Astérisque

MICHAEL ATIYAH

The Jones-Witten invariants of knots

Astérisque, tome 189-190 (1990), Séminaire Bourbaki,
exp. n° 715, p. 7-16

<http://www.numdam.org/item?id=SB_1989-1990__32__7_0>

© Société mathématique de France, 1990, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Séminaire BOURBAKI novembre 1989
42ème année, 1989-90, n° 715

THE JONES-WITTEN INVARIANTS OF KNOTS

par **Michael ATIYAH**

1. INTRODUCTION

One of the most remarkable developments of recent years has been the work initiated by Vaughan Jones [2] [3] on knot invariants. This has all the hallmarks of great mathematics. It produces simple new invariants which solve classical problems and it involves a very wide range of ideas and techniques from practically all branches of mathematics and physics. Here is a list of the areas which have been significantly involved in the theory up to the present : combinatorics, group representations, algebraic geometry, differential geometry, differential equations, topology, Von Neumann algebras, statistical mechanics, quantum field theory. Moreover the subject continues to develop rapidly and a final picture has not yet emerged.

Given this very wide field I have to be very selective for a one-hour presentation. I will concentrate on some aspects and I shall have to omit all the technicalities. Moreover, to shorten the exposition, I will discuss only the simplest case of the theory. Fuller accounts can be found in the papers of Vaughan Jones [3] and Witten [9].

In 1984 Vaughan Jones surprised the experts in knot theory by producing a *polynomial invariant*, now known as the Jones polynomial $V(q)$, which was superficially similar to the classical Alexander polynomial but was, in essential features, rather different. In particular $V(q)$ could distinguish (some) knots from their mirror images. For this and other reasons $V(q)$ turned out to be a very effective tool in knot theory and, as a result, old conjectures of P.G. Tait from the 19th century have now been

established.

The Jones polynomial can be profitably studied from many angles and it has been generalized in several ways to produce further knot invariants. Much of this work has involved important ideas from theoretical physics, essentially physics of 2 dimensions. However a major break-through came in 1988 when Witten [10] gave a simple interpretation of the Jones polynomial in terms of 3-dimensional physics. These ideas of Witten are based on a heuristic use of the Feynman integral, but they lead to very explicit results and calculations which can be verified by alternative rigorous methods. A full mathematical treatment of Witten's theory has yet to appear, so my account has to be somewhat sketchy and incomplete.

Not only does Witten's theory provide a physical "meaning" for the Jones invariants but it also extends them to knots in an arbitrary compact oriented 3-manifold. This is a major generalization which had been attempted unsuccessfully via other methods. Finally, and most significantly, Witten's generalization allows us to define "relative invariants", for 3-manifolds with boundary. In this case the invariants are not numbers but take their values in a vector space associated with the boundary. This facility, of allowing manifolds with boundary, makes the theory much more flexible and greatly facilitates computation, even for the "absolute" case of closed 3-manifolds. The situation may roughly be compared with the story of Lefschetz numbers in classical topology. The number of fixed points of a self-map (analogous to the Jones invariant of a knot) re-interpreted as the Lefschetz number, through the induced map on homology, becomes part of a larger theory (analogous to Witten's theory) and hence more computable.

In the next section I will summarize the key features of the Jones polynomial, before going on in section 3 to describe Witten's theory. In section 4 I will outline the way in which Witten's theory may be developed mathematically. I will make no attempt in this presentation to give the physical interpretation via Feynman integrals. For this I refer to Witten's papers [9] [10]. For a general survey of "topological quantum field theories" see also [1] [8].

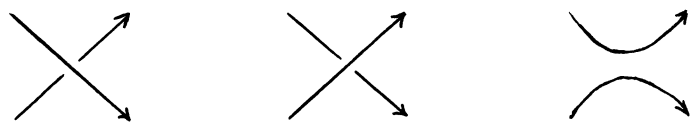
2. THE JONES POLYNOMIAL

We shall deal with oriented knots and links. These are just oriented 1-dimensional submanifolds of the 3-space S^3 : a knot being the case of one component. For an oriented link L the Jones polynomial $V_L(q)$ is a finite Laurent series in the variable $q^{\frac{1}{2}}$ with integer coefficients. Its first basic properties are :

(2.1) $V_L(q) = 1$ when L in the standard unknotted circle,

(2.2) $V_{L^\star}(q) = V_L(q^{-1})$ where $L^\star$ is the mirror image of L .

$V_L(q)$ can be characterized by a *skein relation.* For this we consider a generic plane projection of L , so that all crossing points have just 2 branches, one "over" and one "under". Focussing attention on one crossing point we can then consider the 3 versions of L obtained by allowing the 3 different possibilities as shown below :



L_+ L_- L_0

The skein relation for $V_L(q)$ is the linear relation :

$$q^{-1}V_{L_+}(q) - qV_{L_-}(q) = (q^{\frac{1}{2}} - q^{-\frac{1}{2}})\, V_0(q) \tag{2.3}$$

It is not hard to show that (2.1) and (2.3) uniquely determine $V_L(q)$. The difficulty is to prove consistency, *i.e.* that $V_L(q)$ depends on the link L (up to isotopy) and not on any particular plane projection.

Note.- In fact $V_L(q)$ does not depend on the orientation of L . However this is not true for the generalizations of $V_L(q)$, except that reversing the orientation of *all* components of L will always preserve the generalized Jones polynomials.

Example.- For a (right-handed) trefoil knot $V(q) = -q^4 + q^3 + q$. By (2.2) this distinguishes it from its mirror image, the left-handed trefoil.

Although it is possible to verify the consistency of (2.3) by direct combinatorial methods this is not very enlightening. A better approach, explained in [3], is based on the use of *braids*.

The Artin braid group on n strands B_n can be defined as the fundamental group of the configuration space C_n of n unordered distinct points in the plane. There is an elementary geometric construction which assigns to any braid β an oriented link $\hat{\beta}$ in S^3 . All links arise in this way and the equivalence relation on the union of all B_n given by

$$\beta_1 \sim \beta_2 \Longleftrightarrow \widehat{\beta_1} \text{ isotopic to } \widehat{\beta_2}$$

is explicitly known. Thus one may construct link invariants from suitable braid invariants.

To get the right braid invariants to produce $V_L(q)$, Jones introduces certain representations $\rho_\lambda(q)$ of B_n .

These are representations depending on a parameter q and a partition λ of n . For $q = 1$ they reduce to the irreducible representations ρ_λ of the symmetric group S_n pulled back to B_n via the natural homomorphism $B_n \to S_n$. The representations $\rho_\lambda(q)$ come from representations of the Hecke algebra.

The Jones polynomial $V_L(q)$ for $L = \hat{\beta}$ is now defined as a certain linear combination of the characters of $\rho_\lambda(q)$ evaluated at β . The only partitions λ which are needed here are the partitions of n into (at most) 2 parts.

Note.- For generalizations of $V_L(q)$ one needs all partitions of n . These generalizations lead to polynomials satisfying suitable generalizations of (2.3).

In this braid group approach to the Jones polynomial it is still a mystery why suitable linear combinations of the characters $\rho_\lambda(q)$ should give link invariants. The underlying reason becomes clear in Witten's theory as we shall see.

3. THE WITTEN THEORY

Witten considers oriented links L in an arbitrary compact oriented 3-manifold Y . Moreover both Y and L are assumed to be *framed.* For Y this means we fix a trivialization of the tangent bundle while for L it means that we fix a trivialization of its normal bundle in Y . In both cases only the homotopy class of the pairing will be significant.

Witten's invariant of the pair (Y, L) is a complex valued function of a positive integer k : we denote it by $W_{Y,L}(k)$. There are two extreme cases of special interest:

i) $Y = S^3$.

ii) $L = \phi$.

In the first case when $Y = S^3$ there are standard choices (up to homotopy) for the framing of Y and of any link L . The standard framing on Y is the one which when stabilized (by adding trivial bundles) extends to the interior 4-ball. The standard framing of L is characterized by the property that each component L_j of L has zero linking number with the "parallel" copy L'_j we get by using the framing. With these standard choices of framing the Witten invariant now depends only on the oriented link L . It is related to the Jones polynomial $V_L(q)$ by the formula :

$$W_{S^3,L}(k) = V_L(exp\ \frac{2\pi i}{k+2}) \ . \tag{3.1}$$

This shows that the Witten invariant in this case determines, and is essentially equivalent to the Jones polynomial. Thus Witten's invariant for general Y is indeed a generalization of the Jones invariant.

Case ii) when there is no link leads to an invariant $W_Y(k)$ for an oriented 3-manifold Y . Witten's invariant is naturally normalized so that (for a suitable framing) $W_Y(k) = 1$ for $Y = S^1 \times S^2$. On the other hand the formula for $Y = S^3$ is less trivial, namely

$$W_{S^3}(k) = \sqrt{|\ \frac{2}{k+2}\ sin\ \frac{\pi}{k+2}} \ . \tag{3.2}$$

As mentioned in section 1, Witten's invariant also extends to a "relative" invariant when Y is a 3-manifold with boundary Σ . We assume in

this situation that the 1-manifold L meets the boundary transversally in a finite set of points $\partial L = \mathcal{P} = (P_1, \ldots, P_n)$. The framings on Y, L induce a *stable framing* on Σ and a *normal framing* of each point P_i on Σ (*warning* : we do not at present allow homotopies of these framings).

Witten's relative theory assigns a finite-dimensional complex vector space $H_k(\Sigma, \mathcal{P})$ to each such framed pair $(\Sigma, \mathcal{P})$ and each positive integer k . Reversing the orientation of Σ (and using the natural corresponding framings) converts H into its dual *i.e.*

$$H_k(\Sigma^\star, \mathcal{P}) = H_k^\star(\Sigma, \mathcal{P}) \ . \tag{3.3}$$

Moreover these vectors spaces are *multiplicative* in the sense that for the disjoint sums :

$$H_k(\Sigma_1 \cup \Sigma_2 \ , \ \mathcal{P}_1 \cup \mathcal{P}_2) = H_k(\Sigma_1, \mathcal{P}_1) \otimes H_k(\Sigma_2, \mathcal{P}_2) \ . \tag{3.4}$$

If now

$$\partial(Y, L) = (\Sigma, \mathcal{P}) \ ,$$

then Witten's relative invariant is a vector

$$W_k(Y, L) \in H_k(\Sigma, \mathcal{P}) \ . \tag{3.5}$$

These vector spaces and invariants have various naturality properties which we shall not describe, but the key property is the relation between relative and absolute invariants. Of course if Y is closed so that Σ is empty then formally we want the relative and absolute invariants to coincide and this requires

$$H_k(\phi, \phi) = C \ . \tag{3.6}$$

The significant case however is when we cut a closed 3-manifold Y (and link L) into two parts along a common surface Σ . Thus

$$\begin{aligned} &Y = Y_1 \cup Y_2 \quad \text{along} \quad \Sigma : \quad \partial Y_1 = \Sigma \ , \ \partial Y_2 = \Sigma^\star, \\ &L = L_1 \cup L_2 \quad \text{along} \quad \mathcal{P}. \end{aligned}$$

The vectors

$$W_k(Y_1, L_1) \quad , \quad W_k(Y_2, L_2)$$

then lie in dual spaces (by (3.3)), so that this scalar product is well-defined. The key fact is then

$$W_k(Y, L) = \langle W_k(Y_1, L_1), W_k(Y_2, L_2) \rangle \ . \tag{3.7}$$

By decomposing Y in various ways one can use the relative invariants to help calculate the absolute invariants. In particular (3.7) implies the existence of a skein relation for the absolute invariant when $Y = S^3$. For this one has to know that, for S^2 with 4 points $P_1, \dots P_4$,

$$\dim H_k(S^2, P_1, \dots P_4) = 2 \ . \tag{3.8}$$

Now apply (3.7) with Y_1 a small ball in the neighbourhood of a crossing point of the link L (viewed as nearly planar). Keeping L_2 fixed but taking the 3 possible choices of L_1 (joining the P_i in pairs) we get 3 different vectors in the 2-dimensional space of (3.8). These must satisfy a linear relation (with coefficients independent of L). Taking the scalar product with the vector (in the dual space) coming from (Y_2, L_2) and applying (3.7) we deduce the existence of a skein relation. In this way, once the coefficients have been determined, Witten can identify his absolute invariant with that of Jones as asserted in (3.1).

If we take $Y = \Sigma \times I$, $L = \mathcal{P} \times I$ (with I the unit integral) and use (3.3) and (3.4) we see that $W_k(Y, L)$ can be viewed as an *automorphism* of $H_k(\Sigma, \mathcal{P})$. This depends on framings of (Y, L) *i.e.* on *homotopies* of framings for $(\Sigma, \mathcal{P})$. In fact all such automorphisms are scalar multiplications and depend only on the initial and final framings. The computation of these scalars is an important but delicate part of the theory.

If we ignore scalar factors and replace the vector space $H_k(\Sigma, \mathcal{P})$ by the associated projective space its functorial properties provide an action on it of the group of components of $Diff^+(\Sigma, \mathcal{P})$, the orientation preserving diffeomorphisms of Σ preserving $\mathcal{P}$.

In particular when $\Sigma = S^2$ these are essentially the representations of the braid group arising from the Hecke algebra which Jones employs to get his invariants.

4. MODULI SPACES

Witten defines his theory heuristically by a Feynman integral. This is not rigorous but it does lead to a rigorous theory of the vector spaces $H_k(\Sigma, \mathcal{P})$ which I will now describe.

For simplicity consider first the case when $\mathcal{P} = \phi$, so that we simply have a surface Σ with no marked points. To construct $H_k(\Sigma)$ we first pick a *complex structure* τ on Σ : denote the resulting Riemann surface by Σ_τ . We can then define the moduli space $M(\Sigma_\tau)$ of holomorphic $SL(2, C)$-bundles over Σ_τ . This is a projective variety with a Zariski open set representing *stable* vector bundles, and has been much studied by algebraic geometers [4]. It has an ample generating line-bundle L and we define

$$H_k(\Sigma_\tau) = H^0(M(\Sigma_\tau), L^k)$$

to be the space of holomorphic sections of L^k . This is of course a standard construction in algebraic geometry. What is not so obvious from this point of view, is that *the projective space* of $H_k(\Sigma_\tau)$ *is essentially independent of the complex structure* τ.

