monotone increasing positive function with the properties*

$$\lim_{x\to\infty} \psi(x) = +\infty, \psi(x) \ll (\log x)^A \text{ for some } A > 0, \psi(x) \ll \psi(x(\log x)^{-1}).$$

Then we have

$$|\{p \leq x \ ; \ G(p) > \psi(p)\}| \ \ll \ \pi(x)(\log \psi(x))^{-1}.$$

This is a result about $G(p)$, but the trivial inequality $g(p) \leq G(p)$ implies that the same estimate still holds for $g(p)$, which verifies (4).

To clarify the contents of our theorem, we take, for example, $\psi(x) = \log\log x$. Then we have $g(p) \leq G(p) \leq \log\log p$, except for $O\left(\frac{\pi(x)}{\log\log\log x}\right)$ primes, whose density is zero.

2. Here we consider the average value of $g(p)$.

It is already proved in 1967 by BURGESS-ELLIOTT [2] that

$$\pi(x)^{-1}\sum_{p\leq x} g(p) \ll (\log x)^2(\log\log x)^4.$$

We can improve this estimate, under G.R.H. , as follows :

THEOREM 2. ([8]). *We assume G.R.H.. Then we have, for any* $\varepsilon > 0$,

$$\pi(x)^{-1}\sum_{p\leq x} g(p) \leq \pi(x)^{-1}\sum_{p\leq x} G(p) \ll (\log x)(\log\log x)^{1+\varepsilon}.$$

Making use of the same argument, we have the following corollary. Let $n_2(p)$ be the least quadratic non-residue mod p, MONTGOMERY proved in 1971 that, under G.R.H., $n_2(p) = \Omega((\log p)(\log\log p))$.

(Remark. Very recently, GRAHAM and RINGROSE proved unconditionally that $n_2(p) = \Omega((\log p)(\log\log\log p))$ cf.[9]). Since $g(p) \geq n_2(p)$, under G.R.H. we have

$$g(p) = \Omega((\log p)(\log\log p)) . \tag{5}$$

Now, we can prove that the primes which satisfy the inequality (5) are rather exceptional :

COROLLARY. *We assume G.R.H.. Let B be an arbitrary positive constant, then we have, for any* $\varepsilon > 0$,

$$|\{p \leq x \ ; \ g(p) \geq B(\log p)(\log\log p)\}| \ll \pi(x)(\log x)^{(-1/2+\varepsilon)},$$

where the constant implied by the $\ll$-symbol depends only on B and ε.

3. We want to think about our problem from a little different point of view. We define

$n_k(p)$ = the least positive integer which is not a k-th power residue mod p,

$r_k(p)$ = the least prime which is a k-th power residue mod p,

then, $n_k(p)$ and $r_k(p)$ have the similar property as $g(p)$ and $G(p)$, respectively. In fact, among $p-1$ invertible residue classes mod p, there are $(1-k^{-1})(p-1)$ classes which are not k-th power residue mod p, and, on the assumption of good distribution of these classes, we can expect that $n_k(p)$ is not very far from the constant $k(k-1)^{-1}+1$, etc. Concerning $n_k(p)$ and $r_k(p)$, more than twenty years ago, ELLIOTT obtained the following asymptotic relations (cf.[3], [4] , see also [5], [6], [7]) :

- If $\delta < 4\ \exp(1-k^{-1})$, then

$$\pi(x)^{-1}\sum_{p\leq x} n_k(p)^\delta \ = \ C_{k,\delta}+o(1), \quad \text{as } x\to+\infty,$$

where $C_{k,\delta}$ is a constant depending only on k and δ.

- If $\delta < 4$, then

$$\pi(x)^{-1}\sum_{p\leq x} r_2(p)^\delta \ = \ D_\delta + O\left(\exp\left(-D\frac{\log\log x}{\log\log\log x}\right)\right)\ ,\ D>0\ ,$$

where D_δ is a constant depending on δ.

- If $k\geq 3$, then there exists a constant $\delta(k)<1$, and for any $\delta<\delta(k)$,

$$\pi(x)^{-1}\sum_{p\leq x} r_k(p)^\delta \ = \ D_{k,\delta}+o(1)\ ,\ \text{as } x\to+\infty. \tag{6}$$

where $D_{k,\delta}$ is a constant depending only on k and δ.

Therefore it seems very natural to seek the same asymptotic formula for the averages of $g(p)^\delta$ and $G(p)^\delta$. And actually, we have

THEOREM 3. ([8]). *We assume G.R.H.. If $\delta<\frac{1}{2}$, then we can prove the asymptotic relation :*

$$\begin{cases} \pi(x)^{-1}\sum_{p\leq x} g(p)^\delta = E_\delta+o(1)\ , \\ \pi(x)^{-1}\sum_{p\leq x} G(p)^\delta = E'_\delta+o(1)\ , \end{cases} \tag{7}$$

where E_δ and E'_δ are constants depending only on δ.

So, in some sense, by Theorem 3 we arrived at the same stage with (6) under the assumption of G.R.H..

The asymptotic relations (7) are likely to be true for $\delta = 1$, but it seems very difficult to prove it, if we assume G.R.H. only.

REFERENCES

[1] BURGESS D.A., The least quadratic non-residue, *Ann.of Math.* (2), **55** (1962), 65-71.

[2] BURGESS D.A.-ELLIOTT P.D.T.A., The average of the least primitive root, *Mathematika*, **15** (1968), 39-50.

[3] ELLIOTT P.D.T.A., A problem of Erdős concerning power residue sums, *Acta Arithmetica*, **13** (1967), 131-149.

[4] ELLIOTT P.D.T.A., Some notes on k-th power residues, *Acta Arithmetica*, **14** (1968), 153-162.

[5] ELLIOTT P.D.T.A., The distribution of primitive roots, *Canadian J. of Math.*, **21** (1969), 822-841.

[6] ELLIOTT P.D.T.A., The distribution of power residues and certain related results, *Acta Arithmetica*, **17** (1970), 141-159.

[7] ELLIOTT P.D.T.A., On the mean value of $f(p)$, *Proc. of London Math. Soc.* (3), **21** (1970), 28-96.

[8] ELLIOTT P.D.T.A.-MURATA L., a paper on "The average of the least primitive root modulo p", in preparation.

[9] GRAHAM S.W. - RINGROSE C.J., *Lower bounds for least quadratic non-residues,* preprint.

[10] MATTHEWS K.R., A generalization of Artin's conjecture for primitive roots, *Acta Arithmetica*, **29** (1976), 113-146.

[11] MURATA L., On the magnitude of the least prime primitive root, to appear, *J. of Number Theory*, **36** (1990).

[12] WANG Y. , On the least primitive root of a prime, *Sci. Sinica*, **10** (1961), 1-14.

Present address :
LEO MURATA
Department of Mathematics
Meiji-gakuin University
1518 Kami-kurata, Totsuka,
Yokohama 244, Japan.

Astérisque

HITOSHI NAKADA
GEROLD WAGNER

Duffin-Schaeffer theorem of diophantine approximation for complex numbers

Astérisque, tome 198-199-200 (1991), p. 259-263
<http://www.numdam.org/item?id=AST_1991__198-199-200__259_0>

Duffin-Schaeffer Theorem of Diophantine Approximation for Complex Numbers

by
Hitoshi Nakada and Gerold Wagner

Let $o(d)$ be the set of integers in $\mathbf{Q}(\sqrt{\mathbf{d}})$ for a square-free negative integer d, that is, $o(d)$ is the set

$$\{n + m\omega : n, m \in \mathbf{Z}\}$$

with

$$\omega = \begin{cases} (1+\sqrt{d})/2 & \text{if } d = 1 \pmod 4 \\ \sqrt{d} & \text{if } d = 2, 3 \pmod 4. \end{cases}$$

We put $I := \{z : z = x + y\omega, 0 \leq x, y < 1\}$ and consider the inequality

$$|z - \frac{a}{r}| \ < \ \frac{f(r)}{|r|}, \ \ (a, r) = 1, \ \ a, r \in o(d) \tag{1}$$

for $z \in I$ with a given non-negative function f defined on $o(d)$. We assume that $f(r) = f(u \cdot r)$ for all units in $o(d)$. We denote by $\Phi(r)$ the Euler function of $\mathbf{Q}(\sqrt{\mathbf{d}})$, which is equal to the number of reduced residual classes mod r and is equal to the number of integers relatively prime to r in $r \cdot I$.

By the Borel-Cantelli lemma, it is easy to see that (1) has only finitely many solutions for almost all $z \in I$ (with respect to Lebesgue measure) if

$$\sum_{r \in o(d)} f^2(r) \cdot \Phi(r)/|r|^2 < \infty.$$

Here, we ask the converse of this : are there infinitely many solutions of (1) for almost all $z \in I$ whenever

$$\sum f^2(r) \cdot \Phi(r)/|r|^2$$

diverges? This is a complex version of Duffin-Schaeffer conjecture [1]. Although the one-dimensional (original) Duffin-Schaeffer conjecture remains unsolved, its higher dimensional analogues (which somehow correspond to our situation) have very recently been settled by Pollington and Vaughan (see

[4]). In the sequel, we give a sufficient condition on f to having infinitely many solutions of (1) for almost all z, which corresponds to Duffin-Schaeffer's theorem.

To prove our complex version, we do not follow the original Duffin and Schaeffer's proof but Sprindžuk's one [5]. Then we also have a complex version of Gallagher's theorem [2].

Theorem 1 *Let A_f be the set of $z(\in I)$, for which (1) has infinitely many solutions. Then we have*

$$\mu(A_f) = 0 \text{ or } 1$$

for any non-negative function f, where μ denotes the normalized Lebesgue measure on I.

By using this theorem, we prove the complex Duffin-Schaeffer theorem :

Theorem 2 *Suppose that*

$$\sum_{r\in o(d)} f^2(r) = \infty \tag{2}$$

and there exist infinitely many $R \in \mathbf{N}$ such that

$$\sum_{|r|<R\,,\, r\in o(d)} f^2(r) < c_1 \cdot \sum_{|r|<R\,,\, r\in o(d)} f^2(r)\cdot \Phi(r)/|r|^2 \tag{3}$$

for some constant $c_1 > 0$. Then (1) has infinitely many solutions for almost all $z \in I$

To prove Theorem1, first we note the following :

Lemma 1 *For any $z \in o(d)$ and $r \in o(d), r \neq 0$, there exists an integer $a \in o(d)$ such that*

$$(i) \quad (r,a) = 1$$

and

$$(ii) \quad |r\cdot z - a| < c(\epsilon)\cdot |r|^{\epsilon}.$$

Here $\epsilon > 0$ is arbitrary and $c(\epsilon)$ is a positive constant depending on ϵ only.

This lemma shows that if there exists a sequence of integers $\{r_n\}$ such that $f(r_n) \gg |r_n|^{\epsilon}$ for some $\epsilon > 0$, then (1) has always a solution for each sufficiently large r_n. Thus we can assume that

$$f(r) \ll |r|^{\epsilon}$$

for any $\epsilon > 0$.

It is easy to prove the following two lemmas (see [5]).

Lemma 2 *Let $I_k, k = 1, 2, \cdots$, be a sequence of disks with $\mu(I_k) \to 0$ as $k \to \infty$, and let A_k be a sequence of measurable subsets for which $A_k \subset I_k$ and*

$$\mu(A_k) > \delta \cdot \mu(I_k), \quad k = 1, 2, \cdots,$$

for some $\delta > 0$. Then we have

$$\mu(\cap_{l=1}^{\infty} \cup_{k=l}^{\infty} I_k) = \mu(\cap_{l=1}^{\infty} \cup_{k=l}^{\infty} A_k).$$

Lemma 3 *For every q and s in $o(d)$ with $|q| > 1$, the transformation $T : z \to q \cdot z + s/q \pmod{o(d)}$ of I onto itself is ergodic, that is, if a measurable subset of I is T-invariant, then its Lebesgue measure is 0 or 1 (in the normalized sense).*

Sketch of proof of Theorem 1 We consider a rational integer p which is prime in $o(d)$. Then we follow the proof of Theorem 7 of Sprindžuk[5]. Since there are infinitely many prime integers, we have the desired result.

Now, to prove Theorem 2, we only need to show that

$$\mu(A_f) > 0$$

when (2) and (3) hold. For this, we use the following Lamperti-Rényi's lemma.

Lemma 4 *Let (Ω, B, P) be a probability space. Suppose that $\{A_n\}$ be a sequence of measurable subsets with*

$$\sum P(A_n) = \infty \tag{4}$$

If there exists a subsequence $\{n_m\}$ such that

$$\sum_{k=1}^{n_m} \sum_{l=1}^{n_m} P(A_k \cap A_l) \ll \left[\sum_{k=1}^{n_m} P(A_k)\right]^2 \text{ as } m \to \infty, \tag{5}$$

then

$$P(\cap_{l=1}^{\infty} \cup_{k=l}^{\infty} A_k) > 0.$$

Sketch of proof of Theorem 2 We assume that f is bounded. We put

$$A_r := \{z \in I : \text{there is an integer } a \in o(d) \text{ such that}$$

$$(a, r) = 1 \text{ and } |z - a/r| < f(r)/r\}.$$

Since A_r is the union of $\Phi(r)$ open disks with the radii $f(r)/|r|$, intersected with I, we see that

$$c_2 \cdot \Phi(r) \cdot f^2(r)/|r|^2 < \mu(A_r) < c_3 \cdot \Phi(r) \cdot f^2(r)/|r|^2 \tag{6}$$

for some constants $c_2 > 0$ and $c_3 > 0$. Now we estimate $\mu(A_{r_1} \cap A_{r_2})$ for $|r_1| < |r_2|$. Then we can show that

$$\mu(A_{r_1} \cap A_{r_2}) < c_4 \cdot f^2(r_1) \cdot f^2(r_2)$$

for a constant $c_4 > 0$. From this inequality with (2),(3) and (6), we see that $\{A_r\}$ satisfies (4) and (5). This proves Theorem 2 when f is bounded. Because of the property (3), there exists a set A of integers such that on A $f(r) > 0$, $\Phi(r)/|r|^2 > c_5$ for a constant $c_5 > 0$ and $\sum f^2(r) = \infty$ where r runs over A. Then it is easy to see that the above method holds for unbounded case by cutting f and this completes the proof of Theorem 2.

Remark Let $\{a_n/r_n\}$ be the sequence of solutions of (1) with

$$|r_1| \leq |r_2| \leq \cdots.$$

We suppose that $f(r) = \theta/|r|$ for a positive constant θ. We put

$$\eta_n := r_n^2 \cdot |z - a_n/r_n|/\theta.$$

Then, by using a geometrical method (see [3]), we can show that $\{\ \eta_n\ \}$ is uniformly distributed in the unit disk for almost all z. In general, it is not so hard to see that $\{\ \arg\ (z - a_n/r_n)\ \}$ is dense (mod 2π) for almost all z when $\mu(A_f) > 0$. One may ask whether this is uniformly distributed. If we make some additional conditions on f (see [5]), then we may estimate the asymptotic number of solutions of (1) and this gives the answer of this question. We will discuss these facts in another occasion.

The first author would like to dedicate this paper to the memory of G. Wagner, who was killed in March 1990, after this paper had been submitted for publication, by an avalanche while skiing in the Alps.

References

[1] DUFFIN, R.J. AND A.C.SCHAEFFER, *Khintchine's problem in metric diophantine approximation,* Duke Math.J., 8(1941), pp. 243-255.

[2] GALLAGHER, P.X., *Approximation by reduced fractions,* J. Math. Soc. Japan, 13(1961),pp. 342-345.

[3] NAKADA,H., *On metrical theory of diophantine approximation over imaginary quadratic field,* Acta Arith., 51(1988), 393-403.

[4] POLLINGTON,A.D. AND R.C. VAUGHAN, *The k-dimensional Duffin and Schaeffer conjecture,* Séminaire de Théorie des Nombres Bordeaux, ser.2, 1(1989) , 81-87.

[5] SPRINDŽUK, V.G., *Metric theory of diophantine approximations,* V.H.Winston & Sons, Washington, D.C., 1979.

Hitoshi Nakada
Dept. of Math., Keio University
Hiyoshi 3-14-1, Kohoku, Yokohama 223
Japan

Gerold Wagner
Math. Inst., University of Stuttgart
Pfaffenwaldring 57, D-7000 Stuttgart 80
FRG

Astérisque

JOHAN PAS

Some applications of uniform p-adic cell decomposition

Astérisque, tome 198-199-200 (1991), p. 265-271

<http://www.numdam.org/item?id=AST_1991__198-199-200__265_0>

SOME APPLICATIONS OF UNIFORM p-ADIC CELL DECOMPOSITION

JOHAN PAS[1]
K.U. Leuven

In this paper we summarize some applications of uniform p-adic cell decomposition. The technique of p-adic cell decomposition was developed by Denef [**3,4**], using ideas of Cohen [**2**]. Denef gave two applications of his theorem. A first one was an elementary proof of Macintyre's quantifier elimination for p-adic fields; a second one was a proof of the rationality of the Igusa local zeta function without using Hironaka's resolution of singularities.

Denef's cell decomposition theorem holds for every p-adic field but the decomposition procedure depends on the particular field. In [**13**] and [**14**] we obtain cell decomposition theorems which are uniform in a certain class of p-adic fields. In [**13**] we prove a cell decomposition for a class of henselian valued fields of equicharacteristic zero. By the use of an ultraproduct construction, this provides a decomposition which is uniform, for almost all p, in the class $\{\mathbf{Q}_p\}_{p \text{ prime}}$ of all fields of p-adic numbers. The cell decomposition proved in [**14**] is uniform in the class of all finite unramified extensions of the field $\mathbf{Q}_p$ (with p a fixed prime number). Macintyre [**10**] obtained independently a different cell decomposition which is also uniform in these classes of fields.

The basic idea of cell decomposition is that, given a p-adic field K and a polynomial $f(x)$ with $x = (x_1, \ldots, x_m)$, one can partition K^m into

[1] Research Assistant of the National Fund of Scientific Research (Belgium)

so-called cells, such that on each of these cells the function $f(x)$ takes, in a certain sense, a simpler form. The precise meaning of 'simpler' here is determined by the formalism (defined by a first order language for p-adic fields) in which one proves the cell decomposition theorem. The use of uniform cell decomposition allows one to simplify, uniformly, formulas in the first order language and to obtain a quantifier elimination in this language which is uniform in the class of fields. This is formulated more precisely in section 1. A second application of cell decomposition is the computation of certain p-adic integrals on definable sets. Cell decomposition enables one to partition definable sets in simpler parts for which the integral can be computed. The results here are stated in section 2.

Section 1
Quantifier elimination

We define the first order language $\mathcal{L}$, in which we prove the cell decomposition for valued fields of equicharacteristic zero, and in which we obtain quantifier elimination. The language $\mathcal{L}$ is a language with three sorts of variables, namely variables for the elements of the valued field, variables for elements of the residue field and variables for elements of the value group. The language contains symbols for the standard field operations in the valued field and in the residue field, and symbols for the usual operations in the value group. One also has a function symbol for the valuation map from the field to the value group, and another function symbol for an angular component map modulo P from the field to the residue field. Such an angular component map modulo P is a multiplicative morphism from the group of units of the valued field to the group of units of the residue field, such that the restriction of this morphism to the set of elements of valuation zero is the canonical projection onto the

residue field.

Cell Decomposition Theorem 3.2 of [**13**] implies

THEOREM. ([**13**] Theorem 4.1) *Let K be a henselian valued field of equicharacteristic zero which has an angular component map modulo P. Then K has elimination of field quantifiers in the language $\mathcal{L}$.*

Applying this to ultraproducts $\prod \mathbf{Q}_p/\mathcal{D}$ where $\mathcal{D}$ is a non-principal ultrafilter on the index set of prime numbers we obtain a uniform quantifier elimination for the fields of p-adic numbers.

COROLLARY. ([**13**] Corollary 4.3) *Let φ be a formula in $\mathcal{L}$. Then there exists an $\mathcal{L}$-formula ψ (which is independent of p) without field quantifiers, such that, for almost all primes p, we have*

$$\varphi \longleftrightarrow \psi \qquad \text{on } \mathbf{Q}_p.$$

Section 2
Poincaré series and Igusa local zeta functions

Let $h(x)$ be a polynomial in m variables $x = (x_1, \ldots, x_m)$ over $\mathbf{Z}$, and let K be a finite field extension of $\mathbf{Q}_p$ for some prime number p, such that K is unramified over $\mathbf{Q}_p$, that is, p is a generator for the maximal ideal of the valuation ring R of K. Suppose that the residue field of K has cardinality q. The valuation on K is denoted by $|.|$ and normalized by $|p| = 1/q$.

For every $n \in \mathbf{N}$ we consider the number of solutions of the congruence $h(x) \equiv 0 \bmod p^n$ in R,

$$N(n, K) = \text{Card}\{\, x \bmod p^n \mid x \in R^m, h(x) \equiv 0 \bmod p^n \,\}.$$

The generating function of this sequence

$$P(T, K) = \sum_{n=0}^{\infty} N(n, K)\, T^n$$

is called a *Poincaré series* associated to the polynomial h. Borevich and Shafarevich [1] conjectured that this series is a rational function of T. This conjecture was first proved by Igusa [8,7] using Hironaka's resolution of singularities.

Another type of Poincaré series for h is the series associated to the p-adic points on the variety $h = 0$. Put for $n \in \mathbf{N}$,

$$\widetilde{N}(n, K) = \text{Card}\{\, x \bmod p^n \mid x \in R^m,\ h(x) = 0 \,\},$$

and

$$\widetilde{P}(T, K) = \sum_{n=0}^{\infty} \widetilde{N}(n, K)\, T^n.$$

This series was studied by Oesterlé [12] and Serre [16]. Denef [3] proved that $\widetilde{P}(T, K)$ is a rational function of T.

A first step in the rationality proofs for these Poincaré series, is to relate the series to a certain p-adic integral. For the first series $P(T, K)$ this integral is the so-called *Igusa local zeta function* of h, which is defined as

$$Z(s, K) = \int_{R^m} |h(x)|^s\, |dx| \qquad \text{for } s \in \mathbf{R},\ s > 0, \tag{1}$$

where $|dx|$ is the Haar measure on K^m normalized on R^m. The relation of this integral with the Poincaré series $P(T, K)$ is given by

$$Z(s, K) = \frac{1 + (T - 1)\, P(q^{-m} T)}{T} \qquad \text{for } T = q^{-s}. \tag{2}$$

For $\widetilde{P}(T, K)$ the corresponding integral is

$$I(s, K) = \int_D |w|^s\, |dx|\, |dw| \qquad \text{for } s \in \mathbf{R},\ s > 0,$$

where

$$D = \{\, (x, w) \in R^m \times R \mid \exists\, y \in R^m \ :\ x \equiv y \bmod w \text{ and } h(y) = 0 \,\}.$$

Here we have

$$I(s,K) = \frac{q-1}{q}\widetilde{P}(q^{-(m+1)}T, K) \qquad \text{for } T = q^{-s}. \tag{3}$$

We now want to study the behaviour of these Poincaré series if the field K varies in the class of all fields of p-adic numbers $\{\mathbf{Q}_p\}_{p \text{ prime}}$. By relations (2) and (3) it suffices to study the behaviour of p-adic integrals of the form

$$J(s,K) = \int_W |h(x)|^s \, |dx|,$$

where W is the subset of K^m defined by a formula ψ in the language $\mathcal{L}$.

For this kind of integrals we proved, using the uniform cell decomposition theorem, that if K varies in the class $\{\mathbf{Q}_p\}_{p \text{ prime}}$, the denominator of $J(s,K)$ as a rational function in p^{-s} does not depend on p and the degree of the numerator is bounded independently of p.

THEOREM. ([13] Theorem 5.1) *Let $h(x) \in \mathbf{Z}[x]$ with $x = (x_1, \ldots, x_m)$. Let ψ be an $\mathcal{L}$-formula with free field variables $x_1, \ldots, x_m$. Suppose that $W_p = \{ x \in \mathbf{Q}_p^m \mid \psi(x) \text{ holds} \}$ is bounded for all p. Consider*

$$J(s, \mathbf{Q}_p) = \int_{W_p} |h(x)|^s \, |dx|.$$

Then

$$J(s, \mathbf{Q}_p) = \frac{R_p(T)}{Q(p,T)} \qquad \text{with } T = p^{-s},$$

where (i) *the denominator $Q(p,T)$ is a rational function in p and T, which is a product of factors of the form T, p, or $1 - p^a T^b$ $(a, b \in \mathbf{Z})$;*

(ii) *for every p, $R_p(T)$ is a polynomial in T such that $\deg R_p(T)$ is bounded independently of p.*

The same result holds for the Poincaré series $P(T, \mathbf{Q}_p)$ and $\widetilde{P}(T, \mathbf{Q}_p)$ by (2) and (3).

We were not able to obtain more information on how the numerators $R_p(T)$ depend on the prime p. This problem is probably much more difficult since the coefficients of $R_p(T)$ are related to the number of points on a variety over the finite field $\mathbf{F}_p$ (which is the residue field of $\mathbf{Q}_p$).

We now consider the class of all unramified extension of $\mathbf{Q}_p$ with p a fixed prime number. Since for every $d \in \mathbf{N}$, $d > 0$, there is a unique unramified extension K_d of $\mathbf{Q}_p$ of degree d, we can denote this class by $\{K_d\}_{d\in\mathbf{N},d>0}$. The first order language $\mathcal{L}'$ used in this case is similar to the language $\mathcal{L}$, but here we have to include additional sorts for the residue rings modulo p^n, due to the non-zero characteristic of the residue fields. From Cell Decomposition Theorem 3.2 of [**14**], which is uniform in the class $\{K_d\}_{d\in\mathbf{N},d>0}$, we obtain a result for $J(s, K_d)$ ($d \in \mathbf{N}$, $d > 0$) which is similar to the previous theorem for $J(s, \mathbf{Q}_p)$ (p prime). However the residue field of K_d is the field with p^d elements $\mathbf{F}_{p^d}$. Since the variation with d of the number of points on a variety over $\mathbf{F}_{p^d}$ is known by Dwork's theorem [**6**], we are able to determine more precisely how the numerator of $J(s, K_d)$ depends on d.

THEOREM. ([**15**] Theorem 2.3) *Let $h(x) \in \mathbf{Z}[x]$ with $x = (x_1, \ldots, x_m)$. Let ψ be an $\mathcal{L}'$-formula with free field variables $x_1, \ldots, x_m$. Suppose that $W_d = \{ x \in K_d^m \mid \psi(x) \text{ holds } \}$ is bounded for all d. Consider*

$$J(s, K_d) = \int_{W_d} |h(x)|^s \, |dx|.$$

Then there exist a positive integer d_0, complex numbers $\lambda_1, \ldots, \lambda_t$ and polynomials G, $H \in \mathbf{Z}[T, X_1, \ldots, X_t]$ such that, for $d \geq d_0$,

$$J(s, K_d) = \frac{G(T, p^{d\lambda_1}, \ldots, p^{d\lambda_t})}{H(T, p^{d\lambda_1}, \ldots, p^{d\lambda_t})}, \qquad \text{with } T = p^{-ds}.$$

Meuser [**11**] calls such a function an *invariant function* of the sequence $\{K_d\}_{d\in\mathbf{N},d>0}$. She proved the above theorem for the Igusa local zeta function (see display (1)). In this case $d_0 = 1$.

REFERENCES

1. S.E. Borevich, I.R. Shafarevich, "Zahlentheorie," Birkhäuser, Basel–Stuttgart, 1966.
2. P.J. Cohen, *Decision procedures for real and p-adic fields*, Comm. Pure Appl. Math. **22** (1969), 131–151.
3. J. Denef, *The rationality of the Poincaré series associated to the p-adic points on a variety*, Invent. Math. **77** (1984), 1–23.
4. ———, *p-adic semi-algebraic sets and cell decomposition*, J. Reine Angew. Math. **369** (1986), 154–166.
5. ———, *On the degree of Igusa's local zeta function*, Amer. J. Math. **109** (1987), 991-1008.
6. B. Dwork, *On the rationality of the zeta function of an algebraic variety*, Amer. J. Math. **82** (1960), 631–648.
7. J.-I. Igusa, *Complex powers and asymptotic expansions I*, J. Reine Angew. Math. **268/269** (1974), 110–130; *II*, ibid. **278/279** (1975), 307–321.
8. ———, *Some observations on higher degree characters*, Amer. J. Math. **99** (1977), 393–417.
9. A. Macintyre, *On definable subsets of p-adic fields*, J. Symbolic Logic **41** (1976), 605–610.
10. ———, *Rationality of p-adic Poincaré series : uniformity in p*, Ann. Pure Appl. Logic (to appear).
11. D. Meuser, *The meromorphic continuation of a zeta function of Weil and Igusa type*, Invent. Math. **85** (1986), 493–514.
12. J. Oesterlé, *Réduction modulo p^n des sous-ensembles analytiques fermés de $\mathbf{Z}_p^N$*, Invent. Math. **66** (1982), 325–341.
13. J. Pas, *Uniform p-adic cell decomposition and local zeta functions*, J. Reine Angew. Math. **399** (1989), 137–172.
14. ———, *Cell decomposition and local zeta functions in a tower of unramified extensions of a p-adic field*, Proc. London Math. Soc. **60** (1990).
15. ———, *Igusa local zeta functions and Meuser's invariant functions*, preprint.
16. J.-P. Serre, *Quelques applications du théorème de densité de Chebotarev*, Publ. Math. IHES **54** (1981), 123–202.

1980 *Mathematics subject classifications*: 03C10, 11S40, 11U09

Wiskundig Instituut
Katholieke Universiteit Leuven
Celestijnenlaan 200-B
3030 Heverlee
BELGIUM

e-mail : fgaba03 at blekul11.bitnet

Astérisque

ROLAND QUÊME

On diophantine approximation by algebraic numbers of a given number field : a new generalization of Dirichlet approximation theorem

Astérisque, tome 198-199-200 (1991), p. 273-283

<http://www.numdam.org/item?id=AST_1991__198-199-200__273_0>

ON DIOPHANTINE APPROXIMATION BY ALGEBRAIC NUMBERS OF A GIVEN NUMBER FIELD : A NEW GENERALIZATION OF DIRICHLET APPROXIMATION THEOREM

by

Roland QUÊME

Introduction

It is well known that for all $\alpha \in \mathbb{R}$, $\alpha \notin \mathbb{Q}$ there are infinitely many p/q, $|p|$, $q \in \mathbb{N}$ such that $|\alpha - p/q| < 1/q^2$ (Dirichlet theorem), and that for any real algebraic number $\alpha \notin \mathbb{Q}$ and for any $\varepsilon \in \mathbb{R}$, $\varepsilon > 0$, there exist only finitely many p/q, $|p|$, $q \in \mathbb{N}$ such that $|\alpha - p/q| < 1/q^{2+\varepsilon}$ (Roth theorem).

Let K be a number field of degree n, signature (r, s) and absolute value of discriminant D.
Let B be the Minkowski constant of K ($B = (4/\pi)^s \,.\, (n!/n^n) \,.\, \sqrt{D}$).
Let $\sigma : K \to \mathbb{R}^r \times \mathbb{C}^s$ be the embedding defined by :

$$\sigma(\rho) = (\sigma_1(\rho), \ldots, \sigma_r(\rho), \sigma_{r+1}(\rho), \ldots, \sigma_{r+s}(\rho))$$

where, as usually, $K = \sigma_1(K)$.

For $x, y \in \mathbb{R}^r \times \mathbb{C}^s$ we note $x = (x_j,\ j = 1, \ldots, r+s)$. Then we note $x + y = (x_j + y_j,\ j = 1, \ldots, r+s)$ and $x.y = (x_j.y_j,\ j = 1, \ldots, r+s)$.
We define, for $x \in \mathbb{R}^r \times \mathbb{C}^s$, the distance function and the norm function :

$$d(x) = |x_1| + \cdots + |x_r| + 2|x_{r+1}| + \cdots + 2|x_{r+s}|,$$
$$N(x) = |x_1| \cdots |x_r| . |x_{r+1}|^2 \cdots |x_{r+s}|^2 \ .$$

Let A be the ring of integers of K.

Then we obtain the diophantine approximation theorems :

(i) For $\alpha \in \mathbb{R}^r \times \mathbb{C}^s - \sigma(K)$, there exist infinitely many $\beta = p/q$, $p, q \in A$ such that $0 < d(\alpha\sigma(q) - \sigma(p)) < n^2 . B^{2/n}/d(\sigma(q))$, with arbitrary large distance $d(\sigma(q))$.

(ii) For $\alpha \in \mathbb{R}^r \times \mathbb{C}^s$, $\alpha_j \notin \sigma_j(K)$, $j = 1, 2, \ldots, r+s$, there exist infinitely many $\beta = p/q$, $p, q \in A$ such that $0 < N(\alpha - \sigma(p/q)) < (B/N_{K/\mathbb{Q}}(q))^2$.

We first summarize the state of the art with three types of generalizations found in the quoted literature for diophantine approximation by numbers of a given number field K. Let K be a number field of degree n, signature (r, s). For $\beta \in K$, let $P(\beta)$ be the field polynomial of β,

$$P(\beta) = (x - \sigma_1(\beta)) \cdots$$
$$(x - \sigma_r(\beta))(x - \sigma_{r+1}(\beta))(\overline{x - \sigma_{r+1}(\beta)}) \cdots (x - \sigma_{r+s}(\beta))(\overline{x - \sigma_{r+s}(\beta)}) .$$

Let $C \in \mathbb{N}$ such that $P_1(\beta) = CP(\beta) = b_n\beta^n + \cdots + b_1\beta + b_0$ is a polynomial with integer coprime coefficients b_i, $i = 0, 1, \ldots, n$. Then we define the height of $\beta \in K$ by $H_K(\beta) = \sup_{i=0,\ldots,n} |b_i|$.

The first generalization of Dirichlet theorem found in bibliography is :

Assume that $r > 0$ and choose a real embedding $\sigma_1 : K \to \mathbb{R}$. For every $\alpha \in \mathbb{R} - \sigma_1(K)$, then there exist infinitely many $\beta \in K$ such that $|\alpha - \sigma_1(\beta)| < C_1(K)\max(1, \alpha^2)/H_K(\beta)^2$ where $C_1(K)$ is a constant depending only on K (see SCHMIDT [8] p.253).

The second generalization of Dirichlet theorem is :

Assume that $s > 0$ and choose a complex embedding $\sigma_2 : K \to \mathbb{C}$. For every $\alpha \in \mathbb{C} - \sigma_2(K)$, then there exist infinitely many $\beta \in K$ such that $|\alpha - \sigma_2(\beta)| < C_2(K)/H_K(\beta)$ where $C_2(K)$ is a constant depending only on K (see SCHMIDT [6] p.206).

The third generalization is :

Let $\beta_1, \ldots, \beta_\ell \in K$; let $\mathfrak{b}$ be the fractional ideal of K generated by $(1, \beta_1, \ldots, \beta_\ell)$.

We define the generalized height of the ℓ-tuple $(\beta_1, \ldots, \beta_\ell)$ by :

$$\mathfrak{h}_K(\beta_1, \ldots, \beta_\ell) = N_{K/\mathbb{Q}}(\mathfrak{b}) \prod_{j=1}^{r} \max(1, |\sigma_j(\beta_1)|, \ldots, |\sigma_j(\beta_\ell)|) \prod_{j=r+1}^{r+s} \max(1, |\sigma_j(\beta_1)|, \ldots, |\sigma_j(\beta_\ell)|)^2.$$

(i) if $r > 0$, let $\sigma_3 : K \to \mathbb{R}$ be a real embedding and $\alpha_1, \ldots, \alpha_\ell \in \mathbb{R}$, not all in $\sigma_3(K)$; put in that case $\nu = 1$;

(ii) if $s > 0$, let $\sigma_3 : K \to \mathbb{C}$ be a complex embedding and $\alpha_1, \ldots, \alpha_\ell \in \mathbb{C}$, not all in $\sigma_3(K)$; put in that case $\nu = 2$;

then there is a constant $C_3(K, \alpha_1, \ldots, \alpha_\ell)$ depending only on $K, \alpha_1, \ldots, \alpha_\ell$ such that there exist infinitely many $\beta = (\beta_1, \ldots, \beta_\ell)$, $\beta_i \in K$, with

$$|\alpha_i - \sigma_3(\beta_i)|^\nu < C_3(K, \alpha_1, \ldots, \alpha_\ell).\mathfrak{h}_K(\beta_1, \ldots, \beta_\ell)^{-1-1/\ell}, \; i = 1, 2, \ldots, \ell \qquad (1)$$

(see SCHMIDT [7] p.2).

The main difference between the quoted formulation and our theorem are summarized in the four next points :

1) In classical approximations above, $|\alpha - \beta|$ is obtained for *one* of the conjugates $\beta = \sigma_1(\beta)$. On the other hand, our estimate involves simultaneously *all* the conjugates of the same $\beta \in K$,

for the distance function,

$$d(\alpha\sigma(q) - \sigma(p)) = |\alpha_1\sigma_1(q) - \sigma_1(p)| + \cdots + |\alpha_r\sigma_r(q) - \sigma_r(p)| + 2|\alpha_{r+1}\sigma_{r+1}(q) - \sigma_{r+1}(p)| + \cdots + 2|\alpha_{r+s}\sigma_{r+s}(q) - \sigma_{r+s}(p)|$$

for the norm function,

$$N(\alpha - \sigma(p/q)) = |\alpha_1 - \sigma_1(p/q))| \cdots |\alpha_r - \sigma_r(p/q)|.|\alpha_{r+1} - \sigma_{r+1}(p/q)|^2 \cdots |\alpha_{r+s} - \sigma_{r+s}(p/q)|^2.$$

2) Our approximation theorem cannot be immediately connected to usual simultaneous approximation theorems, because in simultaneous approximation $|f(\alpha_1 - \beta_1)|, \ldots, |f(\alpha_\ell - \beta_\ell)|$ the simultaneous approximations $\beta_1, \ldots, \beta_\ell$ are not conjugate of the same $\beta \in K$ (see for instance (1)).

3) Our result contains not only effective but *explicit* constants with *simple* relationship to the structure of the number fields (the Minkowski constant for instance, with the distance function choosen).

4) Our proof is the exact generalization of the approximation by $\mathbb{Q}$ to approximation by a given number field K, using geometry of numbers properties of number fields embedding in $\mathbb{R}^n$.

Acknowledgments are due to Professors DUBOIS, GYÖRY, LEUTBECHER, SCHLICKEWEI and TOFFIN for helpful remarks which allowed me to write this new version of this note.

Prerequisites-Notations

K : number field

n : degree of K

(r, s) : signature of K

x : $x \in \mathbb{R}^r \times \mathbb{C}^s$, $x = (x_j \mid j = 1, \ldots, r+s)$

$x + y$: $x + y = (x_j + y_j \mid j = 1, \ldots, r+s)$

$x.y$: $x.y = (x_j.y_j \mid j = 1, \ldots, r+s)$

$d(x)$: for $x \in \mathbb{R}^r \times \mathbb{C}^s$, the distance function is defined by :

$$d(x) = |x_1| + \cdots + |x_r| + 2|x_{r+1}| + \cdots + 2|x_{r+s}|$$

$N(x)$: for $x \in \mathbb{R}^r \times \mathbb{C}^s$, the norm form is defined by :

$$N(x) = |x_1| \cdots |x_r| . |x_{r+1}|^2 \cdots |x_{r+s}|^2$$

$U(o, \tau)$: for $\tau \in \mathbb{R}_+$, convex body of $\mathbb{R}^n$ defined by

$$U(o, \tau) = \{x \mid x \in \mathbb{R}^r \times \mathbb{C}^s, d(x) < n\tau\}$$

where $\mathbb{R}^r \times \mathbb{C}^s$ is isomorphically identified to $\mathbb{R}^n$ by

$$x_{r+i} = (R(x_{r+i}), I(x_{r+i})) \ , \ i = 1, \ldots, s \ ,$$

where R and I are the real and imaginary part.

The volume of $U(o,\tau)$ is $v(U(o,\tau)) = 2^r(\pi/2)^s n^n \tau^n/n!$

(see for instance SAMUEL [5] p.70).

A : ring of algebraic integers in K.

$\sigma(A)$: embedding of A in $\mathbb{R}^r \times \mathbb{C}^s$ defined, for $a \in A$, by

$$\sigma(a) = (\sigma_1(a), \ldots, \sigma_r(a), \sigma_{r+1}(a), \ldots, \sigma_{r+s}(a))$$

where $\mathbb{R}^r \times \mathbb{C}^s$ is isomorphically identified to $\mathbb{R}^n$ by

$$\sigma_{r+i}(a) = (R(\sigma_{r+i}(a)), I(\sigma_{r+i}(a))).$$

$\sigma(A)$ is a lattice.

D_0 : Let $w_1, \ldots w_n \in A$ such that $\sigma(w_1), \ldots, \sigma(w_n)$ is a basis of the lattice $\sigma(A)$.

we define classically the fundamental domain D_0 by :

$$D_0 = \{x \mid x \in \mathbb{R}^r \times \mathbb{C}^s \ , \ x = u_1\sigma(w_1) + \cdots + u_n\sigma(w_n) \ , \ 0 \leq u_i < 1\}.$$

$D(\sigma(a))$: fundamental domain of $\sigma(A)$ deduced from the fundamental domain D_0 by the translation $0 \to \sigma(a)$:

$$D(\sigma(a)) = \{(y_j) \in \mathbb{R}^r \times \mathbb{C}^s \ |(y_j - \sigma_j(a))| \ j = 1, \ldots, r+s) \in D_0\}.$$

Results

THEOREM 1. *Let K be a number field of degree n, signature (r,s), and absolute value of discriminant D. Let B be the Minkowski bound of K $(B = (4/\pi)^s.(n!/n^n).\sqrt{D})$. Let A be the ring of integers of K.*
Let $\alpha \in \mathbb{R}^r \times \mathbb{C}^s - \sigma(K)$. Then, for any $m \in \mathbb{R}$, $m > 0$, there are infinitely many different $\beta = p/q$ where $p, q \in A$, such that $d(\sigma(q)) > m$ and

$$0 < d(\alpha.\sigma(q) - \sigma(p)) < (n^2.B^{2/n})/d(\sigma(q)).$$

Proof :

1) Let $\varepsilon \in \mathbb{R}$, $\varepsilon > 0$,

$$\lambda = (1+2\varepsilon)^{1/n}.B^{2/n}/2 = (1+2\varepsilon)^{1/n}.(n!/n^n)^{2/n}.(4/\pi)^{(2s)/n}.D^{1/n}/2.$$

Let $m \in \mathbb{R}_+$, arbitrary large and $\mu = \lambda m^{-1/n}$.
Consider the set $E = U(o, m^{1/n}) \cap \sigma(A)$ where U and σ have the meaning of notations paragraph. From $v(U(o, m^{1/n})) = 2^r(\pi/2)^s n^n m/n!$ and $v(D(o)) = 2^{-s}\sqrt{D}$, we deduce

$$t = \text{Card } (E) = (2^r(\pi/2)^s n^n m)/(n!2^{-s}\sqrt{D}) + O(m^{1-1/n}).$$

Therefore, for m sufficiently large, we have $t > \{2^r \pi^s n^n m/(n!\sqrt{D})\}.\{1-\varepsilon\}$. For any $a \in A$, for all $q_i \in A$ with $\sigma(q_i) \in E$, it is possible to define $p_i(a) \in A$ and $\rho_i(a) \in \mathbb{R}^r \times \mathbb{C}^s$, $i = 1, 2, \ldots, t$, such that $\rho_i(a) = \alpha\sigma(q_i) - \sigma(p_i(a))$, $i = 1, 2, \ldots, t$ and $\rho_i(a) \in D(\sigma(a))$. Notice that the approximation function $d(x)$ is meaningful because $d(\alpha\sigma(q) - \sigma(p)) = 0$ leads to $p = q = 0$: from the definition of $d(x)$, $d(\alpha\sigma(q) - \sigma(p)) = 0$ implies $\alpha_j\sigma_j(q) - \sigma_j(p) = 0$, $j = 1, \ldots, r+s$, and thus $\alpha_j = \sigma_j(p/q)$, $j = 1, \ldots, r+s$ and therefore $\alpha \in \sigma(K)$, which is in contradiction with hypothesis. Thus the $\rho_i(a)$, $i = 1, \ldots, t$, are different each others.

Consider the set $G = \{U(\rho_i(a), \mu/2) \mid i = 1, 2, \ldots, t \ , \ \forall a \in A\}$. G cannot be a packing of $\mathbb{R}^n$ (for packing definition, see for instance LEKKERKERKER [2] p.169) because

$$tv(U(o, \mu/2)) > \{(1-\varepsilon)2^r\pi^s n^n m/(n!\sqrt{D})\}.$$
$$\{2^r(\pi/2)^s n^n(1+2\varepsilon)(n!/n^n)^2(4/\pi)^{2s} D m^{-1}/(2^n 2^n n!)\}$$
$$tv(U(o, \mu/2)) > (1-\varepsilon)(1+2\varepsilon)2^{-s}\sqrt{D} > v(D(o)).$$

Therefore, for m sufficiently large, there exist $\rho_i(a)$ and $\rho_{i'}(b)$ with

$$\rho_i(a) = \alpha\sigma(q_i) - \sigma(p_i(a)) \tag{1}$$
$$\rho_{i'}(b) = \alpha\sigma(q_{i'}) - \sigma(p_{i'}(b)) \tag{2}$$

such that $U(\rho_i(a), \mu/2) \cap U(\rho_{i'}(b), \mu/2) \neq \emptyset$.