More precisely by allowing τ to vary over Teichmüller space we get a holomorphic vector bundle and this bundle has a natural connection whose curvature is a scalar. This shows in particular that the group of components of $Diff^+(\Sigma)$ acts on the associated projective space of covariant constant sections.

The second essential ingredient in the Witten theory is the construction of the vector $W_k(Y) \in H_k(\Sigma)$ when $\partial Y = \Sigma$. There is no way known at present which is both simple and rigorous. A rigorous procedure is to use a sequence of elementary surgeries (or a Morse function) and to build $W_k(Y)$ from these elementary steps. One then has to verify that the result is independent of the surgeries (or Morse functions) chosen.

If we use a Morse function then we are reduced to studying the behaviour of the vector spaces $H_k(\Sigma_\tau)$ as $\tau \to \tau_0$, the complex structure of a singular Riemann surface with ordinary double points. It can be shown that the vector bundle formed by the $H_k(\Sigma_\tau)$ extends over τ_0 and the sub-

space preserved (up to scalars) by the local monodromy of the connection can be identified with $H_k(\Sigma_0)$ where Σ_0 is the desingularization of Σ_{τ_0} .

The homomorphism $H_k(\Sigma_0) \to H_k(\Sigma_\tau)$ is then the vector associated by (3.5) to a 3-manifold Y with $\partial Y = \Sigma_\tau - \Sigma_0$.

The framings on Y, Σ which I have been ignoring at this stage are needed to replace the projective spaces by vector spaces.

For the general case of surfaces Σ with marked points all this theory extends in a natural way. The moduli space $M(\Sigma_\tau)$ has a natural generalization to a moduli space $M(\Sigma_\tau, \mathcal{P})$, using bundles with parabolic structures at the marked points in the sense of Seshadri [6].

Much of the literature on this topic is to be found in papers on *rational conformal field theory*, and the spaces $H_k(\Sigma, \mathcal{P})$ above are referred to as the spaces of conformal blocks. A rigorous mathematical treatment in this framework is given in [7].

A different and more differential-geometric approach is being developed by Axelrod, Witten and Hitchin, but these versions have not yet appeared.

A verification that Witten's invariants of 3-manifolds are well-defined has been given by Reshetikin and Turaev [5], using surgery techniques (the Kirby calculus).

Finally I should recall that I have implicitly just been describing the simplest case of the Witten-Jones theory. In general one picks a compact Lie group G and an irreducible representation V . I discussed only the case $G = SU(2)$, $V = C^2$ (note that $V = V^\star$ which need not hold in general). The theory extends to the more general case without serious modification. In particular the relevant moduli spaces are still well-defined.

REFERENCES

[1] M.F. ATIYAH - *Topological quantum field theories*, Publ. Math. I.H.E.S. 68 (1989), 175-186.

[2] V.F.R. JONES - *A polynomial invariant for knots via von Neumann algebras*, Bull. Amer. Math. Soc., 12 (1985), 103-111.

[3] V.F.R. JONES - *Hecke algebra representations of braid groups and link polynomials*, Ann. of Math. 126 (1987), 335-388.

[4] M.S. NARASIMHAN and C.S. SESHADRI - *Stable and unitary vector bundles on a compact Riemann surface*, Ann. of Math. 82 (1965), 540-567.

[5] N. RESHETIKIN and V. TURAEV - *Invariants of 3-manifolds via link polynomials and quantum groups*, (to appear)

[6] C.S. SESHADRI - *Moduli of vector bundles with parabolic structures*, Bull. Amer. Math. Soc. 83 (1977).

[7] A. TUSCHIYA, K. UENO and Y. YAMADA - *Conformal field theory on universal family of stable curves*, (to appear).

[8] E. WITTEN - *Geometry and quantum field theory*, Lecture at Centennial meeting of A.M.S., August 1988.

[9] E. WITTEN - *Quantum field theory and the Jones polynomial*, Commun. Math. Phys. 121 (1989), 351-399.

[10] E. WITTEN - *Some geometrical applications of quantum field theory*, Proc. International congress on Mathematical Physics, Swansea 1988, 77-116.

Sir Michael ATIYAH

The Master's Lodge
Trinity College
GB-CAMBRIDGE CB2 1TQ
(England)

Astérisque

PIERRE CARTIER

Développements récents sur les groupes de tresses. Applications à la topologie et à l'algèbre

Astérisque, tome 189-190 (1990), Séminaire Bourbaki,
exp. n° 716, p. 17-67

<http://www.numdam.org/item?id=SB_1989-1990__32__17_0>

© Société mathématique de France, 1990, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Séminaire BOURBAKI Novembre 1989
42ème année, 1989-90, n° 716

DÉVELOPPEMENTS RÉCENTS SUR LES GROUPES DE TRESSES APPLICATIONS À LA TOPOLOGIE ET À L'ALGÈBRE

par **Pierre CARTIER**

A mes amis soviétiques retrouvés grâce à la "perestroïka"

0. INTRODUCTION

Les nœuds, ouverts ou fermés, les rubans, les tresses, les cables,$\cdots$ se prêtent à des jeux sans fin. Les applications sérieuses ne manquent pas non plus : cablages électriques, modèles de mécanique des fluides faisant revivre la vieille théorie des tourbillons de Descartes$\cdots$. Dès le siècle dernier, Tait et Thompson, après Cayley, se sont intéressés à ces structures combinatoires. Mais il a fallu attendre le début de ce siècle, avec les travaux de Dehn sur la Topologie, pour obtenir les premiers résultats généraux et rigoureux.

C'est en 1925 qu'Émile Artin [A1] fonde la théorie des tresses. Conformément aux tendances de l'Algèbre allemande contemporaine, il cherche — et réussit avec éclat — comment introduire des groupes adéquats dans le sujet. Aujourd'hui, la définition la plus simple du groupe B_n des tresses à n brins est la suivante : considérons une variété connexe M de dimension d ; *l'espace de configuration* est l'espace des parties finies d'ordre n dans M ; on le note $\Phi_n(M)$. On peut le considérer comme l'espace-quotient $M_*^n / \mathbf{S}_n$, où M_*^n est l'ensemble des suites (numérotées) de n points distincts $x_1, \cdots, x_n$ de M , et où le groupe symétrique $\mathbf{S}_n$ agit par permutation des n points. Le groupe de tresses généralisées est le groupe fondamental $B_n(M)$ de l'espace $\Phi_n(M)$. Lorsque l'on a $d \geq 3$, ce groupe est le produit semi-direct de $\mathbf{S}_n$ et de $\pi_1(M)^n$; cela provient de ce que

M^n_* diffère de M^n par des sous-variétés de codimension ≥ 3 , donc a même groupe fondamental que M^n . Lorsque $d = 1$, considérons seulement le cas $M = \mathbf{R}$; alors $\Phi_n(M)$ est l'ouvert de $\mathbf{R}^n$ formé des points $(x_1, \cdots, x_n)$ tels que $x_1 < \cdots < x_n$, et l'on a $B_n(M) = 0$. Le seul cas intéressant est celui de la dimension d égale à 2. *Le groupe d'Artin est* $B_n = B_n(\mathbf{R}^2)$.

La définition précédente a été introduite par Neuwirth et Fox [A6] en 1962 ! En 1925, Artin avait donné les propriétés de base des groupes B_n au moyen d'arguments de nature combinatoire, en partie heuristiques. Il reviendra de manière plus rigoureuse sur le sujet dans ses articles [A1] de 1947. Rétrospectivement, les arguments d'Artin deuxième manière sont des manipulations sur la suite exacte d'homotopie des fibrés. Encore aujourd'hui, ces sujets de Topologie se divisent *grosso modo* en deux catégories :

— des arguments combinatoires ;

— des théorèmes difficiles (lemme de Dehn, théorème de Markov, théorèmes de Cerf et Kirby) qui permettent en général de montrer qu'une équivalence d'un certain type entre objets géométriques se ramène à une chaîne finie d'équivalences élémentaires.

La difficulté de ces derniers théorèmes est l'un des nombreux avertissements que notre description mathématique du continu n'est peut-être pas adéquate.

L'étude des espaces de configuration est un sujet actif en Topologie ; elle est menée en particulier au Japon et au Viet-Nam (autour de Huynh Mui). Mais les groupes de tresses B_n restaient une curiosité isolée avant 1970. Le réveil a eu plusieurs causes :

a) Arnold s'est intéressé à l'étude des *singularités* et de leur déploiement. Un exemple typique est l'étude des polynômes de degré n à racines simples, soient $P(z) = z^n + a_1 z^{n-1} + \cdots + a_n$; l'hypothèse de simplicité se traduit par la non-nullité du discriminant de P , vu comme polynôme $D(a_1, \cdots, a_n)$ en ses coefficients. Arnold a calculé la cohomologie du complémentaire dans $\mathbf{C}^n$ de l'hypersurface d'équation $D = 0$, espace dont le groupe fondamental est B_n. Un peu plus tard, Brieskorn a généralisé cette étude à certains cas de complémentaires d'une famille finie d'hyperplans (le cas d'Arnold correspond à la famille des hyperplans d'équation $z_i = z_j$ dans $\mathbf{C}^n$ muni des coordonnées $z_1, \cdots, z_n$). Dans ces

exemples, *les groupes de tresses* (et certaines de leurs généralisations) *apparaissent comme groupes de monodromie* ; il appartenait à Zamolodchikov [F9] et Kohno [F3] d'étudier les équations différentielles admettant des singularités polaires liées à ces configurations. Celles-ci fournissent des exemples assez simples où tester les théories générales de l'homotopie rationnelle et de la monodromie (voir mes deux exposés précédents [E5] et [F1]). Par ailleurs, l'étude des théories des champs quantiques conformes a récemment conduit Tsuchiya et Kanie [F11] à l'étude systématique de fonctions de plusieurs variables complexes ayant ce type de ramification.

b) Vers 1968, Iwahori a introduit sous le nom d'*algèbres de Hecke* des déformations $\mathcal{H}_n(q)$ de l'algèbre $\mathbf{C}\,\mathbf{S}_n$ du groupe symétrique (et d'autres groupes similaires). De telles algèbres jouent un rôle important dans l'étude des représentations linéaires des groupes finis simples et des groupes algébriques réductifs sur un corps p-adique (Iwahori, Matsumoto, Tits). Les représentations irréductibles des algèbres $\mathcal{H}_n(q)$ ont été déterminées explicitement par Hoefsmit en 1974 dans [C17] ; les résultats s'insèrent dans le courant actuel de la Combinatoire où l'on étudie les *q-analogues des nombres classiques* (par exemple le polynôme de Gauss $\begin{bmatrix} n \\ i \end{bmatrix}_q$ qui pour $q = 1$ redonne le coefficient binomial $\binom{n}{i}$). On n'avait guère prêté attention au fait que les représentations de $\mathcal{H}_n(q)$ fournissent de nouvelles représentations du groupe de tresses B_n , jusqu'à la découverte fracassante, en 1984, du *polynôme de Jones associé à un nœud.* Ce polynôme a été aussitôt interprété comme une trace associée aux représentations de B_n fournies par l'algèbre $\mathcal{H}_n(q)$ par Jones lui-même [C3, C5] et par Ocneanu [C8].

c) *En Mécanique Statistique*, l'étude de certains modèles, comme le modèle de Potts, conduit à des algèbres apparentées aux algèbres $\mathcal{H}_n(q)$ et appelées *algèbres de Temperley-Lieb* ; elles peuvent servir de point de départ à la construction du polynôme de Jones. Mais, plus important, on a peu à peu découvert l'importance de la *relation de Yang-Baxter*, dont l'une des formes

$$\hat{R}_{12}\,\hat{R}_{23}\,\hat{R}_{12} = \hat{R}_{23}\,\hat{R}_{12}\,\hat{R}_{23} \tag{YB}$$

est très proche de l'une des relations qui servent de définition au groupe B_n. Toute solution de cette équation fournit automatiquement une représenta-

tion du groupe B_n, et de plus les modèles de Mécanique Statistique fournissent des solutions explicites de l'équation (YB). Turaev [D13] a montré comment retrouver tous les invariants polynomiaux des nœuds par cette méthode. V. Jones [G10] et L. Kauffman [G3] ont clairement montré que *la combinatoire des tresses et des nœuds est intimement liée à celle de modèles de Mécanique Statistique.* On pourra consulter le travail de Turaev [D13] pour voir comment tous ces invariants sont obtenus comme cas particulier de la méthode des solutions de Yang-Baxter.

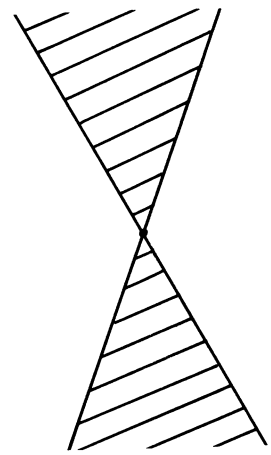
d) Drinfeld [D2] a introduit en 1986 sous le nom de "groupes quantiques" une nouvelle classe d'algèbres de Hopf. À chaque groupe de Lie semi-simple complexe G est attaché un groupe quantique G_q , et chaque représentation linéaire de G se "déforme" en une représentation de G_q , qui fournit *ipso facto* une solution de l'équation de Yang-Baxter [Rosso D7]. Il est remarquable qu'en fait *un groupe quantique soit entièrement déterminé par la catégorie de ses représentations* ; il s'agit là d'une généralisation de la dualité de Tannaka-Krein pour les groupes compacts. Mais on doit à Drinfeld, Reshetikhin et Turaev (et indépendamment à Freyd, Yetter et leurs collaborateurs) la profonde remarque que *la combinatoire des tresses et celle des nœuds se traduit dans le langage des catégories* en exploitant les relations de cohérence introduites par Mac Lane [B1]. Il s'agit là de l'idée, souvent défendue par Grothendieck en particulier, que les catégories sont des objets géométriques bien adaptés à l'étude de l'homotopie.

Tous les thèmes précédents semblent étroitement liés les uns aux autres, comme nous essaierons de le montrer dans cet exposé. La théorie est cependant encore très mouvante, et une synthèse définitive semble prématurée.

Pour terminer cette introduction, nous dirons quelques mots de deux autres thèmes dont chacun mériterait un exposé en propre.

La théorie quantique des champs a fait d'énormes progrès récents dans l'étude des *modèles à* 2 *ou* 3 *dimensions* d'espace-temps : théorie des champs conformes, théorie des cordes. Il se peut que la clé des phénomènes de supraconductivité à "haute température" soit à trouver là. Comme J. Fröhlich l'a remarqué dans [H2] et [H3], les arguments classiques qui permettent de lier le spin à la statistique (principe d'exclusion de Pauli) perdent leur

validité en dimension 2. La raison en est que le double cône d'influence



d'un point cesse d'avoir *un complémentaire connexe* et qu'on peut alors intrinsèquement distinguer "gauche" et "droite". Au lieu de faire intervenir seulement les deux représentations ρ de degré 1 du groupe $\mathbf{S}_n$, distinguant le cas des *bosons* ($\rho(s) = 1$) de celui des *formions* ($\rho(s) =$ signature de s), on doit considérer les représentations du groupe B_n agissant dans l'espace de Hilbert correspondant à n particules. On rejoint là l'étude faite par Tsuchiya et Kanie [F11] de la monodromie des "fonctions à n points" de la théorie, qui jouent le rôle de moments d'une mesure sur un espace fonctionnel.

En théorie des nombres, une question ouverte — et fondamentale — est de prouver que *tout groupe fini G est le groupe de Galois d'une extension finie L du corps* $\mathbf{Q}$ *des nombres rationnels.* Cela revient à étudier la structure du groupe de Galois $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$. Fixons un entier $n \geq 1$; le groupe de tresses B_n se réalise comme un groupe d'automorphismes du groupe libre F_n ; géométriquement, cela revient à considérer F_n comme le groupe fondamental de $\mathbf{C}\backslash S$, où S est une partie finie à n éléments de $\mathbf{C}$. Si l'on suppose que S se compose de nombres rationnels, le groupe de Galois de la plus grande extension du corps de fractions rationnelles $\bar{\mathbf{Q}}(t)$ non ramifiée en dehors de S est le complété profini $\hat{F}_n$ de F_n . On peut plonger B_n dans le groupe des automorphismes de $\hat{F}_n$; soit $\hat{B}_n$ son adhérence dans

$Aut(\hat{F}_n)$. Le groupe de Galois $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ agit aussi dans $\hat{F}_n$, et l'on peut montrer qu'on définit ainsi un *homomorphisme injectif* ψ_S *de* $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ *dans le groupe de tresses complété* $\hat{B}_n$. C'est là l'esquisse du programme de Grothendieck [I1] pour l'étude du groupe de Galois. Nous renvoyons à la bibliographie pour les travaux de Ihara, Oda, Deligne... sur ce sujet.

Remerciements : Ils vont aux organisateurs et aux participants du Colloque d'Ascona (octobre 1989) sur "Géométrie et Théorie quantique des champs". En particulier, je remercie Semenov-Tian-Shansky, Reshetikhin, Wasserman pour des entretiens approfondis et aussi Maillet qui m'a grandement aidé dans la collecte des documents. Je remercie aussi Jones et Freyd pour leurs commentaires vigilants sur cette introduction, et M. Gallois pour une relecture attentive.

1. RAPPELS SUR LES NŒUDS ET LES TRESSES

1.1. On appelle *nœud* dans l'espace euclidien $\mathbf{R}^3$ toute partie fermée de $\mathbf{R}^3$ homéomorphe au cercle $\mathbf{S}^1$; un *entrelac* est la réunion d'un nombre fini de nœuds deux à deux disjoints. Il est commode de rajouter un point à l'infini à $\mathbf{R}^3$, et de raisonner dans l'espace $\mathbf{S}^3$ obtenu, homéomorphe à une sphère à 3 dimensions. Nous orienterons l'espace $\mathbf{S}^3$, ainsi que les nœuds et entrelacs considérés.

On dira que *deux entrelacs* L *et* L' (en particulier deux nœuds) *sont équivalents s'il existe un homéomorphisme de* $\mathbf{S}^3$ *transformant* L *en* L' *et respectant les orientations de* L , L' *et* $\mathbf{S}^3$. Le groupe des homéomorphismes orientés de $\mathbf{S}^3$ sera muni de la convergence uniforme ; il est connexe par arcs. Par suite, si deux entrelacs L et L' sont équivalents, il existe une *isotopie* transformant L en L' , c'est-à-dire une application continue[1] h : $I \times \mathbf{S}^3 \to \mathbf{S}^3$ avec les propriétés suivantes :

a) on a $h(0,x) = x$ pour x dans $\mathbf{S}^3$;

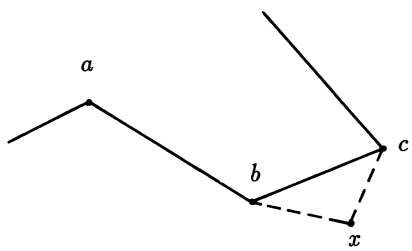
b) pour tout t dans I , l'application $h_t : x \mapsto h(t,x)$ est un homéomorphisme de $\mathbf{S}^3$;

[1] On note I l'intervalle $[0,1]$ de $\mathbf{R}$.

c) L' est l'image de L par l'application h_1 .

On parle d'*isotopie ambiante* pour les entrelacs, car tout l'espace $\mathbf{S}^3$ se déforme de manière à entraîner L vers L' . Une déformation de L en L', au moyen d'une famille continue d'entrelacs, donnerait une équivalence trop faible.

Il existe des nœuds sauvages, découverts par Fox et Artin ; pour les éviter, nous ne considérerons que des nœuds qui sont équivalents à des lignes polygonales, formées de segments de droites. Les entrelacs sont restreints de même. On peut montrer que si deux nœuds polygonaux L et L' sont équivalents, on peut passer de L à L' par des opérations élémentaires du type décrit ci-dessous, et leurs inverses (en nombre fini)

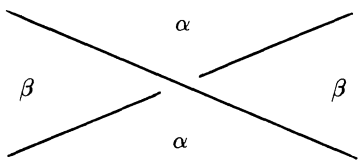


la modification remplace le segment bc par la réunion de bx et xc .

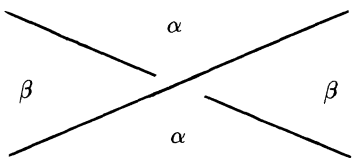
1.2. Pour décrire les entrelacs, on utilise une *projection plane*. Quitte à remplacer un entrelac L par un entrelac équivalent, on peut supposer que la projection orthogonale de L sur un plan P est une réunion de courbes différentiables, avec pour seules singularités des points de croisement doubles avec tangentes distinctes. À chaque croisement, on doit indiquer laquelle des deux branches est au-dessus de l'autre ; compte tenu des orientations, on a les deux dispositions suivantes :

On a indiqué l'indice du croisement égal à $+1$ ou -1 .

A une telle projection D , on associe un *graphe planaire* T , qui ne prend pas en compte les orientations : le complémentaire de D dans le plan P a un nombre fini de composantes connexes qu'on peut colorier avec deux couleurs α et β de telle manière que deux régions qui bordent un même arc de courbe aient des couleurs distinctes. Chacune de ces régions de couleur α définit un sommet de T , et les points de croisement définissent des arêtes de T joignant les deux régions α adjacentes ; chaque arête est munie d'un signe donné par les règles suivantes :

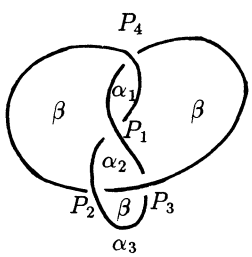


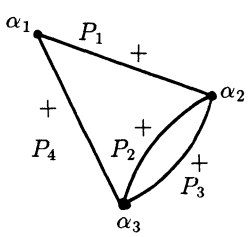
$+1$



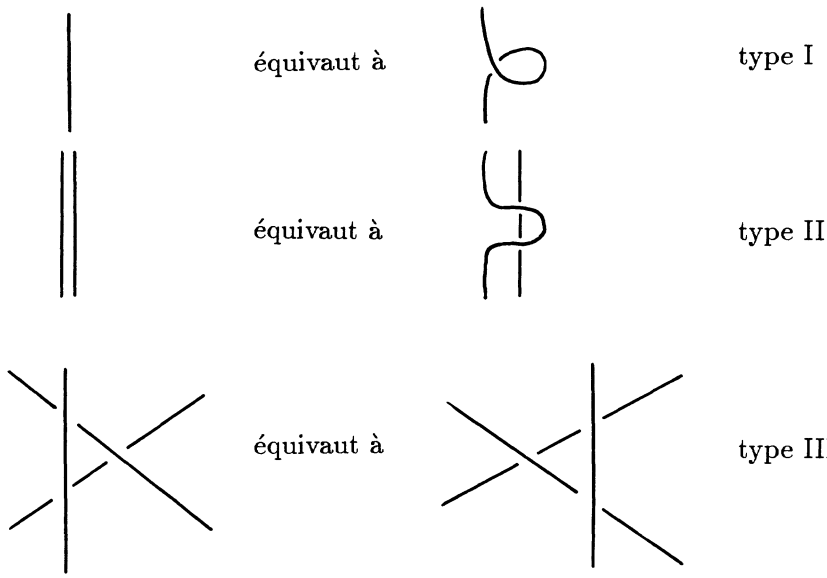
-1

Voici un exemple de graphe associé à une projection de nœud





En général, le même entrelac a plusieurs projections non équivalentes par une isotopie du plan. On peut prouver que l'on peut passer d'une projection D_1 à une projection D_2 du même nœud, à isotopie près, par une suite finie de *transformations de Reidemeister*, qui se répartissent en trois types



Faire attention aux croisements ; on peut mettre les orientations *ad libitum.*

1.3. Soit L un nœud orienté. Il existe une surface orientée S plongée dans $\mathbf{S}^3$, dont le bord soit L (*surface de Seifert*). Si L' est un nœud orienté disjoint de L , on peut par une isotopie ambiante s'arranger pour que S et L' se coupent transversalement en un nombre fini de points $p_1, \cdots, p_r$. Chacun de ces points p_i définit un nombre ε_i égal à ± 1 et déterminé par les orientations. Le nombre $\varepsilon_1 + \cdots + \varepsilon_r$ s'appelle *le nombre d'entrelacements* de L et L' , noté $i(L, L')$.

De manière plus précise, les groupes d'homologie à coefficients entiers de $\mathbf{S}^3 \backslash L$ sont donnés par

$$H_0(\mathbf{S}^3 \backslash L) = \mathbf{Z} \quad , \quad H_1(\mathbf{S}^3 \backslash L) = \mathbf{Z} \quad , \quad H_i(\mathbf{S}^3 \backslash L) = 0 \qquad \text{pour } i \geq 2 \, .$$

Le générateur γ de $H_1(\mathbf{S}^3 \backslash L)$ peut être choisi de sorte que la classe d'homologie définie par L' dans $\mathbf{S}^3 \backslash L$ soit égale à $i(L, L') \, . \, \gamma$.

Comme $H_1(\mathbf{S}^3 \backslash L)$ est isomorphe à $\mathbf{Z}$, il existe une variété M de dimension 3 qui est un revêtement de $\mathbf{S}^3 \backslash L$, galoisien de groupe $\mathbf{Z}$. Le *module d'Alexander* de L , noté $A(L)$, est le groupe d'homologie $H_1(M)$; comme le groupe $\mathbf{Z}$ agit sur M , donc sur son homologie, on peut considérer $A(L)$

comme un module sur l'anneau $\Lambda = \mathbf{Z}[u, u^{-1}]$ des polynômes de Laurent en u , la multiplication par u sur $A(L)$ correspondant à l'action du générateur de $\mathbf{Z}$ agissant sur M . La structure du Λ-module $A(L)$ s'exprime par une suite exacte

$$0 \longrightarrow \Lambda^{2h} \xrightarrow{\alpha} \Lambda^{2h} \longrightarrow A(L) \longrightarrow 0 \ ;$$

l'homomorphisme α est décrit par une matrice de la forme $A(L) = V - u\,{}^tV$, où V est une matrice carrée de type $2h \times 2h$ à coefficients entiers, telle que

$$V - {}^tV = \begin{pmatrix} 0 & I_h \\ -I_h & 0 \end{pmatrix} \tag{1.1}$$

(I_h : matrice unité d'ordre h). Le déterminant $\Delta_L(u)$ de la matrice $A(L)$ s'appelle le *polynôme d'Alexander* du nœud L . A multiplication près par une puissance de u, il ne dépend que du nœud L . On le normalise sous la forme

$$\Delta_L(u) = a_0 + a_1\,u + \cdots + a_{2m}\,u^{2m} \tag{1.2}$$

avec $a_0 \neq 0$; on a alors la relation de symétrie $a_i = a_{2m-i}$.

1.4. Compte tenu de l'identification de $\mathbf{R}^2$ et de $\mathbf{C}$, la définition générale donnée dans l'introduction se reformule ainsi : on note $\mathbf{C}^n_*$ l'ensemble des vecteurs à n coordonnées complexes toutes distinctes ; alors B_n est le groupe fondamental de $\mathbf{C}^n_*/\mathbf{S}_n$, le groupe $\mathbf{S}_n$ opérant par permutation des coordonnées. Le groupe fondamental de l'espace $\mathbf{C}^n_*$ s'appelle le *groupe de tresses pures* ; il se note P_n . Alors P_n est un sous-groupe invariant du *groupe de tresses* B_n et le groupe B_n/P_n est canoniquement isomorphe à $\mathbf{S}_n$.