Then $d(\rho_i(a) - \rho_{i'}(b)) < n\mu$ from the definition of the convex set $U(\rho(a), \mu/2)$.
Let $p = p_i(a) - p_{i'}(b)$, $p \in A$ and $q = q_i - q_{i'}$, $q \in A$. Then, from the value of μ, we deduce

$$d(\alpha\sigma(q) - \sigma(p)) < n\mu = (n(1+2\varepsilon)^{1/n}.B^{2/n}/2)m^{-1/n}. \tag{2'}$$

Consider the sequence of values of ε defined by $\varepsilon_1 = 1$, $\varepsilon_2 = 1/2, \ldots, \varepsilon_k = 1/k, \ldots$ Therefore, for m given, for any ε_k there exist $p(\varepsilon_k)$, $q(\varepsilon_k) \in A$ such that

$$d(\alpha\sigma(q(\varepsilon_k)) - \sigma(p(\varepsilon_k))) < (nB^{2/n}/2).m^{-1/n}.(1 + 2\varepsilon_k)^{1/n}. \qquad (2'')$$

From $\sigma(q(\varepsilon_k)) \in 2E$, we deduce that $d(\sigma(q(\varepsilon_k)))$ is bounded above independently of ε_k. From inequality $(2'')$, we then deduce that $d(\sigma(p(\varepsilon_k))$ is also bounded above independently of ε_k. Like $\sigma(A)$ is a lattice, it is possible to take out an infinite subsequence $k_1, k_2, \ldots, k_j$ such that $p(\varepsilon_{k_1}) = p(\varepsilon_{k_2}) = \cdots = p(\varepsilon_{k_j}) = p$ and $q(\varepsilon_{k_1}) = q(\varepsilon_{k_2}) = \cdots = q(\varepsilon_{k_j}) = q$ and then

$$d(\alpha\sigma(q) - \sigma(p)) \leq (nB^{2/n}/2)m^{-1/n}. \qquad (3)$$

From $\sigma(q_i) \in E$ in (1), we have $d(\sigma(q_i)) < nm^{1/n}$,
From $\sigma(q_{i'}) \in E$ in (2), we have $d(\sigma(q_{i'})) < nm^{1/n}$,
and thus $d(\sigma(q)) < 2nm^{1/n}$ or $m^{-1/n} < 2n/d(\sigma(q))$.

We then have from (3)

$$d(\alpha\sigma(q) - \sigma(p)) < (nB^{2/n}/2)(2n/d(\sigma(q)))$$
$$d(\alpha\sigma(q) - \sigma(p)) < n^2B^{2/n}/d(\sigma(q)) \; . \qquad (3')$$

2) We shall now prove that there are infinitely many different $\beta = p/q$ with

$$d(\alpha\sigma(q) - \sigma(p)) < n^2B^{2/n}/d(\sigma(q)). \qquad (4)$$

Let m_1, $m_2 \in \mathbb{R}_+$, m_1 given, $m_1 < m_2$ with $m_2 \to +\infty$. We have $m_2 > m_1$ and $\mu_1 > \mu_2$ with the meaning of m and μ above.
From $(3')$ inequality, we have

$$d(\alpha\sigma(q_1) - \sigma(p_1)) < n^2B^{2/n}m_1^{-1/n}, \qquad (5)$$
$$d(\alpha\sigma(q_2) - \sigma(p_2)) < n^2B^{2/n}m_2^{-1/n}, \qquad (6)$$

If $\beta_2 = \beta_1$ then $p_2/q_2 = p_1/q_1$ and $\sigma_j(p_2/q_2) = \sigma_j(p_1/q_1)$, $j = 1, \ldots, r+s$. $\alpha_j\sigma_j(q_2) - \sigma_j(p_2) = \sigma_j(q_2)(\alpha_j - \sigma_j(p_1/q_1))$ and thus $N(\alpha\sigma(q_2) - \sigma(p_2)) = N_{K/\mathbb{Q}}(q_2)N(\alpha - \sigma(p_1/q_1))$, $N(\alpha\sigma(q_2) - \sigma(p_2)) \geq N(\alpha - \sigma(p_1/q_1))$. From the geometric mean inequality, $d(\alpha\sigma(q_2) - \sigma(p_2)) \geq nN(\alpha - \sigma(p_1/q_1))^{1/n}$ and then $\mu_2 > N(\alpha - \sigma(p_1/q_1))^{1/n}$, which is possible only for m_2 bounded above. Then, for any $\beta_1 = p_1/q_1$ given which verify (5), there are finitely many couples (p_2, q_2) such that $\beta_2 = p_2/q_2 = p_1/q_1$ and such that (2) is verified. Relation (4) is

verified by infinitely many couples (p, q), because in (3) $d(\alpha\sigma(q) - \sigma(p))$ can be made arbitrary small for m sufficiently large. Therefore there are infinitely many different $\beta = p/q$ such that (4) is verified. 3) We shall prove that there are finitely many different $\beta = p/q$ for one value of q given :
Let $\beta_1 = p_1/q$ and $\beta_2 = p_2/q$. If $q_1 = q_2 = q$ then

$$d(\alpha\sigma(q) - \sigma(p_1)) < n^2 B^{2/n}/d(\sigma(q)) \text{ and } d(\alpha\sigma(q) - \sigma(p_2)) < n^2 B^{2/n}/d(\sigma(q)).$$

Then, we deduce $d(\sigma(p_1 - p_2)) < 2n^2 B^{2/n}/d(\sigma(q))$, which is possible only, for p_1 given, for a finite number of p_2.

4) From 2) and 3), there are infinitely many different q, thus with arbitrary large $d(\sigma(q))$ such that

$$d(\alpha\sigma(q) - \sigma(p)) < (n^2 B^{2/n})/d(\sigma(q)), \quad \text{Q.E.D.}$$

Remark : If α is such that $\alpha_1 = \alpha_2 = \cdots = \alpha_{r+s}$, then an immediate consequence of the Dirichlet approximation theorem is that there are infinitely many p/q, $p, q \in \mathbb{Z} \subset A$ such that $d(\alpha\sigma(q) - \sigma(p)) < n/q = n^2/d(\sigma(q)) < (n^2 B^{2/n})/d(\sigma(q))$: in that particular case, the theorem 1 is an immediate consequence of Dirichlet theorem.

COROLLARY 2 : *Let K be a number field of degree n, signature (r, s) and absolute value of discriminant D. Let B be the Minkowski bound of K $(B = (4/\pi)^s (n!/n^n)/\sqrt{D})$. Let $\alpha \in \mathbb{R}^r \times \mathbb{C}^s$, $\alpha_j \notin \sigma_j(K)$, $j = 1, \ldots, r+s$. Then there are infinitely many $\beta = p/q$, $p, q \in A$ such that*

$$0 < N(\alpha - \sigma(p/q)) < (B/N_{K/\mathbb{Q}}(q))^2.$$

Proof : From geometric mean inequality, we deduce from the theorem 1

$$n^n N(\alpha\sigma(q) - \sigma(p)) < n^{2n} B^2/d(\sigma(q))^n.$$

From geometric mean inequality $n^n N(\sigma(q)) < d(\sigma(q))^n$, and then

$$N(\alpha - \sigma(p/q)) < (B/N(\sigma(q)))^2 = (B/N_{K/\mathbb{Q}}(q))^2.$$

From $\alpha_j \notin \sigma_j(K)$ we deduce $|\alpha_j \sigma_j(q) - \sigma_j(p)| > 0$, $j = 1, \ldots, r+s$, and then

$$N(\alpha - \sigma(p/q)) > 0, \quad \text{Q.E.D.}$$

COROLLARY 3 : *Let K be a number field of degree n, signature (r,s) and absolute value of discriminant D. Let A be the ring of integers of K. For $x \in \mathbf{R}^r \times \mathbf{C}^s$, let $d_2(x)$ be the distance function defined by*

$$d_2(x) = (|x_1|^2 + \cdots + |x_r|^2 + 2|x_{r+1}|^2 + \cdots + 2|x_{r+s}|^2)^{1/2}.$$

(i) then, for every $m \in \mathbf{R}$, $m > 0$ and every $\alpha \in \mathbf{R}^r \times \mathbf{C}^s - \sigma(K)$, there exist infinitely many different p/q with $p, q \in A$ such that

$$0 < d_2(\alpha\sigma(q) - \sigma(p)) < n\{\Gamma(1 + n/2)(4/(\pi n))^{n/2}\sqrt{D}\}^{2/n}/d_2(\sigma(q))$$

with $d_2(\sigma(q)) > m$.

(ii) then, for $\alpha \in \mathbf{R}^r \times \mathbf{C}^s$, $\alpha_j \notin \sigma_j(K)$, $j = 1, \ldots, r+s$, there exist infinitely many $\beta = p/q$ where $p, q \in A$ such that :

$$0 < N(\alpha - \sigma(p/q)) < \{\Gamma(1 + n/2)(4/(\pi n))^{n/2}\sqrt{D}/N_{K/\mathbf{Q}}(q)\}^2.$$

Proof : it is exactly of the same nature than the proofs of theorem 1 and corollary 2 with function $d_2(x)$ instead of function $d(x)$.

Some generalizations

It is possible to study some generalizations of preceding results : we mention some obtained generalizations or problems to solve.

1) In the corollaries 2 and 3, it would be possible to search for a proof that not only $d(\sigma(q))$, but also $N_{K/\mathbf{Q}}(q)$, can be choosen arbitrary large.

2) A "Roth type" theorem could have one of the formulations :

   (i) Let $\varepsilon \in \mathbf{R}, \varepsilon > 0$, for $\alpha \in \mathbf{R}^r \times \mathbf{C}^s - \sigma(K)$, $\alpha_j, j = 1, \ldots, r+s$ algebraic, then there would be only finitely many $\beta = p/q$, $p, q \in A$ such that $d(\alpha\sigma(q) - \sigma(p)) < 1/d(\sigma(q))^{1+\varepsilon}$.

   (ii) if the assertion 1) is true (arbitrary large $N_{K/\mathbf{Q}}(q)$), then for $\varepsilon \in \mathbf{R}_+$, for $\alpha \in \mathbf{R}^r \times \mathbf{C}^s$, $\alpha_j \notin \sigma_j(K)$ $j = 1, \ldots, r+s$, α_j algebraic $j = 1, \ldots, r+s$, there would be only finitely many norms $N_{K/\mathbf{Q}}(q)$ such that

$$0 < N(\alpha - \sigma(p/q)) < 1/N_{K/\mathbf{Q}}(q)^{2+\varepsilon}.$$

Compare to MAHLER [4] result (appendix C) : let $\alpha \in \mathbf{C}^n$, let $\beta \in K$ and $H_K(\beta)$ the height of β as previously defined.

Let $f(\beta) = \prod_{j=1}^{n} \min(1, |\alpha_j - \sigma_j(\beta)|)$.

Let $\delta \in \mathbf{R}$, $\delta > 0$. There are only finitely many β in K with

$$f(\beta) < H_K(\beta)^{-2-\delta}.$$

3) Let $\alpha \in \mathbf{R}^r \times \mathbf{C}^s - \sigma(K)$. It is always possible to find $q_1 \in A$ such that

$$d(\alpha\sigma(q_1) - \sigma(p_1)) < n^2 B^{2/n} / d(\sigma(q_1))$$

and such that for all $q' \neq q_1$, $q' \in A$ with $d(\alpha\sigma(q') - \sigma(p')) < n^2 B^{2/n} / d(\sigma(q'))$ then $d(\sigma(q')) > d(\sigma(q_1))$: $\sigma(A)$ is a lattice, therefore

$$d(\sigma(q_1)) = \min\{d(\sigma(q)) \mid q \in A\ ,\ \exists p\ ,\ d(\alpha\sigma(q) - \sigma(p)) < n^2 B^{2/n} / d(\sigma(q))\}$$

exists. It is always possible to find in the same way $q_2 \in A$ such that

$$d(\alpha\sigma(q_2) - \sigma(p_2)) < d(\alpha\sigma(q_1) - \sigma(p_1)) \text{ with}$$
$$d(\sigma(q_2)) = \min\{d(\sigma(q')) \mid d(\alpha\sigma(q') - \sigma(p')) < d(\alpha\sigma(q_1) - \sigma(p_1))\}.$$

It is then possible to consider $(\sigma(p_1), \sigma(q_1)), \ldots, (\sigma(p_i), \sigma(q_i)), \ldots$ as a sequence of best approximations of $\alpha \in \mathbf{R}^r \times \mathbf{C}^s - \sigma(K)$ by elements of $\sigma(K)$, generalizing the concept of sequences of best approximations of elements $\alpha \in \mathbf{R} - \mathbf{Q}$ by elements of $\mathbf{Q}$. This concept is studied in [10].

4) It is possible to generalize theorem 1 and corollaries 2 and 3 to simultaneous approximation. For instance, let $(\alpha^1, \ldots, \alpha^\ell) \in (\mathbf{R}^r \times \mathbf{C}^s)^\ell - \sigma(K)^\ell$. Then, there exist infinitely many ℓ-tuples $(q_1, \ldots, q_\ell) \in A^\ell$ and $p \in A$ such that

$$0 < d(\alpha^1\sigma(q_1) + \cdots + \alpha^\ell\sigma(q_\ell) - \sigma(p)) < n^{\ell+1} B^{\ell+1} / d(\sigma(q_m))^\ell$$

where $d(\sigma(q_m)) = \max_{i=1,\ldots,\ell}(d(\sigma(q_i)))$.

REFERENCES

[1] A. BAKER. *Transcendental number theory*, Cambridge Univ. Press, (1979).

[2] C.G. LEKKERKERKER. *Geometry of Numbers*, North Holland, (1969).

[3] K.F. ROTH. Rational approximation to rational numbers,*Mathematica* **2** (1955), corrigendum, Ibid (1968).

[4] K. MAHLER. *Lectures on diophantine approximation*, Notre Dame Univ., (1961).

[5] P. SAMUEL. *Théorie Algébrique des Nombres*, Herman, (1971).

[6] W.M. SCHMIDT. Approximation to algebraic numbers, *Enseignement Math.* **17** (1971), 183-253.

[7] W.M. SCHMIDT. Simultaneous approximation to algebraic numbers by elements in a number field, *Monatsh. Math.* **79** (1975), 55-66.

[8] W.M. SCHMIDT. *Diophantine approximation*, Lecture notes in Math. 785, Springer Verlag, (1980).

[9] K.B. STOLARSKY. *Algebraic numbers and diophantine approximation*, Marcel Dekker, New-York, (1974).

[10] R. QUÊME. *A generalization of best approximations method to algebraic number fields*, draft manuscript, 11/89.

Roland QUÊME
32 Hameau de la Caravelle
Port Sud
91650 BREUILLET

Astérisque

PHILIPPE RAMBOUR

Éléments fixes du complété d'une clôture séparable sous l'action de son groupe de Galois

Astérisque, tome 198-199-200 (1991), p. 285-294

<http://www.numdam.org/item?id=AST_1991__198-199-200__285_0>

ÉLÉMENTS FIXES DU COMPLÉTÉ D'UNE CLÔTURE SÉPARABLE SOUS L'ACTION DE SON GROUPE DE GALOIS

par Philippe RAMBOUR

Soit R un anneau, nœthérien, normal, intègre de corps des fractions K, et soit I un idéal de R qui ne soit pas confondu avec R tout entier.

On désigne par :

- R_s l'anneau des entiers sur R d'une clôture séparable K_s de K ;
- G le groupe $\mathrm{Gal}(K_s/K)$;
- $\hat{R}_s$ le complété de R_s pour la topologie définie par IR_s.

Le problème est de déterminer $\hat{R}_s^G$ qui est l'ensemble des éléments fixes du complété de R_s sous l'action de G.

J. Ax a répondu à la question dans le cas où le corps K est un corps local de caractéristique 0 ou p, c'est-à-dire un corps muni d'une valuation à valeur dans un groupe abélien et par laquelle K est hensélien [1]. Dans ce travail nous allons établir le théorème suivant :

THÉORÈME. — *L'anneau R_s est séparé pour la topologie I-adique et s'injecte donc dans $\hat{R}_s$. En caractéristique p, l'anneau $\hat{R}_s$ contient une clôture radicielle de R, notée $\sqrt{R}$, et $\hat{R}_s^G$ l'ensemble des points fixes de $\hat{R}_s$ sous l'action de G n'est autre que l'adhérence de $\sqrt{R}$ dans $\hat{R}_s$.*

Pour obtenir la dernière assertion nous utiliserons des approximations d'un élément de R_s qui dépendront du diamètre des conjugués, méthode mise au point par J. Ax [1].

I. — Séparation de R_s pour la topologie I-adique

PROPOSITION 1. — *Si $I \neq R$ alors $\bigcap_n I^n R_s$ est réduite à 0 et R_s est donc séparé pour la topologie définie par IR_s.*

Démonstration : supposons d'abord que I est un idéal principal. Il existe alors un élément x de R qui est un générateur de I. Puisque R est normal et nœthérien et $I \neq R$ il existe une valuation v vérifiant $v(x) > 0$ et cette valuation se prolonge à R_s. D'où si a appartient à $\bigcap_n I^n R_s$, alors $v(a) = +\infty$ et donc $a = 0$.

Démontrons maintenant la propriété dans le cas où I n'est pas forcément un idéal principal.

Notons S le schéma affine $\operatorname{Spec} R$ et soit $\tilde{S}$ le normalisé de l'éclaté $\hat{S}$ par rapport au sous-schéma fermé $Y = \operatorname{Spec}(R/I)$. Montrons tout d'abord que l'application canonique $\pi : \tilde{S} \to S$ est une application surjective. Pour cela remarquons que l'on peut écrire π comme la composée $\pi_2 \circ \pi_1$ où π_1 est l'application canonique de $\tilde{S}$ dans $\hat{S}$, π_2 l'application canonique de $\hat{S}$ dans S. π_1 et π_2 étant deux applications surjectives, il en est de même pour π.

π_1 est surjective : c'est le *going down* théorème (voir MATSUMURA : Commutative Algebra [2]).

π_2 est surjective : si $V = S - Y$, alors π_2 est un isomorphisme de $\pi_2^{-1}(V)$ sur V. Comme π_2 est propre, π_2 est fermé donc $\pi_2(\hat{S})$ est un fermé de S contenant V. Comme S est intègre S est aussi irréductible donc on a forcément $\pi_2(\hat{S}) = S$.

Soit maintenant $U = \operatorname{Spec} A$ un ouvert affine de $\tilde{S}$. On sait que A est un anneau nœthérien normal et si U est choisi assez petit parmi les ouverts affines vérifiant : $\pi^{-1}(Y) \cap U \neq \emptyset$ alors IA est un idéal principal de A, distinct de A. D'après ce qui a été démontré dans le cas principal on sait que $\bigcap_n I^n A_s = \{0\}$ avec A_s clôture intégrale de A contenue dans K_s. Puisque R est contenu dans A, alors R_s est contenu dans A_s et $\bigcap_n I^n R_s$ est réduite à 0.

II. — $\hat{R}_s$ contient une clôture radicielle de R

PROPOSITION 2. — *Si R est de caractéristique p, l'anneau $\hat{R}_s$ contient une clôture radicielle de R, on la note $\sqrt{R}$.*

Démonstration : soit β un élément de R et N un entier naturel. On va montrer que $\hat{R}_s$ contient une solution de $X^{p^N} = \beta$. Pour cela fixons un élément

non nul de I, appelé a. Pour tout entier naturel m supérieur à N on définit X_m comme étant une racine de l'équation :

$$X^{p^N} - a^{p^m} X = \beta(1).$$

Puisque cette équation est séparable X_m est bien un élément de R_s. Nous allons montrer que la suite $(X_m)_{m>N}$ ainsi définie est une suite de Cauchy dans R_s. Elle sera alors convergente dans $\hat{R}_s$, avec une limite X_0 qui vérifiera, en faisant tendre m vers l'infini dans (1), $X_0^{p^N} = \beta$. Donc X_0 sera donc une racine p^N-ième de β, ce qui démontrera le théorème cherché.

Si m et m' vérifient :$m' > m > N$, on a :

$$X_m^{p^N} - X_{m'}^{p^N} = a^{p^m} X_m - a^{p^{m'}} X_{m'}$$

$$\left(\frac{X_m - X_{m'}}{a^{p^m - N}}\right)^{p^N} = X_m - a^{p^{m'} - p^m} X_m.$$

Cette dernière égalité prouve que $(X_m - X_{m'})/a^{p^{m-N}}$ est un élément entier sur R_s, et puisque R_s est un anneau normal $(X_m - X_{m'})/a^{p^{m-N}}$ est un élément de R_s. Si α cet élément, l'égalité $X_m - X_{m'} = a^{p^{m-N}} \alpha$ permet de savoir que $X_m - X_{m'}$ est un élément de $I^{p^{m-N}}$ ce qui prouve que la suite $(X_m)_{m>N}$ est bien une suite de Cauchy, ce qui achève la démonstration.

III. — Diamètre des conjugués

Dans tout le paragraphe on supposera la caractéristique de K égale à p.

DÉFINITION 1. — *Pour α élément de R_s, avec $\alpha \neq 0$, on pose :*

$$\delta(\alpha) = \max\{n/\alpha \in I^n\}.$$

DÉFINITION 2. — *Si K' est une extension finie de K on pose, si α est un élément de R_s :*

$$\Delta_{K'} = \min\{n/\delta(\sigma(\alpha) - \alpha) \in I^n, \ \sigma \in \mathrm{Gal}(K_s/K')\}.$$

Remarque : si α est un élément de K', on pose :

$$\Delta_{K'}(\alpha) = +\infty.$$

On remarque : $\Delta_{K'}(\alpha) \geq \delta(\alpha)$ pour toute extension finie K' de K.

PROPOSITION 3.. — *Il existe deux réels a et b tels que pour tout* α *de* R_s *il existe* β *de* $\sqrt{R}$ *vérifiant* $\alpha - \beta \in I^{[a\Delta_K(\alpha)]+b}$, *et si* $[K(\alpha) : K]$ *premier à* p, *alors* $\alpha - \beta \in I^{\Delta_K(\alpha)}$.

Démonstration :

(a) Démontrons tout d'abord la proposition dans le cas où $[K(\alpha) : K]$ premier à p. On remarque alors que $\mathrm{Tr}_{K(\alpha)/K}(\alpha)$ appartient à R puisque R est normal et donc $\mathrm{Tr}_{K(\alpha)/K}(\alpha)\Big/[K(\alpha) : K]$ est également un élément de R et de plus :

$$\Big((\mathrm{Tr}_{K(\alpha)/K})(\alpha)\Big/[K(\alpha) : K]\Big) - \alpha = \sum \frac{\alpha' - \alpha}{[K(\alpha) : K]}$$

α' parcourant les K conjugués de α. Ce dernier terme est un élément de $I^{\Delta_K}(\alpha)$.

(b) Pour montrer la proposition dans ce cas nous allons avoir besoin des lemmes suivants :

LEMME 1. — *On se donne* K' *et* $K"$ *deux extensions finies séparables de* K *avec* K' *contenu dans* $K"$ *et vérifiant* $[K" : K'] = p$. *Alors si* α *est un élément de* R_s *appartenant à* $K"$ *on a :*

(i) on peut trouver β *un élément de* R', *où* R' *est l'anneau des entiers de* K', *qui soit tel que :*

$$\alpha^p - \beta \in I^{\Delta_{K'}(\alpha)+\delta(\alpha)(p-1)}$$

(ii) pour tout entier naturel n *non nul on peut trouver un élément* β_n *de* R' *avec :*

$$\alpha^{p^n} - \beta_n \in I^{\Delta_{K'}(\alpha)p^n(1-a^n)} \qquad \text{où} \qquad a = (p-1)/p.$$

Démonstration du Lemme 1 :

Si α est un élément de K' il n'y a rien à démontrer. Sinon $[K'(\alpha) : K']$ vaut p et on peut faire la démonstration ci-dessous.

(i) Si $\alpha_1 \cdots \alpha_p$ désigne les racines du polynôme minimal de α sur K', on pose $\eta_i = \alpha_i - \alpha$. Alors

$$\begin{aligned} N_{K'(\alpha)/K'}(\alpha) &= \prod_{i=1}^{p} \alpha_i = \prod_{i=1}^{p} (\alpha + \eta_i) \\ &= \alpha^p + b_1\alpha^{p-1} + \cdots + b_p. \end{aligned}$$

En remarquant que le b_j sont, au signe près, les j-ième fonctions symétriques élémentaires de η_j pour $1 \leq j \leq p$, et que les η_j sont des éléments de $I^{\Delta_{K'}(\alpha)}$ on obtient facilement que : $N_{K'(\alpha)/K'}(\alpha) - \alpha^p$ est un élément d'un I^N avec :

$$N \geq \min_{1 \leq j \leq p} ((p-j)\delta(\alpha) + j\Delta_{K'}(\alpha)) = \Delta_{K'}(\alpha) + \delta(\alpha)(p-1)$$

en utilisant que $\Delta_{K'}(\alpha) \geq \delta(\alpha)$.

Comme R' est normal, on a $N_{K'(\alpha)/K'}(\alpha)$ élément de R d'où le résultat.

(ii) Démontrons d'abord par récurrence sur n que l'on peut trouver un élément β_n de R' vérifiant :

$$\alpha^{p^n} - \beta_n \in I^{\Delta_{K'}(\alpha)p^n(1-a^n/p)^n)+(p-1)^n\delta(\alpha)}$$

La formule annoncée sera alors une conséquence immédiate de ce résultat.

Si $n = 1$ c'est ce que l'on a obtenu au (i).

Montrons maintenant la formule pour n quelconque. D'après l'hypothèse de récurrence il existe un élément β_{n-1} de R' vérifiant :

$$\alpha^{p^{n-1}} - \beta_{n-1} \in I^{\Delta_{K'}(\alpha)p^{n-1}(1-a^{n-1})+(p-1)^{n-1}\delta(\alpha)}$$

posons $x_{n-1} = \alpha^{p^{n-1}} - \beta_{n-1}$.

$$\delta(x_{n-1}) \geq \Delta_{K'}(\alpha)p^{n-1}(1-a^{n-1}) + (p-1)^{n-1}\delta(\alpha).$$

et

$$\Delta_{K'}(x_{n-1}) = \Delta_{K'}(\alpha)p^{n-1}$$

grâce au (i) on sait qu'il existe β un élément de R' vérifiant

$$x_{n-1}^p - \beta \in I^{\Delta_{K'}(x_{n-1})+\delta(x_{n-1})(p-1)}$$

ce qui implique, d'après les remarques ci-dessus :

$$\begin{aligned}\delta(\alpha^{p^n} - \beta_{n-1}^p - \beta) \geq\ & \Delta_{K'}(\alpha)p^{n-1} \\ & +(p-1)(\Delta_{K'}(\alpha)(1-a^{n-1})p^{n-1} + (p-1)^{n-1}\delta(\alpha)).\end{aligned}$$

C'est-à-dire que si l'on pose $\beta_{n-1}^p + \beta = \beta_n$ et que si l'on fait un petit calcul pour transformer $p^{n-1} + p^{n-1}(1-(p-1/p)^{n-1})(p-1)$ en $p^n(1-(p-1/p)^n)$ on obtient

$$\delta(\alpha^{p^n} - \beta) \geq \Delta_{K'}(\alpha)p^n(1-a^n) + (p-1)^n\delta(\alpha)$$

qui est le résultat annoncé.

LEMME 2. — *Soit* $H_m \supset H_{m-1} \supset \cdots \supset H_1 \supset H_0$ *une tour d'extensions finies séparables de* K *avec* $[H_i : H_{i-1}] = p$ *pour* $1 \leq i \leq m$. *On appelle* R_0 *l'anneau des entiers de* H_0 *par rapport à* R, *et* R_i *l'anneau des entiers de* H_i *sur* R_0. *Si* α *est un élément de* H_m *et si* n *est un entier naturel donné on peut trouver un élément* β_{m-i} *de* R_{m-i} *vérifiant :*

$$\alpha^{p^{ni}} - \beta_{m-i} \in I^{\Delta_{H_0}(\alpha)p^{ni}(1-a^n)^i} \qquad 1 \leq i \leq m.$$

Démonstration : Démontrons ce lemme par récurrence.

Pour $i = 1$ c'est une application immédiate du point (ii) du lemme 1 avec $K' = H_{m-1}$ en remarquant que puisque H_0 est contenu dans H_{m-1}, $\Delta_{H_0}(\alpha) \leq \Delta_{H_{m-1}}(\alpha)$.

Démontrons maintenant le lemme pour un i quelconque $1 \leq i \leq m$.

D'après l'hypothèse de récurrence il existe β_{i-1} élément de R'_{m-i+1} avec

$$\alpha^{p^{(n-i)}} - \beta_{m-i+1} \in I^{\Delta_{H_0}(\alpha)p^{n(i-1)}(1-a^n)^{(i-1)}}. \tag{I}$$

on a

$$\Delta_{H_0}(\beta_{m-i+1}) \geq \Delta_{H_0}(\alpha)p^{n(i-1)}(1-a^n)^{(i-1)}(1)$$

en effet si σ un élément de $Gal(K_s/H_0)$, et si $\alpha' = \sigma(\alpha)$, et si $\beta'_{m-i+1} = \sigma(\beta_{m-i+1})$, alors :

$$\begin{aligned}\beta'_{m-i+1} - \beta_{m-i+1} = \beta'_{m-i+1} - \alpha'^{p^{n(i-1)}} + \alpha'^{p^{n(i-1)}} \\ + \alpha^{p^{n(i-1)}} - \alpha^{p^{n(i-1)}} - \beta_{m-i+1}\end{aligned}$$

en remarquant que : $\beta'_{m-i+1} - \alpha'^{p^{n(i-1)}}$ et $\beta_{m-i+1} - \alpha^{p^{n(i-1)}}$ sont des éléments de $I^{\Delta_{H_0}(\alpha)p^{n(i-1)}(1-a^n)^{(i-1)}}$ et comme $\alpha^{p^{n(i-1)}} - \alpha'^{p^{n(i-1)}}$ dans $I^{\Delta_{H0}(\alpha)p^n(i-1)}$ on obtient l'inégalité (1).

Si l'on applique maintenant le résultat (ii) du lemme 1 avec $K' = H_{m-i}$ on peut trouver un élément de R_{m-i} avec :

$$\beta^{p^n}_{m-i+1} - \beta_{m-i} \in I^{\Delta_{H_{m-i}}(\beta_{m-i+1}).p^n(1-a^n)} \tag{II}$$

et remarquant que $\Delta_{H_{m-i}}(\beta_{m-i+1}) \geq \Delta_{H_0}(\beta_{m-i+1})$

$$\beta^{p^n}_{m-i+1} - \beta_{m-i} \in I^{\Delta_{H_0}(\beta_{m-i+1})p^n(1-a^n)}.$$

Soit d'aprés l'inégalité (1) :

$$\beta^{p^n}_{m-i+1} - \beta_{m-i} \in I^{\Delta_{H_0}(\alpha)p^{ni}(1-a^n)^i} \tag{II'}$$

D'autre part en élevant $\alpha^{p^{n(i-1)}} - \beta_{m-i+1}$ à la puissance p^n la relation (I) donne :

$$\delta(\alpha^{p^{ni}} - \beta_{m-i+1}^{p^n}) \geq \Delta_{H_0}(\alpha)p^{ni}(1-a^n)^i \qquad \text{(I')}.$$

d'où en combinant (II') et (I') :

$$\delta(\alpha^{p^{ni}} - \beta_{m-i}) \geq \Delta_{H_0}(\alpha)p^{ni}(1-a^n)^i.$$

ce qui est le résultat annoncé.

(c) Démonstration de la proposition 3 dans le cas $[\tilde{K} : K] = p^m$.

Où $\tilde{K}$ désigne une extension galoisienne de degré minimale de K contenant α. En utilisant que $\mathrm{Gal}(\tilde{K}(\alpha) : K)$ est résoluble on peut obtenir une tour d'extensions séparables :

$$\tilde{K} = K_m \supset K_{m-1} \supset \cdots \supset K_1 \supset K_0 = K.$$

On appelle R_i l'anneau des entiers de K_i sur R. Soit n un entier naturel. Si on applique le lemme 2 avec $i = m$ et $H_m = \tilde{K}$, $H_0 = K$, on obtient l'existence d'un élément β_0 de R vérifiant :

$$\alpha^{p^{nm}} - \beta_0 \in I^{\Delta_K(\alpha)p^{nm}}(1-a^n)^m.$$

Si l'on choisit maintenant n tel que :

$$1 - (p - 1/p)^n \geq 1/2,$$

on obtient :

$$\alpha^{p^{nm}} - \beta_0 \in I^{\Delta_K(\alpha)[p^{nm}/2]}.$$

Si l'on admet pour l'instant que $x^{p^j} \in I^N$ implique :

$$x \in I^{[N/p^j]-r+1}$$

avec r désignant le nombre de générateurs de I, on obtient que si β vaut $\beta_0^{1/p^{nm}}$ alors :

$$\alpha - \beta \in I^{[\Delta_K(\alpha)[p^{nm}/2]/p^{nm}]-r+1}.$$

En remarquant que l'on peut choisir encore n pour que :

$$[\Delta_K(\alpha)[p^{nm}/2]/p^{nm}] \geq \left[\frac{\Delta_K(\alpha)}{2}\right] - 1.$$

On obtient : $\alpha - \beta \in I^{[\Delta(\alpha)/2]-r}$ ce qui est le résultat voulu. Reste à démontrer le lemme suivant :

LEMME 3. — *Si A est un anneau de caractéristique p pour lequel $x \longmapsto x^p$ est bijectif, si J un idéal de A engendré par r éléments de A, alors si n et N sont deux entiers naturels $x^{p^n} \in J^N$ implique $x \in J^{[N/p^n]-r+1}$.*

Démonstration : démontrons ce lemme grâce à une récurrence sur r, où r désigne le nombre des générateurs.

Si $r = 1$. Alors I est un idéal principal et la propriété $x \longmapsto x^p$ bijectif donne le résultat.

Montrons maintenant la propriété pour r quelconque. Posons $J = (y_1, \cdots, y_r)$ et $H = (y_2, \cdots, y_r)$. Si x est tel que $x^{p^n} \in J^N$ on peut écrire :

$$x^{p^n} = X_0 y_1^N + X_1 y_1^{N-1} + \cdots + X_i y_1^{N-i} + \cdots + X_N$$

avec X_i élément de H^i pour i vérifiant $0 \leq i \leq N$. On obtient ainsi que :

$$x = X_0^{1/p^n} y_1^{N/p^n} + X_1^{1/p^n} y_1^{N-1/p^n} + \cdots + X_i^{1/p^n} y_1^{(N-i)/p^n} + \cdots + X_N^{1/p^n} (1).$$

Comme

$$\left[\frac{N-i}{p^n}\right] \geq \left[\frac{N}{p^n}\right] - \left[\frac{i}{p^n}\right] - 1.$$

y_1^{N-i/p^n} est donc un élément de $J^{[N/p^n]-[i/p^n]-1}$ et d'après l'hypothèse de récurrence appliquée à H on sait que X_i^{1/p^n} est un élément de $H^{[i/p^n]-r+2}$. Donc chaque terme de la sommation (1) appartient à : $J^{[N/p^n]-[i/p^n]-1+[i/p^n]-r+2}$ c'est-à-dire à : $J^{[N/p^n]-r+1}$ ce qui démontre le lemme.

(d) Démonstration de la proposition 3 dans le cas général.

Soit donc α un élément de R_s tel que $[K(\alpha) : K]$ n'est pas un entier premier à p. Si $\tilde{K}$ désigne encore une extension galoisienne de K de degré minimal contenant α, on a : $[\tilde{K} : K] = qp^m$ avec q premier à p.

Si G' est un p-groupe de Sylow de Gal(K(α)/K). Soit H l'ensemble des points fixes de G' dans $\tilde{K}$. On sait qu'alors H est une extension finie de K contenue dans $\tilde{K}$ et telle que :

- $\tilde{K}$ est une extension galoisienne de H.
- $[\tilde{K}(\alpha) : H] = p^n$.

On appelle R' l'anneau des entiers de H. Si n désigne un entier naturel on peut appliquer à $\tilde{K}(\alpha)$ et H ce qui a été fait au (b) avec H dans le rôle de K. On peut donc obtenir γ avec γ élément de R' et :

$$\alpha - \gamma \in I^{[\Delta_H(\alpha)/2]-r}.$$

D'après a) on sait qu'il existe un élément β_0 de R vérifiant $\gamma - \beta_0 \in I^{\Delta_K(\gamma)}$.

Puisque K est contenu dans H, $\Delta_K(\alpha) \leq \Delta_H(\alpha)$ d'où

$$\alpha - \gamma \in I^{[\Delta_K(\alpha)/2]-r} \tag{1}$$

et comme en (b) on peut montrer que :

$$\Delta_K(\gamma) \geq [\Delta_K(\alpha)/2] - r.$$

d'où

$$\gamma - \beta_0 \in I^{[\Delta_K(\alpha)/2]-r}. \tag{2}$$

Les relations (1) et (2) donnent :

$$\alpha - \beta_0 \in I^{[\Delta_K[\alpha)/2]-r}$$

IV. — Éléments fixes sous l'action du groupe $G = \mathrm{Gal}(K_s/K)$

PROPRIÉTÉ 4. — *Si K un corps de caractéristique p, on a, avec les notations introduites au début de l'article :*

$$\hat{R}_s^G = \overline{\sqrt{R}},$$

où $\overline{\sqrt{R}}$ désigne l'adhérence de $\sqrt{R}$ pour la topologie I-adique.

Démonstration : si x est un élément de $\hat{R}_s^G$ pour tout entier N il existe un α qui est un élément de R_s avec $x - \alpha$ éleément de $I^N \hat{R}_s$. Si σ est un élément de G on a toujours $x - \sigma(\alpha)$ élément de $I^N \hat{R}_s$, et donc $\alpha - \sigma(\alpha)$ élément de $I^N \hat{R}_s$ d'où $\Delta_K(\alpha) \geq N$.

Donc on peut trouver, d'après la proposition 3, un élément β dans $\sqrt{R}$ où $\alpha - \beta$ est un élément soit de $I^{[N/2]-r}\hat{R}_s$. Donc $x - \beta$ est un élément de $I^{[N/2]-r}\hat{R}_s$. Il en résulte que x est un élément de l'adhérence de $\sqrt{R}$. La réciprocité étant immédiate on obtient la propriété annoncée.

BIBLIOGRAPHIE

[1] J. Ax. — Zeros of Polynomials over local fields, the Galois Action, *Journal of Algebra*, 15, 1970, 417-428.

[2] H. Matsumura. — Commutative Algebra, Second Edition, Mathematics Lecture Note Series, The Benjamin.cuminings publishing company.

PH. RAMBOUR
Université de Paris-Sud
Département de Mathématiques
URA D0752
Bâtiment 425
F-91405 ORSAY CEDEX

Astérisque

PH. SATGÉ

Quelques problèmes de rationalité liés au théorème de Poncelet

Astérisque, tome 198-199-200 (1991), p. 295-304

<http://www.numdam.org/item?id=AST_1991__198-199-200__295_0>

QUELQUES PROBLÈMES DE RATIONALITÉ LIÉS AU THÉORÈME DE PONCELET

par

Ph. SATGÉ

§0. Introduction. Soit S une conique non singulière du plan projectif sur un corps algébriquement clos de caractéristique 0, soit c un entier naturel, et soit Λ un pinceau linéaire (i.e. un système linéaire de dimension 1) de diviseurs effectifs de degré $c+1$ de la conique S ; le théorème de Poncelet affirme l'existence d'une, et d'une seule, courbe C de degré c possédant la propriété suivante : pour chaque élément D de Λ, tous les points d'intersections des tangentes à S issues des différents points du support de D sont sur la courbe C. Récemment plusieurs auteurs ont donné des démonstrations très élégantes de ce théorème et ont étudiés en détail les propriétés géométriques des courbes C que ce théorème attache aux systèmes linéaires (courbes que, dans la suite, nous appellons courbes de Poncelet) ; on peut, par exemple, trouver un résumé de ces travaux dans le papier de Trautmann [*Tr*]. Notons que ces travaux sont essentiellement géométriques, c'est à dire qu'ils ne s'interessent qu'aux propriétés et à la classification des courbes sur un corps de base algébriquement clos. Ici, au contraire, nous fixons notre attention sur un corps de base quelconque de caractéristique 0 (par exemple un corps de nombres) et nous discutons les propriétés des courbes de Poncelet relatives à ce corps de base k. Plus précisément nous supposons, dans le théorème de Poncelet, que la conique non singulière S du plan projectif est définie sur k; nous nous interessons alors aux deux problèmes suivants : d'une part trouver les conditions à imposer à un pinceau de S pour que la courbe de Poncelet qui lui est associée soit définie sur k, et d'autre part classer les courbes sur k obtenues de cette manière. Curieusement, ces deux questions très naturelles ne semblent pas avoir fait l'objet d'une étude systématique ; c'est cette étude que nous commençons ici. Ce travail est divisé en deux paragraphes. Dans le paragraphe 1 nous résolvons le premier de ces problèmes en montrant que la courbe de Poncelet associée à un pinceau de S est définie sur k si et seulement si le pinceau est invariant par

S.M.F.
Astérisque 198-199-200 (1991)

le groupe de Galois $Gal(\overline{k}/k)$ dans un sens que nous précisons ; nous discutons ensuite quelques propriétés des pinceaux qui possèdent cette propriété. Dans le paragraphe 2, nous abordons le deuxième problème en nous limitant au cas $c = 2$, donc au cas où les courbes de Poncelet sont des coniques ; nous montrons alors le résultat suivant : chaque fois qu'une telle conique de Poncelet est définie sur k, elle est isomorphe sur le corps k à la conique de base S.

Nous avons cherché, dans ce papier, à rester le plus élémentaire possible du point de vue du langage géométrique employé. Nous précisons assez longuement au début du paragraphe 1 le vocabulaire et les notations que nous employons dans la suite (principalement en ce qui concerne les corps de définition). Nous nous sommes limité dans le second paragraphe à l'étude du cas $c = 2$ qui est particulièrement simple ; signalons cependant que c'est le cas $c = 3$ qui a motivé notre étude ; dans ce cas les courbes de Poncelet sont des cubiques, donc des courbes arithmétiquement beaucoup plus intéressantes que les coniques. Techniquement l'étude de ce cas, et plus généralement des cas $c > 2$, est beaucoup plus difficile ; nous comptons revenir sur ces questions dans un autre travail.

Je remercie J.L. Colliot-Thélène pour ses nombreuses remarques (et en particulier pour la démonstration du Lemme 2.5.)

§1. Les questions de rationalités. Commençons par préciser le cadre géométrique dans lequel nous nous plaçons et les notations que nous utilisons. Nous désignons par $\overline{k}[X_0, X_1, X_2]$ l'anneau des polynômes à trois variables et à coefficients dans $\overline{k}$, et par $\mathbf{P}^2$ l'ensemble des points du plan projectif à valeur dans $\overline{k}$, c'est à dire l'ensemble des classes d'homothétie de triplets non nuls d'éléments de $\overline{k}$. Par courbe nous entendons un fermé de Zariski de dimension 1 de $\mathbf{P}^2$ (i.e. un fermé de Zariski dont toutes les composantes irréductibles sont de dimension 1); si X est une courbe, nous notons $I(X)$ l'ideal homogène de l'anneau $\overline{k}[X_0, X_1, X_2]$ formé des polynômes qui s'annulent sur X; enfin si la courbe X est irréductible, i.e. si l'idéal $I(X)$ est premier, nous notons $\overline{k}(X)$ le corps des fonctions rationnelles sur X.

Le fait que l'on travaille en caractéristique 0 justifie les définitions et les assertions qui suivent (celles ci résultent, par exemple, du Lemme 2 et du théorème 7 du chapitre 1, paragraphe 7 de [We]). Nous faisons agir le groupe de Galois $G = Gal(\overline{k}/k)$ sur l'anneau de polynômes $\overline{k}[X_0, X_1, X_2]$, et sur l'ensemble des points du plan, de la façon suivante : l'image par $\sigma \in G$ du polynôme P est le polynôme ${}^{\sigma}P$ obtenu en remplaçant les coefficients de P par leurs images par σ; le résultat de l'action de $\sigma \in G$ sur le point $\underline{x}$ de coordonnées projectives

(x_0, x_1, x_2) est le point ${}^{\sigma}\underline{x}$ de coordonnées projectives $(\sigma(x_0), \sigma(x_1), \sigma(x_2))$. Si X est une courbe et si σ est un élément du groupe de galois G, on note ${}^{\sigma}X$ l'image de X par σ (i.e. l'ensemble des $({}^{\sigma}\underline{x})_{\underline{x}\in X}$) ; il est clair que ${}^{\sigma}X$ est une courbe et que $I({}^{\sigma}X) = {}^{\sigma}(I(X))$ (i.e. l'ensemble des $({}^{\sigma}P)_{P\in I(X)}$). Si X est irréductible, si f est un élément de $\overline{k}(X)$ qui s'écrit $\frac{P}{Q}$ avec P et Q polynômes homogènes de même degré de $\overline{k}[X_0, X_1, X_2]$, et si σ est un élément de G, alors la fonction sur ${}^{\sigma}X$ représentée par le quotient $\frac{{}^{\sigma}P}{{}^{\sigma}Q}$ ne dépend que de f (et non des choix de P et Q) ; on la note ${}^{\sigma}f$. L'application qui à f associe ${}^{\sigma}f$ est un isomorphisme du corps $\overline{k}(X)$ sur le corps $\overline{k}({}^{\sigma}X)$ (dont la restriction à $\overline{k}$ est σ). On dira que X est définie sur k si ${}^{\sigma}X = X$ pour tout $\sigma \in G$, c'est à dire ([*We*], lemme 2, loc.cit.) si l'idéal $I(X)$ admet une base sur le corps k. Ainsi ([*We*], théorème 7, loc.cit.), si X est irréductible et définie sur k, le sous corps $k(X)$ de $\overline{k}(X)$ formé des fonctions qui peuvent s'écrire comme quotient de deux polynômes homogènes de même degré à coefficients dans k, est une extension régulière de k; on sait que cela implique que $k(X)$ est le sous corps de $\overline{k}(X)$ fixé par l'action (semi linéaire) de G. En plus du corps k, nous aurons à considérer des extensions K de k contenues dans $\overline{k}$; pour un tel corps K nous notons G_K le groupe de galois $Gal(\overline{k}/K)$ (on a donc $G = G_k$), et $K(X)$ le sous corps de $\overline{k}(X)$ formé des fonctions qui peuvent s'écrire comme quotient de deux polynomes homogènes de même degré à coefficients dans K; comme ci dessus, $K(X)$ est une extension régulière de K, et donc est le sous corps de $\overline{k}(X)$ fixé par le groupe G_K.