Représentant les éléments de B_n par des lacets dans l'espace $\mathbf{C}^n_*/\mathbf{S}_n$, on obtient la description géométrique suivante. Considérons deux plans parallèles Π_0 et Π_1 dans $\mathbf{R}^3$, et la bande Δ qu'ils limitent. Fixons n points distincts $P^0_1, \cdots, P^0_n$ dans Π_0 et n points distincts $P^1_1, \cdots, P^1_n$ dans Π_1 . Une tresse à n brins est une réunion γ de n arcs simples $\gamma_1, \cdots, \gamma_n$ contenus dans Δ avec les propriétés suivantes :

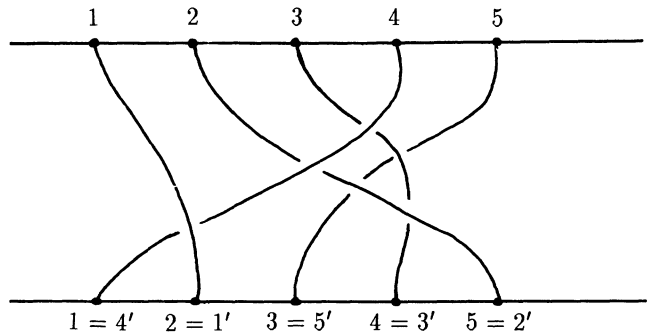
a) les arcs $\gamma_1, \cdots, \gamma_n$ sont deux à deux disjoints ;

b) chacun de ces arcs coupe tout plan Π , parallèle à Π_0 et Π_1 et contenu dans Δ , en un point et un seul ;

c) chaque arc a l'une de ses extrémités en l'un des points P_i^0 ; il se termine alors en $P_{\pi(i)}^1$, où π est la permutation dans $\mathbf{S}_n$ associée à l'élément de B_n défini par γ .

Pour définir l'équivalence, on introduit le groupe Γ des homéomorphismes de Δ qui fixent chacun des points $P_1^0, \cdots, P_n^0, P_1^1, \cdots, P_n^1$ et transforment en lui-même tout plan Π parallèle à Π_0 et Π_1 ; on note Γ_0 la composante connexe par arcs de l'identité dans Γ . Deux tresses γ et γ' sont équivalentes par Γ si et seulement si elles définissent la même permutation $\pi \in \mathbf{S}_n$. On dira qu'elles sont *isotopes* si elles sont équivalentes par le groupe Γ_0 ; les éléments de B_n sont alors les classes d'isotopie de tresses à n brins.

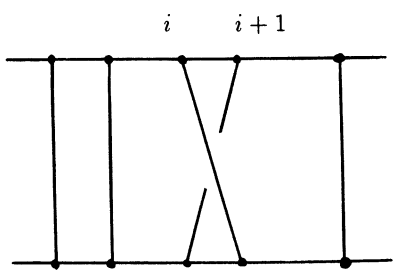
Choisissons un plan P perpendiculaire à Π_0 et Π_1 , et soit D la bande $P \cap \Delta$ dans P . On projette chaque tresse γ perpendiculairement sur P . Quitte à modifier γ par une isotopie, on peut supposer que la projection de γ se compose de n arcs différentiables qui se coupent transversalement en un nombre fini de points, et qui coupent transversalement chaque droite parallèle à $L_i = \Pi_i \cap P$ en un point unique. On adopte la convention précédente pour indiquer les croisements par-dessus ou par-dessous



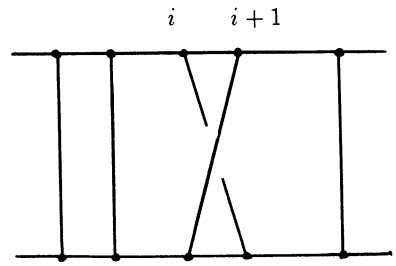
La permutation associée est $i \mapsto i'$, soit ici $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 1 & 3 \end{pmatrix}$.
On laisse au lecteur le soin de définir l'isotopie convenable sur les projections planes de tresses.

1.5. Structure du groupe des tresses

Le groupe B_n admet $n-1$ générateurs $\sigma_1, \cdots, \sigma_{n-1}$, que l'on définit facilement au moyen des projections planes



σ_i



σ_i^{-1}

Le groupe B_n admet la présentation donnée par les relations suivantes[1] :

$$\sigma_i\,\sigma_{i+1}\,\sigma_i = \sigma_{i+1}\,\sigma_i\,\sigma_{i+1} \qquad \text{pour } 1 \leq i \leq n-2 \tag{1.3}$$

$$\sigma_i\,\sigma_j = \sigma_j\,\sigma_i \qquad \text{pour } |i-j| \geq 2. \tag{1.4}$$

De manière analogue, le groupe symétrique $\mathbf{S}_n$ admet une présentation donnée par les générateurs s_i (transposition de i et $i+1$) pour $1 \leq i \leq n-1$, et les relations

$$s_i\,s_{i+1}\,s_i = s_{i+1}\,s_i\,s_{i+1} \qquad \text{pour } 1 \leq i \leq n-2 \tag{1.5}$$

$$s_i\,s_j = s_j\,s_i \qquad \text{pour } |i-j| \geq 2 \tag{1.6}$$

$$s_i^2 = 1 \qquad \text{pour } 1 \leq i \leq n-1. \tag{1.7}$$

Dans la projection de B_n sur S_n , le générateur σ_i donne s_i . Le noyau P_n est donc le plus petit sous-groupe invariant de B_n qui contienne les σ_i^2 .

On définit un groupe B_∞ ayant une suite infinie de générateurs $\sigma_1, \sigma_2, \cdots$ avec les relations (1.3) et (1.4). Le groupe B_n s'identifie au sous-groupe de B_∞ engendré par $\sigma_1, \cdots, \sigma_{n-1}$. Le plongement de B_n dans B_{n+1} ainsi obtenu se représente géométriquement par l'opération suivante : prendre

[1] Les permutations se composent comme les fonctions ; ainsi on a $(\pi\pi'(i) = \pi(\pi'(i))$. Pour la composition des tresses, on est donc conduit à les orienter du haut vers le bas, et tt' représente t en dessous de t'.

une tresse à n brins et ajouter un $(n+1)^e$ brin à droite, assez loin pour ne pas être enlacé avec les autres brins. De manière analogue, on a une chaîne croissante $\mathbf{S}_1 \subset \mathbf{S}_2 \subset \cdots \subset \mathbf{S}_n \subset \mathbf{S}_{n+1} \subset \cdots$ fournie par les groupes de permutations, avec la réunion $\mathbf{S}_\infty$.

La projection de $\mathbf{C}_*^{n+1}$ sur $\mathbf{C}_*^n$ qui transforme $(z_1, \cdots, z_n, z_{n+1})$ en $(z_1, \cdots, z_n)$ est une fibration, dont la fibre F est obtenue en ôtant n points dans $\mathbf{C}$. Le groupe fondamental de F est un groupe libre F_n à n générateurs $a_1, \cdots, a_n$, et dans une fibration, le groupe fondamental de la base opère sur celui de la fibre. On en déduit ceci :

Le groupe de tresses B_n s'identifie au groupe des automorphismes φ de F_n possédant les propriétés suivantes :

a) le produit $a_1 \cdots a_n$ est invariant par φ ;

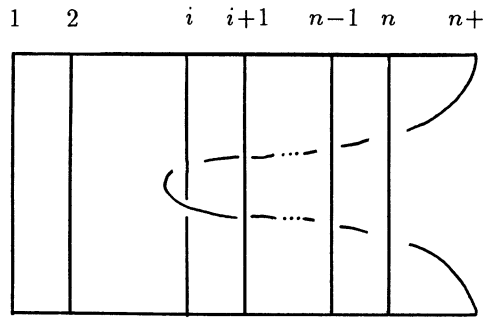
b) il existe une permutation $\pi \in \mathbf{S}_n$ telle que $\varphi(a_i)$ soit conjugué dans F_n à $a_{\pi(i)}$.

Dans cette identification, le générateur σ_i est décrit ainsi :

$$\sigma_i(a_j) = \begin{cases} a_i\, a_{i+1}\, a_i^{-1} & \text{si } j{=}i \\ a_i & \text{si } j = i+1 \\ a_j & \text{si } j = i, i+1 \ . \end{cases} \tag{1.8}$$

En particulier, le groupe de tresses pures P_n est le groupe des automorphismes de F_n qui laissent invariants $a_1 \cdots a_n$ et la classe de conjugaison de chaque a_i . On peut alors identifier P_{n+1} *au produit semi-direct de* P_n *et de* F_n *muni de l'action précédente de* P_n ; dans cette identification, on a

$$a_i = (\sigma_{i+1} \cdots \sigma_n)^{-1}\, \sigma_i^2 (\sigma_{i+1} \cdots \sigma_n) \ . \tag{1.9}$$



Le même raisonnement de fibration a d'autres applications. Notons $\mathcal{A}_n$ l'algèbre de cohomologie de de Rham de $\mathbf{C}_*^n$; la projection de $\mathbf{C}_*^{n+1}$

sur $\mathbf{C}_*^n$ identifie $\mathcal{A}_n$ à une sous-algèbre de $\mathcal{A}_{n+1}$; si l'on note a_i la classe de cohomologie de la forme différentielle $d\log(z_{n+1} - z_i)$ (pour $1 \leq i \leq n$), alors on a $\mathcal{A}_{n+1} = \mathcal{A}_n \oplus \mathcal{A}_n\, a_1 \oplus \cdots \oplus \mathcal{A}_n\, a_n$. Le polynôme de Poincaré de l'espace $\mathbf{C}_*^n$ est donc $\prod_{k=1}^{n-1}(1 + kt)$. Un résultat dû à Fox, et généralisé par Brieskorn [E7] et Deligne [E8] affirme que le revêtement universel de $\mathbf{C}_*^n$ est contractile ; par suite, la cohomologie du groupe B_n est isomorphe à $\mathcal{A}_n$. Enfin, avec les notations du n° 4.3, l'algèbre de Lie $\mathcal{G}_{n+1}$ associée au groupe P_{n+1} est somme directe de la sous-algèbre de Lie $\mathcal{G}_n$ et d'un idéal $\mathcal{I}_n$ qui est une algèbre de Lie libre à n générateurs.

1.6. Relations entre tresses et nœuds

Soit D une droite dans $\mathbf{R}^3$. Un entrelac L qui ne rencontre pas D sera appelé une *tresse fermée* à n brins, d'axe D , si tout demi-plan limité par D rencontre L en n points exactement. Choisissons un demi-plan P_0 limité par D , et notons P_t (pour $0 \leq t \leq 1$) le demi-plan obtenu par la rotation ρ_t d'angle $2\pi t$ autour de D (après choix d'orientations). Posons

$$F_t = \rho_t^{-1}(P_t \cap L)\ . \tag{1.10}$$

Alors la famille $(F_t)_{0 \leq t \leq 1}$ est un lacet dans l'espace de configuration $\Phi_n(P_0)$ et définit donc un élément du groupe de tresses B_n . On déduit de là *une bijection entre les tresses fermées à n brins* (à isotopie près) *et les classes de conjugaison dans B_n* .

À isotopie près, tout entrelac est une tresse fermée pour une droite bien choisie. On déduit de là la *classification de Markov des entrelacs*. Notons B l'ensemble somme des ensembles $B_1, B_2, \cdots$ et $\sim$ la plus petite relation d'équivalence dans B pour laquelle on ait

$$g \sim hgh^{-1} \qquad \text{et} \qquad g \sim g\,\sigma_n \sim g\,\sigma_n^{-1}$$

pour g, h dans B_n . Alors *l'ensemble $\mathcal{M}$ des classes d'équivalence classifie les entrelacs* (non sauvages, à isotopie ambiante près) *dans $\mathbf{R}^3$ ou dans $\mathbf{S}^3$*.

2. INVARIANTS POLYNOMIAUX DES NŒUDS

2.1. Décrivons la stratégie générale fondée sur les représentations linéaires des groupes B_n, selon Jones [C5] et Turaev [D13]. Soit V un espace vectoriel de dimension finie sur $\mathbf{C}$, et soit R un opérateur inversible agissant dans $V \otimes V = V^{\otimes 2}$; on note P l'opérateur de symétrie dans $V^{\otimes 2}$, transformant $x \otimes y$ en $y \otimes x$, et l'on pose $\hat{R} = RP$. De plus, on choisit un entier $n \geq 1$, et l'on note $\hat{R}_{i,i+1}$ l'opérateur dans $V^{\otimes n}$ défini par

$$(2.1)\quad \hat{R}_{i,i+1}(x_1 \otimes \cdots \otimes x_n) = x_1 \otimes \cdots \otimes x_{i-1} \otimes \hat{R}(x_i \otimes x_{i+1}) \otimes x_{i+2} \otimes \cdots \otimes x_n \ .$$

De manière générale, pour tout opérateur T dans $V^{\otimes 2}$, et des entiers i, j tels que $1 \leq i < j \leq n$, on note T_{ij} l'opérateur dans $V^{\otimes n}$ qui "agit comme T sur les facteurs de rang i et j ".