Un diviseur sur une courbe X sera un diviseur au sens de Weil, i.e. une combinaison formelle à coefficients dans $\mathbf{Z}$ (l'anneau des entiers rationnels) de points lisses de X. Si X est irréductible et si Δ est un diviseur sur X, on note $L(\Delta)$ le sous espace vectoriel de $\overline{k}(X)$ formé des fonctions f dont le diviseur (f) vérifie $(f)+\Delta \geq 0$. Si σ est un élément de G et si $\Delta = n_1(\mathrm{P}_1)+..+n_r(\mathrm{P}_r)$ est un diviseur de X (les n_i sont des éléments de $\mathbf{Z}$ et les P_i des éléments de X), alors $n_1({}^{\sigma}\mathrm{P}_1) + .. + n_r({}^{\sigma}\mathrm{P}_r)$ est un diviseur de ${}^{\sigma}X$ que l'on note ${}^{\sigma}\Delta$ et que l'on appelle l'image de Δ par σ; si X est irréductible, on a $L({}^{\sigma}\Delta) = {}^{\sigma}[L(\Delta)]$ (i.e. l'ensemble des $({}^{\sigma}f)_{f\in L(\Delta)}$). Si X est définie sur k, et si K est une extension de k contenue dans $\overline{k}$, on dit que Δ est rationnel sur K si ${}^{\sigma}\Delta = \Delta$ pour tout σ de G_K. Ainsi, si X est irréductible et définie sur k, et si Δ est un diviseur rationnel sur K, le groupe G_K agit semi linéairement sur le $\overline{k}$−espace vectoriel $L(\Delta)$; on note $L_K(\Delta)$ le sous ensemble de $L(\Delta)$ formé des éléments invariants par G_K. Les éléments de $L_K(\Delta)$ sont les éléments de $L(\Delta)$ qui appartiennent à $K(X)$, et la dimension du K−espace vectoriel $L_K(\Delta)$ est égale à la dimension du $\overline{k}$−espace vectoriel $L(\Delta)$. Enfin, si Λ est un pinceau linéaire sur la courbe irréductible X et si Δ est un diviseur sur X linéairement équivalent aux diviseurs du pinceau Λ, on note $L_\Lambda(\Delta)$ le sous ensemble de $L(\Delta)$ formé des fonctions dont le diviseur est de la

forme $\mathrm{D} - \Delta$ avec D dans Λ; dire que Λ est un pinceau linéaire est équivalent à dire que $L_\Lambda(\Delta)$ est un $\overline{k}-$espace vectoriel de dimension 2. Si la courbe X est définie sur k, et si K est une extension de k contenue dans $\overline{k}$, on dit qu'un pinceau linéaire Λ est un $K-$pinceau si l'on peut trouver un diviseur Δ rationnel sur K, linéairement équivalent aux éléments de Λ, et tel que l'espace vectoriel $L_\Lambda(\Delta)$ est défini sur K, i.e. admet une base formée d'éléments de $L_K(\Delta)$; il en est ainsi si et seulement si $L_\Lambda(\Delta)$ est stable sous l'action de G_K. Notons que cette propriété ne dépend pas du choix du diviseur rationnel Δ, linéairement équivalent aux éléments de Λ, que l'on a choisi.

DÉFINITION 1.1. *Soit X une courbe définie sur le corps k, soit Λ un pinceau linéaire sur X, et soit K une extension de k contenue dans $\overline{k}$. On dit que le pinceau Λ est G_K-invariant si, pour tout diviseur* D *de Λ et tout $\sigma \in G_K$, l'image de* D *par σ est encore dans Λ.*

Dans la suite la courbe de base est une conique; nous la notons S plutôt que X. Il est clair qu'un $K-$pinceau est un pinceau G_K-invariant; nous verrons qu'il existe des pinceaux G_K-invariants qui ne sont pas des $K-$pinceaux. L'introduction de la notion de pinceau G_K-invariant est justifiée par la proposition suivante :

PROPOSITION 1.2. *Soit S une conique non singulière définie sur le corps k, Λ un pinceau linéaire sur S, et K une extension de k contenue dans $\overline{k}$. La courbe de Poncelet C associée à Λ est définie sur K si et seulement si le pinceau Λ est G_K-invariant.*

Démonstration : Soit σ un élément de G; par la définition des courbes de Poncelet, la courbe ${}^\sigma C$, transformée de la courbe de Poncelet attachée à Λ par σ, est la courbe de Poncelet attachée au pinceau ${}^\sigma\Lambda$, transformé de Λ par σ (c'est à dire au pinceau dont les éléments sont les transformés par σ des diviseurs de Λ). On a donc ${}^\sigma C = C$ si et seulement si ${}^\sigma\Lambda = \Lambda$, et notre assertion en résulte immédiatement.

Étudions plus en détail les pinceaux G_K-invariants sur une conique non singulière définie sur k.

LEMME 1.3. *Soit S une conique non singulière définie sur le corps k, soit $d > 0$ un entier naturel, et soit K une extension de k contenue dans $\overline{k}$. Si la conique S possède un diviseur effectif de degré d rationnel sur K, alors tout pinceau linéaire de degré d sur S qui est G_K-invariant est un $K-$pinceau.*

Démonstration : Désignons par Δ un diviseur sur S qui est effectif, de degré

d, et rationnel sur K, et par Λ un pinceau linéaire de degré d sur S qui est G_K−invariant. Comme S est une courbe de genre 0, le diviseur Δ est linéairement équivalent aux éléments de Λ; en conséquence, notre assertion est équivalente à l'assertion suivante : l'espace vectoriel $L_\Lambda(\Delta)$ est défini sur K. Comme on l'a rappellé plus haut, il suffit pour cela de prouver que cet espace est stable sous l'action de G_K; soit donc $f \in L_\Lambda(\Delta)$ et $\sigma \in G_K$, et soit D l'élément de Λ tel que $D - \Delta$ est le diviseur de f; le diviseur de ${}^\sigma f$ est ${}^\sigma D - {}^\sigma\Delta = {}^\sigma D - \Delta$ puisque le diviseur Δ est rationnel sur K; le pinceau Λ étant G_K−invariant, le diviseur ${}^\sigma D$ est un élément de Λ, donc ${}^\sigma f$ est dans $L_\Lambda(\Delta)$; cela prouve l'invariance de $L_\Lambda(\Delta)$ sous l'action de G_K, ce que nous voulions.

Pour mémoire rappelons le lemme suivant :

LEMME 1.4. *Soit S une conique non singulière définie sur le corps k et d un entier naturel ;*

i) si d est pair la conique S possède des diviseurs effectifs de degré d rationnels sur k;

ii) si d est impair et si la conique S possède un diviseur de degré d rationnel sur k, alors S possède des points rationnels sur k.

Démonstration : *i)* Il est clair que l'intersection d'une droite rationnelle sur k avec S est un diviseur sur S qui est effectif, de degré 2, et rationnel sur k; les multiples de tels diviseurs donnent des diviseurs rationnels effectifs de n'importe quel degré pair. *ii)* Si $d = 1$ l'assertion est triviale ; sinon on écrit $d = 2d' + 1$, et on note D_1 un diviseur sur S qui est rationnel sur k et qui est de degré d; on choisit alors sur S un diviseur D_2 rationnel sur k de degré $2d'$, diviseur dont l'existence résulte de *i)*. Le diviseur $D = D_1 - D_2$ est un diviseur sur S rationnel sur k et de degré 1. Le k−espace vectoriel $L_k(D)$ est de dimension 2, donc contient des fonctions non nulles ; soit f une telle fonction, le diviseur $(f) + D$ est un diviseur sur S qui est effectif, de degré 1, et rationnel sur k; cela achève la démonstration.

Plaçons nous maientenant dans le cas d impair ; la conjonction des deux lemmes précédents montre que, soit la conique S est triviale (i.e. possède des points rationnels sur k) et alors tout pinceau G−invariant est un k−pinceau, soit elle ne l'est pas et alors elle ne possède pas de k−pinceau (puisque elle ne possède pas de diviseur de degré d rationnel sur k). Dans ce dernier cas les pinceaux G−invariants se décrivent de la manière suivante :

PROPOSITION 1.5. *Soit S une conique non singulière définie sur le corps k et qui ne possède pas de points rationnels sur k, soit d un entier naturel impair, soit K une extension quadratique de k qui est contenue dans $\overline{k}$ et sur laquelle la conique*

S possède des points, et soit Δ un diviseur effectif de degré d qui est rationnel sur K; il existe un et un seul un pinceau linéaire G−invariant contenant Δ. De plus tous les pinceaux G−invariants sont obtenus de cette manière.

Démonstration : Désignons par σ un élément de G qui n'est pas trivial sur K; le diviseur ${}^{\sigma}\Delta - \Delta$ est rationnel sur K et de degré 0, donc est le diviseur d'une fonction g définie sur K. Le transformé ${}^{\sigma}\Delta$ de Δ par σ n'est pas égal à Δ puisque (lemme 1.4. *ii*)) S ne possède pas de diviseur rationnel de degré d sur k, donc la fonction g n'est pas constante. Désignons par Λ le pinceau linéaire dont les éléments sont les $(\alpha + \beta.g) + \Delta$ où α et β sont dans $\overline{k}$; ce pinceau contient le diviseur ${}^{\sigma}\Delta$ puisque ${}^{\sigma}\Delta = (g) + \Delta$, donc c'est le pinceau engendré par les deux diviseurs Δ et ${}^{\sigma}\Delta$. Le diviseur de ${}^{\sigma}g$ est $\Delta - {}^{\sigma}\Delta$, donc ${}^{\sigma}g = \frac{\lambda}{g}$ où λ est un élément de K; ainsi, si $(\alpha + \beta.g) + \Delta$ est un élément de Λ, son image par σ est ${}^{\sigma}[(\alpha + \beta.g) + \Delta] = ({}^{\sigma}\alpha + {}^{\sigma}\beta.{}^{\sigma}g) + {}^{\sigma}\Delta = ({}^{\sigma}\alpha + {}^{\sigma}\beta.\frac{\lambda}{g}) + {}^{\sigma}\Delta = ({}^{\sigma}\alpha.g + {}^{\sigma}\beta.\lambda) - (g) + {}^{\sigma}\Delta = ({}^{\sigma}\alpha.g + {}^{\sigma}\beta.\lambda) + \Delta$ qui est encore dans Λ. Cela montre que Λ est invariant par σ ; comme il est aussi clairement invariant par $Gal(\overline{k}/K)$, il est G−invariant. Le pinceau Λ est donc un pinceau G−invariant qui contient Δ; c'est le seul puisque tout pinceau G−invariant contenant Δ contient aussi ${}^{\sigma}\Delta$, et que Λ est engendré par ces deux diviseurs. Enfin, si Λ est un pinceau G−invariant, alors c'est aussi un pinceau G_K−invariant ; comme S possède des points rationnels sur K, le lemme 1.3. affirme que Λ est un K−pinceau ; en conséquence Λ contient des diviseurs rationnels sur K; si Δ est un tel diviseur, le pinceau Λ est donc l'unique pinceau G−invariant contenant Δ dont on vient de prouver l'existence.

2. Le cas c=2. Dans ce paragraphe S est, comme précédemment, une conique non singulière, et Λ est un pinceau linéaire sur lequel nous faisons les hypothèses suivantes : Λ est de degré 3 (i.e. $c + 1$ avec $c = 2$) et sans point base. La première hypothèse implique que la courbe de Poncelet C associée au pinceau Λ est une courbe de degré 2; remarquons que la deuxième implique que C est non singulière, i.e. montrons le lemme suivant :

LEMME 2.1. *Soit S une conique non singulière et Λ un pinceau linéaire de degré 3 sans point base, alors la courbe de Poncelet associée à Λ est non singulière.*

Démonstration : On sait ([*Tr*], paragraphe 5, corollaire de la proposition 5.1.) que la courbe de Poncelet associée au pinceau sans point base Λ est non singulière si et seulement si la condition suivante est réalisée : si $n_1(\mathbf{P}_1) + .. + n_r(\mathbf{P}_r)$ est un diviseur appartenant au pinceau Λ (les n_i sont des entiers naturels positifs et les $\mathbf{P}_i$ sont des points de S), alors tous les n_i sont inférieurs ou égaux à 3 et l'un d'eux au plus est différent de 1. Dans le cas qui nous interesse, si $n_1(\mathbf{P}_1) + .. + n_r(\mathbf{P}_r)$ est un élément de Λ, la somme des n_i est égale à 3 donc la

condition énoncée ci dessus est satisfaite.

En plus des hypothèses faites au début de ce paragraphe, supposons que S est définie sur k et que le faisceau Λ est $G-$invariant ; la courbe de Poncelet C est alors une conique non singulière (comme nous venons de le voir), qui est définie sur k (comme nous l'avons vu au paragraphe précédent). On a :

PROPOSITION 2.2. *Soit S une conique non singulière définie sur k, et soit Λ un pinceau linéaire de degré 3 sur S qui est $G-$invariant et sans point base. La courbe de Poncelet C associée à Λ est une conique non singulière, définie sur k, et qui possède des points rationnels sur k si et seulement si S en possède.*

Démonstration : Les deux premières assertions ont déja été prouvées. Supposons que la courbe S possède des points rationnels sur k; elle possède alors des diviseurs effectifs de degré 3 rationnels sur k, donc (lemme 1.3.) le pinceau Λ est un $k-$pinceau, et donc il contient des diviseurs rationnels sur k. Soit $\mathbf{D}$ un tel diviseur, et soient $\mathbf{Q}_1,\mathbf{Q}_2,\mathbf{Q}_3$ les trois points d'intersections (non nécessairement tous distincts) des trois tangentes à S issues des trois points du support de $\mathbf{D}$ (si $\mathbf{D}$ contient un point avec une multiplicité m, on compte m-fois la tangente correspondante) ; pour tout $\sigma \in G$, on a ${}^{\sigma}\mathbf{D} = \mathbf{D}$; en conséquence, pour tout $\sigma \in G$, on a $({}^{\sigma}\mathbf{Q}_1) + ({}^{\sigma}\mathbf{Q}_2) + ({}^{\sigma}\mathbf{Q}_3) = (\mathbf{Q}_1)+(\mathbf{Q}_2)+(\mathbf{Q}_3)$ c'est à dire que le diviseur $(\mathbf{Q}_1)+(\mathbf{Q}_2)+(\mathbf{Q}_3)$ de la conique C est rationnel sur k; on en déduit (lemme 1.3. *ii*)) que la conique C admet des points rationnels. Réciproquement, supposons que la conique C admet des points rationnels sur k; rappelons ([*Tr*], *b*) de la démonstration de la proposition 1.3.) que, pour tout point $\mathbf{Q}$ de C, il existe un diviseur $\mathbf{D}$ de S et un seul appartenant au pinceau Λ tel que $\mathbf{Q}$ est l'un des points d'intersections des tangentes à S issues des points du support de $\mathbf{D}$. Choisissons pour $\mathbf{Q}$ un point de C rationnel sur k, et désignons par $\mathbf{D}$ l'unique diviseur de S appartenant à Λ qui est associé à $\mathbf{Q}$ comme on vient de l'expliquer ; pour tout $\sigma \in G$, on a ${}^{\sigma}\mathbf{Q} = \mathbf{Q}$, donc on a ${}^{\sigma}\mathbf{D} = \mathbf{D}$, c'est à dire que le diviseur $\mathbf{D}$ est rationnel sur k; on en déduit (lemme 1.3. *ii*)) que la conique S admet des points rationnels ; cela achève la démonstration.

COROLLAIRE 2.3. *Soit S une conique non singulière définie sur le corps k et soit K un corps contenant k (non nécessairement contenu dans $\overline{k}$). Soit Λ un pinceau linéaire de degré 3 sur S qui est $G-$invariant et sans point base. La courbe de Poncelet C associée à Λ est une conique non singulière, définie sur k, et qui possède des points rationnels sur K si et seulement si S en possède.*

Démonstration : On introduit une cloture algébrique $\overline{K}$ de K; par extension des scalaires, les données S et Λ définissent une conique du plan projectif sur $\overline{K}$ qui est non singulière et définie sur K, et un pinceau $Gal(\overline{K}/K)-$invariant sur

cette conique. La courbe de Poncelet associée à cette conique et à ce pinceau est la courbe obtenue à partir de C par extension des scalaires à K. Notre résultat est donc le résultat de la proposition précédente avec k remplacé par K.

Nous pouvons maintenant prouver le résultat annoncé dans l'introduction :

THÉORÈME 2.4. *Soit S une conique non singulière définie sur k, et soit Λ un pinceau linéaire de degré 3 sur S qui est $G-$invariant et sans point base ; la courbe de Poncelet C associée à Λ est isomorphe à S sur le corps k.*

Démonstration : En vertu du corollaire 2.3. ce théorème résulte du lemme suivant :

LEMME 2.5. *Deux coniques non singulières définies sur le corps k sont isomorphes sur k si et seulement si les extensions de k dans lesquels elles ont des points sont les mêmes.*

Démonstration : Désignons par C_1 et C_2 ces deux coniques ; par hypothèse, où bien elles possèdent toutes les deux des points sur le corps k, où bien aucune d'elles ne possèdent de points sur ce corps. Dans le premier cas les deux coniques sont triviales sur k, i.e. sont isomorphes, sur k, à la droite projective, donc elles sont isomorphes sur k. Dans le deuxième cas nous considérons le corps $k(C_1)$ des fonctions rationnelles sur la conique C_1 qui sont définies sur k; c'est une extension de k dans laquelle C_1 a des points ; par hypothèse cela implique que C_2 a des points dans cette extension. Notons $[C_1]$ (resp. $[C_2]$) les éléments du groupe de Brauer $Br(k)$ de k associés à la conique C_1 (resp. C_2) par le dictionnaire classique. Aucun des deux éléments $[C_1]$ et $[C_2]$ ne sont nuls puisque ni C_1, ni C_2 n'ont de points rationnels sur k, et ces deux éléments sont dans le noyau de l'inflation de $Br(k)$ vers $Br(k(C_1))$ puisque C_1 et C_2 ont toutes les deux des points dans $k(C_1)$. Mais le noyau de l'inflation de $Br(k)$ vers $Br(k(C_1))$ est, comme nous le rappellons ci dessous (Lemme 2.6.), isomorphe à $\mathbf{Z}/2\mathbf{Z}$; on en déduit que $[C_1]$ et $[C_2]$ sont tous les deux égaux à l'élément non nul de ce noyau, donc que $[C_1] = [C_2]$; cela signifie que les coniques C_1 et C_2 sont isomorphes sur k et prouve le "si" du lemme ; le "seulement si" est trivial.

LEMME 2.6. *Soit C une conique plane, projective, non singulière, définie sur k, et sans point rationel sur k; le noyau de l'inflation du groupe de Brauer $Br(k)$ du corps k vers le groupe de Brauer $Br(k(C)$ du corps $k(C)$ est isomorphe à $\mathbf{Z}/2\mathbf{Z}$.*

Démonstration : On note $Div(C)$ le groupe des diviseurs sur C, $P(C)$ le sous groupe de $Div(C)$ formé des diviseurs principaux (i.e. des diviseurs des

éléments non nuls de $\overline{k}(C)$), et $Pic(C)$ le groupe quotient $Div(C)/P(C)$. Comme nous l'avons rappelé au début du premier paragraphe, le groupe de Galois $G = Gal(\overline{k}/k)$ agit sur les points et sur les fonctions de C; ces actions induisent des actions naturelles de G sur les trois groupes $Div(C), P(C)$, et $Pic(C)$. L'application de $\overline{k}(C)^\times$ vers $P(C)$ qui envoie une fonction non nulle sur son diviseur est, par définition de $P(C)$, surjective; comme C est une courbe projective, le noyau de cette surjection est $\overline{k}^\times$. On a donc une suite exacte de $G-$modules $0 \to \overline{k}^\times \to \overline{k}(C)^\times \to P(C) \to 0$; de la suite exacte longue de cohomologie associée, nous extrayons $H^1(G, \overline{k}(C)^\times) \to H^1(G, P(C)) \to Br(k) \to H^2(G, \overline{k}(C)^\times)$. Rappelons que G s'identifie au groupe de Galois de l'extension $\overline{k}(C)/k(C)$; il en résulte d'une part que $H^1(G, \overline{k}(C)^\times) = 0$ (Théorème 90 de Hilbert), et d'autre part que $H^2(G, \overline{k}(C)^\times)$ s'injecte par inflation dans le groupe de Brauer $Br(k(C))$ du corps $k(C)$. Le composé de cette inflation et de la flèche de $Br(k)$ vers $H^2(G, \overline{k}(C)^\times)$ de la suite exacte longue de cohomologie est l'inflation de $Br(k)$ vers $Br(\overline{k}(C))$, donc le noyau de cette inflation est isomorphe à $H^1(G, P(C))$. Nous devons donc montrer que $H^1(G, P(C))$ est isomorphe à $\mathbf{Z}/2\mathbf{Z}$. Pour cela nous remarquons que, par définition de $Pic(C)$, on a une suite exacte de $G-$modules $0 \to P(C) \to Div(C) \to Pic(C) \to 0$; de la suite exacte longue de cohomologie associée on extrait la suite exacte $Div(C)^G \to Pic(C)^G \to H^1(G, P(C)) \to H^1(G, Div(C))$. Rappelons que $H^1(G, Div(C)) = 0$: en effet, pour chaque orbite $c = \{\mathbf{P}_1, .., \mathbf{P}_d\}$ de l'action de G sur les points de C, notons $Div_c(C)$ le sous groupe de $Div(C)$ formé des diviseurs dont le support est inclus dans l'ensemble $\{\mathbf{P}_1, .. \mathbf{P}_d\}$; il est clair que $Div_c(C)$ est un sous $G-$module de $Div(C)$ et que $Div(C)$ est la somme directe $\oplus_c Div_c(C)$ où c décrit toutes les orbites de l'action de G sur C; on a donc $H^1(G, Div(C)) = \oplus_c H^1(G, Div_c(C))$, et on conclut en remarquant que, pour tout orbite c, le $G-$module $Div_c(C)$ est induit au sens de [*Se*.1] (i.e. coinduit au sens de [*Se*.2]), donc que $H^1(G, Div_c(C)) = 0$). La courbe C étant de genre 0, un élément de $Div(C)$ est dans $P(C)$ si et seulement si il est de degré 0; on en déduit d'une part que l'application "degré" de $Div(C)$ sur $\mathbf{Z}$ induit un isomorphisme de $Pic(C)$ sur $\mathbf{Z}$, et d'autre part que l'action de G sur $Pic(C)$ est triviale (en effet, si x est un élément de $Pic(C)$ et si $\mathbf{D}$ est un diviseur dont l'image dans $Pic(C)$ est x, alors, pour tout σ dans G, la classe de ${}^\sigma\mathbf{D}$ est par définition l'image de x par σ; mais le diviseur ${}^\sigma\mathbf{D} - \mathbf{D}$ est de degré 0, donc les images de ${}^\sigma\mathbf{D}$ et de $\mathbf{D}$ dans $Pic(C)$ sont égales). Par hypothèse la conique C ne possède pas de points rationnels, donc (lemme 1.4 *ii*)) elle ne possède pas de diviseurs de degré 1 rationnel sur k, c'est à dire qu'il n'y a pas de diviseur de degré 1 dans le sous groupe $Div(C)^G$ de $Div(C)$. Par contre, $Div(C)^G$ contient les diviseurs intersections de C et des droites rationnels, et ceux ci sont de degré

2. On déduit de ces deux derniers points que le quotient de $Pic(C)^G$ par l'image de $Div(C)^G$ est isomorphe à $\mathbf{Z}/2\mathbf{Z}$, ce qu'on voulait.

REFERENCES

[Se.1] SERRE J.P., *Cohomologie Galoisienne*, L.N. n^0 5, Springer-Verlag, (1965).

[Se.2] SERRE J.P., *Corps locaux*, Pub. Math. Université de Nancago, Hermann, deuxième édition (1968).

[Tr] TRAUTMANN G., *Poncelet curves and associated Theta characteristic*, Expositiones Mathematematicae, Band 6, Heft 1, (1988), pp.29-64.

[We] WEIL A., *Foundations of algebraic geometry*, A.M.S. Colloquium Publications, vol. XXIX, (1946).

Ph. SATGÉ
Université de Caen
Département de Mathématiques
Esplanade de la Paix
14032 CAEN CEDEX
FRANCE

Astérisque

NORBERT SCHAPPACHER

Les conjectures de Beilinson pour les courbes elliptiques

Astérisque, tome 198-199-200 (1991), p. 305-317

<http://www.numdam.org/item?id=AST_1991__198-199-200__305_0>

Les Conjectures de Beilinson pour les courbes elliptiques

Norbert Schappacher

Table des Matières

S.M.F.
Astérisque 198-199-200 (1991)

0. Remarques préliminaires

Dans ce rapport qui se veut une introduction pour non-spécialistes, j'essaie de décrire ce qu'on sait — et ce qu'on ignore — des conjectures de Beilinson relatives aux valeurs spéciales aux points entiers de la fonction L d'une courbe elliptique sur $\mathbf{Q}$. Quelques remarques préliminaires s'imposent.

D'abord, force est de constater que le point de vue des courbes elliptiques proposé ici n'est pas suggéré par la nature des conjectures et résultats en jeu, mais par le désir de rester aussi concret que possible. En fait, nous verrons à plusieurs endroits que le formalisme de Beilinson a tendance à nous faire sortir du cadre des courbes elliptiques.

Soulignons d'ailleurs que 'courbe elliptique' veut dire ici : 'courbe elliptique définie sur $\mathbf{Q}$'. Ceci est essentiel; car dans toutes les conjectures motiviques sur des valeurs spéciales de fonctions L, on traite une variété (plus généralement un motif) V définie sur un corps de nombres K par l'intermédiaire de sa restriction des scalaires à $\mathbf{Q}$, $R_{K/\mathbf{Q}}V$. Si V est une courbe elliptique, alors $R_{K/\mathbf{Q}}V$ est une variété abélienne sur $\mathbf{Q}$ de dimension $[K : \mathbf{Q}]$, ce qui nous jetterait dans des eaux bien plus froides que celles du cas des courbes .....

Le cadre des courbes elliptiques sur $\mathbf{Q}$ — pour peu naturel qu'il soit — me permet d'éviter dans cet exposé le formalisme général et abstrait des conjectures de Beilinson. Bien sûr, le prix qu'on paie est que les diverses méthodes présentées ici sembleront vraiment différentes. Le lecteur intéressé pourra se rapporter aux premiers chapitres du livre [Rapoport, Schappacher, Schneider 1988] pour la théorie générale. D'autre part, à la fin, on mentionnera brièvement quelques résultats obtenus depuis la rédaction de ce livre.

Dernière remarque préliminaire: l'approche qu'on prend ici retrace partiellement l'évolution historique des conjectures dont la version générale et actuelle est due à Beilinson.

1. La fonction L

Soit E une courbe elliptique sur $\mathbf{Q}$. La fonction L de E est définie par le produit eulérien suivant, convergent pour tout $s \in \mathbf{C}$, $\Re(s) > 3/2$.

$$L(E,s) = \prod_p L_p(E,s)^{-1}, \tag{1.0}$$

où, pour tout nombre premier p de *bonne réduction* pour E — c'est-à-dire pour tout p tel qu'on puisse trouver une équation pour E qui, lue *modulo* p, définit une courbe non-singulière $\tilde{E}_p$ sur le corps fini $\mathbf{F}_p$ — le facteur eulérien en p est donné par

$$L_p(E,s) = (1 - a_p p^{-s} + p^{1-2s}); \quad a_p = p + 1 - |\tilde{E}_p(\mathbf{F}_p)|. \tag{1.1}$$

Nous ne précisons pas ici les facteurs eulériens aux *mauvaises places* p — mais *voir* (3.4). De même nous ne définissons pas ici le *conducteur* N de la courbe E. C'est un entier positif divisible précisément par les nombres premiers où E a mauvaise réduction.

Posons

$$\Lambda(E,s) = N^{s/2}\Gamma(s)(2\pi)^{-s}L(E,s).$$

On conjecture que cette fonction possède un prolongement holomorphe à tout le plan complexe satisfaisant à l'équation fonctionnelle suivante, valable pour tout $s \in \mathbf{C}$:

$$\Lambda(E,s) = w\ \Lambda(E,2-s), \tag{1.2}$$

avec un nombre réel w de valeur absolue 1, donc: $w = \pm 1$.

Cette conjecture est connue précisément dans les cas où on sait que $L(E,s)$ est la transformée de Mellin d'une forme modulaire parabolique sur $\Gamma_0(N)$. Ceci s'exprime de façon géométrique en disant que E est paramétrée par une courbe modulaire $X_0(N)$. C'est-à-dire qu'il existe une application non-constante $\phi: X_0(N) \longrightarrow E$ définie sur $\mathbf{Q}$. On conjecture, d'après Taniyama et Shimura, que toute courbe elliptique sur $\mathbf{Q}$ admet une telle paramétrisation, et, d'après Weil, cette conjecture découlerait de certaines propriétés analytiques — dont l'équation fonctionnelle ci-dessus — de certaines fonctions du même type que la fonction $L(E,s)$.

Nous supposerons par la suite que E soit paramétrée par une courbe modulaire $X_0(M)$. Nous disposerons donc du prolongement analytique de $L(E,s)$; mais cette hypothèse nous permettra aussi de faire certaines constructions 'modulaires' ....

Choisissons en fait pour M l'entier positif minimal pour lequel une paramétrisation $\phi: X_0(M) \longrightarrow E$ existe. Alors on sait, d'après une longue suite de travaux dont le plus récent est dû à Carayol [Carayol 1983], que c'est le conducteur de E: $M = N$.

2. Le centre de symétrie

Le but des conjectures de Beilinson relatives à E est de prédire, à un facteur rationnel non nul près, la valeur $L^{(r)}(E,n)$ de la première dérivée non nulle de la fonction $L(E,s)$ en tout entier s. Le premier point qui vient à l'esprit — et dans un sens le plus critique — est $s = 1$, le centre de symétrie de l'équation fonctionnelle. Or, l'ordre r de L en $s = 1$ aussi bien que la valeur $L^{(r)}(E,n)$ font l'objet des *conjectures de Birch et Swinnerton-Dyer*. Ce 'point central' $s = 1$ est aussi traité par les conjectures générales de Beilinson. Mais il en représente un cas limite. C'est d'ailleurs la raison pour laquelle les adaptations nécessaires dans le cadre de Beilinson pour traiter le point central ne sont que brièvement mentionnées dans [Rapoport, Schappacher, Schneider 1988]. Soucieux de présenter les conjectures de Beilinson à l'état pur, nous laisserons de même de côté le point $s = 1$ dans la suite de cet exposé.

3. En sortant du centre

En dehors du centre $s = 1$, l'équation fonctionnelle (1.2), jointe à la convergence du produit eulérien (1.0) aux entiers > 1, détermine déjà l'ordre de $L(E,s)$ aux points entiers: $L(E,n) \neq 0$ pour $n \geq 2$ et $L(E,m) = 0 \neq L'(E,m)$ pour $m \leq 0$.

Le premier couple de nombres qu'il s'agit de caractériser à un multiple rationnel près est donc

$$L'(E,0) \quad \text{et} \quad L(E,2). \tag{3.0}$$

Bloch — *voir* [Bloch 1978] — a formulé et développé la conjecture de Beilinson relative à ces valeurs.[1]

D'après Bloch, on conjecture que les nombres (3.0) sont liés à des régulateurs de certains éléments du groupe $K_2(E)$. Nous ne reprenons pas la définition de ce K-groupe de Quillen.[2] Mais nous allons en voir quelques éléments. Pour le moment, disons simplement qu'on construit une application 'régulateur' sur $K_2(E)$ que nous écrivons de façon un peu naïve en choisissant une différentielle non nulle $\omega \in H^0(E,\Omega^1)$ définie sur $\mathbf{R}$;

$$r_\omega: K_2(E) \longrightarrow \mathbf{R}. \tag{3.1}$$

[1] Avant on savait interpréter des valeurs spéciales de la fonction zêta d'un corps de nombres de façon K-théorique, grâce au travail de Borel [Borel 1974] — *cf.* aussi les conjectures de Lichtenbaum.

[2] L'article fondamental reste, bien sûr, [Quillen 1973].

Le folklore du sujet dit que le noyau de l'homomorphisme r_ω est précisément $K_2(E)_{tors}$.[3] Donc, *si* $K_2(E)$ est de rang 1 *modulo* torsion — *cf.* la conjecture [Bloch 1978, p. 512] —, *alors* l'image de r_ω serait un réseau dans $\mathbf{R}$. Tensoriser par $\mathbf{Q}$ en ferait une $\mathbf{Q}$-droite dans $\mathbf{R}$, dont on conjecture que c'est l'unique $\mathbf{Q}$-droite dans $\mathbf{R}$ qui contient $\omega_1 L'(E,0)$, où

$$\omega_1 = \Big| \int_{E^\circ(\mathbf{R})} \omega \Big| \tag{3.2}$$

est la période réelle de la différentielle choisie.

En fait, le rang de $K_2(E)$ ne vaut pas toujours 1, *i.e.*, n'est pas toujours égal à l'ordre du zéro de $L(E,s)$ en $s=0$. Ceci a été remarqué par Bloch et Grayson [Bloch, Grayson 1986], à l'aide de calculs sur ordinateur, pour certaines courbes elliptiques. Pour comprendre ce qui se passe, il faut considérer de plus près l'arithmétique de la courbe E. Ecrivons une partie de la suite exacte de localisation [Quillen 1973, §7, Prop. 3.1] du modèle régulier $\mathcal{E}$ relative à sa fibre générique E :[4]

$$\coprod_p K'_2(\mathcal{E}_p) \longrightarrow K_2(\mathcal{E}) \longrightarrow K_2(E) \xrightarrow{\partial=\coprod \partial_p} \coprod_p K'_1(\mathcal{E}_p) \longrightarrow (\text{torsion ?}) \tag{3.3}$$

Ici, le premier terme est de torsion et les conjectures générales de Beilinson impliquent que le dernier terme est réduit à son sous-groupe de torsion. Mais les groupes K'_1[5] des fibres spéciales du modèle régulier se calculent explicitement, mise à part la torsion : $K'_1(\mathcal{E}_p) \otimes \mathbf{Q}$ est non nul si et seulement si E a mauvaise réduction multiplicative déployée en p. Autrement dit, si la réduction $\tilde{E}_p$ en p est une courbe singulière avec un point double dont les droites tangentes sont déjà définies sur le corps $\mathbf{F}_p$, non seulement sur $\mathbf{F}_{p^2}$. Dans ce cas on trouve $L_p(E,s) = 1 - p^{-s}$ de sorte qu'on a

$$dim_{\mathbf{Q}}\, K'_1(\mathcal{E}_p) \otimes \mathbf{Q} = 1 = \mathrm{ord}_{s=0}\, L_p(E,s). \tag{3.4}$$

Les *Conjectures de Beilinson* relatives aux nombres (3.0) s'énoncent alors comme ceci:

3.5 Conjecture.

(i) $dim_{\mathbf{Q}}\, K_2(\mathcal{E}) \otimes \mathbf{Q} = 1$.

(ii) $r_\omega(K_2(\mathcal{E}) \otimes \mathbf{Q}) = \omega_1 . L'(E,0)\ \mathbf{Q}$.

4. Problèmes de K-théorie

En essayant de traiter cette conjecture on se heurte à deux difficultés contradictoires : d'une part on ignore si $K_2(E) \otimes \mathbf{Q}$ est un espace vectoriel de dimension finie; d'autre part on a du mal à construire explicitement des éléments non nuls dans cet espace.

---

[3] L'analogie avec le cas des corps de nombres est souvent appropriée. Ici on peut se souvenir de l'application logarithmique sur les unités d'un corps de nombres qui définit son régulateur. — *Cf.* la note suivante.

[4] Voici l'analogie avec le cas d'un corps de nombres k: dans ce cas, le K-groupe correspondant à $\zeta(k,0)$ et $\mathrm{rés}_{s=1}\, \zeta(k,s)$ est K_1, et on a $K_1(k) = k^*$, mais $K_1(\mathcal{O}_k) = \mathcal{O}_k^*$: les unités, qui donnent le régulateur usuel.

[5] Ce sont les groupes analogues aux K-groupes, mais définis en termes de modules cohérents au lieu de modules projectifs. Les théories K' et K coincident sur les schémas réguliers. — Pour calculer les $K'_1(\mathcal{E}_p)$, on se sert de dévissages du type indiqués dans [Quillen 1973, §7, n° 3]. Il s'avère que, à torsion près, on obtient l'homologie du graphe dual de $\mathcal{E}$.

Le premier problème est le plus difficile. Posons $J = H^0(E, \mathcal{K}_2)/\ K_2(\mathbf{Q})$, où $\mathcal{K}_2$ est le faisceau (de Zariski) sur E associé au préfaisceau qui à un ouvert U de E associe $K_2(\Gamma(U, \mathcal{O}_E))$. On sait grâce à Raskind [Raskind 1984] — le cas considéré ici remonte en fait à Bloch — que, pour tout entier $n > 0$, le groupe $J/n.J$ est fini. De plus — *voir* [Soulé 1985] — on sait que $H^0(E, \mathcal{K}_2) \otimes \mathbf{Q} = K_2(E) \otimes \mathbf{Q}$. Par conséquent, $K_2(E)/nK_2(E).K_2(E)_{tors}$ est fini, pour tout $n > 0$. Mais ceci n'implique pas que $K_2(E)/K_2(E)_{tors}$ est de type fini. Faudrait-il construire une espèce de 'hauteur' sur $K_2(E)$ .....?

Quant à la construction d'éléments de $K_2(E) \otimes \mathbf{Q}$, on dispose à présent de deux méthodes différentes : soit on travaille 'sur la courbe elle-même', soit on utilise la paramétrisation modulaire. Chaque fois qu'on a ainsi construit des éléments non nuls dans $K_2(\mathcal{E}) \otimes \mathbf{Q}$, on cherche à comparer leurs régulateurs à $L'(E, 0)$ selon 3.5 (ii). On parle alors du problème de démontrer une *conjecture de Beilinson faible* relative au sous-espace des éléments construits. Bien sûr, si l'on savait démontrer 3.5 (i), toutes ces conjectures faibles seraient équivalentes entre elles, et à la conjecture 3.5 (ii) tout entière.

5. Construction d'éléments de $K_2(E)$ 'sur la courbe E'

Cette première méthode pour se donner des éléments de $K_2(E)$ s'appuie essentiellement sur les points de torsion de E.[6] En fait, pour tout $d > 1$, on construit une application

$$\xi = \xi_d : \mathbf{Q}[E_d]^\circ \longrightarrow K_2(E) \otimes \mathbf{Q}, \tag{5.0}$$

où $\mathbf{Q}[E_d]^\circ$ est le $\mathbf{Q}$-espace vectoriel des diviseurs à coefficients rationnels sur E qui sont *définis sur* $\mathbf{Q}$ *en tant que diviseurs,* de degré zéro et à support dans les points de d-torsion de E.

Nous donnerons une esquisse de la construction de ξ_d dans le numéro suivant. Pour l'instant, caractérisons ξ_d par l'application $r_\omega \circ \xi_d$.

Rappelons que ω_1 est la période réelle de ω. Choisissons ω_2 tel que $\tau = \frac{\omega_2}{\omega_1}$ ait une partie imaginaire $y = \Im(\tau)$ positive et tel que le réseau $L = \mathbf{Z} + \mathbf{Z}\tau \subset \mathbf{C}$ soit le réseau rendant $(\mathbf{C}/L, dz)$ isomorphe à $(E, \frac{\omega}{\omega_1})$ sur $\mathbf{C}$. Nous utiliserons des notations (légèrement modifiées) de [Weil 1976, *chap. VIII*] :

$$A(L) = \frac{y}{\pi}, \quad \langle \gamma, x \rangle = exp\,(\frac{\gamma\overline{x} - x\overline{\gamma}}{A(L)}). \tag{5.1}$$

Pour tout diviseur $\mathbf{a} = \sum_{x \in \mathbf{C}/L} a_x(x)$ sur $E(\mathbf{C})$ et tout entier $\nu \geq 0$, on pose alors, pour tout s tel que $\Re(s) > \frac{\nu}{2} + 1$:

$$K_\nu(0, \mathbf{a}, s) = \sum_{x \in \mathbf{C}/L} a_x \sum_{\gamma \in L}{}' \langle \gamma, x \rangle \frac{\overline{\gamma}^\nu}{(\gamma\overline{\gamma})^s}. \tag{5.2}$$

Pour $s \in \mathbf{C}$ quelconque, les valeurs de ces *doubles séries de Kronecker* sont définies par prolongement analytique.

Avec ces notations, les éléments de $\mathbf{Q}[E_d]^\circ$ s'identifient sur $\mathbf{C}$ à des diviseurs $\mathbf{a}$ comme ci-dessus sur $E(\mathbf{C}) \cong \mathbf{C}/L$. On normalise alors ξ de telle façon que, pour tout $\mathbf{a} = \sum_{d.x=0} a_x(x)$ appartenant à $\mathbf{Q}[E_d]^\circ$, on ait

$$r_\omega(\xi_d(\mathbf{a})) = -d^2\omega_1\,(\frac{y}{\pi})^2 K_1(0, \mathbf{a}, 2). \tag{5.3}$$

Cette méthode nous donne donc la conjecture de Beilinson faible suivante (utiliser l'équation fonctionnelle (1.2) pour traduire (3.5) (ii) en un énoncé en $s = 2$) :

[6] Il y a quelques exemples d'éléments non nuls de $K_2(E)$ obtenus à partir de points rationnels d'ordre *infini* — *voir* [Mestre, Schappacher 1990, 1.3.3].

5.4 Conjecture. *Pour tout $d > 1$ et tout $\mathbf{a} \in \mathbf{Q}[E_d]^\circ$; si $\xi(\mathbf{a}) \in K_2(\mathcal{E}) \otimes \mathbf{Q} \subseteq K_2(E) \otimes \mathbf{Q}$, alors*

$$y^2 K_1(0, \mathbf{a}, 2) \in L(E, 2).\mathbf{Q}.$$

Pour rendre cette conjecture vraiment explicite, il faut pouvoir décider :

(5.5) Pour quel $\mathbf{a} \in \mathbf{Q}[E_d]^\circ$, l'élément $\xi(\mathbf{a})$ de $K_2(E) \otimes \mathbf{Q}$ appartient-il à $K_2(\mathcal{E}) \otimes \mathbf{Q}$?

(5.6) Pour quel $\mathbf{a} \in \mathbf{Q}[E_d]^\circ$, la série $K_1(0, \mathbf{a}, 2)$ est-elle non nulle ?

La réponse complète à la première question est donnée par une formule calculant les symboles modérés ∂_p de (3.3) à un facteur non nul près. *Voir* [Bloch, Grayson 1986], [Mestre, Schappacher 1990, 1.5.1 et 2.5.1] et [Schappacher, Scholl 1990]. La formule dépend des degrés des réstrictions de $\mathbf{a}$ aux composantes irréductibles de la fibre spéciale $\mathcal{E}_p$ et fait intervenir le troisième polynôme de Bernoulli.

En ce qui concerne (5.6), $K_1(0, \mathbf{a}, 2)$ ne devrait pas s'annuler 'sans raison'. Malheureusement il y a en général de très fortes raisons qui forcent la plupart des $K_1(0, \mathbf{a}, 2)$ à être nulles. En effet, la fonction $x \mapsto K_1(x', x, s)$ est impaire. Donc, si le diviseur $\mathbf{a}$ est invariant par $x \mapsto -x$, alors $K_1(0, \mathbf{a}, 2) = 0$. Or, si l'image de Galois par l'action sur les points de d-torsion $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{Aut}(E_d)$ contient -1, cette invariance est forcée par le fait que $\mathbf{a}$ est défini sur $\mathbf{Q}$.

Cette condition sur l'image de Galois est souvent satisfaite. Elle vaut systématiquement pour tout $d > 1$, dès que l'image de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ dans $\mathrm{Aut}(E_{tors}) = GL_2(\hat{\mathbf{Z}})$ est aussi grand que possible, c'est-à-dire d'indice deux — par exemple, si E est la courbe *37A*,[7] discutée dans [Serre 1972, *exemple 5.5.6*].

6. Définition de ξ

Une partie de la suite exacte de localisation de E par rapport à son corps de fonctions rationnelles $\mathbf{Q}(E)$ s'écrit :

$$\coprod_{P \in E} K_2(\mathbf{Q}(P)) \longrightarrow K_2(E) \longrightarrow K_2(\mathbf{Q}(E)) \xrightarrow{\partial = \coprod \partial_P} \coprod_{P \in E} \mathbf{Q}(P)^* \longrightarrow K_1(E) \tag{6.1}$$

Ici, $\mathbf{Q}(P)$ est le corps de définition du point P de E. D'après un théorème de Matsumoto, on a, pour tout corps F,

$$K_2(F) \cong F^* \otimes_{\mathbf{Z}} F^* / \langle f \otimes (1-f) \mid f \in F - \{0, 1\} \rangle. \tag{6.2}$$

De plus, si F est un corps de nombres, alors $K_2(F)$ est un groupe de torsion. On obtient donc une injection $K_2(E) \otimes \mathbf{Q} \hookrightarrow K_2(\mathbf{Q}(E)) \otimes \mathbf{Q}$.

Dans 6.2, le 'symbole' dans $K_2(F)$ correspondant à $f \otimes g$ est noté $\{f, g\}$. Le symbole modéré ∂_P est donné par la formule bien connue

$$\partial_P(\{f, g\}) = (-1)^{ord_P(f) ord_P(g)} \frac{f^{ord_P(g)}}{g^{ord_P(f)}}(P). \tag{6.3}$$

[7] On cite parfois des courbes par le nom qui leur est donné dans la "Table 1" de [Modular Functions ... IV].

Alors l'application ξ_d se construit en termes de symboles $\{f,g\} \in K_2(\mathbf{Q}(E))$. Etant donné $\mathbf{a} \in \mathbf{Q}[E_d]^\circ$, choisissons des fonctions $f,g \in \mathbf{Q}(E)$ de diviseurs $(f) = d\mathbf{a}$, resp. $(g) = 2[d^2(0) - \sum_{d.y=0}(y)]$. Par un lemme de Bloch [Bloch 1980, p. 8.6f], [Deninger, Wingberg 1988, Lemma 5.2], quitte à modifier le symbole $\{f,g\} \in K_2(\mathbf{Q}(E))$ par l'addition d'un symbole du type $\{h,c\}$, $h \in \mathbf{Q}(E)^*, c \in \mathbf{Q}^*$, on tombe dans $K_2(E) \otimes \mathbf{Q}$; c'est l'élément $\xi_d(\mathbf{a})$ recherché.

Le régulateur sur $K_2(\mathbf{Q}(E)) \otimes \mathbf{Q}$ est normalisé par la règle : si $\phi, \psi \in \mathbf{Q}(E)$ avec $(\phi) = \sum p_x(x)$, $(\psi) = \sum q_x(x)$, alors

$$r_\omega(\{\phi,\psi\}) = -\frac{1}{2}\omega_1 \, A(L)^2 \sum_{x,y} p_x q_y \, K_1(0, x-y, 2). \tag{6.4}$$

Ceci mène à la formule (5.3) ci-dessus (noter que les $\{h,c\}$ ont un régulateur nul). Remarquons que, si $d, e > 1$, alors on a

$$\xi_{de} = e^2 \xi_d. \tag{6.5}$$

7. Premier Cas: Courbes à multiplications complexes

Dans ce cas, la conjecture faible 5.4 a été démontrée par Bloch, *cf.* [Bloch 1978], [Bloch 1980]. Un exposé de cette démonstration du point de vue des conjectures générales de Beilinson se trouve dans [Deninger, Wingberg 1988]. Une présentation à la fois élémentaire et très raffinée a été donnée par Rohrlich, [Rohrlich 1987]. Voici son résultat.

7.1 Théorème. *[Rohrlich 1987] Soit E une courbe elliptique sur $\mathbf{Q}$ telle que $\mathrm{End}_{\overline{\mathbf{Q}}} E$ soit isomorphe à un idéal $\mathcal{B} = \mathbf{Z} + \mathbf{Z}\tau$ du corps quadratique imaginaire K. Alors pour tout choix de fonctions $\mathbf{Q}$-rationnelles sur E : $f,g \in \mathbf{Q}(E)$ à support dans E_{tors}, on trouve que*

$$\frac{r_\omega(\{f,g\})}{\omega_1 L'(E,0)} = -\sum_{x,y \in E_{tors}} (\mathrm{ord}_x f)(\mathrm{ord}_y g)\, \alpha(x-y),$$

avec des nombres rationnels $\alpha(x-y)$ qui ne dépendent que de l'orbite de $(x,y) \in E_{tors} \times E_{tors}$ sous l'action diagonale de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ et qui peuvent être calculés explicitement en termes du caractère de Hecke χ de K correspondant à E. De plus, pour un choix convenable de $f,g \in \mathbf{Q}(E)$, on trouve que $r_\omega(\{f,g\}) \neq 0$.

On démontre ce résultat grâce au fait bien connu — dû à Deuring — que la fonction L d'une courbe elliptique définie sur $\mathbf{Q}$ à multiplications complexes par K (définies sur $\overline{\mathbf{Q}}$) est une fonction L de Hecke du corps K : $L(E,s) = L(\chi,s)$. Et la fonction L d'un caractère de Hecke de K s'écrit comme combinaison linéaire de séries de Kronecker — c'est un exercice sur la théorie du corps de classes de K.

Notons qu'une courbe à multiplications complexes a partout bonne réduction potentielle — son invariant j est entier —, donc n'a jamais réduction multiplicative. Par conséquent, ∂ dans 3.3 est identiquement zéro et la question 5.5 a une réponse triviale.

Le cas des courbes à multiplications complexes est donc très favorable à la méthode du §5 poue se donner des éléments de $K_2(E)$. Rappelons quand même, du côté négatif, qu'on ne sait ni la finitude de $dim_{\mathbf{Q}} K_2(\mathcal{E}) \otimes \mathbf{Q} = dim_{\mathbf{Q}} K_2(E) \otimes \mathbf{Q}$, ni si les symboles $\{f,g\}$ considérés dans le théorème engendrent un $\mathbf{Q}$-espace fini.

8. Le cas général

Les courbes sans multiplication complexe sont beaucoup moins bien adaptées à la méthode du §5 — aussi bien pour des raisons théoriques qu'à cause de l'insuffisance de nos connaissances actuelles.

D'abord nous avons déjà remarqué à la fin du §5 qu'il peut très bien arriver en général que les images de toutes les applications ξ_d ne contiennent que des éléments de régulateurs zéro. La méthode du §5 ne nous donne donc pas de conjecture faible non triviale.

Supposons donc pour le reste de ce numéro que l'action de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ est suffisamment petite pour au'il existe des $r_\omega \circ \xi_d$ d'image non nulle. Alors, si E n'a pas de multiplication complexe, on ne sait pas démontrer la conjecture 5.4 — exception faite des rares cas où une comparaison de l'image des ξ_d aux éléments donnés par la méthode modulaire est possible: *voir* §10 plus loin. Toutefois on a des résultats numériques très convaincants, dûs à Bloch et Grayson [Bloch, Grayson 1986].[8] Bien sûr, ces calculs de quotients

$$\frac{y^2\ K_1(0,\mathbf{a},2)}{L(E,2)}$$

ne peuvent jamais *démontrer* que ce sont des nombres rationnels dès que $\partial(\xi_d(\mathbf{a})) = 0$. Mais le fait que Bloch et Grayson trouvent systématiquement et avec une excellente précision des fractions sans facteur premier surprenant est très rassurant. Tout ce qu'on peut *démontrer* sur ordinateur est que certaines séries $K_1(0,\mathbf{a},2)$ sont non nulles.

Il est intéressant de remarquer que ces vérifications numériques sont aussi un test, du côté des séries de Kronecker, de la conjecture suivante, conséquence formelle de 3.3 et 3.5,(i) :

$$dim_{\mathbf{Q}}\ K_2(E) \otimes \mathbf{Q} \stackrel{?}{=} 1 + |\{p \mid L_p(E.s) = 1 - p^{-s}\}| \tag{8.1}$$

En fait, comme on ne calcule que des éléments de la forme $\xi_d(\mathbf{a})$, le test est même plus fin :

Le phénomène des 'relations exotiques'

La différence la plus importante entre le cas général et celui des courbes à multiplications complexes est l'écart entre $K_2(\mathcal{E}) \otimes \mathbf{Q}$ et $K_2(E) \otimes \mathbf{Q}$, décrit selon 3.3 par le symbole modéré ∂. Le comportement de ∂ sur les éléments de la forme $\xi_d(\mathbf{a})$, joint à la conjecture 8.1, prédit donc la dimension du $\mathbf{Q}$-espace engendré par les $\xi_d(\mathbf{a})$. On cherche alors numériquement un nombre correspondant de dépendances linéaires sur $\mathbf{Q}$ entre les nombre réels $K_1(0,\mathbf{a},2)$. On appelle parfois *relations exotiques* ces relations linéaires entre séries de Kronecker forcées par le symbole modéré ∂, et non expliquées par la seule dimension conjecturée de l'espace ambiant $K_2(E) \otimes \mathbf{Q}$.

9. Construction modulaire d'éléments de $K_2(E)$

La deuxième méthode pour se donner des éléments de $K_2(E)$ repose sur l'hypothèse — que nous avons faite vers la fin du §1 — que E est paramétrée par une courbe modulaire. La méthode est due à Beilinson [Beilinson 1985] — pour les détails on renvoie à [Schappacher, Scholl 1988]. Voici l'idée principale.

Dans la construction de ξ au §6, on faisait appel à un lemme de Bloch qui permettait de relever des symboles de $K_2(\mathbf{Q}(E))$ à $K_2(E)$. En général, ce lemme s'applique à une courbe

[8] En préparant notre travail [Mestre, Schappacher 1990], Mestre et moi avons refait quelques-uns des calculs de Bloch et Grayson, et aussi traité d'autres courbes.

(projective lisse) X sur un corps F et des fonctions rationnelles $f, g \in F(X)$ dont les diviseurs sont à support dans un ensemble X^∞ de points de $X(\overline{F})$ tels que, pour tous $x, y \in X^\infty$, le diviseur de degré zéro $(x)-(y)$ soit un point de torsion de la jacobienne $\mathrm{Jac}(X)$. Alors quitte à modifier le symbole $\{f,g\} \in K_2(F(X))$ par un symbole du type $\{h,c\}$, $h \in F(X)^*, c \in F^*$, on peut le relever dans $K_2(X) \otimes \mathbf{Q}$.

On applique ce lemme aux courbes modulaires $X = X(\Gamma)$ relatives aux sous-groupes de congruence Γ de $SL_2(\mathbf{Z})$, avec pour X^∞ l'ensemble des *pointes*. Cet ensemble satisfait l'hypothèse du lemme d'après le théorème de Manin et Drin'feld. Les fonctions f, g seront alors celles dont les diviseurs sont concentrés aux pointes, autrement dit, ce sont des *unités modulaires*.

Soit donc $X = X(\Gamma)$ une courbe modulaire avec $\Gamma \subseteq \Gamma_0(N)$. Par conséquent on a un morphisme propre $\phi : X \longrightarrow X_0(N) \longrightarrow E$. Pour ce genre de morphisme, $\phi_* : K_2(X) \longrightarrow K_2(E)$ existe. Appelons $\mathcal{P}$ le sous-espace de $K_2(E) \otimes \mathbf{Q}$ engendré par tous les éléments de la forme $\phi_*(\{f,g\})$, où f, g sont des unités modulaires sur $X(\Gamma)$ et Γ décrit les sous-groupes de congruence de $\Gamma_0(N)$. Alors Beilinson démontre le

9.1 Théorème. *(i)* $r_\omega(\mathcal{P}) = \omega_1 L'(E,0)$.
(ii) $\mathcal{P} \subseteq K_2(\mathcal{E}) \otimes \mathbf{Q}$.

La démonstration part de la formule qui définit le régulateur d'un symbole $\{f,g\}$. La voici, à un facteur normalisant $*$ près qu'il est inutile de préciser ici.

$$r_\omega(\{f,g\}) = * \int_{X(\mathbf{C})} \log|f| \left(\overline{\frac{dg}{g}}\right) \wedge \phi^*\omega. \tag{9.2}$$

Cette formule est générale, c'est-à-dire qu'elle est aussi valable dans le cadre de l'application ξ construite au §6. Le fait qu'elle se traduit alors en une combinaison de séries de Kronecker se démontre soit par une analyse harmonique — *voir* [Deninger, Wingberg 1988] — soit par d'autres astuces analytiques — comme l'analogue de la méthode de Rankin et Selberg évoqué dans [Rohrlich 1987].[9]

Pour déduire 9.1 (i) de la formule 9.2, on interpréte le terme $\log|f|$ comme une série d'Eisenstein non holomorphe et le terme $\overline{d\log g}$ comme le conjugué complexe d'une série d'Eisenstein holomorphe. Cette dernière se décompose selon des caractères de Dirichlet pairs χ, et l'intégrale qui en résulte se lit finalement comme une convolution de Rankin-Selberg. Elle donne, à quelques facteurs moins essentiels près, le produit $L(E \otimes \chi, 1).L(E,2)$ dont le premier terme correspond à la période ω_1. — Nous renvoyons à [Schappacher, Scholl 1988] pour tous les détails.

La démonstration de 9.1 (ii) était insuffisante dans [Beilinson 1985] et est donnée dans [Schappacher, Scholl 1988, §7].

10. Comparaison entre les deux types de construction d'éléments de $K_2(E)$

Ce qu'on sait démontrer dans cette direction est tellement piètre qu'il convient à peine d'y consacrer un numéro de ce rapport. Le problème est que les points de torsion de la courbe E utilisés dans l'approche du §5 ne se ramènent que très exceptionnellement aux pointes de $X_0(N)$. Plus exactement, soit P un sous-schéma en groupes fini de E défini sur $\mathbf{Q}$. Afin de

[9] Pour ramener les expressions trouvées par Rohrlich aux séries de Kronecker que nous utilisons, il faut encore faire intervenir l'équation fonctionnelle des doubles séries de Kronecker [Weil 1976, p. 80, formule (32)].

comparer directement $r_\omega(\xi_{|P|}(\mathbf{a}))$, pour tout $\mathbf{a} \in \mathbf{Q}[P]^\circ$, au régulateur d'un élément convenable de $\mathcal{P}$, il faudrait que $\phi^{-1}(P) \subseteq X^\infty$. Mais ceci n'arrive presque jamais : le degré de $X_\circ(N) \longrightarrow E$ croît déjà plus vite avec N que le nombre des pointes.

Quelques exemples où une comparaison peut quand même être effectuée se déduisent de certaines courbes *involutoires* convenables : *voir* [Mestre, Schappacher 1990, 1.6]. Le premier exemple, particulièrement simple, est la courbe $E = X_1(11)$ dont la torsion rationnelle est identique à l'ensemble des pointes.[10] Sur ordinateur on vérifie que $K_1(0, \mathbf{a}, 2) \neq 0$ pour un choix convenable de $\mathbf{a}$ à support dans les points rationnels de E. $X_1(11)$ est donc une des rares courbes E sans multiplication complexe pour lesquelles on sait démontrer la conjecture 5.4 pour les diviseurs $\mathbf{a} \in \mathbf{Q}[E(\mathbf{Q})_{tors}]^\circ$.

En général, trouver de tels exemples revient à démontrer que certaines intersections de groupes de congruence sont encore des sous-groupes de congruence. C'est souvent un problème épineux.

11. Généralisation du théorème modulaire.

Dans [Beilinson 1986], Beilinson démontre une 'conjecture de Beilinson faible' pour les courbes elliptiques (paramétrées comme toujours par une courbe modulaire) relative à tous les nombres $L'(E,m)$, $L(E,n)$ avec $m \leq 0$, $n \geq 2$. Pour comprendre la difficulté de la chose, il faut savoir d'abord que les conjectures de Beilinson lient $L(E,n)$ aux régulateurs sur $K^{(n)}_{2(n-1)}(E)$, la partie graduée de poids n par rapport à la filtration γ sur $K_{2(n-1)}(E)$. Pour $n > 2$ cet espace vectoriel est de nature assez différente de $K_2(E) \otimes \mathbf{Q} = K_2^{(2)}(E)$: les indices supérieurs et inférieurs n'étant plus les mêmes, on sort des K-groupes 'à la Milnor'; $K^{(n)}_{2(n-1)}(E)$ n'est plus engendré par des 'symboles', *i.e.*, par des éléments obtenus par cup-produit à partir de K_1. Aucun analogue des méthodes qu'on a vues plus haut n'est donc directement applicable aux K-groupes en question.

Le remède est de passer à une variété auxiliaire $V \xrightarrow{\psi} E$ de dimension telle que l'homomorphisme de Gysin ψ_* aboutissant à $K^{(n)}_{2(n-1)}(E)$ provienne d'un K-groupe 'symbolique' de V. Les variétés utilisées par Beilinson sont les variétés de Kuga-Sato d'ordre $n-2$ attachées aux courbes modulaires $X \longrightarrow X_\circ(N) \longrightarrow E$ comme ci-dessus :

$$V \overset{\text{déf}}{=} \mathcal{A} \times_X \ldots \times_X \mathcal{A},$$

où $\mathcal{A}$ est la courbe elliptique universelle au-dessus de X — on peut supposer $N > 3$ — et on prend $n-2$ fois le produit fibré. Alors V est de dimension relative $n-2$ sur X et donc sur E, et $\psi_* : K^{(2(n-1))}_{2(n-1)}(V) \longrightarrow K^{(n)}_{2(n-1)}(E)$. Les fonctions sur V qui remplacent les unités modulaires du théorème 9.1 sont encore celles dont les diviseurs sont concentrés au-dessus des pointes de X.

C'est Scholl qui a récemment étendu la démonstration de Beilinson à toutes les valeurs aux points entiers (non centraux) des fonctions L de formes modulaires f de poids ≥ 2. Une des difficultés de base de ce travail était de définir un vrai motif (au sens de Grothendieck, découpé par des cycles algébriques ...) dont la fonction L est $L(f,s)$. — *Cf.* [Scholl 1989].

Notons en passant que, en dehors de $s = 0$, $s = 2$, il n'y a conjecturalement pas de différence entre $K^{(n)}_{2(n-1)}(E)$ et $K^{(n)}_{2(n-1)}(\mathcal{E})$. Ceci découle d'une suite analogue à 3.3 et de conjectures sur la K-théorie de schémas sur les corps finis.

---

[10] Noter que, pour la comparaison, il n'est pas suffisant de savoir que les pointes *engendrent* la torsion rationnelle.

12. Le théorème de Deninger.

Dans [Deninger 1989], Deninger démontre une conjecture de Beilinson faible pour les courbes elliptiques à *multiplications complexes* relative à tous les nombres $L'(E,m)$, $L(E,n)$ avec $m \leq 0$, $n \geq 2$. Sa méthode est plus ou moins analogue à celle du §5, mais s'inspire aussi du travail de Beilinson mentionné ci-avant. En fait au lieu des variétés de Kuga-Sato utilisées par Beilinson, Deninger considère le motif $Sym^{2n-3}E$. La clé de sa démonstration est l'observation selon laquelle les multiplications complexes permettent de définir un morphisme de motifs $Sym^{2n-3}E \xrightarrow{\psi} H^1(E)$. En fait un des ingrédients de la définition de ψ est l'application

$$id_E \times \sqrt{d_K} : E \times E \longrightarrow E,$$

où K est le corps des multiplications complexes de E et l'élément $\sqrt{d_K} \in K$ est identifié à un endomorphisme de E. — Pour un peu plus de détails sur la méthode de Deninger, le lecteur peut consulter l'exposé introductoire [Deninger 1988].

Mentionnons que la méthode s'étend assez naturellement à toutes les fonctions L de Hecke des corps quadratiques imaginaires.

13. Généralisation du travail de Bloch et Grayson.

Si l'on veut généraliser le travail de Deninger aux courbes elliptiques sans multiplication complexe, on ne se heurte pas seulement aux difficultés — déjà monstrueuses — rencontrées lors du passage du §7 au §8, mais l'absence d'un morphisme ψ comme ci-avant change assez fondamentalement les règles du jeu: Comme on ne peut plus redescendre à la courbe elle-même, on est amené à comparer de façon numérique les valeurs spéciales $L(Sym^k E, k+1)$ à des déterminants de valeurs spéciales de séries de Kronecker. Ici des obstructions provenant du symbole symbole modéré resurgissent comme au §8, et on découvre numériquement des 'relations exotiques' entre séries de Kronecker.

Ainsi on a vérifié dans [Mestre, Schappacher 1990], pour un certain nombre de courbes E sans multiplication complexe, que

$$\frac{y^4}{\pi^2} \det \begin{pmatrix} K_2(0,\mathbf{a},3) & K_0(0,\mathbf{a},2) \\ K_2(0,\mathbf{b},3) & K_0(0,\mathbf{b},2) \end{pmatrix} \in L(Sym^2 E, 3)\ \mathbf{Q}$$

si les diviseurs $\mathbf{a}, \mathbf{b} \in \mathbf{Q}[E_{tors}]^\circ$ échappent aux obstructions provenant du symbole modéré — obstructions qui se calculent par une formule analogue à celle mentionnée au paragraphe suivant 5.6, mais qui fait maintenant intervenir le quatrième polynôme de Bernoulli. Le fait que le régulateur est devenu un vrai déterminant tient à ce que la dimension du K-groupe en question, $K_3^{(3)}(Sym^2 E)_{\mathbf{Z}}$, est conjecturée d'être 2, tout comme l'ordre du zéro de $L(Sym^2 E, s)$ en $s = 0$.

Au §8 on était amené à supposer que l'action de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ est suffisamment petite pour admettre des $r_\omega \circ \xi_d$ d'image non nulle. Maintenant, le fait qu'on veut avoir un déterminant non nul à l'aide de diviseurs qui échappent aux obstructions provenant du symbole modéré impose des conditions plus sévères. Ainsi on démontre dans [Mestre, Schappacher 1990, 3.4] que, à $\mathbf{Q}$-*isomorphisme près, il n'y a qu'un nombre fini de courbes elliptiques* E *sur* $\mathbf{Q}$ *d'invariant* j *non-entier, munies d'un point rationnel* T *d'ordre fini, telles qu'il existe des diviseurs* $\mathbf{a}, \mathbf{b} \in \mathbf{Q}[\langle T \rangle]^\circ$ *qui échappent aux obstructions provenant du symbole modéré et tels que le déterminant de la matrice*

$$\begin{pmatrix} K_2(0,\mathbf{a},3) & K_0(0,\mathbf{a},2) \\ K_2(0,\mathbf{b},3) & K_0(0,\mathbf{b},2) \end{pmatrix}$$

soit non-nul.

Bibliographie

A. Beilinson (1985), Higher regulators and values of L-functions, *J. Soviet Math.* **30** (1985), 2036–2070.

A. Beilinson (1986), Higher regulators of modular curves; *in : Contemporary Mathematics* **55** (1986), Part I, 1–34

S. Bloch (1978), Algebraic K-theory and Zeta Functions of Elliptic Curves, Proc. ICM Helsinki 1978, 511–515

S. Bloch (1980), Lectures on algebraic cycles; *Duke Univ. Math. Series* **IV**

S. Bloch, D. Grayson (1986), K_2 and the L-functions of elliptic curves. Computer calculations; *in : Contemporary Mathematics* **55** (1986), Part I, 79–88

S. Bloch, K. Kato (1989), $L-$functions and Tamagawa numbers of motives, *preprint*

A. Borel (1974), Cohomologie de SL_n et valeurs de fonctions zêta, Ann. Scuola Normale Superiore **7**, 613–636

H. Carayol (1983), Sur les représentations l- adiques attachées aux formes modulaires de Hilbert, CRAS Paris, Sér. I, t. **296** (25 avril 1983), 629–632

C. Deninger (1988), Higher regulators of elliptic curves with complex multiplication; *in : Sém. Théorie de Nombres Paris* 1986/87, C. Goldstein (ed.), Birkhäuser 1988

C. Deninger (1989), Higher regulators and Hecke L-series of imaginary quadratic fields I, *Inventiones Math.* **96** (1989), 1–69; II, *preprint*

C. Deninger, K. Wingberg (1988), On the Beilinson conjectures for elliptic curves with complex multiplication; *in :* Rapoport, Schappacher, Schneider (ed.s), Beilinson's Conjectures on Special Values of L-Functions, *Perspectives in Math.* **4**, Acad. Press 1988, 249–272

J-F. Mestre, N. Schappacher (1990), Séries de Kronecker et fonctions L des puissances symétriques de courbes elliptiques sur $\mathbf{Q}$, *à paraître* Proc. 1989 Texel Conference, Birkhäuser

Modular Functions of One Variable, IV, Antwerp Proceedings 1972; Springer *Lect. Notes Math.* **476**

D. Quillen (1973), Higher algebraic K-theory, I; *in :* Algebraic K-theory I — Higher K-theories, Proc. Battele Inst. 1972, Springer *Lect. Notes Math.* **341**, 77–139

D. Ramakrishnan (1989a), Regulators, Algebraic Cycles, and Values of L-functions, *Contemporary Mathematics* **83**, 183–310

D. Ramakrishnan (1989b), Problems arising from the Tate and Beilinson conjectures in the context of Shimura varieties; *preprint* 1989

M. Rapoport, N. Schappacher, P. Schneider (ed.s) (1988), Beilinson's Conjectures on Special Values of L-Functions, *Perspectives in Math.* **4**, Acad. Press 1988

W. Raskind (1984), "Le théorème de Mordell-Weil faible" pour $H^0(X,\mathcal{K}_2)/\ K_2k$, CRAS Paris, Sér. I, t. **299** (7 mai 1984), 241–244

D.E. Rohrlich (1987), Elliptic curves and values of L-functions; *in : Can. Math. Soc. Conf. Proc.* **7** (1987), 371–387

N. Schappacher, and A.J. Scholl (1988), Beilinson's Theorem on Modular Curves; *in :* Rapoport, Schappacher, Schneider (ed.s), Beilinson's Conjectures on Special Values of L-Functions, *Perspectives in Math.* **4**, Acad. Press 1988, 273–304

N. Schappacher, A.J. Scholl (1990), The boundary of the Eisenstein symbol, *preprint*

A.J. Scholl (1989), Motives for modular forms; *Inventiones math.* **100**, 419–430

J.-P. Serre (1972), Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Inventiones Math.* **15** (1972), 259–331; *Œuvres*, III: no. 94

C. Soulé (1985), Opérations en K-théorie algébrique, *Can. J. Math.* **37**, 488–550

A. Weil (1976), Elliptic functions according to Eisenstein and Kronecker; *Ergebnisse* **88**, Springer 1976.

Norbert Schappacher
Max-Planck-Institut für Mathematik
Gottfried-Claren-Str. 26
D-5300 Bonn 2
West-Germany

Astérisque

HANS PETER SCHLICKEWEI

Résultats quantitatifs en approximation diophantienne

Astérisque, tome 198-199-200 (1991), p. 319-331

<http://www.numdam.org/item?id=AST_1991__198-199-200__319_0>

RESULTATS QUANTITATIFS EN APPROXIMATION DIOPHANTIENNE

par

Hans Peter SCHLICKEWEI

1. Le Théorème du Sous-espace quantitatif.

Rappelons le théorème de Roth [12]: *Soit α un nombre algébrique de degré $d \geq 2$, soit $\delta > 0$. Alors il n'existe qu'un nombre fini de nombres rationnels $\frac{x}{y}$ tels que*

$$\left|\alpha - \frac{x}{y}\right| < y^{-2-\delta} \tag{1.1}$$

soit satisfait.

Il est bien connu que ce résultat est ineffectif dans le sens suivant: la preuve ne permet pas d'obtenir des bornes supérieures pour *les valeurs absolues* $|x|, |y|$ des solutions de (1.1). En revanche on peut obtenir par la méthode de Roth des bornes supérieures pour *le nombre* de solutions $\frac{x}{y}$ de (1.1). (cf. Davenport et Roth [3], et plus récemment Bombieri et van der Poorten [1] et Luckhardt [8]). Remarquons que (1.1) est presque la même chose que

$$|y||y\alpha - x| < |\mathbf{x}|^{-\delta} \tag{1.2}$$

où $\mathbf{x} = (x, y)$ et $|\mathbf{x}| = \sqrt{x^2 + y^2}$. Dans (1.2) nous avons deux formes linéaires à coefficients algébriques $L_1(\mathbf{x}) = y$, $L_2(\mathbf{x}) = y\alpha - x$ qui sont linéairement indépendantes. La généralisation à n dimensions est le fameux théorème du sous-espace de Wolfgang Schmidt [20] (1972):

Soient $L_1(\mathbf{x}), \dots, L_n(\mathbf{x})$ des formes linéaires linéairement indépendantes à coefficients algébriques en $\mathbf{x} = (x_1, \dots, x_n)$. Soit $\delta > 0$. Considérons l'inégalité

$$|L_1(\mathbf{x}) \cdots L_n(\mathbf{x})| < |\mathbf{x}|^{-\delta} \tag{1.3}$$

où $|\mathbf{x}| = \sqrt{x_1^2 + \cdots + x_n^2}$. Alors il existe un nombre fini de sous-espaces propres $U_1, \dots, U_t$ de $\mathbb{Q}^n$ tels que chaque solution $\mathbf{x} \in \mathbb{Z}^n$ de (1.3) soit contenue dans $\bigcup_{i=1}^{t} U_i$.

Ce théorème a été généralisé indépendamment par Dubois et Rhin [4] et par Schlickewei [13] au cas des valeurs absolues p-adiques.

Dans un travail récent Wolfgang Schmidt a trouvé comment donner une version quantitative de son théorème du sous-espace [22]. Ceci a été généralisé ensuite par Schlickewei aux valuations p-adiques [15] et aux corps des nombres [18]. Nous allons citer ici le résultat principal de [18]. Mais d'abord il nous faut introduire quelques notations.

Soit K un corps de nombres de degré d. Soit $M(K)$ l'ensemble des places de K. A chaque v dans $M(K)$ nous associons la valeur absolue $|\ \ |_v$, normalisée de la manière habituelle: sur $\mathbb{Q}$ on a $|\ \ |_v = |\ \ |$ (valeur absolue standard) si v est archimédienne et $|p|_v = p^{-1}$ si v est au-dessus du nombre premier p. Pour $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_n) \in K^n$ et pour $v \in M(K)$ nous posons

$$|\boldsymbol{\alpha}|_v = \begin{cases} \sqrt{|\alpha_1|_v^2 + \cdots + |\alpha_n|_v^2} & \text{pour } v \text{ archimédienne} \\ \max\limits_{1 \le i \le n} |\alpha_i|_v & \text{pour } v \text{ nonarchimédienne,} \end{cases}$$

et nous écrivons

$$\| \boldsymbol{\alpha} \|_v = |\boldsymbol{\alpha}|_v^{d_v/d}$$

où $d_v = [K_v : \mathbb{Q}_v]$ est le degré local du complété K_v. Finalement nous définissons la hauteur (projective) de $\boldsymbol{\alpha}$ par

$$H(\boldsymbol{\alpha}) = \prod_{v \in M(K)} \| \boldsymbol{\alpha} \|_v .$$

Etant donnée une forme linéaire $L(\mathbf{x}) = \alpha_1 x_1 + \cdots + \alpha_n x_n$ à coefficients dans K nous définissons

$$\| L \|_v = \| \boldsymbol{\alpha} \|_v \quad \text{et} \quad H(L) = H(\boldsymbol{\alpha}).$$

THÉORÈME 1. [18] *Soit K une extension normale de $\mathbb{Q}$ de degré d. Soit S un sous-ensemble de cardinalité s de $M(K)$. Pour chaque $v \in S$, soient $L_1^{(v)}, \dots L_n^{(v)}$ des formes linéaires en $\mathbf{x} = (x_1, \dots, x_n)$, à coefficients dans K, linéairement indépendantes. Soit $0 < \delta < 1$. Considérons l'inégalité*

$$\prod_{v \in S} \prod_{i=1}^{n} \frac{\| L_i^{(v)}(\boldsymbol{\beta}) \|_v}{\| L_i^{(v)} \|_v \| \boldsymbol{\beta} \|_v} < H(\boldsymbol{\beta})^{-n-\delta} . \tag{1.4}$$

Alors il existe des sous-espaces propres $S_1, \dots, S_{t_1}$ de K^n avec

$$t_1 = c(n, d, s, \delta) = \left[(8sd)^{2^{34nd}\, s^6\, \delta^{-2}} \right] \tag{1.5}$$

tels que chaque solution $\boldsymbol{\beta} \in K^n$ de (1.4) ou bien *soit contenue dans $\bigcup_{i=1}^{t_1} S_i$* ou bien *ait une hauteur satisfaisant*

$$H(\boldsymbol{\beta}) < \max \left\{ (n!)^{\frac{9}{\delta}}, \quad H(L_i^{(v)})^{\frac{9nsd}{\delta}} \quad (v \in S;\ i = 1, \dots, n) \right\}. \tag{1.6}$$

Le résultat quantitatif de W. Schmidt [22] traite le cas où S contient une seule valeur absolue archimédienne et où les solutions $\boldsymbol{\beta}$ sont prises dans $\mathbb{Q}^n$.

La partie interessante dans le Théorème 1 est le fait que la borne (1.5) pour le nombre de sous-espaces ne dépende que du degré d de K, de la dimension n, du nombre des valeurs absolues intervenant, et de δ. En particulier la constante ne dépend pas du discriminant du corps, elle ne dépend pas des formes $L_i^{(v)}$ ni des idéaux premiers $\mathfrak{p}$ correspondants aux valeurs absolues nonarchimédiennes dans S. Nous allons voir plus bas que ce théorème donne des bornes supérieures uniformes pour le nombre de solutions d'une grande classe d'équations diophantiennes.

2. Réduction du Théorème 1 au cas rationnel.

Dans [15] nous avons démontré l'énoncé suivant, que est une variante du Théorème 1 dans laquelle les solutions sont rationnelles.

THÉORÈME 2. [15] *Soit K un corps de nombres de degré d. Soit R un sous-ensemble de $M(\mathbb{Q})$ de cardinalité r contenant la place à l'infini. Pour chaque*

$v \in R$, on choisit une extension $|\ |_v$ de v à K, et on se donne des formes linéaires $L_1^{(v)}, \dots, L_n^{(v)}$ en $\mathbf{x} = (x_1, \dots, x_n)$ à coefficients dans K, linéairement indépendantes. Soit $0 < \varepsilon < 1$. Considérons l'inégalité

$$\prod_{v \in S} |L_1^{(v)}(\mathbf{x}) \cdots L_n^{(v)}(\mathbf{x})|_v < \left(\prod_{v \in S} |\det\left(L_1^{(v)}, \dots, L_n^{(v)}\right)|_v \right) |\mathbf{x}|^{-\varepsilon}. \tag{2.1}$$

Alors il existe des sous-espaces propres $T_1, \dots T_{t_2}$ de $\mathbb{Q}^n$ avec

$$t_2 = \left[(8sd!)^{2^{26n}\, s^6\, \delta^{-2}} \right] \tag{2.2}$$

tels que chaque solution $\mathbf{x} \in \mathbb{Z}^n$ de (2.1) ou bien *soit contenue dans $\bigcup_{i=1}^{t_2} T_i$* ou bien *ait une norme $|\mathbf{x}| = \sqrt{x_1^2 + \cdots + x_x^2}$ vérifiant*

$$|\mathbf{x}| < \max\left\{ (n!)^{\frac{8}{\varepsilon}}, \quad H(L_i^{(v)}) \quad (v \in S,\ i = 1, \dots, n) \right\}. \tag{2.3}$$

Nous ne parlerons pas ici de la preuve du Théorème 2. Nous remarquons seulement qu'elle a besoin de toute la machinerie de Thue–Siegel–Roth–Schmidt. Au lieu de donner des détails sur cela nous nous contenterons d'indiquer comment on peut déduire le Théorème 1 du Théorème 2.

Pour transformer (1.4) en une forme ressemblant à (2.1) nous remarquons d'abord que pour chaque $v \in S$ nous avons

$$\| L_1^{(v)} \|_v \cdots \| L_n^{(v)} \|_v \leq \| \det(L_1^{(v)}, \dots, L_n^{(v)}) \|_v \, (H(L_1^{(v)}) \cdots H(L_n^{(v)}))^{d_v}.$$

On voit immédiatement que si

$$H(\boldsymbol{\beta})^{\frac{\delta}{2}} > H^{nds} \text{ où } H = \max\{H(L_i^{(v)}) \ (v \in S; \quad i = 1, \dots, n)\}$$

alors (1.4) implique

$$\prod_{v \in S} \frac{\| L_1^{(v)}(\boldsymbol{\beta}) \cdots L_n^{(v)}(\boldsymbol{\beta}) \|_v}{\| \boldsymbol{\beta} \|_v^n} < \left(\prod_{v \in S} \| \det(L_1^{(v)}, \dots, L_n^{(v)}) \|_v \right) H(\boldsymbol{\beta})^{-n - \frac{\delta}{2}}. \tag{2.4}$$

Notons que (2.4) est homogène en $\boldsymbol{\beta}$. Par conséquent nous pouvons supposer sans perte de généralité que le vecteur $\boldsymbol{\beta}$ dans (2.4) a des composantes entières algébriques dans K.

L'idée générale est maintenant d'utiliser une base entière de K sur $\mathbb{Q}$ disons $\gamma_1, \dots, \gamma_d$ et d'exprimer $\boldsymbol{\beta} = (\beta_1, \dots, \beta_n)$ dans cette base c'est à dire

$$\beta_i = x_{i1}\gamma_1 + \cdots + x_{id}\gamma_d \tag{2.5}$$

avec $x_{ij} \in \mathbb{Z}$, puis de remplacer $\boldsymbol{\beta}$ par $\mathbf{x} = (x_{11}, \dots, x_{1d}, \dots, x_{n1}, \dots, x_{nd}) \in \mathbb{Z}^{nd}$ et enfin d'utiliser le Théorème 2. Grâce à cette transformation, nous pouvons simplifier la situation en supposant que pour tout v dans S, si p est la place de $M(\mathbb{Q})$ que divise v, S contient toutes les places de K au dessus de p. Les formes $L_1^{(v)}, \dots, L_n^{(v)}$ avec $v \mid p$ sont transformées par (2.5) dans des formes $M_{11}^{(p)}, \dots, M_{n1}^{(p)}, \dots, M_{1d}^{(p)}, \dots M_{nd}^{(p)}$ en $x_{11}, \dots, x_{1d}, \dots, x_{n1}, \dots, x_{nd}$, et on voit aisément qu'on a

$$\prod_{\substack{v \in S \\ v \mid p}} \| L_1^{(v)}(\boldsymbol{\beta}) \cdots L_n^{(v)}(\boldsymbol{\beta}) \|_v = |M_{11}^{(p)}(\mathbf{x}) \cdots M_{nd}^{(p)}(\mathbf{x})|_p^{\frac{1}{d}} .$$

En outre nous obtenons

$$\prod_{\substack{v \in S \\ v \mid p}} \| \det(L_1^{(v)}, \dots L_n^{(v)}) \|_v = |\det(M_{11}^{(p)}, \dots M_{nd}^{(p)})|_p^{\frac{1}{d}} |D_K|_p^{-\frac{1}{2d}}$$

où D_K dénote le discriminant de K sur $\mathbb{Q}$. Pour appliquer le Théorème 2 il suffira de remplacer $H(\boldsymbol{\beta})$ par $|\mathbf{x}| = \sqrt{x_{11}^2 + \cdots + x_{nd}^2}$ avec x_{ij} défini dans (2.5).

Usuellement la procédure pour arriver à cette situation consiste à choisir un multiple de $\boldsymbol{\beta}$, disons $\lambda\boldsymbol{\beta}$, tel que $\lambda\boldsymbol{\beta}$ ait des composants entières, et tel que

$$\prod_{v \in M_0(K)} \| \lambda\boldsymbol{\beta} \|_v \geq |D_K|^{-\frac{1}{2}};$$

nous avons noté $M_0(K)$ les places nonarchimédiennes de K. Alors un calcul simple montre, que nous pouvons remplacer (2.4) par

$$\begin{aligned} &\prod_{p \in S(\mathbb{Q})} |M_{11}^{(p)}(\mathbf{x}) \cdots M_{nd}^{(p)}(\mathbf{x})|_p \\ &< \Big(\prod_{p \in S} |\det(M_{11}^{(p)}, \dots, M_{nd}^{(p)})|_p \Big) |D_K|^c \Big(\prod_{v \in M_\infty(K)} \| \boldsymbol{\beta} \|_v \Big)^{-d\frac{\delta}{2}}, \end{aligned} \tag{2.6}$$

où $M_\infty(K)$ désigne les places à l'infini de K, où $S(\mathbb{Q})$ désigne les places de $\mathbb{Q}$ qui sont au-dessous des places de S, et où c est une constante positive, qui ne dépend que de n et de s. Pour remplacer

$$\prod_{v\in M_\infty(K)} \|\boldsymbol{\beta}\|_v \quad \text{par} \quad |\mathbf{x}|$$

on choisit usuellement une unité ε dans K telle que

$$|\varepsilon\boldsymbol{\beta}|_v \le e^{cR_K} \prod_{v\in M_\infty(K)} \|\boldsymbol{\beta}\|_v \tag{2.7}$$

pour chaque valeur absolue archimédienne $|\ |_v$ de K, où R_K est le régulateur de K et où c est une constante positive qui ne dépend que du degré d de K. Mais on ne sait majorer e^{cR_K} que par une expression qui dépend exponentiellement de D_K; une telle borne donnerait finalement une inégalité du type

$$\prod_{p\in S(\mathbb{Q})} |M_{11}^{(p)}(\mathbf{x})\cdots M_{nd}^{(p)}(\mathbf{x})|_p < \Big(\prod_{p\in S(\mathbb{Q})} |\det(M_{11}^{(p)},\dots,M_{nd}^{(p)})|_p\Big) e^{D_K^{c_1}} |\mathbf{x}|^{-\frac{\delta}{4}} \tag{2.8}$$

où c_1 est une constante positive.

Pour obtenir un résultat qualitatif cette méthode suffit, et en effet elle a été appliquée dans W. Schmidt [21] aussi bien que dans Schlickewei [14]. Dans le cas quantitatif la situation est plus compliquée. Pour appliquer le Théorème 2 à (2.8) nous remarquons que le facteur $e^{D_K^{c_1}}$ a une influence dévastatrice: nous obtiendrons une valeur t_1 dans (1.5) qui dépendrait de D_K.

Une méthode pour éviter ce problème est de choisir un multiple entier algébrique de $\boldsymbol{\beta}$, disons $\lambda\boldsymbol{\beta}$, avec $|N_{K/\mathbb{Q}}(\lambda)| \le |D_K|^{\frac{1}{2}}$ tel que (2.7) puisse être remplacé par

$$\max_{v\in M_\infty(K)} |\lambda\boldsymbol{\beta}|_v \le |D_K|^{\frac{1}{2d}} \prod_{v\in M_\infty(K)} \|\boldsymbol{\beta}\|_v, \tag{2.9}$$

ce qui est possible d'après le théorème de Minkowski. Si nous appliquons cette procédure nous aboutissons finalement à

$$\prod_{p\in S(\mathbb{Q})} |M_{11}^{(p)}(\mathbf{x})\cdots M_{nd}^{(p)}(\mathbf{x})|_p < \Big(\prod_{p\in S(\mathbb{Q})} |\det(M_{11}^{(p)},\dots,M_{nd}^{(p)})|_p\Big) |D_K|^c |\mathbf{x}|^{-\frac{\delta}{4}}. \tag{2.10}$$

Il reste une difficulté: nous avons toujours le discriminant dans (2.10), mais d'une manière moins méchante que dans (2.8). Pour maîtriser la situation, le détour que nous prenons consiste à partager les solutions $\boldsymbol{\beta}$ de (1.4) en classes de la manière suivante: deux solutions $\boldsymbol{\beta}$ et $\boldsymbol{\beta}'$ appartiennent à la même classe C_L, si les composantes $\beta_1, \dots, \beta_n$ de $\boldsymbol{\beta}$ et $\beta'_1, \dots, \beta'_n$ de $\boldsymbol{\beta}'$ définissent le même corps intermédiaire L avec $K \supset L \supset \mathbb{Q}$. Comme le nombre de corps intermédiaires L est borné par 2^d, il est clair que notre problème est résolu si nous savons traiter chaque classe C_L.

Maintenant pour la classe C_L correspondant au corps L, nous procédons comme ci-dessus, sauf que nous remplaçons $\boldsymbol{\beta}$ par la transformation (en supposant $\boldsymbol{\beta} \in L^n$)

$$\beta_i = x_{i1}\gamma_1 + \cdots + x_{i\ell}\gamma_\ell$$

où $\gamma_1, \dots, \gamma_\ell$ est une base entière de L sur $\mathbb{Q}$. Nous obtenons ainsi une formule analogue à (2.10), mais avec des formes $M_{11}^{(p)}, \dots, M_{n\ell}^{(p)}$, et avec D_K remplacé par D_L pour les solutions $\boldsymbol{\beta} \in C_L$. D'après un théorème de Silverman [25], pour chaque vecteur $\boldsymbol{\beta}$ dans K^n, qui définit L, nous avons la minoration

$$H(\boldsymbol{\beta}) \geq c(\ell)|D_L|^{1/(2\ell(\ell-1))}. \tag{2.11}$$

Revenons à (1.4) en nous limitant à des solutions $\boldsymbol{\beta}$ dans C_L. En utilisant la borne inférieure (2.11) nous pouvons montrer avec un "principe de trous" que les solutions $\boldsymbol{\beta} \in C_L$ de (1.4) avec $H(\boldsymbol{\beta}) < |D_L|^c$ sont contenues dans l'union d'un nombre de sous-espaces propres de K^n, qui est plutôt petit par rapport à la borne (1.5). En tenant compte de cela nous pouvons en fait supposer que $H(\boldsymbol{\beta})$ est très grand par comparaison à $|D_L|$, ce qui va impliquer dans (2.10) que $|\mathbf{x}|^{\delta/8} > |D_L|^c$. Ainsi nous obtenons pour C_L une inégalité du type

$$\prod_{p \in S(\mathbb{Q})} |M_{11}^{(p)}(\mathbf{x}) \cdots M_{n\ell}^{(p)}(\mathbf{x})|_p < \left(\prod_{p \in S(\mathbb{Q})} \left| \det(M_{11}^{(p)}, \dots, M_{n\ell}^{(p)}) \right|_v \right) |\mathbf{x}|^{-\delta/8}, \tag{2.12}$$

à laquelle nous pouvons appliquer le Théorème 2.

3. Equations en S-unités.

Une des conséquences principales du Théorème 1 est le résultat suivant sur les équations en S-unités.

THÉORÈME 3. [19] *Soit K un corps de nombres de degré d. Soit S un sous-ensemble de $M(K)$ de cardinalité s contenant toutes les places à l'infini. Nous dirons qu'un élément $x \in K^*$ est une S-unité si $\| x \|_v = 1$ pour chaque $v \notin S$. Soient $a_1, \dots, a_n$ des éléments non nuls de K. Alors le nombre $N(a_1, \dots, a_n)$ de solutions de l'équation*

$$a_1 x_1 + \cdots + a_n x_n = 1 \tag{3.1}$$

en S-unités $x_1, \dots, x_n$, tels qu'aucune sous-somme propre $a_{i_1} x_{i_1} + \cdots + a_{i_k} x_{i_k}$ s'annulle, satisfait

$$N(a_1, \dots, a_n) \leq (4sd!)^{2^{36nd!}\, s^6}. \tag{3.2}$$

Le Théorème 3 prouve une vieille conjecture de Siegel [24]. Rappelons que Mahler [9] était le premier à étudier les équations en S-unités dans le cas particulier $n = 2$, $K = \mathbb{Q}$, $a_1 = a_2 = 1$. Il a montré que le nombre de solutions est fini. Dans le cas $n = 2$ Evertse [5] en 1984 a obtenu un résultat beaucoup plus précis que (3.2). En effet il a montré que

$$N(a_1, a_2) \leq 3 \cdot 7^{d+2s}.$$

Pour n quelconque, van der Poorten et Schlickewei [10] en 1982 et indépendamment Evertse [6] en 1984 ont démontré, que (3.1) n'admet qu'un nombre fini de solutions en S-unités. Ces résultats étaient obtenus par une application du théorème du sous-espace $\mathfrak{p}$-adique qualitatif de Schlickewei [14]. En 1988 Evertse et Győry [7] ont démontré

$$N(a_1, \dots, a_n) < C(n, K, S),$$

c'est-à-dire qu'il existe une borne pour $N(a_1, \dots, a_n)$ qui ne dépend pas du choix particulier de $a_1, \dots, a_n$ dans K. Mentionons que le cas rationnel du Théorème 3 a été démontré dans [16].