On cherche une représentation T_R du groupe B_n dans l'espace $V^{\otimes n}$ qui transforme le générateur σ_i en l'opérateur $\hat{R}_{i,i+1}$. Compte tenu de la présentation de B_n donnée par (1.3) et (1.4), la condition nécessaire et suffisante pour que ceci ait lieu est que $\hat{R}$ satisfasse à la relation

$$(2.2)\qquad \hat{R}_{12}\,\hat{R}_{23}\,\hat{R}_{12} = \hat{R}_{23}\,\hat{R}_{12}\,\hat{R}_{23}$$

(égalité d'opérateurs dans $V^{\otimes 3}$). Pour l'opérateur R , cela se transcrit en l'équation de Yang-Baxter (version quantique)

$$(2.3)\qquad R_{12}\,R_{13}\,R_{23} = R_{23}\,R_{13}\,R_{12} \ .$$

Par exemple, si l'on a $R = 1$, les opérateurs R_{ij} sont tous égaux à 1 , et l'équation de Yang-Baxter est satisfaite. Dans ce cas, l'action d'un élément g de B_n est donnée par

$$(2.4)\qquad T_1(g)(x_1 \otimes \cdots \otimes x_n) = x_{\pi^{-1}(1)} \otimes \cdots \otimes x_{\pi^{-1}(n)}$$

où π est l'image de g par l'homomorphisme canonique de B_n sur $\mathbf{S}_n$.

2.2. Voici une classe de solutions de l'équation de Yang-Baxter. Soit V l'espace $\mathbf{C}^N$ avec sa base canonique $e_1, \cdots, e_N$. On note q un nombre complexe non nul. Soit R l'opérateur dans $V^{\otimes 2}$ défini par

$$(2.5)\qquad \begin{cases} R(e_i \otimes e_i) &= q\, e_i \otimes e_i & \\ R(e_i \otimes e_j) &= e_i \otimes e_j & \text{pour } i < j \\ R(e_j \otimes e_i) &= (q - q^{-1})\, e_i \otimes e_j + e_j \otimes e_i & \text{pour } i < j. \end{cases}$$

Alors (2.3) est satisfaite. Pour $q = 1$, l'opérateur R se réduit à l'identité. L'opérateur $\hat{R}$ a les valeurs propres q (multiplicité $N(N+1)/2$) et $-q^{-1}$ (multiplicité $N(N-1)/2$), et l'on a donc $(\hat{R} - q)(\hat{R} + q^{-1}) = 0$. On peut traduire ainsi le résultat obtenu :

a) L'algèbre de Hecke $\mathcal{H}_n(q)$ est une algèbre ayant des générateurs $T_1, \cdots, T_{n-1}$ avec les relations

$$T_i\, T_{i+1}\, T_i = T_{i+1}\, T_i\, T_{i+1} \tag{2.6}$$

$$T_i\, T_j = T_j\, T_i \qquad \text{si } |i-j| \geq 2 \tag{2.7}$$

$$(T_i - q)(T_i + q^{-1}) = 0\ . \tag{2.8}$$

Elle a une base de la forme (T_π) , où π parcourt $\mathbf{S}_n$, avec $T_1 = 1$, et la règle de multiplication

$$T_\pi\, T_i = T_{\pi s_i} \qquad \text{si } \pi(i) < \pi(i+1), \tag{2.9}$$

$$T_\pi\, T_i = T_{\pi s_i} + (q - q^{-1})\, T_\pi \qquad \text{si } \pi(i) > \pi(i+1). \tag{2.10}$$

b) Il existe une représentation linéaire λ_n de l'algèbre $\mathcal{H}_n(q)$ dans l'espace $V^{\otimes n}$, telle que $\lambda_n(T_i)$ soit égal à $\hat{R}_{i,i+1}$ pour $1 \leq i \leq n-1$.

c) Il existe un homomorphisme ε_n du groupe B_n dans le groupe multiplicatif $\mathcal{H}_n(q)^\times$ qui transforme σ_i en T_i . Dans ces conditions, on a

$$T_R(g) = \lambda_n(\varepsilon_n(g)) \qquad \text{pour } g \text{ dans } B_n\ . \tag{2.11}$$

Lorsque $q = 1$, l'algèbre $\mathcal{H}_n(q)$ se réduit à l'algèbre $\mathbf{CS}_n$ du groupe symétrique, de sorte qu'on ait $T_\pi = \pi$. Supposons qu'on ait $q^k \neq 1$ pour $k = 1, \cdots, n$. Alors l'algèbre $\mathcal{H}_n(q)$ est semi-simple et ses représentations simples U_μ sont paramétrées par les partitions $\mu = (\mu_1, \cdots, \mu_n)$ de n (avec la convention $\mu_1 \geq \cdots \geq \mu_n \geq 0$ et $n = \mu_1 + \cdots + \mu_n$). La représentation λ_n de l'algèbre $\mathcal{H}_n(q)$ dans l'espace $(\mathbf{C}^N)^{\otimes n}$ fait intervenir exactement les représentations U_μ correspondant aux partitions $\mu = (\mu_1, \cdots, \mu_n)$ avec $\mu_k = 0$ pour $k > N$; la multiplicité de U_μ est la même que celle du cas spécial $q = 1$ (*cf.* Hoefsmit [C17]).

2.3. On suppose maintenant donnés un espace vectoriel V (de dimension finie sur $\mathbf{C}$), un opérateur inversible R dans $V \otimes V$ satisfaisant à l'équation

de Yang-Baxter, et un opérateur μ dans V satisfaisant aux conditions suivantes :

a) *les opérateurs* R *et* $\mu \otimes \mu$ *commutent* ;

b) *pour tout opérateur* u *dans* $\mathrm{End}(V)$, *on a les relations*

$$Tr((u \otimes \mu).\hat{R}) = \alpha\, Tr(u) \tag{2.12}$$

$$Tr((u \otimes \mu).\hat{R}^{-1}) = \alpha^{-1}\, Tr(u)\ , \tag{2.13}$$

où α est une constante complexe convenable (avec $\alpha \neq 0$).

Notons w l'homomorphisme de B_n dans $\mathbf{Z}$ qui envoie chaque générateur σ_i sur 1 , puis définissons une fonction $\phi^n_{R,\mu}$ sur le groupe B_n par la relation

$$\phi^n_{R,\mu}(g) = \alpha^{-w(g)}\, Tr(\mu^{\otimes n}.T_R(g)) \tag{2.14}$$

où la représentation T_R de B_n dans l'espace $V^{\otimes n}$ satisfait à $T_R(\sigma_i) = \hat{R}_{i,i+1}$ pour $1 \leq i \leq n-1$. Il résulte facilement des hypothèses faites qu'on a les relations

$$\phi^n_{R,\mu}(hgh^{-1}) = \phi^n_{R,\mu}(g) \tag{2.15}$$

$$\phi^{n+1}_{R,\mu}(g\,\sigma_n^{\pm 1}) = \phi^n_{R,\mu}(g) \tag{2.16}$$

pour tout g dans B_n . Compte tenu de la classification de Markov des entrelacs (voir n° 1.6), on peut définir un invariant $T_{R,\mu}(L)$ des classes d'isotopie d'entrelacs, telle que l'on ait

$$T_{R,\mu}(L) = \phi_{R,\mu}(g) \tag{2.17}$$

si l'entrelac L s'obtient en fermant une tresse à n brins correspondant à l'élément g de B_n .

2.4. Pour donner un exemple explicite, revenons au cas $V = \mathbf{C}^N$, l'opérateur R étant décrit par les formules (2.5). On prend pour μ la matrice diagonale d'éléments

$$(-1)^{N+1}\, q^{N-1}\,,\ (-1)^{N+1}\, q^{N-3}\,,\cdots,\ (-1)^{N+1}\, q^{1-N}$$

et l'on pose $\alpha = (-1)^{N+1}\, q^N$. L'invariant de Turaev de degré N est alors défini par

$$T_L^N(q) = (-1)^{N+1}\, \frac{q - q^{-1}}{q^N - q^{-N}}\, T_{R,\mu}(L) \tag{2.18}$$

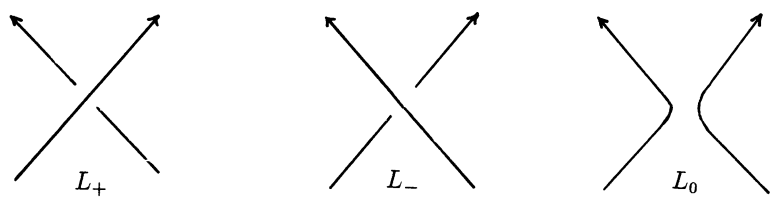
pour tout entrelac L , avec R et μ ainsi précisés ; c'est un polynôme de Laurent en q .

Lorsque $N = 2$, *on retrouve le polynôme de Jones*

$$T_L^2(q) = V_L(q^2) \tag{2.19}$$

(avec les notations de Jones [C2]).

La suite des polynômes $T_L^N(q)$ pour $N = 2, 3, \cdots$ s'exprime au moyen d'un seul polynôme de Laurent en q et q^N . De manière précise, étant donné un entrelac orienté L , choisissons un point de croisement p de L et définissons trois entrelacs L_+ , L_- et L_0 où L_+ est égal à L , et où L_- et L_0 s'obtiennent par les modifications au point p indiquées sur le schéma suivant :



La relation $\hat{R} - \hat{R}^{-1} = q - q^{-1}$ (qui exprime le fait que $\hat{R}$ a les valeurs propres q et $-q^{-1}$) se traduit géométriquement par la relation

$$q^N\, T_{L_+}^N(q) - q^{-N}\, T_{L_-}^N(q) + (-1)^N\, (q - q^{-1})\, T_{L_0}^N(q) = 0\ . \tag{2.20}$$

On montre de manière combinatoire que la projection plane de tout entrelac peut être modifiée en celle d'une réunion de cercles non noués et non enlacés par des transformations de passages supérieurs en passages inférieurs et inversement. Raisonnant par récurrence sur le nombre de points de croisement de la projection de L , on arrive au résultat suivant :

THÉORÈME.— *On peut associer, de manière unique, à toute classe d'isotopie d'entrelac orienté L un polynôme $P_L(x,y,z)$ en $x, x^{-1}, y, y^{-1}, z, z^{-1}$, homogène de degré 0 et satisfaisant aux deux relations*

$$x\,P_{L_+} + y\,P_{L_-} + z\,P_{L_0} = 0 \tag{2.21}$$

avec les conventions ci-dessus, et

$$P_0 = 1 \tag{2.22}$$

où 0 représente un cercle. De plus, l'invariant de Turaev est donné par la formule

$$T_L^N(q) = P_L(q^N, -q^N, (-1)^N(q-q^{-1}))\ . \tag{2.23}$$

Le polynôme $P_L(x,y,z)$ n'est autre que le polynôme HOMFLY défini par les six auteurs [C12]. Il contient comme cas particuliers le polynôme d'Alexander

$$\Delta_L(q) = P(1,-1,q-q^{-1}) \tag{2.24}$$

et celui de Jones

$$V_L(q^2) = P_L(q^2, -q^{-2}, q-q^{-1})\,. \tag{2.25}$$

Remarque : Conservons les mêmes définitions de R et μ . On définit une forme linéaire τ_n sur l'algèbre de Hecke $\mathcal{H}_n(q)$ par la formule

$$\tau_n(a) = Tr(\lambda_n(a)\,.\,\mu^{\otimes n})\ ; \tag{2.26}$$

la représentation λ_n de l'algèbre $\mathcal{H}_n(q)$ dans l'espace $(\mathbf{C}^N)^{\otimes n}$ est définie par $\lambda_n(T_i) = \hat{R}_{i,i+1}$. Alors τ_n est une trace, c'est-à-dire qu'on a $\tau_n(ab) = \tau_n(ba)$. D'autre part, en plongeant de manière évidente $\mathcal{H}_n(q)$ dans $\mathcal{H}_{n+1}(q)$, on a les deux relations

$$\tau_{n+1}(a\,T_n) = \alpha\,\tau_n(a) \tag{2.27}$$

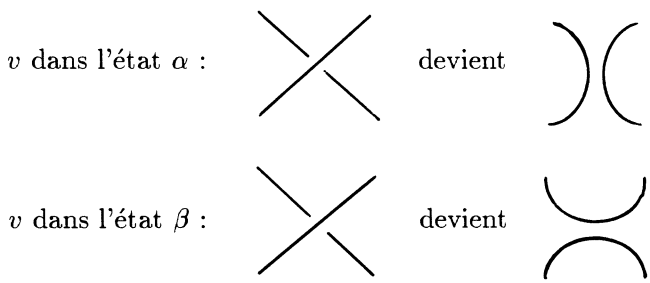
$$\tau_{n+1}(a) = \beta\,\tau_n(a) \tag{2.28}$$

avec les constantes

$$\alpha = (-1)^{N+1}\, q^N \quad , \quad \beta = (-1)^{N+1}\, \frac{q^N - q^{-N}}{q - q^{-1}} \ .$$

Dans [C16], Vogel a déterminé *a priori* toutes les suites de traces τ_n sur les algèbres $\mathcal{H}_n(q)$ satisfaisant aux relations (2.27) et (2.28) pour des valeurs arbitraires de α et β . Le cas $\beta = 1$ est celui étudié par Jones, qui a donné le branle initial à toute cette théorie.

2.5. Un autre type d'invariant a été construit par L. Kauffman. Considérons d'abord une projection plane D d'un entrelac L . Soit V l'ensemble des points de croisement. Nous inspirant de la *Mécanique Statistique*, nous supposerons que chaque point v de V peut être dans deux états, notés α et β ; un état de D est une application ω de V dans $\{\alpha, \beta\}$. Étant donné un état ω, nous notons $m(\omega)$ le nombre de points de V dans l'état α , et $n(\omega)$ ceux dans l'état β . D'autre part, nous modifions le diagramme D simultanément en tous ses sommets selon la règle



Le diagramme ainsi modifié n'a plus de points de croisement et se compose d'un nombre $p(\omega)$ de cercles disjoints. Le poids associé à un état ω est

$$\pi(\omega) = A^{m(\omega)}\, B^{n(\omega)}\, d^{p(\omega)} \ .$$

On associe à D le polynôme $K_D(A, B, d)$ égal à la somme des poids $\pi(\omega)$ pour les $2^{|V|}$ états possibles de D . Il s'agit là de l'analogue d'une fonction de partition en Mécanique Statistique.

Jusqu'ici, nous n'avons pas tenu compte de l'orientation de l'entrelac L ou de sa projection D . Mais on déduit de l'existence du polynôme de Kauffman $K_D(A, B, d)$ l'existence d'un nouvel invariant polynomial $Q_L(x, y)$.

C'est un polynôme à coefficients entiers en x, x^{-1} , y et y^{-1} avec les propriétés caractéristiques suivantes :

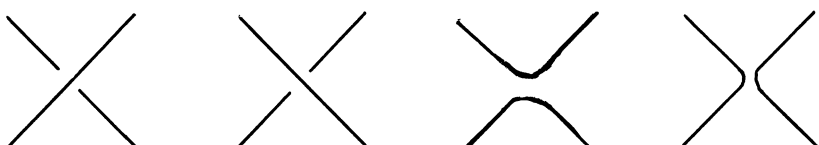
a) si L est un cercle non noué, on a $Q_L = 1$;

b) soit D une projection plane de l'entrelac L et soit $w(D)$ la somme des multiplicités des points de croisement (conformément aux conventions du n° 1.2). Alors $\widetilde{Q}_D(x,y) = x^{w(D)}\, Q_L(x,y)$ ne dépend pas de l'orientation de L (et de D) ;

c) on a la relation

$$\widetilde{Q}_{D_+} + \widetilde{Q}_{D_-} = y\,\widetilde{Q}_{D_0} + y^{-1}\,\widetilde{Q}_{D_\infty}$$

si les quatre diagrammes D_+ , D_- , D_0 et D_∞ diffèrent en un sommet selon le schéma suivant :



On peut retrouver le polynôme de Jones $V_L(q^2)$ comme spécialisation du polynôme de Kauffman $Q_L(x,y)$. De plus, Turaev a donné une interprétation de $Q_L(x,y)$ au moyen du schéma (V, R, μ) .

3. CATÉGORIES ET ALGÈBRES DE HOPF

3.1. Considérons un ensemble E et une application φ de $E \times E$ dans E ; nous voulons formuler en général l'associativité de φ . Pour cela, on définit par récurrence une suite d'ensembles finis $\Sigma_1, \Sigma_2, \cdots$ par les règles

$$(3.1)\quad \Sigma_1 = \{0\} \quad , \quad \Sigma_n = (\Sigma_1 \times \Sigma_{n-1}) \cup (\Sigma_2 \times \Sigma_{n-2}) \cup \cdots \cup (\Sigma_{n-1} \times \Sigma_1)\,.$$

Par récurrence sur $n \geq 1$, on associe à chaque élément σ de Σ_n une application $\bar{\sigma}$ de E^n dans E :

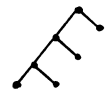
a) si $n = 1$, on a $\sigma = 0$ et $\bar{\sigma}(x) = x$ pour tout $x \in E$;

b) si $n > 1$, il existe un entier p tel que $1 \leq p \leq n-1$, et deux éléments $\sigma' \in \Sigma_p$ et $\sigma'' \in \Sigma_{n-p}$ tels que $\sigma = (\sigma', \sigma'')$; on a

$$\bar{\sigma}(x_1, \cdots, x_n) = \varphi(\bar{\sigma}'(x_1, \cdots, x_p), \bar{\sigma}''(x_{p+1}, \cdots, x_n)) \ . \tag{3.2}$$

On peut représenter les éléments de Σ_n par des arbres binaires à n sommets libres ; donnons deux exemples d'éléments de Σ_4 et leurs représentations graphiques

$\alpha = (0,(0,(0,0)))$



$\beta = (((0,0),0),0)$.

Si nous abrégeons $\varphi(a,b)$ en (ab) , les fonctions associées à α et β sont données par

$$\begin{cases} \bar{\alpha}(a,b,c,d) & = (\mathrm{a}(\mathrm{b}(\mathrm{cd}))) \\ \bar{\beta}(a,b,c,d) & = (((\mathrm{ab})\mathrm{c})\mathrm{d}) \ . \end{cases} \tag{3.3}$$

Les ensembles Σ_1 et Σ_2 ont un seul élément, et Σ_3 a deux éléments λ et μ dont les fonctions associées sont

$$\bar{\lambda}(a,b,c) = ((ab)c) \quad , \quad \bar{\mu}(a,b,c) = (a(bc)) \ . \tag{3.4}$$

On dit que la loi φ est *associative* si l'on a $((ab)c) = (a(bc))$ pour a, b, c dans E , c'est-à-dire $\bar{\lambda} = \bar{\mu}$. S'il en est ainsi, pour tout entier $n \geq 1$, toutes les applications de E^n dans E associées aux éléments de Σ_n coïncident. On peut par exemple vérifier de deux manières l'égalité $\bar{\alpha} = \bar{\beta}$

$$(a(b(cd))) = ((ab)(cd)) = (((ab)c)d) \tag{3.5}$$

$$(a(b(cd))) = (a((bc)d) = ((a(bc))d) = (((ab)c)d) \ . \tag{3.6}$$

Ces formules correspondent à deux chaînes de transformations élémentaires sur les arbres binaires.

3.2. Nous appliquons ce qui précède au cas d'une catégorie $\mathcal{C}$ et d'un foncteur Φ de $\mathcal{C} \times \mathcal{C}$ dans $\mathcal{C}$; ainsi Φ induit une loi de composition sur

l'ensemble $\mathrm{Ob}(\mathcal{C})$ des objets de $\mathcal{C}$ et aussi sur l'ensemble $\mathrm{F}\ell(\mathcal{C})$ des flèches de $\mathcal{C}$. Si ces deux lois sont associatives, on dira que Φ est dit *strictement associatif*. En pratique, c'est rarement le cas ; par exemple, si $\mathcal{C}$ est la catégorie des espaces vectoriels sur $\mathbf{C}$, et qu'on prenne $\Phi(U,V) = U \otimes V$, on sait que les espaces $(U \otimes V) \otimes W$ et $U \otimes (V \otimes W)$ sont isomorphes, mais non égaux.

Supposons alors qu'on dispose d'un isomorphisme $\alpha(a,b,c)$ de $\Phi(a,\Phi(b,c))$ sur $\Phi(\Phi(a,b),c)$ fonctoriel en les objets a, b et c de $\mathcal{C}$. Par itération du foncteur Φ , on associe à chaque élément σ de Σ_n un foncteur σ_* de $\mathcal{C}^n$ dans $\mathcal{C}$. En utilisant α , on montre que les foncteurs σ_* et τ_* associés à deux éléments de Σ_n sont isomorphes. Par exemple, les deux chaînes d'égalités (3.5) et (3.6) s'interprètent en donnant deux isomorphismes ε et η du foncteur α_* sur le foncteur β_* ; on a explicitement[1], en écrivant ab pour $\Phi(a,b)$:

$$\varepsilon(a,b,c,d) = \alpha(ab,c,d)\alpha(a,b,cd) \tag{3.7}$$

$$\eta(a,b,c,d) = \Phi(\alpha(a,b,c),d)\alpha(a,bc,d)\Phi(a,\alpha(b,c,d)) \ . \tag{3.8}$$

Noter que les flèches dans $\mathcal{C}$ se composent de la droite vers la gauche. On dit que θ est une *contrainte d'associativité pour* Φ si l'on a toujours $\varepsilon(a,b,c,d) = \eta(a,b,c,d)$. S'il en est ainsi, *l'interprétation de toutes les chaînes allant de* $\sigma_*(a_1,\cdots,a_n)$ *à* $\tau_*(a_1,\cdots,a_n)$ *conduit au même isomorphisme du foncteur* σ_* *sur le foncteur* τ_* (pour σ et τ dans Σ_n). Ce théorème est dû à Mac Lane [B1].

De manière analogue, une *contrainte de commutativité* pour Φ est un isomorphisme $\rho(a,b)$ de $\Phi(a,b)$ sur $\Phi(b,a)$, fonctoriel en les objets a et b de $\mathcal{C}$ et tel que l'on ait

$$\Phi(\rho(a,c),b)\alpha(a,c,b)\Phi(a,\rho(b,c)) = \alpha(c,a,b)\rho(ab,c)\alpha(a,b,c) \ . \tag{3.9}$$

Cette relation traduit l'égalité des deux chaînes de transformations

$$a(bc) = a(cb) = (ac)b = (ca)b \ ,$$

[1] Cette interprétation d'une démonstration algébrique comme une flèche d'une catégorie joue un rôle important dans certaines études récentes sur la compilation et les transformations de programmes.

$$a(bc) = (ab)c = c(ab) = (ca)b \ .$$

On pourra traduire la contrainte d'associativité en un *diagramme pentagonal* et celle de commutativité en un *diagramme hexagonal.*

Si les contraintes d'associativité et de commutativité sont remplies et si $\rho(a,b)$ est inverse de $\rho(b,a)$ pour tous les objets a, b , alors pour tout σ dans Σ_n , le foncteur $\sigma_*(a_1, \cdots, a_n)$ dépend "symétriquement" des objets $a_1, \cdots, a_n$ de $\mathcal{C}$.

3.3. *La dualité de Tannaka pour les groupes algébriques* repose sur les deux théorèmes suivants de Chevalley [B15], où V désigne un espace vectoriel de dimension finie (sur $\mathbf{C}$) et G un sous-groupe algébrique de $\mathrm{GL}(V)$.

THÉORÈME A.— *Toute représentation linéaire (π, W) de G correspondant à une application polynomiale de G dans $\mathrm{GL}(W)$ peut se réaliser, à l'équivalence près, dans un sous-quotient d'un espace de la forme $\bigoplus_{i=1}^{s} V^{\otimes n_i} \otimes (V^\vee)^{\otimes m_i}$, où $V^\vee$ est le dual de V .*

THÉORÈME B.— *Il existe un nombre fini d'entiers $r_1, \cdots, r_k$ et des droites D_i dans $V^{\otimes r_i}$ (pour $1 \leq i \leq k$) tels que G se compose des éléments de $\mathrm{GL}(V)$ qui stabilisent chacune des droites $D_1, \cdots, D_k$.*

Supposons alors que $\mathcal{C}$ soit une famille de représentations $(\pi_i, W_i)_{i \in I}$ du groupe G , polynomiales au sens du théorème A. On suppose de plus que $\mathcal{C}$ est stable par somme directe, produit tensoriel, passage au dual et aux sous-espaces et espaces quotients. Si $\mathcal{C}$ contient une représentation fidèle, alors toute représentation polynomiale de G est isomorphe à l'une des représentations (π_i, W_i) . Cela résulte du théorème A.

Mais, d'après le théorème B, le groupe lui-même peut être reconstruit à partir de la famille de ses représentations. Par hypothèse, la famille $\mathcal{C}$ est stable par produit tensoriel ; notons $i \times j$ l'élément de I tel que $\pi_{i \times j} = \pi_i \otimes \pi_j$ et $W_{i \times j} = W_i \otimes W_j$. *Supposons donnée une famille d'automorphismes $g_i \in \mathrm{GL}(W_i)$ satisfaisant aux deux conditions* :

a) *on a $f\, g_i = g_j\, f$ pour toute application G-équivariante f de W_i dans W_j* ;

b) *on a $g_{i \times j} = g_i \otimes g_j$.*

Dans ces conditions, il existe un unique élément g de G tel que $\pi_i(g) = g_i$ pour tout $i \in I$.

Lorsque le groupe G est réductif, toutes ses représentations linéaires sont semi-simples (= complètement réductibles). La reconstruction précédente du groupe G peut être modifiée : on part de la classe $\mathcal{S}$ des représentations simples (= irréductibles), notées (π_λ, W_λ) pour λ dans Λ . Notons $H_{\lambda\times\mu,\nu}$ l'ensemble des applications linéaires u de $W_\lambda \otimes W_\mu$ dans W_ν telles que l'on ait

$$u \,.\, (\pi_\lambda(g) \otimes \pi_\mu(g)) = \pi_\nu(g) \,.\, u \tag{3.10}$$

pour tout g dans G . Alors toute collection d'automorphismes $g_\lambda \in \mathrm{GL}(W_\lambda)$ qui satisfait à la relation

$$u \,.\, (g_\lambda \otimes g_\mu) = g_\nu \,.\, u \ , \tag{3.11}$$

quels que soient λ, μ, ν dans Λ et u dans $H_{\lambda\times\mu,\nu}$, provient d'un unique élément g de G par la règle $g_\lambda = \pi_\lambda(g)$.

Le cas classique des groupes compacts s'obtient par les modifications suivantes: on considère seulement les représentations unitaires continues dans des espaces de Hilbert de dimension finie ; ainsi $\pi_i(g)$ est un opérateur unitaire dans W_i . Dans la reconstruction du groupe G , on impose aux g_i (ou aux g_λ) d'être des opérateurs unitaires. Les deux versions ci-dessus sont valables, et le groupe G est un groupe de Lie si et seulement si G possède une représentation fidèle, ou — ce qui revient au même — si la classe $\mathcal{C}$ est engendrée par un nombre fini de représentations au moyen des opérations permises : somme directe, produit tensoriel, dual, sous-espace et espace-quotient. Nous ajouterons deux remarques :

a) les représentations linéaires continues d'un groupe compact sont semi-simples ;

b) tout sous-groupe fermé du groupe unitaire $U(n)$ est l'intersection $G \cap U(n)$ avec $U(n)$ d'un unique sous-groupe algébrique de $\mathrm{GL}(n, \mathbf{C})$.

3.4. Il y a de nombreuses situations où le groupe n'est pas donné à l'avance, mais où on dispose de ce qui sera la classe de ses représentations. La question se pose en Géométrie algébrique où Grothendieck a inventé la

"philosophie des motifs" à ce sujet, et en Physique mathématique où l'on aimerait traduire les règles de supersélection (certaines règles de conservation généralisant par exemple celle de la charge électrique) par l'existence d'un groupe de jauge. Il y a deux chaînes de recherches indépendantes : l'une commencée par Grothendieck a bénéficié des contributions de Saavedra, Milne et Deligne ; l'autre, dans le cadre des espaces de Hilbert, doit presque tout à Doplicher, Roberts et Woronowicz.