Ce qui est interessant avec la borne (3.2) n'est pas tellement la forme explicite mais d'abord le fait que la borne ne dépend pas de $a_1, \dots, a_n$, ensuite que la dépendance en K ne fait intervenir que le degré d de K, et enfin que la borne dépend seulement de la cardinalité de S (et non pas des idéaux premiers particuliers contenus dans S).

La preuve du théorème 3 se fait à partir du Théorème 1 de la manière suivant. Au lieu de (3.1), nous étudions l'équation homogène

$$a_1x_1 + \cdots + a_nx_n + a_{n+1}x_{n+1} = 0 \tag{3.3}$$

en S-unités $x_1, \ldots, x_{n+1}$, où aucune sous-somme propre $a_{i_1}x_{i_1} + \cdots + a_{i_k}x_{i_k}$ ne s'annulle, et nous prouvons que le nombre de solutions projectives $(x_1, \ldots, x_{n+1})$ de (3.3) est borné par (3.2). Posons

$$\beta_i = a_ix_i \quad (i = 1, \ldots, n+1) \quad \text{et} \quad \boldsymbol{\beta} = (\beta_1, \ldots, \beta_n). \tag{3.4}$$

Il suffit de traiter l'équation

$$\beta_1 + \cdots + \beta_{n+1} = 0. \tag{3.5}$$

Nous introduisons les formes linéaires

$$\begin{aligned} L_1(\boldsymbol{\beta}) &= \beta_1 \\ &\vdots \\ L_n(\boldsymbol{\beta}) &= \beta_n \\ L_{n+1}(\boldsymbol{\beta}) &= \beta_1 + \cdots + \beta_n. \end{aligned} \tag{3.6}$$

Notons que nous avons $L_{n+1}(\boldsymbol{\beta}) = -\beta_{n+1}$ à cause de (3.5) et (3.4). Comme les x_i sont des S-unités nous obtenons grâce à (3.4)

$$\prod_{v\in S} \| L_1(\boldsymbol{\beta}) \cdots L_{n+1}(\boldsymbol{\beta}) \|_v = \prod_{v\in S} \| a_1 \cdots a_{n+1} \|_v . \tag{3.7}$$

Pour $v \notin S$, nous avons $\| \beta_i \|_v = \| a_i \|_v$. Choisissons pour chaque $v \in S$ un indice $i(v)$ avec

$$\| \beta_{i(v)} \|_v = \max_{1\le j\le n+1} \| \beta_j \|_v$$

et posons $I(v) = \{1, \ldots, n+1\} \backslash \{i(v)\}$. Alors (3.7) implique

$$\prod_{v\in S} \prod_{i\in I(v)} \| L_i(\boldsymbol{\beta}) \|_v = \left(\prod_{v\in S} \| a_1 \cdots a_{n+1} \|_v \right) \prod_{v\in S} \max_{1\le j\le n+1} \| \beta_j \|_v^{-1} . \tag{3.8}$$

Après un calcul simple nous déduisons de (3.8) en posant
$A = (\prod_{v\in S} \| a_1 \cdots a_{n+1} \|_v)(\prod_{v\notin S} \max_{1\le i\le n+1} \| a_i \|_v^{n+1})$

$$\prod_{v\in S} \prod_{i\in I(v)} \frac{\| L_i(\boldsymbol{\beta}) \|_v}{\| L_i \|_v \| \boldsymbol{\beta} \|_v} < c(n) A H(\boldsymbol{\beta})^{-n-1}. \tag{3.9}$$

Si nous supposons que

$$H(\boldsymbol{\beta})^{\frac{1}{2}} > c(n)A, \tag{3.10}$$

nous pouvons appliquer le Théorème 1 à (3.9) avec $\delta = \frac{1}{2}$. Par conséquent les solutions de (3.5) avec (3.10) sont contenues dans la réunion de $c(n, d, s, \frac{1}{2})$ sous-espaces propres de l'espace U de K^{n+1} défini par (3.5).

Il reste à considérer les solutions petites, qui ne satisfont pas (3.10), c.à.d. les solutions $\boldsymbol{\beta}$ telles que

$$H(\boldsymbol{\beta}) \leq c_1(n)A^2. \tag{3.11}$$

Pour cela nous appliquons un "principe de trous", qui utilise d'une manière essentielle l'équation (3.5) et qui donne comme résultat que les solutions de (3.5) satisfaisant

$$B \leq H(\boldsymbol{\beta}) \leq BA^{1/(2(n^2-1))} \tag{3.12}$$

sont contenues dans la réunion d'au plus $(n+1)^{2s}\, 2^{2n^2 s}$ sous-espaces propres de l'espace U des solutions de (3.5). Comme l'intervalle $[1, A^2]$ peut être couvert par au plus $4(n^2-1)$ intervalles du type (3.12), nous voyons, que les petites solutions (satisfaisant (3.11)) sont contenues dans la réunion d'au plus $4(n^2-1)(n+1)^{2s}2^{2n^2 s}$ sous-espaces propres de U.

Finalement toutes les solutions de (3.5) sont contenues dans la réunion d'au plus $c(n, d, s)$ sous-espaces propres de U. Le Théorème 3 s'en détuit par récurrence.

Il est bien connu, que le Théorème 3 a beaucoup d'applications (suites récurrentes, équations diophantiennes, théorie algébrique de nombres ...). Indiquons pour terminer deux conséquences simples.

Dans la session de problèmes aux Journées Arithmétiques de Luminy 1989 Bourgain a posé la question suivante: *Soit α un nombre algébrique de degré d, tel que pour tout $n \in \mathbb{N}$ on a $\mathbb{Q}(\alpha^n) = \mathbb{Q}(\alpha)$. Existe-t-il une constante $c = c(\alpha)$ ayant la propriété suivante: Pour chaque sous-espace linéaire propre W de l'espace vectoriel $\mathbb{Q}(\alpha)$ sur $\mathbb{Q}$ l'ensemble $\{n \mid n \in \mathbb{N},\ \alpha^n \in W\}$ a une cardinalité inférieure à $c(\alpha)$?* Il avait besoin de cet énoncé dans [2]. En appliquant le Théorème 3 nous pouvons démontrer

THÉORÈME 4. [11] *Une telle constante $c(\alpha)$ existe; plus précisément on peut prendre*

$$c(\alpha) = (4(1+\omega(\alpha)))^{2^{40(d+1)!}(1+\omega(\alpha))^6}$$

où $\omega = \omega(\alpha)$ est égal au nombre des idéaux premiers dans $\mathbb{Q}(\alpha)$ divisant (α).

Une autre conséquence se situe dans le contexte d'un problème, qui à première vue peut paraître plutôt élémentaire. *Soient b_1, b_2 deux nombres naturels > 1. Soit $c \geq 1$ une constante donnée.* En 1973 Senge et Straus [23] ont démontré: *pour qu'il n'existe qu'un nombre fini de nombres naturels n dont la somme des chiffres dans le développement en base b_1 et en base b_2 soit bornée par c, il faut et il suffit que b_1 et b_2 soient multiplicativement indépendants.* Ils ont démontré cela en appliquant la version $\mathfrak{p}$-adique du Théorème de Roth. On peut formuler le problème d'une manière différente en étudiant les solutions de l'équation exponentielle

$$a_1^{(1)} b_1^{n_1} + \cdots + a_{k_1}^{(1)} b_1^{n_{k_1}} - a_1^{(2)} b_2^{m_1} - \cdots - a_{k_2}^{(2)} b_2^{m_{k_2}} = 0,$$

où les $a_i^{(j)}$ sont les chiffres dans le développement b_j-adique. Le Théorème 3 en effet permet de traiter une question plus générale.

THÉORÈME 5. [17] *Soit $k \geq 2$. Soient $b_1, \ldots b_k$ des nombres rationnels supérieurs à 1. Soit $c \geq 1$ une constante. Alors l'équation*

$$\pm n_1 \pm \cdots \pm n_k = 0$$

n'admet qu'un nombre fini de solutions en nombres naturels $n_1, \ldots, n_k$ tels que la somme des chiffres de n_i dans le développement en base b_i est bornée par c si et seulement si pour chaque paire (i,j) avec $i \neq j$ b_i et b_j sont multiplicativement indépendants.

En outre, si cette hypothèse est vérifiée, le nombre de solutions est borné par

$$(8\omega)^{2^{28kc}\omega^6},$$

où ω est le nombre de facteurs premiers différents de $b_1 \cdots b_k$.

Références

[1] E. BOMBIERI et A. J. VAN DER POORTEN, Some quantitative results related to Roth's Theorem. *J. Austral. Math. Soc. (Series A)* **45** (1988), 233–248; Corrigenda **48** (1990), 154–155.

[2] J. BOURGAIN, The Riesz–Raikov Theorem for algebraic numbers, à paraître.

[3] H. DAVENPORT et K. F. ROTH, Rational approximation to algebraic numbers, *Mathematika* **2** (1955), 160–167.

[4] E. DUBOIS et G. RHIN, Sur la majoration de formes linéaires à coefficients algébriques réels et p-adiques; Démonstration d'une conjecture de K. Mahler, *C.r. hebd. Séanc. Acad. Sci. Paris* A **282** (1976), 1211–1214.

[5] J. H. EVERTSE, On equations in S-units and the Thue–Mahler equation, *Inventiones Math.* **75** (1984), 561–584.

[6] J. H. EVERTSE, On sums of S-units and linear recurrences, *Compositio Math.* **53** (1984), 225–244.

[7] J. H. EVERTSE et K. GYÖRY, On the numbers of solutions of weighted unit equations, *Compositio Math.* **66** (1988), 329–354.

[8] H. LUCKHARDT, Herbrand–Analysen zweier Beweise des Satzes von Roth: polynomiale Anzahlschranken, *Journ. of Symb. Logic.* **54** (1989), 234–263.

[9] K. MAHLER, Zur Approximation algebraischer Zahlen I. (Über den größten Primteiler binärer Formen), *Math. Ann.* **107** (1933), 691–730.

[10] A. J. VAN DER POORTEN et H. P. SCHLICKEWEI, The growth conditions for recurrence sequences, *Macquarie Math. Reports*, No. **82–0041**, 1982.

[11] A. J. VAN DER POORTEN et H. P. SCHLICKEWEI, A diophantine problem in harmonic analysis, à paraître dans *Math. Proc. Camb. Phil. Soc.*

[12] K. F. ROTH, Rational approximations to algebraic numbers, *Mathematika* **2** (1955), 1–20.

[13] H. P. SCHLICKEWEI, Linearformen mit algebraischen Koeffizienten, *Manuscripta Math.* **18** (1976), 147–185.

[14] H. P. SCHLICKEWEI, The $\mathfrak{p}$-adic Thue–Siegel–Roth–Schmidt theorem, *Arch. Math.* **29** (1977), 267–270.

[15] H. P. SCHLICKEWEI, The number of subspaces occurring in the p-adic subspace theorem in diophantine approximation, *Journ. Reine Angew. Math* **406** (1990), 44–108.

[16] H. P. SCHLICKEWEI, An explicit upper bound for the number of solutions of the S-unit equaiton, *Journ. Reine Angew. Math.* **406** (1990), 109–120.

[17] H. P. SCHLICKEWEI, Linear equations in integers with bounded sum of digits, à paraître dans *Journ. of Number Theory*.

[18] H. P. SCHLICKEWEI, The quantitative subspace theorem for number fields, soumis pour publication.

[19] H. P. SCHLICKEWEI, S-unit equations over number fields, à paraître dans *Inventiones Math.*

[20] W. M. SCHMIDT, Norm form equations, *Annals of Math.* **96** (1972), 526–551.

[21] W. M. SCHMIDT, Simultaneous approximation to algebraic numbers by elements of a number field, *Monatsh. Math.* **79** (1975), 55–66.

[22] W. M. SCHMIDT, The subspace theorem in diophantine approximations, *Compositio Math.* **69** (1989), 121–173.

[23] H. G. SENGE et E. G. STRAUS, PV–numbers and sets of multiplicity, *Per. Math. Hung.* **3** (1973), 93–100.

[24] C. L. SIEGEL, Über einige Anwendungen diophantischer Approximationen, *Abh. Preuß. Akad. Wiss., Phys.-math. Kl. No. 1*, 70 pp. (1929).

[25] J. H. SILVERMAN, Lower bounds for height functions, *Duke Math. Journ.* **51** (1984), 395–403.

Abteilung für Mathematik
Universität Ulm
Oberer Eselsberg
D 7900 Ulm
République Fédérale d'Allemagne

Astérisque

JEAN-PIERRE SERRE

Motifs

Astérisque, tome 198-199-200 (1991), p. 333-349

<http://www.numdam.org/item?id=AST_1991__198-199-200__333_0>

MOTIFS

Jean-Pierre SERRE

1. Introduction

Voici déjà 25 ans que Grothendieck a eu l'idée de la théorie des motifs. Dans l'introduction à "Récoltes et Semailles" ([9], p.xviii), il en dit ceci :

"Parmi toutes les choses mathématiques que j'avais eu le privilège de découvrir et d'amener au jour, cette réalité des motifs m'apparaît encore comme la plus fascinante, la plus chargée de mystère - au coeur même de l'identité profonde entre la "géométrie" et l' "arithmétique". Et le "yoga des motifs" auquel m'a conduit cette réalité longtemps ignorée est peut-être le plus puissant instrument de découverte que j'aie dégagé dans cette première période de ma vie de mathématicien."

Grothendieck lui-même n'a à peu près rien publié[1] sur le "yoga des motifs", à part de brèves allusions dans [7] et [8]. La théorie est restée longtemps confidentielle - tout en étant une source constante d'inspiration dans les questions les plus diverses : structures de Hodge, conjectures de Weil, fonctions L, sommes exponentielles, périodes, etc.

Le présent exposé n'est qu'une introduction. Pour plus de détails, on pourra consulter les textes cités dans la Bibliographie, et notamment [1], [2], [4], [6], [10], [11], [14], [15], [20]. Une Annexe reproduit la première lettre que j'aie reçue de Grothendieck sur les motifs (août 1964), ainsi que deux passages de "Récoltes et Semailles" ([9], 206-207 et 209-211).

[1] Il a fait un séminaire là-dessus à l'IHES en 1967 (cité dans [6]), mais ce séminaire n'a pas été rédigé. Il aurait également aimé en faire le sujet d'une série d'exposés au séminaire Bourbaki, mais il réclamait pour cela un minimum de dix séances ; étant à l'époque responsable du séminaire, j'avais refusé.

2. Méthodes topologiques en géométrie algébrique (groupes de cohomologie)

L'usage de telles méthodes, dans le cas classique où le corps de base est C, remonte à Poincaré, et a été particulièrement développé par Lefschetz, Hodge et bien d'autres. Que cela puisse aussi se faire en caractéristique p a été pressenti par Weil, à la fin des années quarante, lorsqu'il a énoncé les "conjectures de Weil" (cf.[**21**]) après en avoir démontré le cas particulier de la dimension 1. Une dizaine d'années plus tard, l'introduction par Grothendieck de la *topologie étale* (SGA 4 et SGA 5) a permis de définir des groupes de cohomologie ayant les propriétés voulues.

De façon plus précise, soit X une variété algébrique sur un corps k ; supposons pour simplifier que X soit projective et lisse. Soit $\overline{k}$ une clôture algébrique de k , et soit $\overline{X}$ la $\overline{k}$-variété déduite de X par extension des scalaires de k à $\overline{k}$. Alors, pour tout nombre premier $\ell \neq$ caract.k , les groupes de cohomologie étale $H^i_{et}(\overline{X}, \mathbf{Q}_\ell)$ sont des $\mathbf{Q}_\ell$-espaces vectoriels de dimension finie ayant toutes les propriétés requises : dualité de Poincaré, formule de Künneth, formule de Lefschetz, etc. De plus, le groupe de Galois $\mathrm{Gal}(\overline{k}/k)$ opère de façon naturelle sur ces espaces, ce qui donne naissance à des représentations ℓ-adiques particulièrement intéressantes, surtout lorsque k est un corps de nombres, cf.[**19**].

D'autres groupes de cohomologie peuvent être définis. Ainsi, si caract.k = 0, l'hypercohomologie du complexe des formes différentielles fournit des groupes de cohomologie "de de Rham" $H^i_{DR}(X,k)$; ce sont des k-espaces vectoriels filtrés de dimension finie. Si de plus k est plongeable dans C, le choix d'un tel plongement conduit à des groupes de cohomologie "de Betti" $H^i_B(X, \mathbf{Q})$, qui sont des Q-espaces vectoriels de dimension finie ; leurs produits tensoriels avec C sont bigradués (structure de Hodge).

Pour X et i fixés, tous ces espaces ont même dimension : le i-ème nombre de Betti de la variété X. Ils sont liés entre eux par des isomorphismes de compatibilité variés ; par exemple, si k est plongé dans C, on a un isomorphisme "de périodes" :

$$H^i_B(X, \mathbf{Q}) \otimes_{\mathbf{Q}} \mathbf{C} \simeq H^i_{DR}(X,k) \otimes_k \mathbf{C}.$$

3. Motifs

La situation décrite ci-dessus n'est pas tout à fait satisfaisante. On dispose de trop de groupes de cohomologie qui ne sont pas suffisamment liés entre eux

- malgré les isomorphismes de compatibilité. Par exemple, si X et Y sont deux variétés (projectives, lisses), et $f : H^i_{et}(X, \mathbf{Q}_\ell) \to H^i_{et}(Y, \mathbf{Q}_\ell)$ une application $\mathbf{Q}_\ell$-linéaire, où ℓ est un nombre premier fixé, il n'est pas possible en général de déduire de f une application analogue pour la cohomologie ℓ'-adique, où ℓ' est un autre nombre premier. Pourtant, on a le sentiment que c'est possible pour certains f, ceux qui sont "motivés" (par exemple ceux qui proviennent d'un morphisme de Y dans X, ou plus généralement d'une correspondance algébrique entre X et Y). Encore faut-il savoir ce que "motivé" veut dire !

Une façon plus précise de poser cette question est de demander si l'on peut construire une catégorie $\mathbf{Q}$-abélienne $\underline{M}(k)$ ainsi qu'un foncteur contravariant

$$X \longmapsto h(X) = \oplus\, h^i(X) \qquad , \qquad h^i(X) \in \mathrm{ob}(\underline{M}(k)),$$

ayant (entre autres) les propriétés suivantes :

a) Si A et B sont des objets de $\underline{M}(k)$, $\mathrm{Hom}(A, B)$ est un $\mathbf{Q}$-espace vectoriel de dimension finie (i.e. les objets de $\underline{M}(k)$ se comportent comme des espaces vectoriels de dimension finie).

b) Il existe pour tout $\ell \neq \mathrm{caract}.k$ un foncteur

$$T_\ell : \underline{M}(k) \to G\text{-}\mathbf{Q}_\ell \text{ -représentations (où } G = \mathrm{Gal}(\overline{k}/k))$$

tel que $H^i_{et}(\overline{X}, \mathbf{Q}_\ell)$ se déduise de $h^i(X)$ par application du foncteur T_ℓ.

c) Enoncé analogue à b) pour la cohomologie de de Rham, lorsque $\mathrm{caract}.k = 0$.

d) Enoncé analogue pour la cohomologie de Betti lorsque k est plongé dans $\mathbf{C}$.

Bref, $h(X)$ devrait jouer le rôle d'une *cohomologie rationnelle* dont les autres cohomologies se déduisent.

Comment définir $\underline{M}(k)$ et le foncteur h ? La première question que l'on se pose est celle-ci : que sont les objets de $\underline{M}(k)$? En fait, ce n'est pas là un point important ; comme Grothendieck nous l'a appris, les objets d'une catégorie ne jouent pas un grand rôle, ce sont les morphismes qui sont essentiels[2]. On peut donc, comme première approximation, définir une catégorie $\underline{M}^0(k)$ dont les

[2] Exemple élémentaire : si l'on veut construire une catégorie équivalente à celle des k-espaces vectoriels de dimension finie, on peut prendre pour objets les entiers ≥ 0 et définir $\mathrm{Hom}(m,n)$ comme l'ensemble des matrices $m \times n$ à coefficients dans k ; c'est le point de vue "matriciel" en algèbre linéaire.

objets sont les variétés projectives lisses sur k, et définir h comme le foncteur qui, à une telle variété X, attache X elle-même ; bien sûr, il faut aussi dire ce qu'est $\mathrm{Hom}(X,Y)$ dans la catégorie $\underline{M}^0(k)$, et c'est là le point décisif.

Le premier choix fait par Grothendieck est le suivant (je l'énonce en supposant que toutes les composantes de X ont même dimension - le cas général se ramène à celui-là par additivité) :

$\mathrm{Hom}(X,Y) = \mathbf{Q} \otimes C(X,Y)$, où $C(X,Y)$ est le *groupe des classes de cycles algébriques* de $X \times Y$, de codimension égale à $\dim X$, modulo l'équivalence numérique[3].

(Les éléments de $C(X,Y)$ peuvent être vus comme des correspondances algébriques allant de Y vers X : le foncteur h est contravariant.)
La composition des morphismes se définit sans difficulté.

En fait, la construction ci-dessus n'est qu'une première étape dans la définition de la catégorie des motifs. Il est nécessaire d'agrandir $\underline{M}^0(k)$:

a) En ajoutant (de façon purement formelle) les *noyaux des projecteurs* (un "projecteur" est un élément idempotent d'un $\mathrm{Hom}(X,X)$).

On obtient ainsi la catégorie $\underline{M}^{eff}(k)$ des *motifs effectifs* sur k. Ses objets sont les couples (X,π), où X est un objet de $\underline{M}^0(k)$ et π un idempotent de $\mathrm{End}(X)$. Cette catégorie est munie de produits tensoriels ; elle a un élément unité 1 qui est $h(X)$ pour X réduit à un point.

b) En ajoutant (de façon également formelle) l'inverse L^{-1} du motif L défini par $h(\mathbf{P}_1) = 1 \oplus L$ (i.e. $L = h^2(\mathbf{P}_1)$).

Le motif L^{-1} est le *motif de Tate* ; il correspond, du point de vue galoisien, aux caractères cyclotomiques.

Soit $\underline{M}(k)$ la catégorie obtenue après les deux opérations a) et b). C'est la catégorie des motifs cherchée (ou en tout cas l'une de ses incarnations). Si l'on admet les "conjectures standard", cette catégorie est une $\mathbf{Q}$-catégorie abélienne semi-simple (cf. [6], [11], [14] pour plus de détails) ; c'est même une *catégorie tannakienne*, au sens de [5] et [16] : les produits tensoriels et Hom internes ont toutes les propriétés habituelles. Les foncteurs

$$T_\ell : \underline{M}(k) \to \mathbf{G}\text{-}\mathbf{Q}_\ell\text{-représentations} \quad (\ell \neq \mathrm{caract}.k)$$

[3] A la place de l'équivalence numérique, on pourrait prendre l'équivalence *linéaire*, qui conduit aux groupes de Chow ; cela donne une théorie plus fine, cf. [20].

se définissent sans difficulté, et il en est de même des foncteurs liés aux cohomologies de de Rham et de Betti. Enfin, $\underline{M}(k)$ est *graduée* : tout élément h a une décomposition canonique $h = \sum_{i \in \mathbf{Z}} h^i$ qui reflète celle de la cohomologie. Un élément h tel que $h^j = 0$ pour $j \neq i$ est dit *pur de poids* i ; ainsi, le motif de Tate est pur de poids -2.

4. Autres définitions

La définition de $\underline{M}(k)$ donnée ci-dessus n'est réellement commode que si l'on admet les "conjectures standard" (cf. [7]) ainsi que la conjecture de Hodge (et aussi celle de Tate, qui est son analogue ℓ-adique). Malheureusement, aucun progrès n'a été fait sur ces conjectures depuis les années soixante. On ignore par exemple si les projecteurs associés à la décomposition de Künneth

$$H^n(X \times Y) = \bigoplus_{a+b=n} H^a(X) \otimes H^b(Y)$$

sont donnés par des cycles algébriques (ils sont pourtant aussi bien motivés qu'on peut l'être). Or l'algébricité de ces projecteurs est nécessaire si l'on veut prouver que tout motif est somme directe de motifs purs, ce qui est l'une des propriétés les plus importantes des motifs.
On est ainsi conduit (suivant les besoins) à changer la théorie en modifiant la définition de Hom, c'est-à-dire la définition des flèches "motivées". A l'heure actuelle, la définition qui semble la plus commode est celle utilisée par Deligne [3], basée sur les "cycles de Hodge absolus", le corps k étant supposé de caractéristique 0. *Grosso modo* (voir [3] pour des énoncés précis), cela revient à définir $\mathrm{Hom}(X, Y)$ comme l'ensemble des familles de flèches

$$H_\lambda(X) \to H_\lambda(Y),$$

définies pour toutes les cohomologies H_λ du n°2 (ℓ-adique, de Rham, Betti) et satisfaisant à toutes les compatibilités naturelles ; les projecteurs de Künneth en sont des exemples. Pour les variétés abéliennes, Deligne a prouvé que

"Hodge $\Rightarrow$ Hodge absolu".

C'est là un résultat très utile. Il entraîne (cf. [3], [19]) que les groupes de Galois ℓ-adiques attachés aux modules de Tate des variétés abéliennes sont contenus dans les points ℓ-adiques des groupes de Mumford-Tate correspondants.

5. Exemples de décompositions de motifs

Je me borne à des cas simples, qui ne nécessitent aucune conjecture, comme l'a montré Manin [14].

- *Espace projectif* $\mathbf{P}_n$

La formule donnant le nombre de points de $\mathbf{P}_n$ sur un corps à q éléments :

$$|\mathbf{P}_n(\mathbf{F}_q)| = 1 + q + \cdots + q^n,$$

suggère la décomposition suivante du motif $h(\mathbf{P}_n)$:

$$h(\mathbf{P}_n) = 1 \oplus L \oplus \cdots \oplus L^n,$$

et cela peut effectivement se démontrer (sur un corps de base quelconque).

- *Eclatements*

Soit Y une sous-variété fermée lisse de X, et soit X_Y l'éclatée de X le long de Y. Supposons que Y soit partout de codimension d dans X. On a alors :

$$h(X_Y) = h(X) \oplus h(Y) \otimes (L \oplus L^2 \oplus \cdots \oplus L^{d-1})$$

comme le suggère le calcul du nombre de points de $X_Y(k)$ lorsque $k = \mathbf{F}_q$:

$$\begin{aligned} |X_Y(\mathbf{F}_q)| &= |X(\mathbf{F}_q)| - |Y(\mathbf{F}_q)| + |Y(\mathbf{F}_q)|.|\mathbf{P}_{d-1}(\mathbf{F}_q)| \\ &= |X(\mathbf{F}_q)| + |Y(\mathbf{F}_q)|(q + q^2 + \cdots + q^{d-1}). \end{aligned}$$

- *Courbes*

Supposons que X soit une courbe projective lisse, géométriquement connexe. On a

$$h(X) = 1 \oplus h^1(X) \oplus L,$$

avec $h^1(X) = h^1(\text{Jac } X)$, où Jac X est la jacobienne de X.

(On peut presque écrire "$h^1(X) = \text{Jac } X$" ; en effet, la catégorie des motifs effectifs de poids 1 est équivalente à la catégorie des variétés abéliennes à isogénie près - ce qui explique le succès des méthodes de Weil en dimension 1.)

- *Surfaces cubiques dans* $\mathbf{P}_3$

Si X est une telle surface, supposée lisse, on a :

$$h(X) = 1 \oplus h^2(X) \oplus L^2 \quad \text{et} \quad h^2(X) = L \otimes (1 \oplus V_6),$$

où V_6 est un motif de poids 0 et de rang 6, provenant d'une représentation galoisienne $\mathrm{Gal}(\overline{k}/k) \to \mathbf{GL}_6(\mathbf{Q})$, à image contenue dans le groupe de Weyl du système de racines de type E_6, cf. [14].

On pourrait multiplier les exemples, élémentaires ou non (hypersurfaces cubiques de $\mathbf{P}_4$, surfaces $K3, \ldots$). Dans chaque cas, la théorie des motifs donne une décomposition en morceaux qui permet d'isoler les facteurs les plus intéressants (tel le facteur V_6 pour une surface cubique) ; et ces morceaux eux-mêmes peuvent se recombiner pour former d'autres motifs. Ce jeu de construction (le *meccano* des motifs) se traduit, lorsque k est fini, par des relations entre nombres de points, et, lorsque k est un corps global, par des identités entre fonctions L. C'est l'un des charmes de la théorie.

6. Groupes de Galois motiviques

Admettons les conjectures standard, ainsi que la conjecture de Hodge, et supposons k plongeable dans $\mathbf{C}$. La catégorie $\underline{M}(k)$ est alors une $\mathbf{Q}$-catégorie abélienne semi-simple tannakienne. De plus, cette catégorie possède un *foncteur fibre* sur $\mathbf{Q}$, à savoir le foncteur de Betti relatif à un plongement fixé de k dans $\mathbf{C}$. Il en résulte (cf.[5],[16]) que $\underline{M}(k)$ est équivalente, comme catégorie tannakienne, à la catégorie des représentations linéaires d'un groupe pro-algébrique $\underline{G}_k$ sur $\mathbf{Q}$, le *groupe de Galois motivique* (cf.[9], p.206-207, reproduit en Annexe). Ce groupe est réductif. A torsion galoisienne près, il ne dépend pas du plongement choisi de k dans $\mathbf{C}$. Le quotient de $\underline{G}_k$ par sa composante neutre $\underline{G}_k^0$ s'identifie au groupe de Galois usuel $\mathrm{Gal}(\overline{k}/k)$, vu comme groupe pro-algébrique de dimension 0.

Si k est un corps de nombres, le plus grand quotient abélien de $\underline{G}_k$ n'est autre que la limite projective des groupes $S_{\mathfrak{m}}$ définis et étudiés dans [18], chap.II.

Lorsqu'on remplace $\underline{M}(k)$ par la sous-catégorie tannakienne $\underline{M}_X(k)$ engendrée par un motif X, le groupe pro-algébrique $\underline{G}_k$ est remplacé par un quotient $\underline{G}_{k,X}$ qui est un groupe linéaire réductif (algébrique, i.e. de type fini sur $\mathbf{Q}$) ; sa composante neutre $\underline{G}_{k,X}^0$ est le *groupe de Mumford-Tate* de X. Ainsi, si E est une courbe elliptique sans multiplications complexes, le groupe $\underline{G}_{k,E}$

est le groupe $\mathbf{GL}_2$; il en résulte, vu la classification des représentations de ce groupe, que tout objet de $\underline{M}_E(k)$ est somme directe de motifs de la forme

$$L^r \otimes \mathrm{Sym}^s E \text{ , avec } r \in \mathbf{Z} \text{ et } s \geq 0.$$

Si ℓ est un nombre premier, et si X est un motif, l'action de $\mathrm{Gal}(\overline{k}/k)$ sur la cohomologie ℓ-adique de X se fait par l'intermédiaire d'un groupe de Lie ℓ-adique qui est un sous-groupe compact du groupe $\underline{G}_{k,X}(\mathbf{Q}_\ell)$. Lorsque k est de type fini sur $\mathbf{Q}$, on conjecture que ce sous-groupe est *ouvert*, i.e. que l'action de $\mathrm{Gal}(\overline{k}/k)$ est "aussi grosse que possible" ; dans certains cas (voir [19], C.3.8 pour un énoncé précis), on conjecture même que ce groupe est un sous-groupe compact maximal de $G_{k,X}(\mathbf{Q}_\ell)$ pour presque tout ℓ.

7. Motifs et formes automorphes

En 1967, Weil [22] énonce une conjecture (dite "de Weil", ou "de Shimura-Taniyama", ou "de Taniyama-Weil", suivant les auteurs) affirmant que toute courbe elliptique sur $\mathbf{Q}$ est "modulaire". Dès cette date, il était clair (cf. par exemple [17]) que cette conjecture devait s'étendre à tout motif sur tout corps de nombres, à condition d'utiliser des "formes automorphes" plus générales - celles pour lesquelles Langlands [12] venait justement de définir des fonctions L ayant les propriétés habituelles (avec Hecke remplaçant Frobenius). En d'autres termes, la catégorie des motifs sur un corps de nombres devrait être plongeable dans la catégorie des représentations automorphes des groupes réductifs (pour des énoncés plus précis, voir [1] , [13]). C'est là l'un des aspects les plus passionnants de ce que l'on appelle la "philosophie de Langlands".

8. Motifs mixtes

Jusqu'à présent, nous n'avons considéré que des motifs associés à des variétés projectives lisses. Que peut-on dire dans le cas général ?

Supposons pour simplifier que k soit de caractéristique 0. Soit X une k-variété quelconque. On peut écrire X comme union disjointe de sous-variétés localement fermées X_α qui soient quasi-projectives et lisses ; d'après le théorème de résolution des singularités, chaque X_α est de la forme $\overline{X}_\alpha - D_\alpha$, avec $\overline{X}_\alpha$ projective lisse et $\dim D_\alpha < \dim X$. En procédant par récurrence sur $\dim X$, on obtient une décomposition :

$$x = \coprod Y_i - \coprod Z_j \text{ ,}$$

où les Y_i et les Z_j sont projectives et lisses. On est ainsi amené à définir le

"motif virtuel"

$$h(X) = \sum_i h(Y_i) - \sum_j h(Z_j),$$

la somme de droite étant prise dans le groupe de Grothendieck $M(k)$ de la catégorie $\underline{M}(k)$, cf. Annexe 1. Bien entendu, on doit vérifier que $h(X)$ ne dépend pas de la décomposition de X choisie, ce qui résulte des conjectures[4] sur les représentations ℓ-adiques mentionnées au n°6.

Exemple. Si Y est une variété projective lisse et si X est le cône affine de base Y, on a $h(X) = 1 + L \otimes h(Y) - h(Y)$.

La construction ci-dessus revient à faire une somme du genre "Jordan-Hölder", ce qui est raisonnable dans la catégorie $\underline{M}(k)$ puisque celle-ci est (conjecturalement) semi-simple. On peut cependant être plus exigeant, et vouloir définir des "Ext" non triviaux entre motifs. Cela revient à introduire une nouvelle catégorie, celle des "motifs mixtes". La définition que l'on doit adopter n'est nullement évidente, cf. Deligne [4] et Jannsen [10]. Je n'en dirai rien, et je me bornerai pour terminer à citer deux énoncés conjecturaux montrant l'intérêt des Ext dans la catégorie en question :

- Si k est un corps de nombres, on a :

$$\mathrm{Ext}^1(1, L^{-n}) \overset{?}{=} \mathbf{Q} \otimes K_{2n-1}(k) \qquad \text{pour tout } n \geq 1,$$

ce qui relie motifs et K-théorie.

- Si A est une variété abélienne sur k, on a :

$$\mathrm{Ext}^1(h^1(A), 1) \overset{?}{=} \mathbf{Q} \otimes A(k).$$

Ce dernier énoncé est particulièrement satisfaisant ; il montre que le groupe de Mordell-Weil peut se lire dans la catégorie des motifs mixtes (plus généralement, tous les termes figurant dans la formule de Birch et Swinnerton-Dyer doivent avoir une interprétation motivique).

****

Note : Une première rédaction de cet exposé, faite par Michel Waldschmidt, m'a été très utile. Je l'en remercie vivement.

[4] J'ignore si cette indépendance peut se démontrer sans utiliser aucune conjecture.

ANNEXE
Quelques textes de Grothendieck sur les motifs

1. *Extrait d'une lettre datée du 16.8.1964*

"Cher Serre,

... Cette question est d'ailleurs liée à la suivante, sans doute bien hors de notre portée. Soit k un corps, algébriquement clos pour fixer les idées, et soit $L(k)$ le "groupe K" défini par les schémas de type fini sur k, avec comme relations celles qui proviennent d'un découpage en morceaux (l'initiale L est suggérée bien sûr par les liens avec les fonctions L). Soit $M(k)$ le "groupe K" défini par les "motifs" sur k. J'appelle "motif" sur k quelque chose comme un groupe de cohomologie ℓ-adique d'un schéma algébrique sur k, mais considéré comme indépendant de ℓ, et avec sa structure "entière", ou disons pour l'instant "sur $\mathbf{Q}$", déduite de la théorie des cycles algébriques. La triste vérité, c'est que pour le moment je ne sais pas définir la catégorie abélienne des motifs, bien que je commence à avoir un yoga assez précis sur cette catégorie, disons $\underline{M}(k)$. Par exemple, pour tout ℓ premier $\neq p$, on a un foncteur exact T_ℓ de $\underline{M}(k)$ dans la catégorie des vectoriels de dimension finie sur $\mathbf{Q}_\ell$, avec opérations du pro-groupe $(\mathrm{Gal}(\overline{k_i}/k_i))_i$ dessus, où k_i parcourt les sous-extensions[5] de type fini de k et $\overline{k_i}$ est la clôture algébrique de k_i dans $\overline{k}$; ce foncteur est fidèle, mais bien entendu pas pleinement fidèle. Si k est de caractéristique 0, il y a également un foncteur T_∞ de $\underline{M}(k)$ dans la catégorie des vectoriels de dimension finie sur k (le "foncteur de De Rham-Hodge", alors que T_ℓ est le "foncteur de Tate"). En tout cas, si on admet les deux ingrédients que tu sais (Hodge-Künneth) de l'hyp. de Riemann-Weil, je sais construire explicitement (en fait sur tout préschéma de base plus ou moins, pas seulement sur un corps) la sous-catégorie des objets *semi-simples* de $\underline{M}(k)$ (essentiellement comme des facteurs directs, définis par des classes de correspondances algébriques, d'un $H^i(X, \mathbf{Z}_\ell)$, où X est une variété projective non singulière). Il n'en faut pas plus pour construire le groupe $M(k)$ (et je pense qu'on pourrait en donner une description indépendante des conjectures que j'ai dites, si on voulait). Ainsi, pour tout ℓ, on a un homomorphisme de $M(k)$ dans le "groupe K", soit $M_\ell(k)$, défini par les $\mathbf{Q}_\ell$-G-modules de type fini sur $\mathbf{Q}_\ell$, où G est le groupe profini défini plus haut, ou si tu préfères, la pro-algèbre de Lie associée (qui a l'avantage sur le groupe d'être un pro-objet *strict*, i.e. à morphismes de transition surjectifs). Ceci dit, prenant des sommes alternées de cohomologies à support compact, on trouve un homomorphisme naturel

$$L(k) \to M(k),$$

[5] Les k_i sont les sous-corps de k qui sont de type fini sur le corps premier.

qui est d'ailleurs un homomorphisme d'anneaux (pour le produit cartésien à gauche, le produit tensoriel à droite). La question générale qui se pose est alors de savoir ce qu'on peut dire sur cet homomorphisme, est-il très loin d'être bijectif ? Note que les deux membres de cet homomorphisme sont munis de filtrations naturelles, via la dimension des préschémas, et l'homomorphisme est compatible avec ces filtrations. La question ci-dessus sur les jacobiennes[6] peut encore se formuler ainsi : $L^{(1)} \to M^{(1)}$ est-il surjectif ? (En effet, à un facteur trivial $\mathbf{Z}$ près, provenant de la dimension 0, $M^{(1)}$ n'est autre que le groupe K défini par les VA définies sur k).

Je ne me hasarde à aucune conjecture générale sur l'homomorphisme plus haut, j'espère simplement par des considérations heuristiques de ce genre finir par arriver à une construction effective de la catégorie des motifs, ce qui me semble un point essentiel de mon "long-run program". Par contre, il y a d'autres conjectures en pagaille que je ne me prive pas de faire, pour préciser le yoga. Par exemple, que $M(k) \to M_\ell(k)$ est injectif, plus précisément que deux motifs simples non isomorphes (je devrais peut-être dire plutôt : non isogènes) donnent lieu à des composants simples ℓ-adiques deux à deux distincts. La conjecture de Tate se généralise en énonçant que, pour X projective non singulière, la filtration "arithmétique" des $H^i(X)$ (via la filtration de X par la dimension) est déterminée par la filtration déjà signalée de $M(k)$, ou encore la filtration de $H^i(X, \mathbf{Z}_\ell)$ est déterminée par la structure de module galoisien (ou plutôt pro-galoisien) à l'aide de la filtration correspondante de $M(k)$. Par exemple, en dimension impaire, le morceau de filtration maximale de $H^{2i-1}(X, \mathbf{Z}_\ell(i))$ est aussi le plus grand "morceau abélien" et correspond au module de Tate de la jacobienne intermédiaire $J^i(X)$ (définie par les cycles algébriquement équivalents à 0 de codimension i sur X).

Je te signale d'ailleurs que j'ai bel et bien une construction de telles jacobiennes intermédiaires (de dimension majorée par $b_{2i-1}/2$ comme il se doit). Malheureusement, même conjecturalement, je n'ai pas encore compris le lien entre la positivité à la Hodge et la forme de Néron-Tate relative à l'autodualité de J^i pour $\dim X = 2i - 1$, et j'aimerais en parler avec toi un jour avant ton départ. Pour les surfaces, on obtient bien une démonstration du théorème de l'index de Hodge à l'aide des fourbis de Néron et Tate, essentiellement en se ramenant à la positivité de l'autodualité d'une jacobienne d'une courbe ; et je

[6] Il s'agit de la question suivante : le groupe K des variétés abéliennes (à isogénie près) est-il engendré par les jacobiennes ? (Note de J-P. Serre.)

ne suis toujours pas convaincu que ce principe de démonstration par réduction à la dimension 1 n'a pas une portée plus générale.

...

Bien à toi.

A. Grothendieck "

2. *Extrait de "Récoltes et Semailles", p.206-207*

"... Quand, il y a trois semaines à peine, je me suis étendu en une page ou deux sur le yoga des motifs, comme un de mes "orphelins" et qui me tenait à coeur plus qu'aucun autre, j'ai dû être bien à côté de la plaque ! Sans doute ai-je rêvé, quand il me semblait me souvenir d'années de gestation d'une vision, ténue et élusive d'abord, et s'enrichissant et se précisant au cours des mois et des années, dans un effort obstiné pour essayer de saisir le "motif" commun, la quintessence commune, dont les nombreuses théories cohomologiques connues alors étaient autant d'incarnations différentes, nous parlant chacune dans son propre langage sur la nature du "motif" dont elle était l'une des manifestations directement tangibles. Sans doute je rêve encore, en me souvenant de la forte impression que m'avait faite telle intuition de Serre, qui avait été amené à voir un groupe de Galois profini, un objet donc qui semblait de nature essentiellement discrète (ou, du moins, se réduisant tautologiquement à de simples systèmes de groupes *finis*), comme donnant naissance à un immense système projectif de groupes ℓ-adiques *analytiques*, voire de groupes *algébriques* sur $\mathbf{Q}_\ell$ (en passant à des enveloppes algébriques convenables), qui avaient même une tendance à être réductifs - avec du coup l'introduction de tout l'arsenal des intuitions et méthodes (à la Lie) des groupes analytiques et algébriques. Cette construction avait un sens pour tout nombre premier ℓ, et je sentais (ou je rêve que j'ai senti...) qu'il y avait un mystère à sonder sur la relation de ces groupes algébriques pour des nombres premiers différents ; qu'ils devaient tous provenir d'un même système projectif de groupes algébriques sur le seul sous-corps commun naturel à tous ces corps de base, savoir le corps $\mathbf{Q}$, le corps "absolu" de caractéristique nulle. Et puisque j'aime rêver, je continue à rêver que je me souviens être entré dans ce mystère entrevu, par un travail qui sûrement n'était qu'un rêve puisque je ne "démontrais" rien ; que j'ai fini par comprendre comment la notion de motif fournissait la clé de ce mystère - comment, par le seul fait de la présence d'une catégorie (ici celle des motifs "lisses" sur un schéma de base donné, par exemple les motifs sur un corps de base donné),

ayant des structures internes similaires à celles qu'on trouve sur la catégorie des représentations linéaires d'un pro-groupe algébrique sur un corps k (le charme de la notion de pro-groupe algébrique m'ayant été révélé précédemment par SERRE également), on arrive à reconstituer bel et bien un tel pro-groupe (dès qu'on dispose d'un "foncteur fibre" convenable), et à interpréter la catégorie "abstraite" comme la catégorie de ses représentations linéaires.

Cette approche vers une "théorie de Galois motivique" m'était soufflée par l'approche que j'avais trouvée, des années avant, pour décrire le groupe fondamental d'un espace topologique ou d'un schéma (ou même d'un topos quelconque - mais là je sens que je vais blesser des oreilles délicates que "les topos n'amusent pas"...), en termes de la catégorie des revêtements étales sur l' "espace" envisagé, et les foncteurs fibres sur celle-ci. Et le langage même des "*groupes de Galois motiviques*" (que j'aurais pu aussi bien appeler "groupes fondamentaux" motiviques, les deux genres d'intuitions étant pour moi la même chose, depuis la fin des années cinquante...), et celui des "foncteurs fibres" (qui correspondent très exactement aux "incarnations manifestes" dont il était question plus haut, savoir aux différentes "théories cohomologiques" qui s'appliquent à une catégorie de motifs donnée) - ce langage était fait pour exprimer la nature profonde de ces groupes et suggérer à l'évidence leurs liens immédiats avec les groupes de Galois et avec les groupes fondamentaux ordinaires.