Le problème est donc de reconstruire un groupe algébrique à partir d'une catégorie de "représentations". Si G est un sous-groupe algébrique de $\mathrm{GL}(n, \mathbf{C})$, on lui associe l'algèbre $A = A(G)$ des fonctions "polynomiales" sur G , de la forme $P(g_{11}, \cdots, g_{nn})/(\det g)^s$, pour $g = (g_{ij})$, avec un polynôme P à n^2 variables et un entier $s \geq 0$. Les points de G correspondent aux homomorphismes d'algèbres de A dans $\mathbf{C}$, et la multiplication dans G se dualise en un homomorphisme Δ de A dans $A \otimes A$ tel que $\Delta(P) = \sum_i P'_i \otimes P''_i$ signifie $P(g'g'') = \sum_i P'_i(g')P''_i(g'')$. De même, l'unité de G correspond à un homomorphisme $\varepsilon : A \to \mathbf{C}$ et l'inversion $g \mapsto g^{-1}$ dans G à un homomorphisme $S : A \to A$. Les objets

$$A\,,\ \Delta : A \to A \otimes A\,,\ \varepsilon : A \to \mathbf{C}\,,\ S : A \to A$$

satisfont à des conditions qui caractérisent axiomatiquement les *algèbres de Hopf*. Les représentations linéaires polynomiales de G correspondent aux comodules V sur A (application structurale $V \to A \otimes V$) de dimension finie sur $\mathbf{C}$. Parmi les algèbres de Hopf, celles qui correspondent aux groupes algébriques sont celles qui satisfont à la condition (fondamentale) que l'algèbre A est commutative et la condition (secondaire) que l'algèbre A a un nombre fini de générateurs.

3.5. Le passage des groupes algébriques aux groupes "quantiques" se fait en affaiblissant l'hypothèse de commutativité de la multiplication.

Nous partons d'une catégorie abélienne $\mathcal{C}$ munie d'un foncteur exact et fidèle dans la catégorie des espaces vectoriels de dimension finie sur $\mathbf{C}$. De manière concrète, on dispose d'une famille $(V_i)_{i \in I}$ de tels espaces vectoriels, et pour chaque paire i, j d'un sous-espace $\mathcal{H}_{i,j}$ de l'ensemble $\mathrm{Hom}(V_i, V_j)$ des applications linéaires de V_i dans V_j . On suppose que la famille des

V_i est stable par somme directe finie, et que le noyau et le conoyau d'un élément de $\mathcal{H}_{ij}$ sont encore dans la famille $(V_i)_{i\in I}$ (avec des conditions convenables sur la composition).

Sous ces hypothèses, la catégorie $\mathcal{C}$ se compose des comodules sur une coalgèbre A qu'on reconstruit comme suit : on note V la somme directe des V_i ; on identifie $\prod_i \mathrm{End}(V_i)$ à une sous-algèbre E de $\mathrm{End}(V)$ et la somme directe des $\mathcal{H}_{ij}$ à une autre sous-algèbre H (sans unité) de $\mathrm{End}(V)$. Soit F l'ensemble des éléments de E qui commutent à tous ceux de H ; c'est une sous-algèbre fermée de $\prod_i \mathrm{End}(V_i)$ munie de la topologie produit ; le dual topologique de F est la coalgèbre cherchée.

Le produit $m : A \otimes A \to A$ s'obtiendra en munissant la catégorie $\mathcal{C}$ d'un foncteur $\Phi : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$ avec une contrainte d'associativité ; on écrira $i \times j$ pour $\Phi(i,j)$. On suppose qu'on a $V_{i\times j} = V_i \otimes V_j$ et que la contrainte d'associativité de $i \times (j \times k)$ sur $(i \times j) \times k$ correspond à l'isomorphisme canonique de $V_i \otimes (V_j \otimes V_k)$ sur $(V_i \otimes V_j) \otimes V_k$. Grâce à cela, la multiplication dans A sera définie et associative. De manière analogue, l'unité dans A correspond à un objet particulier $\mathbf{1}$ dans $\mathcal{C}$ tel que $\mathbf{1} \times i$ et $i \times \mathbf{1}$ soient isomorphes à i . L'antipodisme $S : A \to A$ correspond à un foncteur de dualité $i \mapsto i^\vee$ dans $\mathcal{C}$ avec un isomorphisme fonctoriel de $\mathrm{Hom}_{\mathcal{C}}(i \times j, k)$ sur $\mathrm{Hom}_{\mathcal{C}}(i, j^\vee \times k)$; on impose de plus que $V_{i^\vee}$ soit le dual de l'espace V_i .

La commutativité de l'algèbre A correspond dans ce cadre à une contrainte de commutativité $\rho : i \times j \to j \times i$ dans la catégorie $\mathcal{C}$ compatible avec celle des espaces vectoriels, en ce sens que ρ induit l'isomorphisme $x \otimes y \mapsto y \otimes x$ de $V_{i\times j} = V_i \otimes V_j$ sur $V_{j\times i} = V_j \otimes V_i$.

Drinfeld vient d'examiner, sous le nom de *quasi-algèbres de Hopf*, ce qui se passe lorsque l'on donne dans la catégorie $\mathcal{C}$ un foncteur $\Phi : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$ tel que $V_{i\times j} = V_i \otimes V_j$, muni de contraintes d'associativité et de commutativité qui n'ont plus rien à voir avec celles du produit tensoriel. Pour chaque entier $n \geq 1$, notons $A^{\otimes n}$ la coalgèbre produit tensoriel de n facteurs égaux à A , et $\mathcal{A}_n$ l'algèbre duale de $A^{\otimes n}$. La multiplication $a \otimes b \mapsto ab$ dans A se dualise en un coproduit $\Delta : \mathcal{A}_1 \to \mathcal{A}_2$, de même Δ' est duale de la multiplication opposée $a \otimes b \mapsto ba$ dans A .

Supposons d'abord que la contrainte d'associativité soit compatible au produit tensoriel. Il existe alors un élément inversible R de $\mathcal{A}_2$ tel que l'on

ait

$$\Delta'(a) = R\,\Delta(a)\,R^{-1} \qquad \text{pour tout } a \in \mathcal{A}_1 \ . \tag{3.12}$$

Pour i dans I , le comodule V_i sur A est aussi un module sur le dual $\mathcal{A}_1$ de A ; de même $V_{i\times j} = V_i \otimes V_j$ est un comodule sur $A^{\otimes 2}$, donc un module sur $\mathcal{A}_2$, et R définit un opérateur R_{ij} dans $V_i \otimes V_j$. La contrainte de commutativité dans la catégorie $\mathcal{C}$ est alors l'isomorphisme $P_{ij}\,R_{ij}$ de $V_i \otimes V_j$ sur $V_j \otimes V_i$, où $P_{ij}(x_i \otimes x_j) = x_j \otimes x_i$. La relation (3.12) exprime le défaut de commutativité de l'algèbre A , puisque $R = 1$ correspond au cas où A est commutative. Le diagramme hexagonal se traduit alors par les formules

$$\Delta_{12}(R) = R_{13}\,R_{23} \tag{3.13}$$

$$\Delta_{23}(R) = R_{13}\,R_{12} \tag{3.14}$$

qui entraînent la relation de Yang-Baxter

$$R_{12}\,R_{13}\,R_{23} = R_{23}\,R_{13}\,R_{12} \ . \tag{3.15}$$

Noter que R_{12} par exemple est égal à R agissant sur les facteurs 1 et 2 de $A^{\otimes 3}$ par $\langle R_{12}, a_1 \otimes a_2 \otimes a_3\rangle = \langle R, a_1 \otimes a_2\rangle.\langle \varepsilon, a_3\rangle$. De même, Δ_{12} est dual de l'application $a_1 \otimes a_2 \otimes a_3 \mapsto a_1 a_2 \otimes a_3$ de $A^{\otimes 3}$ dans $A^{\otimes 2}$.

La déviation éventuelle entre les contraintes d'associativité pour la catégorie $\mathcal{C}$ et pour le produit tensoriel se traduira par l'existence d'un élément inversible ϕ de $\mathcal{A}_3$. Le diagramme hexagonal et l'équation de Yang-Baxter prendront alors les formes modifiées

$$\Delta_{12}(R) = \phi_{312}\,R_{13}\,\phi_{132}^{-1}\,R_{23}\,\phi_{123} \tag{3.13 bis}$$

$$\Delta_{23}(R) = \phi_{231}^{-1}\,R_{13}\,\phi_{213}\,R_{12}\,\phi_{123}^{-1} \tag{3.14 bis}$$

$$R_{12}\,\phi_{312}\,R_{13}\,\phi_{132}^{-1}\,R_{23}\,\phi_{123} = \phi_{321}\,R_{23}\,\phi_{231}^{-1}\,R_{13}\,\phi_{213}\,R_{12} \ . \tag{3.15 bis}$$

Le diagramme pentagonal se traduit par l'identité suivante dans $\mathcal{A}_4$

$$\Delta_{34}(\phi)\,\Delta_{12}(\phi) = \phi_{234}\,.\,\Delta_{23}(\phi)\,.\,\phi_{123} \ . \tag{3.16}$$

3.6. Donnons un exemple simple pour conclure. Considérons l'espace $V = \mathbf{C}^N$ avec sa base naturelle $e_1, \cdots, e_N$; soit q un nombre complexe qui n'est pas une racine de l'unité. L'algèbre de Hecke $\mathcal{H}_n(q)$ est semi-simple et agit sur l'espace $V^{\otimes n}$ comme il a été expliqué au n° 2.2. Considérons la catégorie $\mathcal{C}$ dont les objets sont les espaces $V^{\otimes n}$, où les seuls morphismes sont les endomorphismes des $V^{\otimes n}$ fournis par les éléments de $\mathcal{H}_n(q)$. On considère le foncteur Φ qui associe à $V^{\otimes m}$ et $V^{\otimes n}$ leur produit tensoriel $V^{\otimes(m+n)}$. La contrainte d'associativité est celle des produits tensoriels; par contre, la contrainte de commutativité de $V^{\otimes m} \otimes V^{\otimes n}$ sur $V^{\otimes n} \otimes V^{\otimes m}$ est $P^{(m,n)}\, R^{(m,n)}$ où $P^{(m,n)}$ est la contrainte usuelle et

$$R^{(m,n)} = \prod_{i=1}^{m} \prod_{j=1}^{n} R_{i,m+j} \tag{3.17}$$

(avec les notations du n° 2.2).

L'algèbre de Hopf A_N obtenue admet les générateurs t_{ij} (pour $1 \leq i \leq N$, $1 \leq j \leq N$) satisfaisant aux relations

$$T^{(1)}\, T^{(2)}\, R = R\, T^{(2)}\, T^{(1)} \tag{3.18}$$

où T est la matrice des t_{ij} , où $T^{(1)} = T \otimes I_N$, $T^{(2)} = I_N \otimes T$. Lorsque $q = 1$, ceci exprime la commutativité des t_{ij} . Le coproduit est donné dans A_N par

$$\Delta(t_{ij}) = \sum_{k=1}^{N} t_{ik} \otimes t_{kj} \ . \tag{3.19}$$

Il s'agit là de la déformation de l'algèbre[1] des fonctions polynômes sur $\mathrm{GL}(N, \mathbf{C})$ que Faddeev et Woronowicz considèrent comme le groupe quantique associé au groupe $\mathrm{GL}(N, \mathbf{C})$. Le point de vue dual (Drinfeld, Jimbo) est celui de la déformation $U_q(\mathrm{g}\ell(N, \mathbf{C}))$ de l'algèbre enveloppante de l'algèbre de Lie $\mathrm{g}\ell(N, \mathbf{C})$.

[1] Il faudra en fait adjoindre à A_N l'inverse du déterminant quantique $\det_q T$, un polynôme qui pour $q = 1$ se réduit au déterminant de la matrice T .

4. ÉQUATIONS DIFFÉRENTIELLES ET MONODROMIE

4.1. Nous considérons le sous-espace ouvert $\mathbf{C}^n_*$ de $\mathbf{C}^n$ formé des vecteurs à composantes distinctes. On pose

$$\omega_{ij} = d\log(z_i - z_j) = \frac{d\,z_i - d\,z_j}{z_i - z_j} \tag{4.1}$$

pour $i \neq j$, en notant $z_1, \cdots, z_n$ les coordonnées sur $\mathbf{C}^n$; les ω_{ij} sont des formes différentielles holomorphes sur $\mathbf{C}^n_*$ et elles satisfont aux relations quadratiques

$$\omega_{ij} \wedge \omega_{jk} + \omega_{jk} \wedge \omega_{ki} + \omega_{ki} \wedge \omega_{ij} = 0 \tag{4.2}$$

$(i, j, k$ distincts). De plus, on a $\omega_{ij} = \omega_{ji}$. Soit $\mathcal{A}_n$ l'algèbre de formes différentielles holomorphes engendrée (sur $\mathbf{C}$) par les ω_{ij} . Les relations (4.2) forment une présentation de cette algèbre anticommutative. De plus, les formes appartenant à $\mathcal{A}_n$ constituent des représentants de la cohomologie de de Rham de $\mathbf{C}^n_*$, d'où un isomorphisme $H^*(\mathbf{C}^n_*; \mathbf{C}) \simeq \mathcal{A}_n$ (théorème d'Arnold).