Je me rappelle encore du plaisir et de l'émerveillement, dans ce jeu avec des foncteurs fibres, et avec les torseurs sous les groupes de Galois qui font passer des uns aux autres en "twistant", de retrouver dans une situation particulièrement concrète et fascinante tout l'arsenal des notions de cohomologie non commutative développée dans le livre de Giraud, avec la gerbe des foncteurs-fibres (ici au-dessus du topos étale, ou mieux, du topos $fpqc$ de $\mathbf{Q}$ - des topos non triviaux et intéressants s'il en fût !), avec le "lien" (en groupes ou pro-groupes algébriques) qui lie cette gerbe, et les avatars de ce lien, se réalisant par des groupes ou pro-groupes algébriques divers, correspondant aux différentes "sections" de la gerbe, c'est-à-dire aux divers foncteurs cohomologiques. Les différents points complexes (par exemple) d'un schéma de caractéristique nulle donnaient naissance (via les foncteurs de Hodge correspondants) à autant de sections de la gerbe, et à des torseurs de passage de l'une à l'autre, ces torseurs et les pro-groupes opérant sur eux étant munis de structures algébrico-géométriques remarquables, exprimant les structures spécifiques de la cohomologie de Hodge ... "

3. *Extrait de "Récoltes et Semailles", p.209-211*

"... Puis il y a eu un troisième "rêve motifs", qui était comme le mariage des deux rêves précédents - quand il s'est agi d'interpréter, en termes de structures sur les groupes de Galois motiviques et sur les torseurs sous ces groupes qui servent à "tordre" un foncteur fibre pour obtenir (canoniquement) tout autre foncteur fibre[7], les différentes structures supplémentaires dont est munie la catégorie des motifs et dont une des toutes premières est justement celle de la filtration par les poids. Je crois me souvenir que là moins que jamais il n'était question de devinettes, mais bien de traductions mathématiques en bonne et due forme. C'étaient autant "d'exercices" inédits sur les représentations linéaires de groupes algébriques que j'ai faits avec grand plaisir pendant des jours et des semaines, sentant bien que j'étais en train de cerner de plus en plus près un mystère qui me fascinait depuis des années ! La notion la plus subtile peut-être qu'il a fallu appréhender et formuler en termes de représentations a été celle de "polarisation" d'un motif, en m'inspirant de la théorie de Hodge et en essayant d'en décanter ce qui gardait un sens dans le contexte motivique. C'était là une réflexion qui a dû se faire vers le moment de ma réflexion sur une formulation des "conjectures standard", inspirées l'une et l'autre par l'idée de Serre (toujours lui !) d'un analogue "kählérien" des conjectures de Weil.

Dans une telle situation, quand les choses elles-mêmes nous soufflent quelle est leur nature cachée et par quels moyens nous pouvons le plus délicatement et le plus fidèlement l'exprimer, alors que pourtant beaucoup de faits essentiels semblent hors de la portée immédiate d'une démonstration, le simple instinct nous dit d'écrire simplement noir sur blanc ce que les choses nous soufflent avec insistance, et d'autant plus clairement que nous prenons la peine d'écrire sous leur dictée ! Point n'est besoin de se soucier de démonstrations ou de constructions complètes - s'encombrer de telles exigences à ce stade-là du travail reviendrait à s'interdire l'accès de l'étape la plus délicate, la plus essentielle d'un travail de découverte de vaste envergure - celle de la naissance d'une vision, prenant forme et substance hors d'un apparent néant. Le simple fait d'*écrire*, de *nommer*, de *décrire* - ne serait-ce d'abord que décrire des intuitions élusives ou de simples "soupçons" réticents à prendre forme - a un *pouvoir créateur*. C'est là l'instrument entre tous de la passion de connaître, quand celle-ci s'investit en des choses que l'intellect peut appréhender. Dans la démarche de la découverte en ces choses-là, ce travail en est l'étape créatrice entre toutes, qui toujours

[7] Tout comme les groupes fondamentaux $\pi_1(x),\pi_1(y)$ de quelque "espace" X en deux "points" x et y se déduisent l'un de l'autre en "tordant" par le torseur $\pi_1(x,y)$ des classes de chemins de x à y ...

précède la démonstration et nous en donne les moyens - ou, pour mieux dire, sans laquelle la question de "démontrer" quelque chose ne se pose même pas, avant que rien encore de ce qui touche l'essentiel n'aurait été formulé et vu. Par la seule vertu d'un effort de formulation, ce qui était informe prend forme, se prête à examen, faisant se décanter ce qui est visiblement faux de ce qui est possible, et de cela surtout qui s'accorde si parfaitement avec l'ensemble des choses connues, ou devinées, qu'il devient à son tour un élément tangible et fiable de la vision en train de naître. Celle-ci s'enrichit et se précise au fil du travail de formulation. Dix choses soupçonnées seulement, dont aucune (la conjecture de Hodge disons) n'entraîne conviction, mais qui mutuellement s'éclairent et se complètent et semblent concourir à une même harmonie encore mystérieuse, acquièrent dans cette harmonie force de vision. Alors même que toutes les dix finiraient par se révéler fausses, le travail qui a abouti à cette vision provisoire n'a pas été fait en vain, et l'harmonie qu'il nous a fait entrevoir et qu'il nous a permis de pénétrer tant soit peu n'est pas une illusion mais une réalité, nous appelant à la connaître. Par ce travail, seulement, nous avons pu entrer en contact intime avec cette réalité, cette harmonie cachée et parfaite. Quand nous savons que les choses ont raison d'être ce qu'elles sont, que notre vocation est de les connaître, non de les dominer, alors le jour où une erreur éclate est jour d'exultation - tout autant que le jour où une démonstration nous apprend au-delà de tout doute que telle chose que nous imaginions était bel et bien l'expression fidèle et véritable de la réalité elle-même... "

BIBLIOGRAPHIE

[1] L. CLOZEL, *Motifs et formes automorphes : applications du principe de fonctorialité,* in *Automorphic Forms, Shimura Varieties and L-Functions* (L. Clozel et J.S. Milne édit.), vol. 1, 77-159, Acad. Press (1990).

[2] P. DELIGNE, *Valeurs de fonctions L et périodes d'intégrales*, Proc. Symp. Pure Math. 33, A.M.S., vol. 2, 313-346 (1979).

[3] P. DELIGNE, *Hodge cycles on abelian varieties* (notes by J.S. Milne), Lect. Notes in Math. 900, 9-100, Springer-Verlag (1982).

[4] P. DELIGNE, *Le groupe fondamental de la droite projective moins trois points,* in *Galois Groups over* **Q** (Y. Ihara, K. Ribet, J-P. Serre édit.), 79-297, Springer-Verlag (1989).

[5] P. DELIGNE et J.S. MILNE, *Tannakian categories*, Lect. Notes in Math. 900, 101-228, Springer-Verlag (1982).

[6] M. DEMAZURE, *Motifs des variétés algébriques*, Sém. Bourbaki 1969-1970, exposé 365, Lect. Notes in Math. 180, Springer-Verlag (1971).

[7] A. GROTHENDIECK, *Standard conjectures on algebraic cycles*, Bombay Coll. on Algebraic Geometry, Oxford, 193-199 (1969).

[8] A. GROTHENDIECK, *Hodge general conjecture is false for trivial reasons*, Topology 8 (1969), 299-303.

[9] A. GROTHENDIECK, *Récoltes et Semailles : réflexions et témoignage sur un passé de mathématicien*, Montpellier (1985).

[10] U. JANNSEN, *Mixed motives and algebraic K-theory*, Lect. Notes in Math. 1400, Springer-Verlag (1990).

[11] S. KLEIMAN, *Motives*, in Proc. 5th Nordic Summer School, Oslo (1970), 53-82, Wolters-Noordhoff, Groningen (1972).

[12] R.P. LANGLANDS, *Euler Products*, Yale (1967).

[13] R.P. LANGLANDS, *Automorphic representations, Shimura varieties, and motives. Ein Märchen*, in *Automorphic Forms, Representations and L-Functions*, Proc. Symp. Pure Math. 33, vol. 2, 205-246 (1979).

[14] Y. MANIN, *Correspondances, motifs et transformations monoïdales* (en russe), Mat. Sbornik 77 (1968), 475-507 (trad. anglaise : Math. USSR Sb. 6 (1968), 439-470).

[15] M. RAPOPORT, N. SCHAPPACHER et P. SCHNEIDER (édit.), *Beilinson's conjectures on special values of L-functions*, Perspectives in Maths. 4, Acad. Press (1988).

[16] N. SAAVEDRA RIVANO, *Catégories tannakiennes*, Lect. Notes in Math. 265, Springer-Verlag (1972).

[17] J-P. SERRE, *Résumé des cours de 1966-1967*, Annuaire du Collège de France, 51-52 (1967) (= *Oe.*78).

[18] J-P. SERRE, *Abelian ℓ-adic representations and elliptic curves*, Benjamin, New-York (1968), (2ème édition : Addison-Wesley (1989)).

[19] J-P. SERRE, *Représentations ℓ-adiques*, Kyoto Symp. on Number Theory, 177-193 (1977) (= *Oe.*112).

[20] C. SOULÉ, *Groupes de Chow et K-théorie de variétés sur un corps fini*, Math. Ann. 268 (1984), 317-345.

[21] A. WEIL, *Numbers of solutions of equations in finite fields*, Bull. A.M.S. 55 (1949), 497-508 (= C.P. [1949*b*]).

[22] A. WEIL, *Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen*, Math. Ann. 168 (1967), 149-156 (= C.P. [1967*a*]).

J-P. SERRE
Collège de France
75231 PARIS Cedex 05

Astérisque

JEAN-PIERRE SERRE

Lettre à M. Tsfasman

Astérisque, tome 198-199-200 (1991), p. 351-353

<http://www.numdam.org/item?id=AST_1991__198-199-200__351_0>

LETTRE A M. TSFASMAN

Jean-Pierre SERRE

Paris, le 24 Juillet 1989

Cher Tsfasman,

Voici une solution du problème sur le nombre maximum de points d'une hypersurface que vous avez posé à Luminy.

Notations

$\mathbf{F}_q$ est un corps fini à q éléments ;

$\mathbf{P}_n(\mathbf{F}_q)$ est l'espace projectif de dimension n sur $\mathbf{F}_q$; son nombre d'éléments est $p_n = q^n + q^{n-1} + \cdots + 1$;

$f = f(X_0, \ldots, X_n)$ est un polynôme homogène $\neq 0$, de degré $d \leq q+1$, à coefficients dans $\mathbf{F}_q$;

$S = S(f)$ est le lieu des zéros de f dans $\mathbf{P}_n(\mathbf{F}_q)$;

$N = N(f)$ est le nombre d'éléments de S.

THÉORÈME – *On a* :

$$N \leq d\, q^{n-1} + p_{n-2} \,. \tag{1}$$

Démonstration

Le cas $d = q+1$ est trivial, car $d\, q^{n-1} + p_{n-2}$ est alors égal à p_n. *Je supposerai donc $d \leq q$ dans ce qui suit.*

Je raisonnerai par récurrence sur n, les cas $n = 0, 1$ étant faciles. On peut donc supposer $n \geq 2$.

Soient $g_1, \ldots, g_\delta$ les différents facteurs linéaires (à homothétie près) de f (sur le corps de base $\mathbf{F}_q$, bien entendu), et soient $G_1, \ldots, G_\delta$ les hyperplans de

$\mathbf{P}_n(\mathbf{F}_q)$ définis par les g_i. La réunion G des G_i est contenue dans S. On va distinguer deux cas, suivant que G est égal à S ou non.

(i) *On a* $G = S$.

Pour $m = 1, 2, \ldots, \delta$, on a

$$|G_1 \cup \ldots \cup G_m| \leq mq^{n-1} + p_{n-2} \ . \tag{2}$$

Cela se voit par récurrence sur m, en remarquant que G_{m+1} a $p_{n-1} = q^{n-1} + p_{n-2}$ points, et que $G_{m+1} \cap (G_1 \cup \ldots \cup G_m)$ a au moins p_{n-2} points. Comme $m \leq d$, l'inégalité (2) entraîne (1). (On voit de plus qu'il ne peut y avoir égalité dans (1) que si $\delta = d$, et si les g_i engendrent un espace de dimension 2, i.e. si les hyperplans G_i ont un espace de dimension $n-2$ en commun.)

(ii) *On a* $G \neq S$.

Choisissons un point $P \in S$, avec $P \notin G$. Si H est un hyperplan de $\mathbf{P}_n(\mathbf{F}_q)$, passant par P, la restriction de f à H n'est pas identiquement nulle, vu le choix de P. On peut donc appliquer à $S \cap H$ l'hypothèse de récurrence : on a

$$|S \cap H| \leq d\, q^{n-2} + p_{n-3} \ . \tag{3}$$

Je vais maintenant employer un procédé combinatoire standard : soit X l'ensemble des couples (P', H) où :

$$\begin{cases} P' & \text{est un point de } S - \{P\} \ ; \\ H & \text{est un hyperplan passant par } P \text{ et } P' \ . \end{cases}$$

Pour P' fixé dans $S - \{P\}$, le nombre des H passant par P et P' est égal à p_{n-2}. On en déduit :

$$|X| = (N-1)p_{n-2} \ . \tag{4}$$

D'autre part, pour H fixé passant par P, le nombre des $P' \in S - \{P\}$ situés sur H est égal à $|S \cap H| - 1 \leq d\, q^{n-2} + p_{n-3} - 1$. Comme le nombre des H passant par P est égal à p_{n-1}, on déduit de là :

$$|X| \leq p_{n-1}(d\, q^{n-2} + p_{n-3} - 1) \ . \tag{5}$$

En combinant (4) et (5), on obtient :

$$N \leq 1 + p_{n-1}(d\, q^{n-2} + p_{n-3} - 1)/p_{n-2} \ . \tag{6}$$

Un calcul ennuyeux, mais sans difficulté, montre que ceci équivaut à

$$N \leq d\,q^{n-1} + p_{n-2} - (q+1-d)q^{n-2}/p_{n-2}\ . \tag{7}$$

Comme $q+1-d$ est >0, on en déduit :

$$N < d\,q^{n-1} + p_{n-2}\ , \tag{8}$$

ce qui est meilleur que (1). D'où le théorème.

Remarques

1) Dans le cas (ii), on peut obtenir une inégalité un peu meilleure que (8), à savoir :

$$N \leq d\,q^{n-1} + p_{n-2} - (q+1-d)\ . \tag{9}$$

2) La démonstration prouve en même temps que, si $d \leq q$, il ne peut y avoir égalité dans (1) que dans le cas trivial où S est réunion de d hyperplans contenant une même variété linéaire de codimension 2.

Par contre, pour $d = q+1$, on peut prouver qu'il y a égalité dans (1) si et seulement si f est combinaison linéaire des polynômes $X_iX_j^q - X_jX_i^q$; si n est impair, l'hypersurface $f=0$ peut être absolument irréductible, et lisse (exemple : $n=3$, et $f = X_0X_1^q - X_1X_0^q + X_2X_3^q - X_3X_2^q$).

Bien à vous

J-P. SERRE
6 avenue de Montespan
75116 PARIS
France

Astérisque

C. SOULÉ

Géométrie d'Arakelov et théorie des nombres transcendants

Astérisque, tome 198-199-200 (1991), p. 355-371

<http://www.numdam.org/item?id=AST_1991__198-199-200__355_0>

GEOMETRIE D'ARAKELOV ET THEORIE DES NOMBRES TRANSCENDANTS

par

C. SOULÉ

0. Introduction

0.1. Les travaux récents de VOJTA [23] et FALTINGS [8] ont établi un lien remarquable entre la théorie de l'approximation des nombres algébriques et la théorie d'Arakelov. Celle-ci permet d'étendre le résultat classique de Thue-Siegel-Dyson-Gel'fond à des courbes de genre supérieur à un, obtenant ainsi une nouvelle preuve de la conjecture de MORDELL [23] et, plus généralement, de montrer des résultats de finitude sur les points rationnels de certaines sous-variétés des variétés abéliennes [8]. Nous tâcherons ici de présenter les résultats principaux de la géométrie d'Arakelov, et d'indiquer comment elle intervient dans ces travaux.

0.2. L'objectif premier de la géométrie d'Arakelov est l'étude des fibrés algébriques sur les variétés arithmétiques, munis d'une métrique hermitienne sur le fibré holomorphe associé. Que cette notion soit importante dans l'étude des équations diophantiennes se voit dès la définition de la hauteur d'un point P de l'espace projectif $\mathbf{P}^N(\mathbb{Q})$ (hauteur "naïve"). En effet, si $L_P \subset \mathbb{Z}^{N+1}$ désigne le $\mathbb{Z}$-module libre de rang un formé de 0 et des divers choix de coordonnées homogènes entières de P, la hauteur (logarithmique) de P est un invariant du fibré inversible L_P sur Spec $(\mathbb{Z})$ muni de la norme $\| \ \|$ induite par la métrique standard sur $\mathbf{C}^{N+1}$ (l'opposé de son degré arithmétique, cf. (8) ci-dessous) :

$$h(P) = \log \|s\| \ , \tag{1}$$

où s est n'importe quel générateur de L_P, i.e. un choix $(x_0, \ldots, x_N) \in \mathbb{Z}^{N+1}$ de coordonnées sans diviseur commun, et

$$\|s\|^2 = \sum_{i=0}^{N} |x_i|^2 \ .$$

0.3. Un autre exemple est donné par les fonctions auxiliaires des démonstrations de transcendance, ou d'approximation des nombres algébriques. Considérons par exemple la preuve du théorème de Dyson. Etant donné un nombre algébrique α de degré m sur $\mathbb{Q}$, et $\varepsilon > 0$, ce théorème affirme qu'il n'y a qu'un nombre fini de nombres rationnels p/q tels que

$$\left| \frac{p}{q} - \alpha \right| < \frac{1}{q^{\sqrt{2m}+\varepsilon}} \ .$$

Pour le montrer on prouve qu'il existe un polynôme à coefficients entiers en deux variables $P(x,y) \neq 0$, homogène de degré (d_1, d_2), dont la taille est (explicitement) bornée et qui s'annule beaucoup au point (α, α), ainsi que ses dérivées. Plus précisément, son indice en ce point, i.e.

$$\sigma = \mathrm{Sup} \left\{ s \in \mathbb{R} \text{ tel que, si } \frac{i_1}{d_1} + \frac{i_2}{d_2} < s \text{ , alors } \left(\frac{\partial}{\partial x} \right)^{i_1} \left(\frac{\partial}{\partial y} \right)^{i_2} P(\alpha, \alpha) = 0 \right\},$$

est grand. Etant données deux bonnes approximations p_1/q_1 et p_2/q_2 de α, on étudie alors l'indice de P en $(p_1/q_1, p_2/q_2)$ pour conclure que q_2/q_1 doit rester borné.

On peut voir un tel polynôme P comme une section du fibré en droites $\mathcal{O}(d_1, d_2)$ sur $\mathbb{P}^1 \times \mathbb{P}^1$, dont il faut contrôler la norme.

0.4. Une conséquence du théorème de Riemann-Roch-Grothendieck arithmétique (Théorème 1 ci-dessus) est une borne sur les sections non nulles d'un fibré ample sur une variété arithmétique (Théorème 2). Une variante de cet énoncé est une des étapes de la preuve de VOJTA [23] (cf. §.2).

0.5. FALTINGS généralise dans [8] le travail de VOJTA au cas des variétés abéliennes. Une extension astucieuse de la méthode classique de construction de la fonction auxiliaire lui permet d'éviter l'usage du théorème de Riemann-Roch-Grothendieck arithmétique. Il a cependant recours à la théorie d'Arakelov pour la définition et l'étude d'une hauteur pour les variétés projectives sur un corps de nombres. On verra ci-dessous (Théorème 3) que cette hauteur

est essentiellement celle définie par PHILIPPON [7] [8], c'est à dire la hauteur logarithmique des coordonnées de Chow de cette variété. PHILIPPON utilise cette notion pour obtenir des critères d'indépendance algébrique [17], améliorant des résultats de NESTERENKO.

0.6. Cet article ne présente pas de résultat original, si ce n'est le Théorème 3 (dont une version voisine a été obtenue, indépendamment, par PHILIPPON). Les deux premiers paragraphes sont principalement un résumé des travaux de GILLET et l'auteur.

Je remercie D. BERTRAND pour plusieurs discussions, et pour m'avoir parlé de la hauteur des variétés projectives.

1. Un théorème de Riemann-Roch-Grothendieck arithmétique

1.1. Appelons *variété arithmétique* la donnée d'un schéma X régulier, projectif et plat sur $\mathbb{Z}$, et *fibré hermitien* sur X la donnée $\overline{E} = (E, h)$ d'un fibré algébrique E sur X et d'une métrique hermitienne lisse h sur le fibré holomorphe $E_{\mathbb{C}}$ induit par E sur l'ensemble $X(\mathbb{C})$ des points complexes de X. Nous supposerons aussi que h est invariante par l'involution de conjugaison complexe, notée F_∞.

Choisissons une métrique Kählerienne, invariante par F_∞, sur $X(\mathbb{C})$. On peut alors associer à tout fibré hermitien $\overline{E}$ sur X un nombre réel $\chi(\overline{E})$, analogue arithmétique de la caractéristique d'Euler-Poincaré. Il est défini comme suit. Pour tout entier $q \geq 0$, on sait que le groupe de cohomologie cohérente $H^q(X, E)$ est un groupe abélien de type fini. On désigne par $\sharp H^q(X, E)_{\text{tors}}$ le cardinal de son sous-groupe de torsion.

Par ailleurs, soit $A^{0q}(X(\mathbb{C}), E_{\mathbb{C}})$ l'espace des formes différentielles de type $(0, q)$ sur $X(\mathbb{C})$ à coefficients dans $E_{\mathbb{C}}$. Les métriques choisies sur $E_{\mathbb{C}}$ et $X(\mathbb{C})$ fournissent un produit scalaire $< , >_{L^2}$ sur $A^{0q}(X(\mathbb{C}), E_{\mathbb{C}})$: étant données deux telles formes η et η' on pose

$$< \eta, \eta' >_{L^2} = \int_{X(\mathbb{C})} < \eta(x), \eta'(x) > \frac{\omega_0^n}{n!} \tag{2}$$

où $n = \dim(X/\mathbb{Z})$ et

$$\omega_0 = \sum_{\alpha,\beta} \frac{i}{2\pi} h_X \left(\frac{\partial}{\partial z_\alpha}, \frac{\partial}{\partial z_\beta} \right) dz_\alpha d\overline{z}_\beta \tag{3}$$

pour tout choix de coordonnées locales z_α sur $X(\mathbf{C})$ (h_X est la métrique choisie sur l'espace tangent de $X(\mathbf{C})$).

L'espace vectoriel complexe engendré par $H^q(X,E)$ s'identifie à celui des formes harmoniques de type $(0,q)$ sur $X(\mathbf{C})$ à coefficients dans $E_{\mathbf{C}}$:

$$H^q(X,E)_{\mathbf{Z}} \otimes \mathbf{C} \cong H^q(X(\mathbf{C}),E_{\mathbf{C}}) \cong \mathcal{H}^{0q}(X(\mathbf{C}),E_{\mathbf{C}}). \tag{4}$$

Il est donc muni du produit scalaire L^2.

On désigne par $\mathrm{vol}_{L^2}(H^q(X,E))$ le volume, pour ce produit scalaire, du quotient $H^q(X(\mathbf{C}),E_{\mathbf{C}})^+/H^q(X,E)$ où $(\ )^+$ désigne le sous-espace invariant par F_∞.

L'opérateur de Cauchy-Riemann de $E_{\mathbf{C}}$

$$\overline{\partial} : A^{0q}(X(\mathbf{C}),E_{\mathbf{C}}) \longrightarrow A^{0,q+1}(X(\mathbf{C}),E_{\mathbf{C}})$$

admet un adjoint $\overline{\partial}^*$ pour le produit scalaire L^2. Le Laplacien

$$\Delta_q = \overline{\partial}\,\overline{\partial}^* + \overline{\partial}^*\overline{\partial}$$

sur $A^{0q}(X(\mathbf{C}),E_{\mathbf{C}})$ possède une fonction zêta

$$\zeta_q(s) = \sum_{n\geq 1} \lambda_n^{-s}$$

où $\lambda_1 \leq \lambda_2 \leq \lambda_3 \leq \ldots$ désigne les valeurs propres non nulles de Δ_q (comptées avec multiplicité). Cette série converge si $\mathcal{R}e(s) > n$, et la fonction $\zeta_q(s)$ admet un prolongement méromorphe au plan complexe, qui n'a pas de pôle en $s=0$. On peut donc prendre sa dérivée $\zeta_q'(0)$ en ce point.

On pose alors :

$$\chi(\overline{E}) = \sum_{q\geq 0}(-1)^q \left(\log \sharp H^q(X,E)_{\mathrm{tors}} - \log \mathrm{Vol}_{L^2} H^q(X,E) + \frac{1}{2}\, q\zeta_q'(0)\right). \tag{5}$$

(Ce nombre réel est le degré arithmétique du fibré déterminant de la cohomologie de E, muni de la métrique de QUILLEN [16] [19] [2] [12]).

1.2. Notre objectif est de donner une formule pour $\chi(\overline{E})$. Pour ce faire on introduit des *groupes de Chow arithmétiques* $\widehat{CH}^p(X)$, $p \geq 0$, de la façon suivante [9] [10].

Soit $Z \in Z^p(X)$ un cycle de codimension p sur X, c'est à dire un élément $Z = \sum_\alpha n_\alpha Z_\alpha$ du groupe abélien libre engendré par l'ensemble $X^{(p)}$ des sous-schémas fermés irréductibles de codimension p de X. On peut associer à Z un courant δ_Z sur $X(\mathbf{C})$, donné par intégration sur $Z(\mathbf{C})$ des formes différentielles η (de degré adéquat) :

$$\delta_Z(\eta) = \sum_\alpha n_\alpha \int_{Z_\alpha(\mathbf{C})} \eta \,. \tag{6}$$

Le courant δ_Z appartient à l'espace $\mathcal{D}^{pp}(X)$ des courants réels S de type (p,p) sur $X(\mathbf{C})$ tels que $F_\infty^*(S) = (-1)^p S$. On appelle *courant de Green* pour Z la donnée d'un courant $g \in \mathcal{D}^{p-1,p-1}(X)$ tel que $dd^c g + \delta_Z$ soit lisse, c'est à dire donné par intégration contre une forme différentielle ω sur $X(\mathbf{C})$ (ici $dd^c = \overline{\partial}\partial/2i\pi$).

Un exemple d'une telle situation s'obtient en considérant un fibré hermitien $\overline{L} = (L,h)$ de rang un sur X, et une section rationnelle s de L sur X. En effet, la formule de Poincaré-Lelong affirme que

$$dd^c(-\log h(s,s)) + \delta_{\mathrm{div}\,(s)} = c_1(L,h) \tag{7}$$

est la première forme de Chern de $\overline{L}$ (elle ne dépend pas du choix de s). Par conséquent $-\log h(s,s)$ est un courant de Green pour le diviseur $\mathrm{div}\,(s)$ de s.

Pour tout entier $p \geq 0$ on désigne par $\widehat{CH}^p(X)$ le groupe abélien engendré par les couples (Z,g), où $Z \in Z^p(X)$ et g est un courant de Green pour Z, modulo le sous-groupe engendré par les couples $(0, \partial u + \overline{\partial} v)$ (où u et v sont des courants de type $(p-2,p-1)$ et $(p-1,p-2)$ respectivement) et $(\mathrm{div}(f), -\log|f|^2)$, où f est une fonction rationnelle sur $Y \in X^{(p-1)}$ et $\log|f|^2$ est le courant sur $X(\mathbf{C})$ donné par l'intégrale indéfinie

$$(\log|f|^2)(\eta) = \int_{Y(\mathbf{C})} (\log|f|^2)\eta \,.$$

Si $p = 1$ par exemple, tout élément de $\widehat{CH}^1(X)$ est la classe $\hat{c}_1(\overline{L})$ du couple $(\mathrm{div}\,(s), -\log h(s,s))$, où $\overline{L} = (L,h)$ est un fibré hermitien inversible sur X et $s \neq 0$ une section rationnelle de L (la classe $\hat{c}_1(\overline{L})$ ne dépend pas du choix de s). Quand $X = \mathrm{Spec}\,(\mathbf{Z})$, le groupe $\widehat{CH}^1(\mathbf{Z})$ est isomorphe à $\mathbf{R}$, la classe de $\hat{c}_1(\overline{L})$ est le degré arithmétique de $\overline{L}$:

$$\deg(\overline{L}) = -\log\|s\| \,, \quad \text{si} \quad L = \mathbf{Z}s \ (\text{et } \|s\|^2 = h(s,s)) \,. \tag{8}$$

1.3. Les groupes $\widehat{CH}^p(X)$ sont munis d'un produit d'intersection [10]

$$\widehat{CH}^p(X) \otimes \widehat{CH}^q(X) \longrightarrow \widehat{CH}^{p+q}(X)_{\mathbb{Q}} \tag{9}$$

(Si A est un groupe abélien, $A_{\mathbb{Q}} = A \otimes_{\mathbb{Z}} \mathbb{Q}$).

Formellement, ce produit s'obtient en associant à (Z, g) et (Z', g') la classe de $(Z \cap Z', g\delta_{Z'} + \omega g')$, où $\omega = dd^c g + \delta_Z$. Il y a de sérieuses difficultés avec cette formule, car le cycle $Z \cap Z'$ n'est pas toujours défini (on ne dispose pas d'un "moving lemma" sur $\mathbb{Z}$) et le produit de courants $g\delta_{Z'}$, nécessite aussi une définition adéquate. La première difficulté conduit à remplacer $\widehat{CH}^{p+q}(X)$ par $\widehat{CH}^{p+q}(X)_{\mathbb{Q}}$. Ceci n'est pas nécessaire si $p \leq 1$ ou $q \leq 1$, ou si X est lisse sur l'anneau des entiers d'un corps de nombres (cf. loc. cit.).

La formule suivante nous sera utile. Si η est une forme lisse de $\mathcal{D}^{p-1,p-1}(X)$, on note $a(\eta) \in \widehat{CH}^p(X)$ la classe du couple $(0, \eta)$. Alors, pour tout élément $x \in \widehat{CH}^q(X)$, on a

$$a(\eta)x = a(\eta\omega(x)) \tag{10}$$

où $\omega(x) = dd^c g + \delta_Z$, si (Z, g) est un représentant de x.

Un morphisme $f : X \to Y$ entre variétés arithmétiques induit des morphismes d'image inverse

$$f^* : \widehat{CH}^p(Y) \to \widehat{CH}^p(X)$$

et d'image directe

$$f_* : \widehat{CH}^p(X) \to \widehat{CH}^{p-\delta}(X) \ ,$$

où δ est la dimension relative. On a la formule de projection

$$f_*(xf^*(y)) = f_*(x)y \ . \tag{11}$$

En particulier, si $n = \dim(X/\mathbb{Z})$ est la dimension relative de X, le morphisme

$$f_* : \widehat{CH}^{n+1}(X) \to \widehat{CH}^1(\mathbb{Z}) = \mathbb{R}$$

associe à (Z, g) le nombre

$$f_*(Z, g) = \log \sharp H^0(Z, \mathcal{O}_Z) + \frac{1}{2} \int_{X(\mathbb{C})} g \ . \tag{12}$$

On obtient un accouplement (appelé nombre d'intersection)

$$\widehat{CH}^p(X) \otimes \widehat{CH}^{n+1-p}(X) \to \mathbf{R}$$

en associant à $x \otimes y$ l'élément $f_*(xy)$. Ce nombre d'intersection sera parfois noté seulement xy.

1.4. Il existe une théorie des *classes caractéristiques* à valeurs dans les groupes $\widehat{CH}^p(X)$ pour les fibrés hermitiens sur X [11]. La première classe de Chern $\hat{c}_1(\overline{L})$ a été définie plus haut. On a aussi un caractère de Chern

$$\widehat{ch}(\overline{E}) \in \bigoplus_{p \geq 0} \widehat{CH}^p(X)_{\mathbf{Q}} ,$$

qui commute aux images inverses, est additif sur les sommes directes orthogonales, multiplicatif pour le produit tensoriel, et tel que, pour tout fibré hermitien inversible $\overline{L}$,

$$\widehat{ch}(\overline{L}) = \exp\left(\hat{c}_1(\overline{L})\right) . \tag{13}$$

De plus la forme $\omega(\widehat{ch}(\overline{E}))$ sur $X(\mathbf{C})$ associée à $\widehat{ch}(\overline{E})$ est le représentant usuel du caractère de Chern de $E_{\mathbf{C}}$ en cohomologie (donné par le choix de la métrique sur $E_{\mathbf{C}}$).

1.5. Avant d'énoncer le résultat principal, il nous faut encore introduire une classe caractéristique

$$R(E_{\mathbf{C}}) \in H^*(X(\mathbf{C}), \mathbf{R})$$

dans la cohomologie réelle de $X(\mathbf{C})$, pour tout fibré holomorphe $E_{\mathbf{C}}$. Cette classe commute aux morphismes d'image inverse, elle est additive sur les suites exactes, et sa valeur pour tout fibré inversible $L_{\mathbf{C}}$ dont $x = c_1(L_{\mathbf{C}}) \in H^2(X(\mathbf{C}), \mathbf{R})$ est la première classe de Chern, est donnée par la formule

$$R(L_{\mathbf{C}}) = \sum_{\substack{m \text{ impair} \\ m \geq 1}} \left(2\zeta'(-m) + \zeta(-m)(1 + \frac{1}{2} + \cdots + \frac{1}{m})\right) \frac{x^m}{m!} , \tag{14}$$

où $\zeta(s)$ désigne la fonction zêta de Riemann, et $\zeta'(s)$ sa dérivée.

1.6. Si $\alpha \in \bigoplus_{p \geq 0} \widehat{CH}^p(X)_{\mathbf{Q}}$, on désigne par $[\alpha]^{(p)}$ sa composante de degré p.

THÉORÈME 1 : *Soient* $f : X \to \mathrm{Spec}\ (\mathbf{Z})$ *une variété arithmétique de dimension relative* n, *munie d'une métrique Kählerienne invariante par* F_∞, *et* $\overline{E}$ *un fibré hermitien sur* X. *Alors*

$$\chi(\overline{E}) = f_*\left([\widehat{ch}(\overline{E})\widehat{Td}(X)]^{(n+1)}\right) - \frac{1}{2}\int_{X(\mathbf{C})} ch(E_{\mathbf{C}})Td(X)R(X)\ . \tag{15}$$

1.7. *Remarques* :

- Dans (15), $Td(X)$ (resp. $R(X)$) est la classe de Todd (resp. la classe R) du fibré tangent à $X(\mathbf{C})$. Quand X est lisse sur $\mathbf{Z}$, $\widehat{Td}(X)$ est la classe de Todd arithmétique [11] du fibré tangent à X. En général la classe $\widehat{Td}(X)$ est associée au dual du complexe cotangent.
- On montre dans [13] qu'un énoncé tel que (15) reste valable si X est singulier quand sa fibre générique est lisse. On peut aussi remplacer la base Spec $(\mathbf{Z})$ par une variété arithmétique arbitraire.
- Le théorème 1 étend les résultats antérieurs d'ARAKELOV, FALTINGS [7] et DELIGNE [6]. Sa démonstration repose sur plusieurs travaux [1] [2] [3] [4] [5] [10] [11] [12].

2. Petites sections et conjecture de Mordell

2.1. On déduit du Théorème 1 le résultat suivant :

THÉORÈME 2 [13] : *Soient* X *une variété arithmétique,* $n = \dim(X/\mathbf{Z})$ *et* $\overline{L}$ *un fibré hermitien inversible sur* X. *On suppose que* L *est ample sur* X *et que la forme de Chern* $c_1(\overline{L})$ *est positive. Pour tout nombre réel* $\varepsilon > 0$, *et tout fibré hermitien* $\overline{E}$ *sur* X, *il existe un entier* k_0 *tel que, si* $k \geq k_0$, $E \otimes L^{\otimes k}$ *possède une section non nulle* s *sur* X *dont la norme en tout point* $x \in X(\mathbf{C})$ *est bornée comme suit :*

$$\|s(x)\| \leq \exp\left(k\left(\varepsilon - \frac{\overline{L}^{n+1}}{(n+1)L^n}\right)\right)\ . \tag{16}$$

Ici $\overline{L}^{n+1} = f_*(\hat{c}_1(\overline{L})^{n+1}) \in \mathbf{R}$ désigne la self-intersection arithmétique de $\overline{L}$, et $L^n = f_*(c_1(L_{\mathbf{C}})^n) \in \mathbf{Z}$ sa self-intersection géométrique.

2.2. Pour montrer le Théorème 2 on suppose d'abord que $\overline{L}^{n+1} > 0$. On utilise le Théorème 1 pour calculer $\chi(\overline{E} \otimes \overline{L}^k)$ en fonction de k. On trouve (en utilisant

(13)) que

$$\chi(\overline{E} \otimes \overline{L}^{\otimes k}) = r \frac{\overline{L}^{n+1}}{(n+1)!} k^{n+1} + O(k^n) , \tag{17}$$

où r est le rang de E (notons que l'énoncé précis du Théorème 1 n'est pas entièrement nécessaire, cf. [13]). Puisque L est ample, si k est grand et $q > 0$, le groupe $H^q(X, \otimes L^{\otimes k})$ est nul. Par ailleurs BISMUT et VASSEROT ont montré que

$$\sum_{q \geq 0} (-1)^{q+1} q \zeta_q'(0) = O(k^n \log(k)) . \tag{18}$$

Les formules (5) et (17) montrent donc que

$$\log \mathrm{Vol}_{L^2} H^0(X, E \otimes L^{\otimes k}) = r \frac{\overline{L}^{n+1}}{(n+1)!} k^{n+1} + O(k^n \log(k)) .$$

Comme le volume de la boule unité pour la norme L^2 est $O(k^n \log k)$, le théorème de MINKOWSKI, joint à un argument de GROMOV permettant de passer de la norme L^2 à la norme sup [13], montre que, si k est grand, $E \otimes L^{\otimes k}$ a une section $s \neq 0$ sur X telle que $\|s(x)\| \leq 1$ pour tout point $x \in X(\mathbf{C})$. Le cas général s'en déduit en multipliant la métrique de $\overline{L}$ par une constante pour se ramener au cas où $\overline{L}^{n+1} > 0$ [15].

2.3. La preuve ci-dessus montre aussi que le nombre de sections s satisfaisant (16) est au moins $\varepsilon r \frac{n^{d+1}}{d!} L^d$, où r est le rang de E. On peut alors appliquer le principe des boîtes de Dirichlet pour montrer qu'une des sections s (et ses dérivées) a un zéro d'ordre donné en un point de la fibre générique de X (cf. [15]).

2.4. La nouvelle démonstration par VOJTA de la conjecture de MORDELL [23] est une extension en genre positif du théorème de DYSON (cf. 0.3.). Le rôle du polynôme auxiliaire P est joué par une section non nulle s d'un fibré en droites de la forme

$$L = pr_1^*(\omega)^{\otimes a} \otimes pr_2^*(\omega)^{\otimes b} \otimes \mathcal{O}(\Delta)^{\otimes c}$$

sur une désingularisation du produit $X \times X$ de deux copies d'une surface arithmétique semi-stable de genre ≥ 2. Ici a, b, c sont des entiers convenablement choisis, $pr_i : X \times X \to X$, $i = 1, 2$, désigne les deux projections, Δ est la

diagonale, et ω le fibré dualisant relatif de X. VOJTA obtient une borne sur la norme d'une telle section s par la méthode du Théorème 2. Cependant L n'est pas ample (mais $H^2(X \times X, L) = 0$ et la restriction de L à la fibre générique est ample) et la forme de Chern $c_1(\overline{L})$ n'est pas positive (mais sa restriction à un des facteurs est positive). On peut étendre l'argument de 2.2 à cette situation [23]. VOJTA étudie ensuite l'indice de s en un point rationnel (P, Q) de $X \times X$. Il montre que la hauteur de P est bornée par un multiple de la hauteur de Q, ce qui montre la finitude de l'ensemble des points rationnels de X.

3. Hauteur des variétés projectives

3.1. FALTINGS simplifie dans [8] l'argument de VOJTA, et l'étend au cas des sous-variétés des variétés abéliennes. En particulier, il obtient une section bornée d'un fibré ample par une méthode plus proche de la méthode classique de l'approximation diophantienne, qui évite de recourir au théorème de Riemann-Roch arithmétique.

Un des outils de [8] est la notion suivante de hauteur pour les variétés projectives. Soit k un corps de nombres, et $\mathcal{O}_k$ l'anneau des entiers de k. Si $N \geq 1$ est un entier, on désigne par $\mathbf{P}^N$ l'espace projectif du fibré trivial de rang $N+1$ sur $\mathcal{O}_k$. On considère $\mathbf{P}^N$ comme une variété arithmétique (sur $\mathbf{Z}$) au sens de 1.1. L'ensemble $\mathbf{P}^N(\mathbf{C})$ des points complexes de $\mathbf{P}^N$ est donc la réunion de $[k : \mathbf{Q}]$ copies de l'espace projectif complexe de dimension N, noté $\mathbf{CP}^N$. Si on munit $\mathcal{O}_k^{N+1}$ de la métrique standard, on obtient une action du groupe unitaire $U = U(N+1)$ sur $\mathbf{P}^N(\mathbf{C})$. Il existe une unique structure de Kähler sur $\mathbf{P}^N(\mathbf{C})$ invariante par U. Les formes harmoniques sont les formes invariantes par U, et la projection orthogonale $H : \mathcal{D}^{pp}(\mathbf{P}^N) \to \mathcal{H}^{pp}(\mathbf{P}^N)$ des courants sur les formes harmoniques s'obtient en associant à $g \in \mathcal{D}^{pp}(\mathbf{P}^N)$ sa moyenne $\int_U u^*(g)du$, où du est la mesure de Haar de volume un de U.

Etant donné un sous-schéma fermé irréductible $X \subset \mathbf{P}^N$, on désigne par g_X le courant de Green pour X tel que $dd^c(g_X) + \delta_X$ est une forme harmonique sur $\mathbf{P}^N(\mathbf{C})$, et $H(g_X) = 0$. Un tel courant g_X existe et est unique modulo les courants de la forme $\partial u + \overline{\partial} v$. On désigne par $\widehat{X} \in \widehat{CH}^{N-n}(\mathbf{P}^N)$ la classe de (X, g_X) avec $n = \dim(X) - 1$. Si la fibre générique $X_k = X \bigotimes_{\mathcal{O}_k} k$ de X est non vide, $n = \dim X_k$.

Par ailleurs, on munit le fibré en droite tautologique $\mathcal{L}$ sur $\mathbf{P}^N$ de la métrique quotient de la métrique standard par la surjection canonique

$\mathbb{C}^{N+1} \to \mathcal{L}_{\mathbb{C}}$. Si $f : \mathbb{P}^N \to \mathrm{Spec}(\mathbb{Z})$ est le morphisme de définition de $\mathbb{P}^N$, on pose [8]

$$h(X) = f_* \left(\widehat{X}.\widehat{c}_1(\overline{\mathcal{L}})^{n+1} \right) \in \mathbb{R} \ . \tag{19}$$

On appelle $h(X)$ *la hauteur* de X. La formule (19) est à rapprocher de la définition du degré $\deg(X_k) \in \mathbb{Z}$ de la variété X_k. Si $c_1(\mathcal{L}_k) \in CH^2(\mathbb{P}^N_k) = \mathbb{Z}$ est la première classe de Chern de la restriction de $\mathcal{L}$ à X_k (dans le groupe de Chow usuel), et $[X_k] \in CH^{N-n}(\mathbb{P}^N_k)$ la classe de X_k, on a

$$[k : \mathbb{Q}] \deg(X_k) = f_* \left([X_k] c_1(\mathcal{L}_k)^n \right) \tag{20}$$

dans $\mathbb{Z} = CH^0(\mathrm{Spec}\ \mathbb{Q})$. On notera que si $c_1(\overline{\mathcal{L}})$ est la première forme de Chern de $\overline{\mathcal{L}}$ on a aussi

$$[k : \mathbb{Q}] \deg(X_k) = \int_{X(\mathbb{C})} c_1(\overline{\mathcal{L}})^n \ . \tag{21}$$

FALTINGS montre que $h(X) \geq 0$ et étudie le comportement de $h(X)$ par projection linéaire. Il en déduit que $h(X)$ fournit une borne pour la taille des équations de X sur $\mathbb{Z}$ ([8],cor.2.12).

Si X_k est une sous-variété irréductible de codimension n de $\mathbb{P}^N_k$ et X son adhérence dans $\mathbb{P}^N$, on pose

$$h(X_k) = h(X) \ . \tag{22}$$

Cette définition s'étend par linéarité au cas d'un cycle arbitraire sur $\mathbb{P}^N_k$. Si $P \in \mathbb{P}^N(k)$ est un point rationnel et X_k la variété de dimension zéro correspondante, le nombre $h(P) = h(X_k)$ coïncide avec la hauteur logarithmique du point P (voir 0.2. quand $k = \mathbb{Q}$).

3.2. PHILIPPON définit dans [17] et [18] la hauteur d'une variété projective comme étant celle de la forme de Chow associée. Plus précisément, appelons $\overset{\vee}{\mathbb{P}}{}^N_k$ l'espace projectif dual de $\mathbb{P}^N_k$. Un point ξ de $\overset{\vee}{\mathbb{P}}{}^N_k$ s'interprète comme un hyperplan de $\mathbb{P}^N_k$, d'équation $\xi.x = 0$. La sous-variété $Y_k \subset (\overset{\vee}{\mathbb{P}}{}^N_k)^{n+1}$ formée des $(n+1)$-uplets $(\xi^0, \xi^1, \ldots, \xi^n)$ d'hyperplans tels que leur intersection $\xi^0 \cap \xi^1 \cap \ldots \cap \xi^n$ rencontre X_k est une hypersurface. Etant données des coordonnées homogènes ξ^α_j, $j = 0, \ldots, N$, pour chacun des $\xi^\alpha, \alpha = 0, \ldots, n$, l'équation de Y_k s'écrit $F(\xi^\alpha_j) = 0$, où F est multihomogène de degré $d = \deg(X_k)$ (F est unique à scalaire près) [20] [21].

Soient $S^N \subset \mathbf{C}\mathbf{P}^N$ la sphère unité et $d\nu$ la mesure de probabilité sur $(S^N)^{n+1} \subset (\mathbf{C}\mathbf{P}^N)^{n+1}$ invariante sous l'action de $\overset{\vee}{U} = (U(N+1))^{n+1}$. Si v est une place finie de k, notons Nv le nombre d'éléments du corps résiduel, et $|\alpha|_v = (N_v)^{-v(\alpha)}$ pour tout nombre $\alpha \in k$ de valuation $v(\alpha)$. On pose alors

$$|F|_v = \max_I |a_I|_v \ , \tag{23}$$

où a_I parcourt l'ensemble des coefficients de F. La hauteur de Philippon est donnée par la formule

$$h'(X_k) = \sum_v \log |F|_v + \sum_{\sigma : k \to \mathbf{C}} \int_{(S^N)^{n+1}} \log |\sigma(F)| d\nu \ , \tag{24}$$

où v parcourt l'ensemble des places finies et σ l'ensemble des plongements complexes de k. La formule du produit montre que ce nombre ne dépend pas du choix de F.

THÉORÈME 3 : *Avec les définitions* (19),(22) et (24) *ci-dessus, on a*

$$h(X_k) = h'(X_k) + \frac{1}{2}(n+1)\left(\sum_{j=1}^{N} \frac{1}{j}\right)[k : \mathbb{Q}] \deg(X_k) \ . \tag{25}$$

3.3. Le théorème 3 est l'analogue arithmétique du fait que les degrés de X_k et F coïncident. Pour le démontrer nous allons d'abord comparer $h'(X_k)$ et la hauteur de Y_k au sens de [8]. Notons $\overset{\vee}{\mathbf{P}}{}^N$ l'espace projectif du fibré dual du fibré trivial de rang $N+1$ sur $\mathcal{O}_k$, $\overset{\vee}{\mathcal{L}}$ le fibré tautologique sur $\overset{\vee}{\mathbf{P}}{}^N$ muni de la métrique standard, et $\overset{\vee}{c} = \hat{c}_1(\overset{\vee}{\mathcal{L}}) \in \widehat{CH}^1(\overset{\vee}{\mathbf{P}}{}^N)$ sa première classe de Chern arithmétique. Si $\alpha = 0, \ldots, n$ on désigne par $\mathrm{pr}_\alpha : (\overset{\vee}{\mathbf{P}}{}^N)^{n+1} \to (\overset{\vee}{\mathbf{P}}{}^N)$ la α-ième projection, et l'on pose

$$\mathcal{L}_\alpha = \mathrm{pr}_\alpha^* \mathcal{L} \text{ et } c_\alpha = \mathrm{pr}_\alpha^*(\overset{\vee}{c}) = \hat{c}_1(\overline{\mathcal{L}}_\alpha) \in \widehat{CH}^1((\overset{\vee}{\mathbf{P}}{}^N)^{n+1}) \ .$$

Soit F une équation de Y_k à coefficients dans $\mathcal{O}_k$. C'est une section sur $\overset{\vee}{P} = (\overset{\vee}{\mathbf{P}}{}^N)^{n+1}$ du fibré inversible $\bigotimes_{a=0}^{n} \mathcal{L}_\alpha^{\otimes d}$. Si l'on munit $\overset{\vee}{P}(\mathbf{C})$ de la structure de Kähler standard, on peut définir comme en 3.1 une classe

$$\widehat{\mathrm{div}}(F) = (\mathrm{div}(F), g_{\mathrm{div}(F)}) \in \widehat{CH}^1(\overset{\vee}{P}) \ .$$

Puisque le couple $(\mathrm{div}(F), -\log\|F\|^2)$ représente $\hat{c}_1\left(\bigotimes_{a=0}^{n}\overline{\mathcal{L}}_\alpha^{\otimes d}\right) = d(c_0+\cdots+c_n)$ et puisque $c_1\left(\bigotimes_{a=0}^{n}\overline{\mathcal{L}}_\alpha^{\otimes d}\right)$ est harmonique on a :

$$\widehat{\mathrm{div}(F)} = d(c_0+\cdots+c_n) + a(H(\log\|F\|^2)) \ . \tag{26}$$

Si $\mu_\alpha = \omega(c_\alpha)$ désigne la première forme de Chern de $\overline{\mathcal{L}}_\alpha$, on déduit de (26) (en utilisant (10) et en omettant désormais f_* dans l'écriture d'un nombre d'intersection)

$$\widehat{\mathrm{div}(F)}c_0^N\ldots c_n^N = d\left(\sum_{\alpha=0}^{n}c_\alpha^{N+1}\right)\left(\int_{\overset{\vee}{P}(\mathbb{C})}\mu_0^N\ldots\mu_n^N\right)/[k:\mathbb{Q}] + \int_{\overset{\vee}{P}(\mathbb{C})}H(\log\|F\|)\mu_0^N\ldots\mu_n^N \ . \tag{27}$$

La première intégrale ci-dessus est égale à $[k:\mathbb{Q}]$, et la seconde se ramène à celle de (24) puisque

$$\|F(\xi_j^\alpha)\|^2 = \frac{|F(\xi_j^\alpha)|^2}{\left(\prod_{\alpha=0}^{n}(\sum_{j=0}^{N}|\xi_j^\alpha|^2)\right)} \ , \tag{28}$$

$$\text{i.e.}\quad \int_{\overset{\vee}{P}(\mathbb{C})}H(\log\|F\|)\mu_0^N\ldots\mu_n^N = \sum_{\sigma:k\to\mathbb{C}}\int_{(S^N)^{n+1}}\log|\sigma(F)|d\nu \ . \tag{29}$$

Si Y est l'adhérence de Y_k dans $\overset{\vee}{P}$ et $\overset{\vee}{P}_v$ la réduction de $\overset{\vee}{P}$ modulo v, le cycle $\mathrm{div}(F)$ s'écrit :

$$\mathrm{div}(F) = [Y] + \sum_v \inf(v(a_I))[\overset{\vee}{P}_v] \ . \tag{30}$$

Si l'on combine (27) (29) (30) (10) et (24) on obtient

$$\hat{Y}.c_0^N\ldots c_n^N = \deg(X_k)\left(\sum_{\alpha=0}^{n}c_\alpha^{N+1}\right) + h'(X_k) \ . \tag{31}$$

3.4. Puisque $\overset{\vee}{\mathbb{P}}^N$ paramétrise les hyperplans de $\mathbb{P}^N$, le produit $\mathbb{P}^N\times\overset{\vee}{\mathbb{P}}^N$ contient un hyperplan canonique, d'équation $\xi.x = 0$. C'est le diviseur d'une section $f\in$

$\Gamma(\mathbf{P}^N \times \overset{\vee}{\mathbf{P}}{}^N; \mathcal{L} \otimes \overset{\vee}{\mathcal{L}})$. Pour $\alpha = 0, \ldots, n$ on désigne par $f_\alpha \in \Gamma(\mathbf{P}^N \times \overset{\vee}{\mathbf{P}}; \mathcal{L} \otimes \mathcal{L}_\alpha)$ la section correspondante, dont le diviseur a pour équation $\xi^\alpha . x = 0$. L'intersection des diviseurs $\mathrm{div}(f_\alpha)$ est la variété W d'équations $\xi^\alpha . x = 0, \alpha = 0, \ldots, n$. Si $\mathrm{pr}_1 : \mathbf{P}^N \times \overset{\vee}{P} \to \mathbf{P}^N$ et $\mathrm{pr}_2 : \mathbf{P}^N \times \overset{\vee}{P} \to \overset{\vee}{P}$ désignent les deux projections, on a par définition $Y_k = \mathrm{pr}_2(\mathrm{pr}_1^{-1}(X_k) \cap W_k)$.

Par ailleurs, si v est une place finie de k et $X \neq \mathbf{P}^N$, le fermé $\mathrm{pr}_2(pr_1^{-1}(X) \cap W)$ ne contient pas $\overset{\vee}{P}_v$, puisque, sur une extension finie du corps résiduel, il existe $n+1$ hyperplans dont l'intersection ne rencontre pas X modulo v. De plus la projection harmonique du courant $\overset{\vee}{\mathbf{P}}(\mathbf{C})$ est la moyenne de ses translatés $\int_{\overset{\vee}{U}} \overset{\vee}{u}{}^*(g) d\overset{\vee}{u}$, où $d\overset{\vee}{u}$ désigne la mesure de Haar de volume un sur $\overset{\vee}{U}$. Le groupe $\overset{\vee}{U}$ opère aussi sur $\mathbf{P}^N \times \overset{\vee}{P}(\mathbf{C})$, et sur $\widehat{\mathrm{div}}(f_\alpha)$ par sa α-ième projection sur $U(N+1)$. Il en résulte que l'élément $\prod_{\alpha=0}^{n} \widehat{\mathrm{div}}(f_\alpha)$ est représenté par un couple (W, g_W) où g_W est un courant tel que $\int_{\overset{\vee}{U}} \overset{\vee}{u}{}^*(g_W) d\overset{\vee}{u} = 0$.

Enfin $\mathrm{pr}_1^*(\widehat{X})$ est invariant sous l'action de $\overset{\vee}{U}$ et l'intégrale de g_X sur $\mathbf{P}^N(\mathbf{C})$ est nulle. On peut donc conclure que

$$\widehat{Y} = \mathrm{pr}_{2*}\left(\mathrm{pr}_1^*(\widehat{X}) \prod_{\alpha=0}^{n} \widehat{\mathrm{div}}(f_\alpha)\right) \tag{32}$$

dans $\widehat{CH}^1(\overset{\vee}{P})$.

3.5. Pour calculer la projection harmonique $H(-\log \|f\|^2)$ sur $\mathbf{P}^N \times \overset{\vee}{P}(\mathbf{C})$, il suffit de calculer la moyenne de $-\log \|f\|^2$ pour l'action de U sur $x \in \mathbf{P}^N(\mathbf{C})$, car si u^t est le transposé de $u \in U$, on a $f(x, \xi) = f(ux, u^t \xi)$. Cette moyenne ne dépend donc pas du choix de ξ. Elle a été calculée par STOLL [22] (cf. aussi [11]). Si μ est la première forme de Chern de $\overline{\mathcal{L}}$, et μ^N la mesure de Fubini-Study, on a

$$H(-\log \|f\|^2) = \int_{\mathbf{P}^N(\mathbf{C})} \log\left(\sum_{i=0}^{N} |x_i|^2 / |x_0|^2\right) \mu^N = \sum_{j=1}^{N} \frac{1}{j} \cdot$$

On a donc, dans $\widehat{CH}^1(\mathbf{P} \times \overset{\vee}{\mathbf{P}}{}^N)$,

$$\widehat{\mathrm{div}}(f) = \hat{c}_1(\mathcal{L}) + \hat{c}_1(\overset{\vee}{\mathcal{L}}) + a\left(\sum_{j=1}^{N} \frac{1}{j}\right) \cdot \tag{33}$$

D'après (32) on en déduit que, si $c = \hat{c}_1(\mathcal{L})$,

$$\hat{Y} = \mathrm{pr}_{2*}\left(\mathrm{pr}_1^*(\widehat{X}) \prod_{\alpha=0}^{n} \left(c + c_\alpha + a\left(\sum_{j=0}^{n} \frac{1}{j}\right)\right)\right) \cdot \tag{34}$$

3.6. Les seuls groupes de Chow non nuls de $\mathrm{Spec}(\mathbb{Z})$ sont $\widehat{CH}^0(\mathbb{Z}) = \mathbb{Z}$ et $\widehat{CH}^1(\mathbb{Z}) = \mathbb{R}$. Par conséquent, d'après (10), si $\alpha \in \widehat{CH}^p(\mathbb{P}^N)$ et $\beta \in \widehat{CH}^q(\overset{\vee}{P})$, on a

$$f_*(\mathrm{pr}_1^*(\alpha)\mathrm{pr}_1^*(\beta)) = \begin{cases} f_*(\omega(\alpha))f_*(\beta) & \text{si } p = N \text{ et } q = (n+1)N+1 \\ f_*(\alpha)f_*(\omega(\beta)) & \text{si } p = N+1 \text{ et } q = (n+1)N \\ 0 & \text{sinon .} \end{cases}$$

La formule de projection (11) pour pr_2, (34), (10) et (21) montrent donc que

$$\hat{Y}c_0^N \ldots c_n^N = \widehat{X}.c^{n+1} + \deg(X_k)\left(\sum_{\alpha=0}^{n} c_\alpha^{N+1} + \frac{1}{2}[k:\mathbb{Q}](n+1)\sum_{j=0}^{N}\frac{1}{j}\right) \cdot \tag{35}$$

Avec (31) et (19) ceci conclut la preuve du Théorème 3.

3.7. Le Théorème 3 est aussi conséquence du Théorème 2 de [18]. Il résulte du Théorème 3 que l'ensemble des variétés X_k de degré et de hauteur bornés est fini.

Les questions ouvertes sont nombreuses. Par exemple, quel est l'analogue arithmétique du théorème de Bezout ? Peut-on obtenir de nouveaux critères d'indépendance algébrique ? La notion de hauteur des variétés peut-elle servir à montrer que les groupes de Chow d'une variété lisse sur k sont de type fini ?

REFERENCES

[1] J.-M. BISMUT : Superconnection currents and complex immersions, *Inventiones*, Fasc.1, **99** (1990), 59-113.

[2] J.-M. BISMUT, H. GILLET et C. SOULÉ : Analytic torsion and holomorphic determinant bundles I, II, III,*Comm. in Math. Physics* **115** (1988), 49-78, 79-126, 301-351.

[3] J.-M. BISMUT, H. GILLET et C. SOULÉ : Bott-Chern currents and complex immersions, *Duke Math. J.*,no.1, **60** (1990), 255-284.

[4] J.-M. BISMUT, H. GILLET et C. SOULÉ : *Complex Immersions and Arakelov Geometry, The Grothendieck Festschrift*, Vol.I, Progress in Maths., Birkhaüser Boston, (1990) 249-331.

[5] J.-M. BISMUT, G. LEBEAU : Immersions complexes et métriques de Quillen,*CRAS Paris* **309** (1989), 487-491.

[6] P. DELIGNE : Le déterminant de la cohomologie dans Current trends in Arithmetical Algebraic Geometry, *Contemporary Math.* **67** (1987), 93-178.

[7] G. FALTINGS : Calculus on Arithmetic Surfaces, *Annals of Math.* **119** (1984), 387-424.

[8] G. FALTINGS : *Diophantine approximation on abelian varieties*, (1989), preprint.

[9] H. GILLET et C. SOULÉ : Classes caractéristiques en théorie d'Arakelov, *CRAS Paris* **301** (1985), 439-442.

[10] H. GILLET et C. SOULÉ : *Intersection on arithmetic varieties*, Publ. Math. I.H.E.S., à paraître.

[11] H. GILLET et C. SOULÉ : Characteristic classes for algebraic vector bundles with hermitian metric I et II, *Annals of Math.* **131** (1990), 163-203 et 205-238.

[12] H. GILLET et C. SOULÉ : *Analytic torsion and the Arithmetic Todd genus*, avec un appendice de D. Zagier, Topology, à paraître.

[13] H. GILLET et C. SOULÉ : Amplitude arithmétique, *CRAS Paris* **307** (1988), 887-890.

[14] H. GILLET et C. SOULÉ : Un théorème de Riemann-Roch arithmétique, *CRAS Paris* **309** (1989), 929-932.

[15] H. GILLET et C. SOULÉ : à paraître.

[16] F.F. KNUDSEN et D. MUMFORD : The projectivity of the moduli space of stable curves I : Preliminaries on "det" and "div", *Math. Scand.* **39** (1976), 19-55.

[17] P. PHILIPPON : Critères pour l'indépendance algébrique,*Publ. Math. IHES* **64** (1986), pp. 5-52.

[18] P. PHILIPPON : *Sur des hauteurs alternatives*, 1989, preprint.

[19] D. QUILLEN : Determinants of Cauchy-Riemann operators over a Riemann surface, *Funct. Anal. Appl.* (1985), 31-34.

[20] P. SAMUEL : *Méthodes d'algèbre abstraite en géométrie algébrique*, Ergebnisse 4, Springer-Verlag, (1955).

[21] I.R. SHAFAREVICH : *Basic algebraic geometry*, Ergebnisse 213, Springer-Verlag, (1974).

[22] W. STOLL : About the value distribution of holomorphic maps into projective space, *Acta Math.* **123** (1969), 83-114.

[23] P. VOJTA : Siegel's theorem in the compact case, *Annals of Math.*, à paraître.

C. SOULÉ
I.H.E.S.
35, route de Chartres
91440 BURES SUR YVETTE

Astérisque

MICHAEL A. TSFASMAN

Global fields, codes and sphere packings

Astérisque, tome 198-199-200 (1991), p. 373-396

<http://www.numdam.org/item?id=AST_1991__198-199-200__373_0>

GLOBAL FIELDS, CODES AND SPHERE PACKINGS

by

Michael A. TSFASMAN

Introduction

We are going to apply some simple algebraic geometry and number theory to codes and sphere packings. These constructions look rather exciting since on the one hand they lead to considerable progress in codes and packings, and on the other hand they concern rather deep properties of global fields. Moreover they look quite lucid and simple. Here we present *eight* constructions of this kind leading to asymptotically good families.

Section 0 provides some necessary definitions concerning codes and packings (this paper is addressed to those knowing what a global field is). Then (in §§1-8) we discuss eight constructions. Each of them is characterized by the following data : 1) we use either number (N), or function (F) fields ; 2) we use either additive (A), or multiplicative (M) structure ; 3) we obtain either lattice packings (L), or codes (C) ; 4) the construction either depends on a divisor (D), or not. These are the meanings of abbreviations we use in the titles of sections. For each construction we estimate parameters and try to produce asymptotically good families.

Section 1 is due to the author (it is exposed, e.g. in [LI/TS] §7, [CO/SL] ch.8 §7, [TS/VL] ch.5). The construction of §2 was historically the first and is due to GOPPA [GO 1], its asymptotic significance was first understood in [TS/VL/ZI] (for a detailed exposition see [TS/VL]). Section 3 is due to LENSTRA [LE]. The next four constructions (§§4-7) are due to ROSENBLOOM and the author [RO/TS]. The construction of §5 has been independently discovered by QUEBBEMANN [QU]. The construction of §8 is again due to GOPPA [GO 2]. The last section is devoted to some remarks and open problems.

I would like to thank all above-mentioned mathematicians for sending me preprints, and M. ROSENBLOOM for many stimulating discussions. This paper has been finished during my stay in France, and I would like to express my gratitude to the University of Paris 7, to C.I.R.M., and personally to J-L. COLLIOT-THÉLÈNE, G. LACHAUD, J-J. SANSUC, Cyrille and Anna VELIKANOV, and all my friends and colleagues for their kind hospitality.

0. Packings and Codes

Notation. In what follows log denotes $\log_2$, and ln denotes $\log_e$. By $\sim$ we mean asymptotic equality and by $\gtrsim$ asymptotic inequality (up to a function tending to 0).

Sphere packings. We first consider a classical problem of packing equal non-overlapping spheres in $\mathbb{R}^n$. Let L be the set of centers and set

$$d = d(L) = \inf_{v,u \in L, v \neq u} |u - v|,$$

d is the *minimum distance* of the packing, it equals the maximum possible diameter of non-overlapping open spheres centered in L.

The *density* of L is the part of $\mathbb{R}^N$ covered by spheres; to be precise, it can be defined as

$$\Delta = \Delta(L) = \limsup_{c \to \infty} \frac{\mathrm{vol}(S \cap B_c)}{\mathrm{vol}(B_c)} ,$$

vol being the standard volume in $\mathbb{R}^N$, $S = \{x \in \mathbb{R}^N | \ |x - u| < \frac{d}{2}$ for some $u \in L\}$, $B_c = \{x \in \mathbb{R}^N | \ |x| \leq c\}$.

Let $V_N = \frac{\pi^{N/2}}{\Gamma(\frac{N}{2}+1)}$ be the volume of unit sphere. We define some other parameters setting

$$\begin{aligned} \delta(L) &= \frac{\Delta(L)}{V_N} , \\ \nu(L) &= \log \delta(L) , \\ \gamma(L) &= 4(\delta(L))^{2/N} , \\ \lambda(L) &= -\frac{1}{N} \log \Delta(L) ; \end{aligned}$$

$\delta(L)$ is called the *center density*, and the most important (for our purposes) parameter $\lambda(L)$ is called the *density exponent.*

Lattices. The most interesting case is when L is an additive subgroup of $\mathbb{R}^N$, i.e. a lattice (we suppose that $d(L) > 0$ and $\Delta(L) > 0$). For a lattice L

$$\lambda(L) = -\frac{1}{N} \log \left(\frac{d(L)^N V_N}{2^N \det L} \right) ,$$

where $\det L = \mathrm{vol}(\mathbb{R}^N/L)$ is the volume of fundamental domain.

Each lattice corresponds to a quadratic form $f(x)$ on a free $\mathbb{Z}$-module of rank N, and the problem of finding the smallest possible λ (i.e. the largest possible Δ) is equivalent to another classical problem of finding a form of discriminant 1 with the maximum value of $\gamma(L) = \min_{x \in \mathbb{Z}^N - \{0\}} f(x)$, cf. [Mi].

Asymptotic behaviour. In this paper we are interested in lattices of high rank. Let $\{L_N \subset \mathbb{R}^N\}$ be a family of lattices with $N \to \infty$. Set

$$\lambda(\{L_N\}) = \liminf_{N \to \infty} \lambda(L_N).$$

A family of lattices is called *asymptotically good* iff $\lambda(\{L_N\}) < \infty$. Using the Stirling formula we see that

$$\lambda(\{L_N\}) \ \sim \ -\log \sqrt{\frac{\pi e}{2}} + \log \sqrt{N} - \log d(L) + \frac{1}{N} \log(\det L).$$

Note that asymptotically $\gamma \ \sim \ \dfrac{2N}{\pi e}\, 4^{-\lambda}$.

It is known that $\lambda(\{L_N\}) \geq 0.599$ (the Kabatianski-Levenshtein bound, valid also for non-lattice packings) and that there exist families of lattices with $\lambda(\{L_N\}) \leq 1$ (the Minkowski existence bound).

However it is in fact very difficult to construct asymptotically good lattices explicitly (cf.[Co/Sl] , [Li/Ts]), and each construction leading to good lattices is of interest. (Natural families of lattices, such as $\mathbb{Z}^N$ and root lattices A_N and D_N , are asymptotically bad).

Codes. Let $\mathbb{F}_q$ be a finite field. Being finite the space $\mathbb{F}_q^n$ is equipped with the natural notion of volume (the number of points) and with the *Hamming norm* $\|v\| = |\{i \mid v_i \neq 0\}|$. Hence for this space there also exists a packing problem. A *code* is a set of points $C \subseteq \mathbb{F}_q^n$, n is called its *length*, $k = \log_q |C|$ is its *log-cardinality*, $d = \min_{v,u \in C, v \neq u} \|u - v\|$ is its *minimum distance*. The relative parameters are the *rate* $R = R(C) = k/n$, and the *relative distance* $\delta = \delta(C) = d/n$.

Linear codes. A code is called *linear* iff it is a linear subspace. For such a code k is an integer and $d = \min_{v \in C - \{0\}} \|v\|$.

Asymptotic behaviour. Let $\{C_n \subseteq \mathbb{F}_q^n\}$ be a family of codes with $n \to \infty$. In contrast with sphere packings, codes have two asymptotic parameters δ and R (the reason is that in $\mathbb{R}^N$ rescaling is possible and we can always set $d(L) = 1$). Set

$$\delta(\{C_n\}) = \limsup_{n \to \infty} \delta(C_n),$$
$$R(\{C_n\}) = \limsup_{n \to \infty} R(C_n).$$

A family of codes is called *asymptotically good* iff $\delta(\{C_n\}) > 0$ and $R(\{C_n\}) > 0$.

It is known that for any $\delta \in \left[0, \frac{q-1}{q}\right]$ there exist families of linear codes $\{C_n\}$ with

$$\delta(\{C_n\}) = \delta$$

and

$$R(\{C_n\}) \geq 1 - H_q(\delta)$$

(the Gilbert-Varshamov existence bound) ; here

$$H_q(x) = x \ \log_q(q-1) - x \ \log_q x - (1-x)\log_q(1-x).$$

is the q-ary entropy function. There also exist upper bounds which we do not discuss here. Again it is difficult to construct good codes explicitly.

There are many interesting links between codes and lattices, cf.[Co/ Sl].

1. Additive lattices (NAL)

Construction. Let K be a number field and let $\mathcal{O}_K$ be its ring of integers, $[K : \mathbb{Q}] = N = s + 2t$ where s is the number of real embeddings $K \hookrightarrow \mathbb{R}$ and t is the number of conjugate pairs of complex embeddings $K \hookrightarrow \mathbb{C}$. Together they form the standard embedding

$$\sigma : K \hookrightarrow \mathbb{R}^s \times \mathbb{C}^t = \mathbb{R}^N$$

which is a homomorphism of $\mathbb{Q}$-algebras. Let $L = \sigma(\mathcal{O}_K)$.

Parameters. For $x = (x_1, \ldots, x_s\ ;\ y_1 + iz_1, \ldots, y_t + iz_t) \in \mathbb{R}^s \times \mathbb{C}^t$ let $N(x) = x_1 \cdots x_s (y_1^2 + z_1^2) \cdots (y_t^2 + z_t^2)$. Then $N(\sigma(f)) = N_{K/\mathbb{Q}}(f)$ is the norm of $f \in K$. Let $\mathcal{D}_K$ be the discriminant of K.

LEMMA 1.1. *Let $L = \sigma(\mathcal{O}_K)$. Then*

(i) $\det L = 2^{-t}\sqrt{|\mathcal{D}_K|}$,

(ii) $\sqrt{s+t} \geq d(L) \geq \sqrt{\frac{s}{2} + t}$,

and if $t = 0$ then $d(L) = \sqrt{N}$. COROLLARY 1.2. *Suppose that K is either totally real, or totally complex. Then*

$$\delta(L) = \frac{N^{N/2}}{2^N \sqrt{|\mathcal{D}_K|}} ,$$

$$\lambda(L) = 1 - \tfrac{1}{2}\log N - \tfrac{1}{N}\log V_N + \tfrac{1}{N}\log\sqrt{|\mathcal{D}_K|}.$$

Proof of Lemma 1.1 : (i) is straightforward (see [LA], ch.5, §2, Lemma 2). (ii) Let $x = \sigma(f) = (x_1, \ldots, x_s\ ;\ y_1 + iz_1, \ldots, y_t + iz_t)$. We have

$$|\sigma(f)| = \sqrt{\sum_{j=1}^{s} x_j^2 + \sum_{j=1}^{t}(y_j^2 + z_j^2)}.$$

For $f = 1$, $|\sigma(1)| = \sqrt{s+t}$. The arithmetic-mean geometric-mean inequality yields

$$\sqrt{\sum_{j=1}^{s} x_j^2 + \sum_{j=1}^{t}(y_j^2 + z_j^2)} \geq \frac{1}{\sqrt{2}} \sqrt{\sum_{j=1}^{s} x_j^2 + 2\sum_{j=1}^{t}(y_j^2 + z_j^2)} \geq$$

$$\geq \sqrt{\frac{s+2t}{2}} \left(\prod_{j=1}^{s} x_j^2 \prod_{j=1}^{t}(y_j^2 + z_j^2)^2 \right)^{1/2N} = \sqrt{\frac{s}{2} + t}\ \ |N_{K/\mathbb{Q}}(f)|^{1/N} \geq \sqrt{\frac{s}{2} + t} ,$$

since $N_{K/\mathbb{Q}}(f) \in \mathbb{Z}$. In the totally real case

$$\sqrt{\sum_{j=1}^{N} x_j^2}\ \ \geq \sqrt{N} \left(\prod_{j=1}^{N} x_j^2 \right)^{1/2N} = \sqrt{N}\ \ |N_{K/\mathbb{Q}}(f)|^{1/N} \geq \sqrt{N}. \qquad \blacksquare$$

Unramified towers. Now let the field K vary so that $N \to \infty$, and K is either totally real, or totally complex. Then

$$\lambda(L) \ \sim \ -\log\sqrt{\frac{\pi e}{2}} + \frac{1}{N}\log\sqrt{|\mathcal{D}_K|}.$$

If we want to construct good lattices the last term should be bound. It is definitely so if K runs over an unramified tower of fields over some K_0, in which case it is just constant. We get :

THEOREM 1.3. *If a number field K_0 of degree N_0 has an infinite unramified tower of fields $K \supset K_0$ which are either totally real, or totally complex, then it yields an asymptotically good family of lattices $\{L_N \subset \mathbb{R}^N\}$ with*

$$\lambda(\{L_N\}) \ \sim \ -\log\sqrt{\frac{\pi e}{2}} + \frac{1}{N_0}\log\sqrt{|\mathcal{D}_{K_0}|}. \qquad \blacksquare$$

For $K_0 = \mathbb{Q}(\cos\frac{2\pi}{11}\ ,\ \sqrt{-46})$ we get $\lambda \sim 2.2218\ldots$ (for this field $[K_0 : \mathbb{Q}] = 10$, $|\mathcal{D}_{K_0}| = 2^{15}\cdot 11^8 \cdot 23^5$, and MARTINET proved that it has an infinite abelian tower). On the other hand, ODLYZKO-SERRE inequalities for the discriminant (based on the "explicit formulae") show that for any K we cannot get asymptotically less than $1.193\ldots$ (and $1.694\ldots$ assuming the generalized Riemann hypothesis).

Congruence lattices. Let $\mathfrak{a}$ be a fractional ideal in K. Consider the additive subgroup

$$L(\mathfrak{a}) = \mathfrak{a}^{-1} = \{f \in K \mid f\mathfrak{a} \subseteq \mathcal{O}_K\}.$$

The corresponding lattice $L_\mathfrak{a} = \sigma(L(\mathfrak{a}))$ up to a multiplication by some $m \in \mathbb{Z}$ is a sublattice in L, and we can estimate its parameters more or less in the same manner as before. (This is the NALD-case).

2. Function field codes (FACD)

Construction. Here is a straightforward analogue. Let $K = \mathbb{F}_q(X)$ be a function field, X being a smooth projective curve over a finite field $\mathbb{F}_q$. Fix a set of points $\mathcal{P} = \{P_1, \ldots, P_n\} \subseteq X(\mathbb{F}_q)$ and let $M_\mathcal{P} = \{f \in K \mid f$ is regular at $\mathcal{P}\}$. There is a natural map

$$\varphi_\mathcal{P} : M_\mathcal{P} \to \mathbb{F}_q^n\ ,$$
$$\varphi_\mathcal{P}(f) = (f(P_1), \ldots, f(P_n)).$$

Let D be a divisor on X such that $\mathcal{P} \cap \operatorname{Supp} D = \emptyset$. Consider

$$L(D) = \{f \in K \mid (f) + D \geq 0\}.$$

The image $C = \varphi_{\mathcal{P}}(L(D)) \subseteq \mathbb{F}_q^n$ is a code.

Parameters. Let g be the genus of X and $a = \deg D$. Of course, the length n of C equals $|\mathcal{P}|$.

LEMMA 2.1. *Let $a < n$. Then for the code C*

(i) $d \geq n - a$,

(ii) $k = \dim L(D) \geq a - g + 1$,

and if $a \geq 2g - 1$ then $k = a - g + 1$.

Proof : (i) follows from the fact that the number of zeroes of $f \in L(D)$ cannot exceed $\deg D$. It also shows that (for $a < n$) $\varphi_{\mathcal{P}}$ is monomorphic on $L(D)$.

(ii) follows from the Riemann-Roch theorem. ∎

Asymptotic behaviour. Lemma 2.1 shows that

$$\delta + R \geq 1 - \frac{g-1}{n} \cdot$$

Consider a family of curves of growing genus with

$$\frac{|X(\mathbb{F}_q)|}{g} \to A.$$

Then we get a family of codes with $n \to \infty$ and

$$\delta + R \gtrsim 1 - A^{-1},$$

if $A > 1$ these codes are asymptotically good. The DRINFELD-VLĂDUŢ theorem states that $A \leq \sqrt{q} - 1$, and it is known that for $q = p^{2m}$ there exist families of curves with $A = \sqrt{q} - 1$. Let $\mathcal{P} = X(\mathbb{F}_q)$ (to be scrupulous about $\mathcal{P} \cap \operatorname{Supp} D = \emptyset$ we can also put $\mathcal{P} = X(\mathbb{F}_q) - P_0$, $D = aP_0$; it does not influence asymptotics, we never mention such things below).

THEOREM 2.2. *A family of curves of growing genus g such that*

$$\frac{|X(\mathbb{F}_q)|}{g} \to A > 1$$

yields an asymptotically good family of codes such that for any $\delta \leq 1 - A^{-1}$ *there is a subfamily* $\{C_n\}$ *with* $\delta(\{C_n\}) = \delta$ *and*

$$R(\{C_n\}) \geq 1 - A^{-1} - \delta.$$

For $q = p^{2m}$ *we can set* $A = \sqrt{q} - 1$. ∎

It is not difficult to see that on some segment of the d-axis for $q = p^{2m} \geq 49$ these codes are better than the GILBERT-VARSHAMOV bound.

3. Number field codes (NAC)

The construction of §1 can be generalized using non-archimedian places. Let $S = S_f \cup S_\infty$ be a fixed finite set of places of a number field K. For $v \in S_f$ let $k(v)$ be the residue field, for $v \in S_f$ let $k(v) = \mathbb{R}$ for real places and $k(v) = \mathbb{C}$ for complex ones. Let $\mathfrak{a}$ be a fractional ideal such that $S_f \cap \operatorname{Supp} \mathfrak{a} = \emptyset$. For any $v \in S$ there is a natural map $\sigma_v : L(\mathfrak{a}) \to k(v)$. Together they form a map

$$\sigma_S : L(\mathfrak{a}) \to \bigoplus_{v \in S} k(v).$$

Everything is quite natural, but what we get is neither a code, nor a lattice (except for the case $S = S_\infty$ discussed in §1). Here is a way out.

Construction. Let $[K : \mathbb{Q}] = N = s + 2t$. Fix two integers $q \geq r > 1$. Let S_f be the set of places v of K such that for some $c(v) \in \mathbb{Z}$

$$r \leq N(v)^{c(v)} \leq q \ ,$$

where $N(v) = |k(v)|$. Let $S = S_f \cup S_\infty$, S_∞ being the set of all archimedian places, let $n = |S| = |S_f| + s + t$. To make our consideration simpler we suppose that the field is totally real, i.e. t=0.

Let

$$U = \{x \in \mathbb{R}^N \mid 0 < x_i < r^{a/N}\}.$$

There exists a shift U' of U such that $|U' \cap \sigma(\mathcal{O}_K)| \geq r^a / \sqrt{|\mathcal{D}_K|}$, $\sigma(\mathcal{O}_K)$ being the lattice studied in §1. Divide each side of the cube U' into q equal parts, and identify the set of q^N small cubes with $\mathbb{F}_q^N$. Define $\varphi_\infty : U' \cap \sigma(\mathcal{O}_K) \to \mathbb{F}_q^N$ mapping each point to the small cube it lies in ; let φ_v be the component of φ_∞ corresponding to $v \in S_\infty$. For $v \in S_f$ let φ_v be the map

$$U' \cap \sigma(\mathcal{O}_K) \hookrightarrow \mathcal{O}_K \to \mathcal{O}_K / v^{c(v)} \hookrightarrow \mathbb{F}_q \ ,$$

where we identify the place $v \in S_f$ with the corresponding prime ideal, and $\mathcal{O}_K/v^{c(v)} \hookrightarrow \mathbb{F}_q$ is some fixed embedding of sets.

Let $\varphi_S : U' \cap \sigma(\mathcal{O}_K) \to \mathbb{F}_q^n$ be defined as $\varphi_S = (\varphi_{v_1}, \varphi_{v_2}, \ldots)$ for all $v \in S$. The image $C = \varphi_S(U' \cap \sigma(\mathcal{O}_K)) \subseteq \mathbb{F}_q^n$ is a (non-linear) code of length n.

Parameters. The parameters are estimated by the following result reminding one of Lemma 2.1.

LEMMA 3.1. *Let $a \leq n$. Then*

(i) $d \geq n + 1 - a$,

(ii) $k \geq a \log_q r - \log_q \sqrt{|\mathcal{D}_K|}$.

Proof: (i) Let $f_1, f_2 \in U' \cap \sigma(\mathcal{O}_K)$. Set

$$A = \{v \in S_\infty \mid \varphi_v(f_1) = \varphi_v(f_2)\},$$
$$B = \{v \in S_f \mid \varphi_v(f_1) = \varphi_v(f_2)\}.$$

On one hand $|f_1 - f_2|_v \leq r^{a/N}$ for any $v \in S_\infty$ and $|f_1 - f_2|_v \leq \dfrac{r^{a/N}}{q}$ for $v \in A$. On the other hand $f_1 - f_2 \in v^{c(v)}$ for any $v \in B$, and $N(v^{c(v)}) \geq r$. Let $\alpha = |A|$, $\beta = |B|$. We have

$$r^\beta \leq N_{K/\mathbb{Q}}(f_1 - f_2) < \frac{r^a}{q^\alpha} \leq r^{a-\alpha}.$$

Therefore $\alpha + \beta < a$, i.e. $d > n - a$.

(ii) We see that if $a \leq n$ then φ_S is an embedding and

$$|U' \cap \sigma(\mathcal{O}_K)| \geq r^a / \sqrt{|\mathcal{D}_K|}.$$ ∎

This lemma is also valid for $t \neq 0$, but the proof is slightly more difficult.

Asymptotic behaviour. Fix q and r and consider a family of fields K of growing degree. Let

$$\gamma = \liminf_K \frac{\log_q \sqrt{|\mathcal{D}_K|}}{n} ,$$

where $n = s + t + |S_f|$. We get a family of non-linear codes with $n \to \infty$ and

$$R \gtrsim (1 - \delta) \log_q r - \gamma ,$$

if $\gamma < \log_q r$ then there exist asymptotically good codes among them.

It is possible to prove (using the "explicit formulae again") that $\gamma > (\sqrt{q}-1)^{-1}$ which shows that the parameters of these codes are worse than in §2. On the other hand for $r = \frac{q+1}{2}$ there exist fields with $\gamma \leq \text{const} \cdot \frac{\log q}{q^{1/4}}$, where const does not depend on q. Summing up we get THEOREM 3.2. *A family of number fields K of growing degree with* $\liminf \frac{\log_q \sqrt{|\mathcal{D}_K|}}{n} = \gamma < \log_q r$ *where* $n = s + t + |S_f|$, S_f *being the set of non-archimedian places v such that for some* $c(v) \in \mathbb{Z}$, $r \leq N_{K/\mathbb{Q}}(v)^{c(v)} \leq q$
(r and q being fixed), yields a family of asymptotically good non-linear codes with $\delta(\{C_n\}) = \delta$ *and*

$$R(\{C_n\}) \geq (1-\delta)\log_q r - \gamma.$$

We can set $\gamma = \text{const}\, \frac{\log q}{q^{1/4}}$. ∎

It is not difficult to see that for a large q on some segment of the δ-axis these codes are better than the GILBERT-VARSHAMOV bound, though worse than in §2.

4. Multiplicative lattices (NML)

Up to this moment we have used the additive groups of global fields. Now we are going to exploit their multiplicative structure.

Construction. We start with a number field K of degree $N = s + 2t$ and a finite number of its places $S = S_\infty \cup S_f$ which includes all the archimedian ones, let $n = |S|$. Let $\mathcal{O}_S^*$ be the set of S-units, i.e. $f \in \mathcal{O}_S^*$ iff all the prime divisors of its numerator and denominator belong to S.

There is a natural map

$$\varphi_S : \mathcal{O}_S^* \to \mathbb{R}^n ,$$
$$f \mapsto \{\ln \|f\|_v\} ,$$

where $v \in S$, and $\| \ \|_v$ is the normalized absolute value, i.e. $\|f\|_v = |\sigma_v(f)|$ for real places, $\|f\|_v = |\sigma_v(f)|^2$ for complex ones, and $\|f\|_v = N(v)^{-\text{ord}_v(f)}$ for $v \in S_f$. It is clear that $\ker \varphi_S = W$ is the group of roots of 1 in K, and that $\text{Im}\ \varphi_S \subset H = \{x \in \mathbb{R}^n \mid \sum x_i = 0\}$ because of the product formula.

Parameters. Let R be the regulator of K and let h be its class number. Set $h(f) = \sum_v |\ln \|f\|_v|$ for $f \in K^*$, this is the height function (sorry that it is denoted by the same letter as the class number); $h(f) = 0$ iff $f \in W$. We set $h(K) = \min_{f \in K^* - W} h(a)$ and call it the *height* of the field K.

LEMMA 4.1. *Let* $L_S = \varphi_S(\mathcal{O}_S^*)$. *Then*

(i) $d(L_S) \geq \dfrac{1}{\sqrt{n}}\, h(K)$,

(ii) *if* K *is totally real, then*

$$d(L_S) \geq \frac{[K:\mathbb{Q}]}{\sqrt{n}} \ln\left(\frac{1+\sqrt{5}}{2}\right),$$

(iii) $rk\ L_S = n - 1$ *and*

$$\det L_S \leq \sqrt{n}\ Rh \prod_{v \in S_f} \ln N(v).$$

Proof: (i) is obvious since $\sqrt{\sum_{i=1}^{n} x_i^2} \geq \dfrac{1}{\sqrt{n}} \sum |x_i|$.

(ii) In [Sc] it is proved that for any totally real field K

$$h(K) \geq [K:\mathbb{Q}] \ln\left(\frac{1+\sqrt{5}}{2}\right) .$$

(iii) Let the first coordinates in $\mathbb{R}^n$ correspond to $v \in S_\infty$. Consider the orthogonal projection

$$T : H \to H_0 = \left\{ x \in \mathbb{R}^n \mid \sum_{i=1}^{s+t} x_i = 0 \right\} = H_1 \oplus \mathbb{R}^{n-s-t} ,$$

where $H_1 = \{x \in \mathbb{R}^{s+t} \mid \sum x_i = 0\}$, T multiplies volumes by $\sqrt{s+t}/\sqrt{n}$. Since $H_1 \cap T(L_S)$ is the lattice of units, $\det(T(L_S) \cap H_1) = \sqrt{s+t}\ R$ and $\det T(L_S) = \sqrt{s+t}\ R \det(pr_2\, T(L_S))$. Using the obvious

$$\left[\sum_{v \in S_f} \mathbb{Z} \ln N(v) : pr_2\, T(L_S) \right] \leq h$$

we get the answer. ∎

Asymptotic behaviour. We start, as in §1, considering unramified towers of fields. In such towers $\frac{1}{N}\log\sqrt{|\mathcal{D}_K|}$ is constant. To bound $\frac{Rh}{|W|}$ we can use standard estimates for the residue of ζ-function of K.

If we put $s = 2$ in the proof of Lemma 1 of [LA] ch.XVI, §.1, we get

$$\frac{Rh}{|W|} \leq \frac{2|\mathcal{D}_K|}{\pi^{s+2t}}$$

(this is not the best estimate but the most obvious one).

In the totally real case $|W| = 2$. Put $S = S_\infty$ and consider unramified towers of totally real fields. We get

THEOREM 4.2. *If a number field K_0 of degree N_0 has an unramified tower of totally real fields then it yields an asymptotically good family of lattices $\{L_N \subset \mathbb{R}^N\}$ with*

$$\lambda(\{L_N\}) \leq -\log\sqrt{\frac{\pi^3 e}{2}} - \log\,\ln\left(\frac{1+\sqrt{5}}{2}\right) + \frac{1}{N_0}\log|\mathcal{D}_{K_0}|.$$

For $K_0 = \mathbb{Q}(\sqrt{2}\ ,\ \sqrt{70035})$ we get $\lambda \lesssim 8.4046$ (for this field $N_0 = 4$, $|\mathcal{D}_{K_0}| = 2^8 \cdot 3^2 \cdot 5^2 \cdot 7^2 \cdot 23^2 \cdot 29^2$ and MARTINET proved that is has a required tower).

5. Function field lattices (FML)

Here is a direct function field analogue of the construction of §4.

Construction. In the notation of §2, let

$$\mathcal{O}_{\mathcal{P}}^* = \{f \in K^* | \mathrm{Supp}(f) \subseteq \mathcal{P}\}\ .$$

Let $\mathrm{Div}_{\mathcal{P}}(X)$ denote the group of divisors supported in $\mathcal{P}$, $\mathrm{Div}_{\mathcal{P}}^\circ(X)$ of those of degree 0, $\mathrm{Pr}_{\mathcal{P}}(X)$ the subgroup of principal divisors. Let $J_X = \mathrm{Div}^\circ(X)/\mathrm{Pr}(X)$ be the Jacobian of X.

There is a natural map

$$\begin{aligned}\varphi_{\mathcal{P}} : \mathcal{O}_{\mathcal{P}}^* &\longrightarrow \mathrm{Div}_{\mathcal{P}}(X) \simeq \mathbb{Z}^n\ ,\\ f &\longmapsto (f)\ .\end{aligned}$$

It is clear that $\operatorname{Ker} \varphi_{\mathcal{P}} = \mathbb{F}_q^*$ is again the group of roots of 1 in K, and that

$$\operatorname{Im} \varphi_{\mathcal{P}} \subseteq \operatorname{Div}_{\mathcal{P}}^{\circ}(X) \simeq A_{n-1} = \{x \in \mathbb{Z}^n | \sum x_i = 0\} .$$

We set

$$L_{\mathcal{P}} = \varphi_{\mathcal{P}}(\mathcal{O}_{\mathcal{P}}^*) \subseteq A_{n-1} \otimes \mathbb{R} \simeq \mathbb{R}^{n-1} .$$

Parameters. Let us start with a bound for the number of points on the Jacobian :

LEMMA 5.1. $|J_X(\mathbb{F}_q)| \leq \left(1 + q + \dfrac{|X(\mathbb{F}_q)| - q - 1}{g}\right)^g .$

Proof. We know that $|J_X(\mathbb{F}_q)| = \prod_{i=1}^{2g}(1 - \omega_i)$, ω_i being the Frobenius roots, $|\omega_i| = \sqrt{q}$, $\omega_{g+i} = \overline{\omega}_i$. The arithmetic-mean geometric-mean inequality yields

$$\prod_{i=1}^{2g}(1 - \omega_i) = \prod_{i=1}^{g}(q + 1 - \omega_i - \overline{\omega}_i) \leq \left(\frac{\sum_{i=1}^{g}(q + 1 - \omega_i - \overline{\omega}_i)}{g}\right)^g ,$$

and the statement follows from

$$-\sum_{i=1}^{g}(\omega_i + \overline{\omega}_i) = |X(\mathbb{F}_q)| - q - 1 . \qquad \blacksquare$$

Now we can estimate the parameters of $L_{\mathcal{P}}$.

LEMMA 5.2. *Let* $L_{\mathcal{P}} = \varphi_{\mathcal{P}}(\mathcal{O}_{\mathcal{P}}^*)$. *Then*

(i) $d(L_{\mathcal{P}}) \geq \min_{f \in \mathcal{O}_{\mathcal{P}}^* - \mathbb{F}_q^*} \sqrt{2 \deg f} \geq \sqrt{\dfrac{2|X(\mathbb{F}_q)|}{q+1}}$,

(ii) $rk\, L_{\mathcal{P}} = n - 1$ *and*

$$\det L_{\mathcal{P}} \leq \sqrt{n}\ |J_X(\mathbb{F}_q)| \leq \sqrt{n}\left(1 + q + \frac{|X(\mathbb{F}_q)| - q - 1}{g}\right)^g .$$

Proof: (i) Let $f \in \mathcal{O}_{\mathcal{P}}^*$, $f \notin \mathbb{F}_q^*$, $\varphi_{\mathcal{P}}(f) = (x_1, \ldots, x_n) \in \mathbb{Z}^n$. Then

$$|\varphi_{\mathcal{P}}(f)| = \sqrt{\sum x_i^2} \geq \sqrt{\sum |x_i|} = \sqrt{2 \deg f} ,$$

since $x_i \in \mathbb{Z}$, $\sum x_i = 0$, $\deg f = \sum_{x_i>0} x_i$. Any $f \in K$ maps $\mathbb{F}_q$-points to $\mathbb{F}_q$-points of $\mathbb{P}^1$. Therefore

$$|X(\mathbb{F}_q)| \leq (q+1)\deg f$$

and we get the second inequality.

(ii) We know that $\det A_{n-1} = \sqrt{n}$, and $\det L_{\mathcal{P}} = [A_{n-1} : L_{\mathcal{P}}] \det A_{n-1}$. Then $A_{n-1} \simeq \mathrm{Div}^\circ_{\mathcal{P}}(X) \subset \mathrm{Div}^\circ(X)$, and $L_{\mathcal{P}} = \mathrm{Pr}_{\mathcal{P}}(X) = \mathrm{Pr}(X) \cap \mathrm{Div}^\circ_{\mathcal{P}}(X)$. Therefore

$$[A_{n-1} : L_{\mathcal{P}}] \leq [\mathrm{Div}^\circ(X) : \mathrm{Pr}(X)] = |J_X(\mathbb{F}_q)| \ .$$

Lemma 5.1 gives the second inequality. ∎

Asymptotic behaviour. As in §2 we consider families of curves of growing genus with $\dfrac{|X(\mathbb{F}_q)|}{g} \to A$, and set $\mathcal{P} = X(\mathbb{F}_q)$. We get

THEOREM 5.3. *A family of curves of growing genus g such that*

$$\frac{|X(\mathbb{F}_q)|}{g} \to A > 0$$

yields an asymptotically good family of lattices $\{L_N \subset \mathbb{R}^N\}$ with

$$\lambda(\{L_N\}) \leq -\log\sqrt{\pi e} + \log\sqrt{q+1} + A^{-1}\log(1+q+A) \ . \quad \blacksquare$$

We are again interested to take the largest possible A. Let $q = p^{2m}$, then we can consider curves with $A = \sqrt{q}-1$. For such curves we can even do slightly better than Lemma 5.1 :

LEMMA 5.4. *For a family of curves X with*

$$\frac{|X(\mathbb{F}_q)|}{g} \to \sqrt{q} - 1$$

there is an asymptotic equality

$$\frac{1}{g}\log|J_X(\mathbb{F}_q)| \sim \log q + (\sqrt{q}-1)\log\frac{q}{q-1} \ .$$

Proof : Let $N_r = |X(\mathbb{F}_{q^r})|$. Then

$$N_r = q^r + 1 - \sum_{i=1}^{2g} \omega_i^r \ ,$$

where $\omega_i = \sqrt{q}\,\alpha_i$, $|\alpha_i| = 1$, and $\alpha_i^{-1} = \alpha_{g+i}$ for $i = 1, \ldots, g$. We are interested in $M = |J_X(\mathbb{F}_q)| = \prod_{i=1}^{2g}(1 - \omega_i)$. Let $b = \log_q g$. Then

$$\frac{1}{g}\left|\sum_{m=b+1}^{\infty}\frac{q^{-m/2}}{m}\sum_{i=1}^{2g}\alpha_i^m\right| \le 2\sum_{m=b+1}^{\infty}\frac{q^{-m/2}}{m} \to 0 \quad \text{when} \quad g \to \infty\ .$$

Since $0 \le |\alpha_i^n + \alpha_i^{n-1} + \cdots + 1|^2 = (n+1) + \sum_{j=1}^{n}(n+1-j)(\alpha_i^j + \alpha_i^{-j})$, we have

$$n + 1 \ge -\sum_{j=1}^{n}(n+1-j)(\alpha_i^j + \alpha_i^{-j})\ ,$$

summing it over $i = 1, \ldots, 2g$ and using $\sum \alpha_i^j = \sum \alpha_i^{-j}$, and $-\sum_{i=1}^{2g}\alpha_i^j = N_j\, q^{-j/2} - q^{j/2} - q^{-j/2}$ we get

$$g(b+1) \ge \sum_{j=1}^{b}(b+1-j)[N_j\, q^{-j/2} - q^{j/2} - q^{-j/2}]\ ,$$

or

$$1 \ge \sum_{j=1}^{b}(1 - \frac{j}{b+1})\,\frac{N_1}{g}\,q^{-j/2} + \sum_{j=1}^{b}(1 - \frac{j}{b+1})\,\frac{(N_j - N_1)}{g}\,q^{-j/2} - \\ - \frac{1}{g}\sum_{j=1}^{b}(1 - \frac{j}{b+1})(q^{j/2} + q^{-j/2})\ .$$

The last term is less than

$$\frac{1}{g}\sum_{j=1}^{b}q^{j/2} + \frac{1}{g}\sum_{j=1}^{b}q^{-j/2}$$

which tends to 0 when $g \to \infty$. The first term tends to

$$\frac{N_1}{g}\sum_{j=1}^{\infty}q^{-j/2} = \frac{N_1}{g}\,(\sqrt{q} - 1)^{-1} \to 1\ ,$$

therefore

$$\sum_{j=1}^{b}\frac{N_j - N_1}{g}\,q^{-j/2} \to 0\ .$$

Now we are able to estimate

$$\frac{1}{g}\ln M = \frac{1}{g}\ln\prod_{i=1}^{2g}(1-\omega_i) = \frac{1}{g}\ln\left(q^g\prod_{i=1}^{2g}(1-\alpha_i q^{-1/2})\right)$$

$$= \ln q + \frac{1}{g}\sum_{i=1}^{2g}\ln(1-\alpha_i q^{-1/2}) = \ln q - \frac{1}{g}\sum_{m=1}^{\infty}\frac{q^{-m/2}}{m}\sum_{i=1}^{2g}\alpha_i^m$$

$$= \ln q + \frac{1}{g}\sum_{m=1}^{b}\frac{q^{-m/2}}{m}[N_m q^{-m/2} - q^{m/2} - q^{-m/2}]$$

$$- \frac{1}{g}\sum_{m=b+1}^{\infty}\frac{q^{-m/2}}{m}\sum_{i=1}^{2g}\alpha_i^m .$$

The last term tends to 0, and the second term is

$$\frac{1}{g}\sum_{m=1}^{b}\frac{q^{-m/2}}{m}[N_m q^{-m/2} - q^{m/2} - q^{-m/2}] =$$

$$= \sum_{m=1}^{b}\frac{N_1}{g}\frac{q^{-m}}{m} + \sum_{m=1}^{b}\frac{q^{-m}}{m}\frac{(N_m - N_1)}{g} - \frac{1}{g}\sum_{m=1}^{b}\frac{1}{m} - \frac{1}{g}\sum_{m=1}^{b}\frac{q^{-m}}{m} .$$

The first term tends to

$$(\sqrt{q}-1)\sum_{m=1}^{\infty}\frac{q^{-m}}{m} = (\sqrt{q}-1)\ln\frac{q}{q-1}$$

and all the rest tend to zero. ∎

Using Lemma 5.4 we get

THEOREM 5.5. *A family of curves of growing genus g such that*

$$\frac{|X(\mathbb{F}_q)|}{g} \to \sqrt{q}-1$$

yields an asymptotically good family of lattices $\{L_N \subset \mathbb{R}^N\}$ with

$$\lambda(\{L_N\}) \le -\log\sqrt{\pi e} + \log\frac{\sqrt{q+1}}{q-1} + \frac{\sqrt{q}}{\sqrt{q}-1}\log q . \quad ∎$$

For $q = 9$ we get $\lambda \lesssim 1.8687\ldots$

6. Congruence sublattices (FMLD)

The construction of §5 can be slightly elaborated. We consider some specific sublattices of $L_{\mathcal{P}}$.

Construction. Let D be a positive divisor on X, $D = a_i P_i$, $r_i = \deg P_i$, $N(P_i) = q^{r_i}$, $a = \deg D = \sum a_i r_i$. We identify D and P_i with the corresponding ideals. Suppose that $\mathcal{P} \cap \operatorname{Supp} D = \emptyset$. Let

$$\mathcal{O}^*_{\mathcal{P},D} = \{f \in \mathcal{O}^*_{\mathcal{P}} \mid f \equiv 1 (\operatorname{mod} D)\} ,$$

and consider the lattice $L_{\mathcal{P},D} = \varphi_{\mathcal{P}}(\mathcal{O}^*_{\mathcal{P},D}) \subseteq L_{\mathcal{P}}$.

Parameters. Here are the estimates.

LEMMA 6.1. *Let $L_{\mathcal{P},D} = \varphi_{\mathcal{P}}(\mathcal{O}^*_{\mathcal{P},D})$. Then*

(i) $d(L_{\mathcal{P},D}) \geq \sqrt{2a}$,

(ii) $rk\, L_{\mathcal{P},D} = n - 1$ *and*

$$\det L_{\mathcal{P},D} \leq \sqrt{n}\, |J_X(\mathbb{F}_q)|\, \frac{q^a}{q-1} \prod (1 - q^{-r_i}) .$$

Proof: (i) We use the first inequality of Lemma 5.2 (i), which in our case reads $d(L_{\mathcal{P},D}) \geq \min_{f \in \mathcal{O}^*_{\mathcal{P},D} - \{1\}} \sqrt{2 \deg f}$, and notice that $\deg f = \deg(f-1) \geq \deg D = a$.

(ii) Lemma 5.2 (ii) estimates $\det L_{\mathcal{P}}$, and we have only to estimate $[L_{\mathcal{P}} : L_{\mathcal{P},D}]$. Look at the embedding $\mathcal{O}^*_{\mathcal{P}} \hookrightarrow \prod \widehat{\mathcal{O}}^*_{P_i}$, where $\widehat{\mathcal{O}}^*_{P_i}$ is the group of units in the completion of the local ring at P_i.
Let $\widehat{\mathcal{O}}^*_{P_i,a_i} = \{x \in \widehat{\mathcal{O}}^*_{P_i} \mid x \equiv 1 (\operatorname{mod} P_i^{a_i})\}$. We have

$$\mathcal{O}^*_{\mathcal{P},D} = \mathcal{O}^*_{\mathcal{P}} \cap (\prod \widehat{\mathcal{O}}^*_{P_i,a_i})$$

and

$$[\mathcal{O}^*_{\mathcal{P}} : \mathcal{O}^*_{\mathcal{P},D}] \leq \left[\prod \widehat{\mathcal{O}}^*_{P_i} : \prod \widehat{\mathcal{O}}^*_{P_i,a_i}\right] = \prod ((q^{r_i} - 1) q^{r_i(a_i - 1)}) .$$

Then $\operatorname{Ker} \varphi_{\mathcal{P}} = \mathbb{F}_q^*$ and $\mathcal{O}^*_{\mathcal{P},D} \cap \operatorname{Ker} \varphi_{\mathcal{P}} = \{1\}$, therefore $[\mathcal{O}^*_{\mathcal{P}} : \mathcal{O}^*_{\mathcal{P},D}] = (q-1)[L_{\mathcal{P}} : L_{\mathcal{P},D}]$. ∎

Asymptotic behaviour. Consider the same family of curves as in §5, let $\mathcal{P} = X(\mathbb{F}_q)$ and let D be such that $\lim \dfrac{\deg D}{|X(\mathbb{F}_q)|} = (2 \ln q)^{-1}$ (this choice appears to be optimal). We get

THEOREM 6.2. *A family of curves of growing genus g such that*

$$\frac{|X(\mathbb{F}_q)|}{g} \to \sqrt{q} - 1,$$

with the appropriate choice of divisors, yields an asymptotically good family of lattices $\{L_N \subset \mathbb{R}^N\}$ with

$$\lambda(\{L_N\}) \leq -\log\sqrt{\frac{\pi}{2}} + \frac{1}{2}\log(\ln q) + \frac{\sqrt{q}}{\sqrt{q}-1}\log q - \log(q-1)\,. \qquad \blacksquare$$

For $q = 2209 = 47^2$ we get $\lambda \lesssim 1.3888\ldots$

7. Number field case (NMLD)

Now we return to the number field case and discuss an analogue of congruence lattices of §6. Here we also obtain good lattices.

Construction. In the notation of §4 let $\mathfrak{a} \subset \mathcal{O}_K$ be an ideal, $\mathfrak{a} = \prod v_i^{a_i}$, such that $v \notin S_f$ (i.e. $S_f \cap \operatorname{Supp} \mathfrak{a} = \emptyset$).
Let

$$\mathcal{O}^*_{S,\mathfrak{a}} = \{f \in \mathcal{O}^*_S \mid f \equiv 1 (\operatorname{mod} \mathfrak{a})\}$$

and consider the lattice $L_{S,\mathfrak{a}} = \varphi_S(\mathcal{O}^*_{S,\mathfrak{a}}) \subseteq L_S$.

Parameters. Everything is quite similar to §6, though the estimates are slightly worse. Let $W_\mathfrak{a} = W \cap \mathcal{O}^*_{S,\mathfrak{a}}$.

LEMMA 7.1. *Let $L_{S,\mathfrak{a}} = \varphi_S(\mathcal{O}^*_{S,\mathfrak{a}})$. Then*

(i) $d(L_{S,\mathfrak{a}}) \geq \dfrac{2}{\sqrt{n}}\,(\ln N_{K/\mathbb{Q}}(\mathfrak{a}) - (s+2t)\ln 2)$,

(ii) $rk\, L_{S,\mathfrak{a}} = n - 1$ *and*

$$\det L_{S,\mathfrak{a}} \leq (\det L_S) N_{K/\mathbb{Q}}(\mathfrak{a}) \prod\Big(1 - \frac{1}{N_{K/\mathbb{Q}}(v_i)}\Big)[W : W_\mathfrak{a}]^{-1} \leq$$

$$\sqrt{(s+t)(n-s-t)}\operatorname{Rh}\Big(\prod_{v\in S_f} \ln N(v)\Big) N_{K/\mathbb{Q}}(\mathfrak{a}) \Big(\prod(1 - \frac{1}{N_{K/\mathbb{Q}}(v_i)})\Big)[W : W_\mathfrak{a}]^{-1}\,.$$

Proof: (i) Let $\varphi_S(f) = (x_1, x_2, \ldots, x_n)$, $x_i = \ln \|f\|_{v_i}$. Then

$$|\varphi_S(f)| = \sqrt{\sum x_i^2} \geq \frac{1}{\sqrt{n}} \sum |x_i| = \frac{2}{\sqrt{n}} \sum_{x_i > 0} x_i.$$

We have

$$\sum_{x_i>0} x_i = \sum_{\substack{v\in S\\ \|f\|_v>1}} \ln\|f\|_v = \sum_{\substack{v\in S_\infty\\ \|f\|_v>1}} \ln\|f\|_v + \sum_{\substack{v\in S_f\\ \mathrm{ord}_v(f-1)<0}} (-\mathrm{ord}_v(f-1))\ln N(v)$$

$$= \sum_{\substack{v\in S_\infty\\ \|f\|_v>1}} \ln\|f\|_v - \sum_{\substack{v\in S_\infty\\ \|f-1\|_v>1}} \ln\|f-1\|_v + \sum_{\substack{v\in S_\infty\\ \|f-1\|_v<1}} (-\ln\|f-1\|_v) +$$

$$+ \sum_{\substack{v\notin S_\infty\\ \|f-1\|_v<1}} (\mathrm{ord}_v(f-1))\ln N(v)$$

(we have used the equality $\mathrm{ord}_v(f-1) = \mathrm{ord}_v f$ for $\mathrm{ord}_v f < 0$, and the product formula). We omit the third term (it is non-negative), the fourth term is at least $\ln N_{K/\mathbb{Q}}(\mathfrak{a})$ since $f-1 \in \mathfrak{a}$, and the sum of the first two terms is at least $-\sum_{v\in S_\infty} \ln\|2\|_v$ since $\max\{0, \ln\|z\|\} + \max\{0, \ln\|1-z\|\}$ is minimum for $z=-1$ (both for $z\in\mathbb{R}$ and $z\in\mathbb{C}$).

(ii) Knowing Lemma 4.1 (ii) we have only to estimate $[L_S : L_{S,\mathfrak{a}}]$. Note that $\mathrm{Ker}\,\varphi_S = W$, $\mathrm{Ker}\,\varphi_S \cap \mathcal{O}^*_{S,\mathfrak{a}} = W_\mathfrak{a}$, and proceed as in the proof of Lemma 6.1 (ii). ∎

Asymptotic behaviour. The proof of Lemma 7.1 (i) shows also that if $\log N_{K/\mathbb{Q}}(\mathfrak{a}) > s+2t$ then $W_\mathfrak{a} = \{1\}$ since $\varphi_S(f) = 0$ for $f \in W_\mathfrak{a}$. We choose $\mathfrak{a}$ in such a way that $\frac{1}{n}\log N_{K/\mathbb{Q}}(\mathfrak{a}) \sim \frac{s+2t}{n} + \log e$ (it is in fact optimal), K runs over an unramified tower.

As in §4 we have $\frac{Rh}{|W|} \le \frac{2|\mathcal{D}_K|}{\pi^{s+2t}}$. Let us choose S in such a way that $\frac{s+2t}{n}$ is constant in the tower and that both S and $\mathrm{Supp}\,\mathfrak{a}$ completely split in it (of course this restricts the choice of the tower). We get

THEOREM 7.2. *If a number field K_0 of degree N_0 has an infinite unramified tower in which sets of its places S_0 (with $n_0 = |S_0|$) and* $\mathrm{Supp}\,\mathfrak{a}_0$ *split completely then it yields an asymptotically good family of lattices $\{L_N \subset \mathbb{R}^N\}$ with*

$$\lambda(\{L_N\}) \le -\log\sqrt{\frac{2\pi}{e}} + \frac{1}{n_0}\log|\mathcal{D}_{K_0}| - \frac{N_0}{n_0}(\log\pi - 1) +$$

$$+ \frac{1}{n_0}\sum_{v\in S_{0f}} \log(\ln N(v)) + \frac{1}{n_0}\sum_{v_i|\mathfrak{a}} \log\left(1 - \frac{1}{N_{K_0/\mathbb{Q}}(v_i)}\right). \quad ∎$$

For the totally complex field $\mathbb{Q}(\cos\frac{2\pi}{11}, \sqrt{-46})$ and $S_0 = S_\infty$ we get $\lambda \lesssim 11.1512$.

For the totally real field $\mathbb{Q}(\sqrt{2}, \sqrt{70035})$ and $S = S_\infty$ we get $\lambda \lesssim 8.7920$. These are not best choices, but what we get is always much worse than in §6.

8. Congruence codes (FMCD)

The construction we are now going to expose corresponds to function field congruence lattices of §6 in the same way as number field codes of §3 correspond to additive number field lattices of §1.

Construction. In the notation of §6 suppose that $D = pD'$ for some positive divisor D' (where p is the characteristic of $\mathbb{F}_q$, $q = p^m$).

Let $C = L_{\mathcal{P},D}/((p\mathbb{Z})^n \cap L_{\mathcal{P},D}) \subseteq (\mathbb{Z}/p)^n = \mathbb{F}_p^n$. It is a p-ary code of length n.

To study C we have to give another construction of the same code. Let $\Omega(\sum_{P_i \in \mathcal{P}} P_i - D)$ be the space of differential forms ω on X such that $(\omega) + \sum P_i - D \geq 0$.

There are natural maps

$$d\log : \mathcal{O}^*_{\mathcal{P},D} \to \Omega(\sum P_i - D) ,$$
$$f \mapsto \frac{df}{f}$$

(here we use the condition $D = pD'$, it yields $\frac{df}{f} \equiv 0 (\mathrm{mod}\ D)$) and

$$\mathrm{Res}_{\mathcal{P}} : \Omega(\sum P_i - D) \to \mathbb{F}_q^n ,$$
$$\omega \mapsto (\mathrm{Res}_{P_1}(\omega), \ldots, \mathrm{Res}_{P_n}(\omega)) .$$

It is well known that $C' = \mathrm{Im}\ \mathrm{Res}_{\mathcal{P}}$ is a code dual to that of §2 (and its parameters are $d' \geq a - 2g + 2$, $k' \geq n - a + g - 1$, $k' = n - a + g - 1$ for $a < n$). We have the following obvious commutative diagram

$$\begin{array}{ccccccc} \mathcal{O}^*_{\mathcal{P},D} & \xrightarrow{\varphi_{\mathcal{P}}} & L_{\mathcal{P},D} & \longrightarrow & C & \hookrightarrow & \mathbb{F}_p^n \\ {\scriptstyle d\log}\downarrow & & & & & & \downarrow \\ \Omega(\sum P_i - D) & & \xrightarrow{\qquad\qquad \mathrm{Res}_{\mathcal{P}} \qquad\qquad} & & & & \mathbb{F}_q^n \end{array}$$

i.e. $C = C' \cap \mathbb{F}_p^n$.

Parameters. Now we are ready to estimate parameters.

LEMMA 8.1. *Let* $C = L_{\mathcal{P},D}/((p\mathbb{Z})^n \cap L_{\mathcal{P},D}) = C' \cap \mathbb{F}_p^n \subseteq \mathbb{F}_p^n$. *Then*

(i) $d \geq d' \geq a - 2g + 2$;

(ii) $k \geq n - 1 - m\,\dfrac{p-1}{p}\,a$.

Proof: (i) The first inequality is obvious. Let $\omega \in \Omega(\sum P_i - D)$, then the number of non-zero residues of ω equals the number of its poles (all poles being simple) which is at least $\deg D - 2g + 2$.

(ii) Let $B = L_{\mathcal{P},D} \cap (p\mathbb{Z})^n$. Then

$$\begin{aligned} p^k = |C| = [L_{\mathcal{P},D} : B] = \\ = [A_{n-1} : A_{n-1} \cap (p\mathbb{Z})^n][A_{n-1} \cap (p\mathbb{Z})^n : B][A_{n-1} : L_{\mathcal{P},D}]^{-1} \,. \end{aligned}$$

We have $[A_{n-1} : A_{n-1} \cap (p\mathbb{Z})^n] = p^{n-1}$. The multiplication by p maps isomorphically A_{n-1} onto $A_{n-1} \cap (p\mathbb{Z})^n$ and $L_{\mathcal{P},D'}$ onto B. Therefore

$$\begin{aligned} [A_{n-1} \cap (p\mathbb{Z})^n : B][A_{n-1} : L_{\mathcal{P},D}]^{-1} = \\ = [A_{n-1} : L_{\mathcal{P},D'}][A_{n-1} : L_{\mathcal{P},D}]^{-1} = [L_{\mathcal{P},D'} : L_{\mathcal{P},D}]^{-1} \,. \end{aligned}$$

Proceeding as in the proof of Lemma 6.1 (ii) we see that

$$[L_{\mathcal{P},D'} : L_{\mathcal{P},D}] \leq q^{\deg D - \deg D'} = p^{m\frac{p-1}{p}a} \,.$$

Summing up we get $k \geq n - 1 - m\,\dfrac{p-1}{p}\,a$. ∎

Asymptotic behaviour. As usual the best results are obtained for $\frac{|X(\mathbb{F}_q)|}{g} \to A$, A being as large as possible (always $A \leq \sqrt{q} - 1$).

THEOREM 8.2. *A family of curves over $\mathbb{F}_q$, $q = p^m$, of growing genus g such that $\frac{|X(\mathbb{F}_q)|}{g} \to A > \frac{2m(p-1)}{p}$ yields an asymptotically good family of p-ary codes such that for any $\delta < \frac{p}{m(p-1)} - 2A^{-1}$ there is a subfamily $\{C_n\}$ with $\delta(\{C_n\}) = \delta$ and*

$$R(\{C_n\}) \geq 1 - m\,\frac{p-1}{p}\,(2A^{-1} + \delta)\,. \qquad \blacksquare$$

One easily checks that for $m = 1$ this result is worse than that of Theorem 2.2. The result of Theorem 8.2 can be generalized to p^r-ary codes (just change p by p^r), but the construction using $L_{\mathcal{P},D}$ goes out (cf. [KA/TS]).

9. Remarks and open problems

Here we list some natural remarks and questions, without any particular order.

1. What are the best constants in §4 and §7 ?

2. We have mostly restricted ourselves (in the function field case) to $\mathcal{P} \subseteq X(\mathbb{F}_q)$. All the constructions in fact work for any set of places of K, though places of high degree usually spoil parameters. Can places of higher degree be of any use ?

3. In the number field case we have usually supposed that $S \supseteq S_\infty$. Can we get anything good without this condition ?

4. Each section of this paper was encoded by three or four letters. Formally speaking there are 16 possibilities. What can we say about those we have not mentioned ?

5. In §2 we have an asymptotic equality for λ, and in all the other cases but estimates. What are the true values of λ (asymptotically) ?

6. Can we use "explicit formulae" plus some other considerations to give *lower* bounds of the density exponent of what we are able to get by our constructions ?

7. In the function field case the best families of curves (those with $\frac{|X(\mathbb{F}_q)|}{g} \to \sqrt{q}-1$) are provided by modular curves which form *ramified* towers (the ramification being rather "small"). What are their analogues in the number field case ?

8. The results we have obtained concern packings either in $\mathbb{R}^N$ or in $\mathbb{F}_q^N$. Our constructions also lead to natural lattices in $\mathbb{F}_q((T))^N$ and in products of p-adic fields. What are the correct parameters (how to put the problem) in those cases ?

9. Function field multiplicative lattices can be also constructed starting from curves over any field, provided that we know the finiteness of the subgroup in Jacobian generated by $\mathcal{P}$. Consider modular curves (say, over $\mathbb{C}$) and $\mathcal{P}$ consisting of cusp points which are of finite order (the MANIN-DRINFELD theorem). How to estimate parameters ?

10. What can be done with varieties (over $\mathbb{F}_q$ and arithmetic) of dimension more than 1 ? For example what are the densities of MORDELL-WEIL lattices on abelian varieties ?

11. $K^* = K_1(K)$ and the map we have used in §§4-7 is the regulator map. What can be done with the help of higher regulators on $K_i(K)$?

REFERENCES

[Co/Sl] J.H. CONWAY, N.J.A. SLOANE, *Sphere packings, lattices and groups*, Springer, N.Y., 1988.

[Go 1] V.D. GOPPA, Codes on algebraic curves, *Soviet Math. Dokl.*, **24** (1981), 170-172.

[Go 2] V.D. GOPPA, *Geometry and codes*, Kluwer Acad. Publ., 1988.

[Ka/Ts] G.L. KATSMAN, M.A. TSFASMAN, A remark on algebraic-geometric codes, *Contemp. Math.*, **93** (1989), 197-199.

[La] S. LANG, *Algebraic number theory*, Addison-Wesley, 1970.

[Le] H.W. LENSTRA JR., *Codes from algebraic number fields*, in : Fundamental contributions in the Netherlands since 1945, North-Holland, Amsterdam, v.II (1986), 95-104.

[Li/Ts] S.N. LITSYN, M.A. TSFASMAN, Constructive high-dimensional sphere packings, *Duke Math. J.*, **54** (1987), 147-161.

[MI] J. MILNOR, *Hilbert's problem 18 : on crystallographic groups, fundamental domains, and on sphere packings*, Proc. Symp. Pure Math., AMS, Providence RI, **28** (1976), 491-506.

[QU] H.-G. QUEBBEMANN, *Lattices from curves over finite fields*, Preprint, 1989.

[RO/TS] M. YU. ROSENBLOOM, M.A. TSFASMAN, Multiplicative lattices in global fields, *Invent. Math.*, **101** (1990), 687-696.

[SC] A. SCHINZEL, On the product of the conjugates outside the unit circle of an algebraic number, *Acta Arithm.*, **24** (1973), 385-399. Addendum, *Acta Arithm.*, **26** (1975), 329-331.

[TS/VL] M.A. TSFASMAN, S.G. VLĂDUŢ, *Algebraic-geometric codes*, Kluwer Acad. Publ., 1990.

[TS/VL/ZI] M.A. TSFASMAN, S.G. VLĂDUŢ, TH. ZINK, Modular curves, Shimura curves, and Goppa codes, better than the Varshamov-Gilbert bound, *Math. Nachr.*, **109** (1982), 21-28.

M.A. TSFASMAN
Institute for Problems
of Information Transmission
19, Ermolovoi st.
MOSCOW 101447
U.S.S.R.

Astérisque

W. VEYS

Relations between numerical data of a embedded resolution

Astérisque, tome 198-199-200 (1991), p. 397-403

<http://www.numdam.org/item?id=AST_1991__198-199-200__397_0>

RELATIONS BETWEEN NUMERICAL DATA OF AN EMBEDDED RESOLUTION

W. VEYS

INTRODUCTION.

Let k be an algebraically closed field of charasteristic zero and let $f \in k[x,y]$.
Let (X,h) be an embedded resolution of $f = 0$ in the affine plane $\mathbb{A}^2$, constructed by successive blowing-ups, and denote by $E_i, i \in T$, the irreducible components of $h^{-1}(f^{-1}\{0\})$.
We associate to each $E_i, i \in T$, a pair of numerical data (N_i, ν_i), where N_i and $\nu_i - 1$ are the multiplicities of E_i in the divisor of respectively $f \circ h$ and $h^*(dx \wedge dy)$ on X.

Fix one exceptional curve E with numerical data (N,ν) and say E intersects k times another irreducible component. Denote these components by $E_1, \ldots, E_k$. Then we have the relation

$$(*) \qquad \sum_{i=1}^{k} (\alpha_i - 1) + 2 = 0,$$

where $\alpha_i = \nu_i - \frac{\nu}{N} N_i$ for $i = 1, \ldots, k$.
When $f(x,y)$ is absolutely analytically irreducible, only $k = 1, 2$ or 3 occurs. The cases $k = 1$ and $k = 2$ were shown by Strauss [6, Th.1.] and Meuser [5, Lemma 1], and the case $k = 3$ by Igusa [3, Lemma 2]. Loeser [4, Lemme II.2] proved the general relation.

Now we can obviously extend the definitions above to higher dimensions. Even if we only consider surfaces there are two essential differences compared with the situation for curves, causing extra difficulties in generalizing the relation $(*)$. In dimension one an exceptional curve E, when created by some blowing-up, is isomorphic to the projective line $\mathbb{P}^1$; and its strict transforms by the following blowing-ups of the resolution remain isomorphic to $\mathbb{P}^1$. Moreover the number of intersection points with other $E_i, i \in T$, remains the same

during the (canonical) resolution process.
In dimension two an exceptional surface E is created as the projective plane $\mathbb{P}^2$ or as some ruled surface. But its strict transform $\tilde{E}$ by the next blowing-up of the resolution can be either isomorphic to E or to E with some points blown-up. And moreover, in the latter case, there are more intersections of other $E_i, i \in T$, with $\tilde{E}$ than with E.

Our result is essentially the following. Let E be a fixed exceptional variety. There are *basic relations* (B1 and B2) associated to the creation of E in the resolution process, generalizing the relation $(*)$. And there are *additional relations* (A) associated to each blowing-up of the resolution that "changes" E.

§1. EMBEDDED RESOLUTION.

Let k be an algebraically closed field of characteristic zero and let $f \in k[x_1, \ldots, x_{n+1}]$ be a polynomial over k.
Let Y denote the zero set of f in affine $(n+1)$-space $\mathbb{A}^{n+1}$ over k and $Y_\ell, \ell \in I$, its reduced irreducible components. We exclude the trivial case $f \in k$, so Y is a subscheme of codimension one of $\mathbb{A}^{n+1}$.
We fix an embedded resolution (X, h) for Y in $\mathbb{A}^{n+1}$ in the sense of Hironaka's Main Theorem II [2, p.142] by means of *monoidal transformations* or *blowing-ups*. It consists of the following data.

Set $X_0 = \mathbb{A}^{n+1}$, $Y^{(0)} = Y$, *and* $Y_\ell^{(0)} = Y_\ell$ for all $\ell \in I$.
For $i = 0, \ldots, r-1$ we have a finite succession of monoidal transformations $g_i : X_{i+1} \to X_i$ with irreducible nonsingular center $D_i \subset X_i$ and exceptional variety $E_{i+1}^{(i+1)} \subset X_{i+1}$ subject to the following conditions.
Let $E_j^{(i+1)}$, $Y^{(i+1)}$ and $Y_\ell^{(i+1)}$ denote the strict transform of respectively $E_j^{(i)}$, $Y^{(i)}$ and $Y_\ell^{(i)}$ in X_{i+1} by g_i for $j = 1, \ldots, i$ and all $\ell \in I$. Then

(1) for $i = 0, \ldots, r-1$ we have $D_i \subset Y^{(i)}, codim(D_i, X_i) \geqslant 2$, and the multiplicity on $Y^{(i)}$ of all $x \in D_i$ equals the maximal multiplicity on $Y^{(i)}$;

(2) $\bigcup_{1 \leqslant j \leqslant i} E_j^{(i)}$ has only normal crossings and only normal crossings with D_i (in X_i) for $i = 1, \ldots, r-1$; and

(3) $(\bigcup_{1 \leqslant j \leqslant r} E_j^{(r)}) \bigcup (\bigcup_{\ell \in I} Y_\ell^{(r)}) = [(g_{r-1} \circ \cdots \circ g_0)^{-1}(Y)]_{red}$ has only normal crossings in X_r . In particular all $Y_\ell^{(r)}, \ell \in I$, are nonsingular.

Now we set $X = X_r$ and $h = g_{r-1} \circ \cdots \circ g_0$.
The *numerical data of the resolution* (X, h) *for* Y are defined as follows.

For all irreducible components E of $(h^{-1}Y)_{red}$ (i.e. for all $E_j^{(r)}, 1 \leqslant j \leqslant r$, and all $Y_\ell^{(r)}$), let N be the multiplicity of E in the divisor of $f \circ h$ on X, and let $\nu - 1$ be the multiplicity of E in the divisor of $h^*(dx_1 \wedge \cdots \wedge dx_{n+1})$ on X. We have $N, \nu \in \mathbb{N}_0$; and if Y is reduced, then all $Y_\ell^{(r)}$ have numerical data $(N, \nu) = (1, 1)$.

§2. CHANGES ON AN EXCEPTIONAL VARIETY DURING THE RESOLUTION PROCESS.

From now on we fix one $j \in \{1, \ldots, r\}$ and drop the j-indices, i.e. we set $E^{(i)} = E_j^{(i)}$ for all $i = j, \ldots, r$ and $(N, \nu) = (N_j, \nu_j)$.

We describe how the exceptional variety E_j and its intersections with other exceptional varieties and with the strict transform of Y change by the blowing-ups g_i, $j \leqslant i < r$. So we fix one such $g_i : X_{i+1} \longrightarrow X_i$ and set during this section $g = g_i$ and $D = D_i$.

Since $E^{(i)}$ has normal crossings with D we have the following important fact (see e.g. [1,p.605]).

(1) The restriction $g' : E^{(i+1)} \longrightarrow E^{(i)}$ of g to $E^{(i+1)}$ is the blowing-up of $E^{(i)}$ with (nonsingular) center $D \cap E^{(i)}$.

Note that $D \cap E^{(i)}$ can eventually be reducible. The total blow-up of $E^{(i)}$ with center $D \cap E^{(i)}$ can then be considered as the result of consecutive blowing-ups of $E^{(i)}$ with centers the irreducible components of $D \cap E^{(i)}$.

Let E^* denote the exceptional divisor of the blowing-up g' and $\bar{Z}$ the strict transform in $E^{(i+1)}$ of any subscheme Z of $E^{(i)}$ by g'. Then

$$E^* = E_{i+1}^{(i+1)} \cap E^{(i+1)}, \tag{2}$$

and if $\operatorname{codim}(D \cap E^{(i)}, E^{(i)}) \geqslant 2$, we have

$$\begin{aligned} \overline{E_k^{(i)} \cap E^{(i)}} &= E_k^{(i+1)} \cap E^{(i+1)} \qquad \text{and} \\ \overline{(Y_k^{(i)} \cap E^{(i)})_{red}} &= (Y_k^{(i+1)} \cap E^{(i+1)})_{red}. \end{aligned} \tag{3}$$

The remaining situation $\operatorname{codim}(D \cap E^{(i)}, E^{(i)}) = 1$ occurs if and only if $D \subset E^{(i)}$ and $dim\, D = n - 1$. In this case we have that g' is an isomorphism making E^* correspond to D.

When D is not contained in respectively $(Y_k^{(i)} \cap E^{(i)})_{red}$ and $E_k^{(i)} \cap E^{(i)}$, the statement (3) above is still valid by the same argument.
Now if some irreducible component of $(Y_k^{(i)} \cap E^{(i)})_{red}$ is equal to D, then we can have *in a small enough neighbourhood of* E^* either

$$(4) \qquad Y_k^{(i+1)} \cap E^{(i+1)} = \emptyset \quad \text{or} \quad (Y_k^{(i+1)} \cap E^{(i+1)})_{red} = E^*.$$

If some irreducible component of $E_k^{(i)} \cap E^{(i)}$ is equal to D, then we have *in a small enough neighbourhood of* E^* always

$$(5) \qquad E_k^{(i+1)} \cap E^{(i+1)} = \emptyset.$$

§3. RELATIONS ASSOCIATED TO THE BLOWING-UPS OF AN EXCEPTIONAL VARIETY.

Fix again one blowing-up $g_i|_{E^{(i+1)}} : E^{(i+1)} \to E^{(i)}$ with $D_i \cap E^{(i)} \neq \phi$ and $codim(D_i \cap E^{(i)}, E^{(i)}) \geqslant 2$, and one irreducible component D of $D_i \cap E^{(i)}$. We will associate a relation between numerical data to the blowing-up g of $E_{(i)}$ with center D, which can be considered as a composition factor of $g_i|_{E^{(i+1)}}$. (Here we suppose g to be the first blowing-up in the decomposition of $g_i|_{E^{(i+1)}}$ into such factors.)

Let $E'_k, k \in T$, *be the reduced irreducible components of intersections of* $E^{(i)}$ *with other exceptional varieties* $E_t^{(i)}, 1 \leqslant t < i$, *or with components* $Y_\ell^{(i)}, \ell \in I$, *of the strict transform* $Y^{(i)}$ *of* Y. *According to the statements* (2) - (5) *of* §4, *the repeated strict transform of* E'_k *in* $E^{(r)}$ *by the consecutive* $g_\ell|_{E^{(\ell+1)}} : E^{(\ell+1)} \to E^{(\ell)}, i \leqslant \ell < r$, *is equal to some irreducible component of the intersection of* $E^{(r)}$ *with another component of* $(h^{-1}Y)_{red}$, *say with* $E_k^{(r)}$ *or* $Y_k^{(r)}$.
— *Furthermore* $E_k^{(r)}$ *is different from the corresponding* $E_i^{(r)}$ *and/or* $Y_\ell^{(r)}$ *if and only if the center of some* $g_\ell|_{E^{(\ell+1)}} : E^{(\ell+1)} \to E^{(\ell)}, i \leqslant \ell < r$, *contains the repeated strict transform of* E'_k *in* $E^{(\ell)}$ *!* —

Let E'_e *denote the exceptional variety of the blowing-up* g. *Also the repeated strict transform of* E'_e *in* $E^{(r)}$ *by the other factors of* $g_i|_{E^{(i+1)}}$ *and the consecutive* $g_\ell|_{E^{(\ell+1)}} : E^{(\ell+1)} \to E^{(\ell)}, i+1 \leqslant \ell < r$, *is an irreducible component of the intersection of* $E^{(r)}$ *with some other exceptional variety, say with* $E_e^{(r)}$.
— *Again we have that* $E_e^{(r)}$ *is different from* $E_{i+1}^{(r)}$ *if and only if the center of*

some $g_\ell|_{E^{(\ell+1)}}$, $i+1 \leqslant \ell < r$, *contains the repeated strict transform of* E'_e *in* $E^{(\ell)}$! —

We have the following relation between the numerical data of $E^{(r)}, E_e^{(r)}$ *and* $E_k^{(r)}$ *or* $Y_k^{(r)}, k \in T$.
Set $\alpha_e = \nu_e - \frac{\nu}{N} N_e$ *and* $\alpha_k = \nu_k - \frac{\nu}{N} N_k$ *for* $k \in T$. *Then*

RELATION A.

$$\alpha_e = \sum_{k \in T} \mu_k(\alpha_k - 1) + d,$$

where $d = codim(D, E^{(i)}) \geqslant 2$ *and* $\mu_k, k \in T$, *is the multiplicity of the generic point of* D *on* E'_k.

§4. RELATIONS ASSOCIATED TO THE CREATION OF AN EXCEPTIONAL VARIETY.

Set from now on $E = E^{(j)}$, $D = D_{j-1}$, $\Pi = g_{j-1}|_E : E \longrightarrow D$ and $k = codim(D, X_{j-1})$.

Let $E'_i, i \in T$, *be the irreducible components of intersections of* E *with other exceptional varieties or with the strict transform of* Y. *The strict transform of* E'_i *in* $E^{(r)}$ *by the consecutive* $g_\ell|_{E^{(\ell+1)}} : E^{(\ell+1)} \longrightarrow E^{(\ell)}, j \leqslant \ell < r$, *is equal to some irreducible component of the intersection of* $E^{(r)}$ *with another irreducible component of* $(h^{-1}Y)_{red}$, *say with* $E_i^{(r)}$ *or* $Y_i^{(r)}$, *having numerical data* (N_i, ν_i). *As usual* $\alpha_i = \nu_i - \frac{\nu}{N} N_i$ *for* $i \in T$, *where* (N, ν) *are the numerical data of* E.

RELATION B1. *We have*

$$\sum_{i \in T} d_i(\alpha_i - 1) + k = 0,$$

where $d_i, i \in T$, *is the degree of the intersection cycle* $E'_i \cdot F$ *on* F *for a general fibre* $F \cong \mathbb{P}^{k-1}$ *of* $\Pi : E \longrightarrow D$ *over a point of* D.

When $Pic\, D$ is not trivial we have also

RELATION B2. *Let $d_i, i \in T$, be the degree of the intersection cycle $E_i' \cdot F$ on F for a general fibre $F \cong \mathbb{P}^{k-1}$ of Π over a point of D. When $d_i = 0$, let $E_i' = \Pi^* B_i$ with $B_i \in Pic\, D$. Then we have*

$$\sum_{\substack{i \in T \\ d_i \neq 0}} \frac{1}{k d_i^{k-1}} (\alpha_i - 1) \Pi_*(E_i'^k) + \sum_{\substack{i \in T \\ d_i = 0}} (\alpha_i - 1) B_i = K_D$$

in $Pic\, D$, where K_D is the canonical divisor on D.

Remark. Relation $B2$ should not be seen as an expression in $Pic\, D \otimes \mathbb{Q}$ buth just as a more elegant notation for the expression with integer coefficients, obtained by reducing to the same denominator.

Example 1.

When Y is a curve ($n = 1$), only blowing-ups with a point as center occur. We have $E \cong \mathbb{P}^1$ and, since all E_i' are points on $E, d_i = 1$ for $i \in T$. So we obtain the familiar relation

$$\sum_{i \in T} (\alpha_i - 1) + 2 = 0.$$

Example 2.

When Y is a surface ($n = 2$), we only need blowing-ups with a point or a nonsingular curve as center. If D is a point, then $E \cong \mathbb{P}^2$ and relation B1 is

$$\sum_{i \in T} d_i (\alpha_i - 1) + 3 = 0,$$

where $d_i, i \in T$, is the degree of the curve E_i' in E.
If D is a nonsingular curve, then E is a projective space bundle over D with fibres isomorphic to $\mathbb{P}^1$. Relation B1 is in this case

$$\sum_{i \in T} d_i (\alpha_i - 1) + 2 = 0,$$

where $d_i, i \in T$, is the number of intersections of the curve E_i' with a "general" fibre F of Π.

If moreover D is projective (when Y has no other than isolated singularities only such curves occur as center of blowing-ups), then relation B2 becomes a numerical relation by taking degrees in $Pic\, D$.

Let g denote the genus of D and $\kappa_i = \deg E_i'^2, i \in T$, the *self-intersection number of* E_i' in E. Then we get

$$\sum_{\substack{i \in T \\ d_i \neq 0}} \frac{\kappa_i}{2d_i}(\alpha_i - 1) + \sum_{\substack{i \in T \\ d_i = 0}} (\alpha_i - 1) = 2g - 2.$$

(When $E_i' = \Pi^* B_i$ we must have $\deg B_i = 1$ since E_i' is irreducible.)

REFERENCES

1. P. Griffiths and J. Harris, *Principles of Algebraic Geometry*, John Wiley and Sons.
2. H. Hironaka, *Resolution of singularities of an algebraic variety over a field of characteristic zero*, Ann. Math. **79** (1964), 109-326.
3. J. Igusa, *Complex powers of irreducible algebraic curves, in Geometry today,*, Giornate di Geometria, Roma 1984, Progress in Mathematics **68** (1985), 207-230, Birkhaüser.
4. F. Loeser, *Fonctions d'Igusa p-adiques et polynômes de Bernstein*, Amer. J. Math. **110** (1988), 1-21.
5. D. Meuser, *On the poles of a local zeta function for curves*, Inv. Math. **73** (1983), 445-465.
6. L. Strauss, *Poles of a two variable p-adic complex power*, Trans. Amer. Math. Soc. **278,2** (1983), 481-493.

VEYS WILLEM
K.U.LEUVEN
DEPARTEMENT WISKUNDE
CELESTIJNENLAAN 200-B
3030 LEUVEN
BELGIUM

Astérisque

AST

Abstract

Astérisque, tome 198-199-200 (1991), p. 405

<http://www.numdam.org/item?id=AST_1991__198-199-200__405_0>

The "Journées Arithmétiques" presents every two years a wide panorama on the state of the art in the Theory of Numbers. This book contains five reports : M. Laurent, On some recent results on transcendence ; N. Schappacher : The Beilinson conjectures for elliptic curves ; J.-P. Serre : Motives ; C. Soulé : Arakelov Geometry and transcendantal number theory ; M. Tsfasman : Global fields, codes and sphere packings. Moreover twenty-six communications are included.