4.2. Donnons-nous un espace vectoriel W de dimension finie sur $\mathbf{C}$, et des endomorphismes A_{ij} de W . On considère la forme différentielle $\Omega = \sum'_{i<j} A_{ij}\,\omega_{ij}$ sur $\mathbf{C}^n_*$, à valeurs dans $\mathrm{End}(W)$, et le système différentiel $dF = \Omega F$; les solutions sont des fonctions holomorphes $F(z) = F(z_1, \cdots, z_n)$ définies sur des ouverts de $\mathbf{C}^n_*$ à valeurs dans $\mathrm{End}(W)$. Soit γ un lacet de classe C^∞ dans $\mathbf{C}^n_*$, donné paramétriquement sous la forme $(\gamma(t))_{0 \leq t \leq 1}$. Si $F_a(z)$ est une solution de $dF = \Omega F$ au voisinage de $\gamma(0)$, on peut prolonger analytiquement $F_a(z)$ le long de γ . La fonction $F_b(z)$ obtenue est une solution de l'équation $dF = \Omega F$ au voisinage de $\gamma(1) = \gamma(0)$; elle est donnée par la formule de Lappo-Danilewski

$$F_b(z) = F_a(z)\,T(\gamma) \tag{4.3}$$

avec l'expression suivante pour le transport parallèle

$$T(\gamma) = \sum_{k \geq 0} \int_{\Delta_k} A(t_1) \cdots A(t_k)\; dt_1 \cdots dt_k \;. \tag{4.4}$$

Dans cette formule intégrale, le domaine d'intégration Δ_k est défini par les inégalités $0 \leq t_1 \leq t_2 \leq \cdots \leq t_k \leq 1$ et la forme différentielle opératorielle $A(t)\,dt$ s'obtient par la substitution $z = \gamma(t)$ dans Ω .

4.3. Le système différentiel $dF = \Omega F$ est *complètement intégrable* si $T(\gamma)$ ne dépend que de la classe d'homotopie du lacet γ (d'origine fixée). Le critère classique est le suivant

$$d\Omega - \Omega \wedge \Omega = 0 \; ; \tag{4.5}$$

les deux membres appartiennent à $\mathcal{A}_n \otimes \mathrm{End}\, W$, et vu le théorème d'Arnold cité en 4.1, cette relation équivaut aux suivantes :

$$[A_{ij}, A_{ik} + A_{jk}] = 0 \qquad \text{pour } i, j, k \text{ distincts} \tag{4.6}$$

$$[A_{ij}, A_{k\ell}] = 0 \qquad \text{pour } i, j, k, \ell \text{ distincts} \; . \tag{4.7}$$

S'il en est ainsi, choisissons un point-base a dans $\mathbf{C}^n_*$ et réalisons le groupe de tresses pures P_n comme le groupe $\pi_1(\mathbf{C}^n_*; a)$. La formule de transport parallèle (4.4) appliquée aux lacets en a fournit une représentation linéaire du groupe P_n dans l'espace W ; elle transforme la classe d'homotopie du lacet γ en l'automorphisme $T(\gamma)^{-1}$ de W.

Introduisons l'algèbre de Lie $\mathcal{G}_n$ quotient de l'algèbre de Lie libre de générateurs $X_{ij} = X_{ji}$ (pour $i < j$) par l'idéal engendré par les éléments :

$$[X_{ij}, X_{ik} + X_{jk}] \qquad \text{et} \qquad [X_{ij}, X_{k\ell}]$$

sous les mêmes conditions que (4.6) et (4.7). On note ξ_{ij} l'image de X_{ij} dans $\mathcal{G}_n$ et l'on introduit la forme différentielle "générique"

$$\omega = \sum_{i<j} \omega_{ij} \otimes \xi_{ij} \tag{4.8}$$

dans $\mathcal{A}_n \otimes \mathcal{G}_n$.

Le résultat précédent peut se traduire en disant que toute représentation linéaire ρ de $\mathcal{G}_n$ dans l'espace W (envoyant ξ_{ij} sur A_{ij} , donc ω sur Ω) définit une représentation linéaire T du groupe P_n dans W. Réciproquement, toute représentation du groupe P_n par des automorphismes unipotents de

W provient d'une représentation ρ de $\mathcal{G}_n$ par des endomorphismes nilpotents de W [1]. Il est donc raisonnable de considérer *l'algèbre de Lie* $\mathcal{G}_n$ *comme l'algèbre de Lie du groupe* P_n (ou aussi du groupe B_n dans lequel il est d'indice fini) et les relations

$$[\xi_{ij}, \xi_{ik} + \xi_{jk}] = 0 \quad , \quad [\xi_{ij}, \xi_{k\ell}] = 0 \tag{4.9}$$

comme l'analogue infinitésimal des relations (1.3) et (1.4) de définition de B_n . Cette interprétation est renforcée par le théorème suivant (cas particulier des théorèmes sur la monodromie que j'ai exposés dans [F1]) :

Soit $(\mathbf{C}\,P_n)^\wedge$ *le complété de l'algèbre du groupe* $\mathbf{C}\,P_n$ *pour la topologie I-adique, où I est l'idéal d'augmentation* (engendré par les $g - 1$ pour g dans P_n). *De manière analogue, complétons l'algèbre enveloppante* $U\,\mathcal{G}_n$ *en* $(U\,\mathcal{G}_n)^\wedge$ *pour la topologie J-adique, où J est l'idéal bilatère engendré par* $\mathcal{G}_n$ *dans* $U\,\mathcal{G}_n$. *Les algèbres* $(\mathbf{C}\,P_n)^\wedge$ *et* $(U\,\mathcal{G}_n)^\wedge$ *sont isomorphes, et le groupe* P_n *se plonge dans* $(\mathbf{C}\,P_n)^\wedge$.

4.4. Voici une manière de construire des solutions des équations (4.6) et (4.7). *L'équation de Yang-Baxter classique* s'écrit sous la forme

$$[r_{12}(u_{12}), r_{13}(u_{13})] + [r_{12}(u_{12}), r_{23}(u_{23})] + [r_{13}(u_{13}), r_{23}(u_{23})] = 0\,. \tag{4.10}$$

La signification est la suivante : V est un espace vectoriel de dimension finie, $r(u)$ est un opérateur dans $V \otimes V$ dépendant du paramètre complexe u de manière holomorphe ou méromorphe, on pose $u_{ij} = u_i - u_j$ et $r_{ij}(u)$ désigne $r(u)$ agissant sur les facteurs d'indices i et j (avec $i < j$) du produit tensoriel triple $V^{\otimes 3}$. D'après Belavin et Drinfeld [F2], on obtient comme suit une solution de (4.10) : choisissons une algèbre de Lie semi-simple

[1] Dans [F5], Kohno démontre la réciproque sous l'hypothèse que la représentation de P_n est "assez voisine de l'identité". Il se réfère pour cela à un résultat de Golubeva (Math. USSR Izvest. **17** (1981), p. 227-241) qui ne s'applique malheureusement pas au cas utilisé. On peut cependant réparer la démonstration en utilisant le théorème d'approximation de M. Artin.

complexe $\mathcal{G}$, de forme de Killing B , une base (I_μ) de $\mathcal{G}$ orthonormale pour B et une représentation linéaire ρ de $\mathcal{G}$ dans V . On pose alors

$$r(u) = t/u \qquad \text{avec} \qquad t = \sum_\mu \rho(I_\mu) \otimes \rho(I_\mu) \,. \tag{4.11}$$

En utilisant le fait que l'élément $\sum_\mu I_\mu \otimes I_\mu$ de $\mathcal{G} \otimes \mathcal{G}$ est invariant par la représentation adjointe de $\mathcal{G}$, on établit les relations

$$\big[t_{12}, t_{13} + t_{23}\big] = \big[t_{23}, t_{12} + t_{13}\big] = 0 \tag{4.12}$$

et (4.10) s'ensuit immédiatement. Par ailleurs, si l'on note W l'espace $V^{\otimes n}$, les opérateurs t_{ij}, agissant dans W selon nos conventions habituelles, satisfont aux relations

$$\big[t_{ij}, t_{ik} + t_{jk}\big] = 0 \quad , \quad \big[t_{ij}, t_{k\ell}\big] = 0 \tag{4.13}$$

analogues à (4.6) et (4.7). Si l'on fait agir simultanément le groupe symétrique $\mathbf{S}_n$ sur $\mathbf{C}^n_*$ (par permutation des coordonnées) et sur $W = V^{\otimes n}$ de la manière habituelle, la forme différentielle $\Omega = \lambda \sum_{i<j} t_{ij}\, \omega_{ij}$ est invariante par $\mathbf{S}_n$ pour toute valeur complexe de λ ; on obtient alors un système complètement intégrable sur l'espace de configuration $\Phi_n(\mathbf{C}) = \mathbf{C}^n_*/\mathbf{S}_n$. Par intégration, on en déduit une représentation de monodromie T_λ de $B_n = \pi_1(\Phi_n(\mathbf{C}))$ dans W . Il résulte des raisonnements classiques de Fuchs sur les singularités des équations différentielles que l'opérateur $T_\lambda(\sigma_j)$ dans W correspondant au générateur σ_j de B_n est conjugué dans $GL(V^{\otimes n})$ à $P_j \exp \pi i\, \lambda\, t_{j,j+1}$, où P_j est l'échange des facteurs de rang j et $j+1$ dans le produit tensoriel $V^{\otimes n}$.

4.5. Drinfeld a réussi dans [D9] à identifier la représentation T_λ de B_n . Écrivons l'équation $dF = \Omega F$ sous la forme de Zamolodchikov

$$\frac{\partial F}{\partial z_j} = \lambda \sum_{\substack{k=1 \\ k \neq j}}^{n} \frac{t_{jk}}{z_j - z_k} \,.\, F \;; \tag{4.14}$$

elle est invariante si l'on soumet chaque variable z_j à la même transformation affine $z_j \mapsto a\, z_j + b$. Par suite, pour $n = 3$, on obtient des solutions

sous la forme

$$F(z_1, z_2, z_3) = G\left(\frac{z_1 - z_2}{z_1 - z_3}\right)(z_1 - z_3)^{\lambda(t_{12}+t_{13}+t_{23})} \; ; \tag{4.15}$$

sur le revêtement universel de $\mathbf{C}^3_*$, le logarithme de $z_1 - z_3$ a un sens et l'on a posé $(z_1 - z_3)^\alpha = \exp \alpha \log(z_1 - z_3)$ (comme il se doit). La fonction G est définie sur le revêtement universel de $\mathbf{C}\backslash\{0,1\}$, à valeurs dans $\mathrm{End}(V^{\otimes 3})$, et satisfait à l'équation différentielle

$$\frac{dG}{dx} = \lambda\left(\frac{t_{12}}{x} + \frac{t_{23}}{x-1}\right) G(x) \; . \tag{4.16}$$

Conformément à la théorie de Fuchs, il y a une solution $G_1(x)$ se comportant comme $x^{\lambda t_{12}}$ pour x tendant vers 0 , et une solution $G_2(x)$ se comportant comme $(1-x)^{\lambda t_{23}}$ pour x tendant vers 1 . Ces deux solutions diffèrent par une constante, d'où un automorphisme $\phi_V(\lambda)$ de $V^{\otimes 3}$ tel que $G_1(x) = G_2(x)\,\phi_V(\lambda)$ pour tout x . On montre facilement qu'il existe une série formelle $\phi(\lambda)$ en la variable λ, à coefficients dans $(U\mathcal{G})^{\otimes 3}$, indépendante de la représentation linéaire (ρ, V) de $\mathcal{G}$, dont l'image par $\rho^{\otimes 3}$ donne le développement en série de $\phi_V(\lambda)$.

En étudiant le comportement asymptotique des solutions de l'équation de Zamolodchikov pour $n = 4$, lorsque certaines des différences $z_j - z_k$ tendent vers 0 , on établit l'analogue suivant de la relation (3.16)

$$\Delta_{34}(\phi)\,\Delta_{12}(\phi) = \phi_{234}\,.\,\Delta_{23}(\phi)\,.\,\phi_{123} \; , \tag{4.17}$$

à interpréter comme égalité de séries formelles en λ à coefficients dans $(U\mathcal{G})^{\otimes 4}$. Dans cette formule, le coproduit $\Delta : U\mathcal{G} \to (U\mathcal{G})^{\otimes 2}$ est le classique, tel que $\Delta(x) = x \otimes 1 + 1 \otimes x$ pour x dans $\mathcal{G}$. Drinfeld démontre ensuite, par une procédure récursive, l'existence d'une série formelle $F(\lambda)$ à coefficients dans $(U\mathcal{G})^{\otimes 2}$, telle que $F(0) = 1$ et

$$\phi(\lambda) = F_{23}(\lambda)(\Delta_{23}\,F)(\lambda)(\Delta_{12}\,F)(\lambda)^{-1}\,F_{12}(\lambda)^{-1} \; . \tag{4.18}$$

On modifie le coproduit dans $(U\mathcal{G})[[\lambda]]$ en posant

$$\Delta_\lambda(a) = F(\lambda)\,\Delta(a)\,F(\lambda)^{-1} \tag{4.19}$$

pour a dans $U\mathcal{G}$. D'après les équations (4.17) et (4.18), le *nouveau coproduit* Δ_λ *est coassociatif.* Grâce à un théorème d'unicité convenable, Drinfeld montre que *l'algèbre* $(U\mathcal{G})[[\lambda]]$ *munie du coproduit* Δ_λ *est isomorphe à la quantification de Drinfeld-Jimbo de* $U\mathcal{G}$. Notons $F_{21}(\lambda)$ l'image de $F(\lambda) = F_{12}(\lambda)$ par la symétrie de $(U\mathcal{G})^{\otimes 2}$. Alors, on définit une série formelle $R(\lambda)$ à coefficients dans $(U\mathcal{G})^{\otimes 2}$ par la formule

$$R(\lambda) = F_{21}(\lambda) \cdot \left(\exp \lambda \sum_{\mu} (I_\mu \otimes I_\mu)/2 \right) \cdot F_{12}(\lambda)^{-1} \ . \tag{4.20}$$

Elle satisfait à l'équation de Yang-Baxter

$$R_{12}(\lambda)\, R_{13}(\lambda)\, R_{23}(\lambda) = R_{23}(\lambda)\, R_{13}(\lambda)\, R_{12}(\lambda) \tag{4.21}$$

(égalité de séries formelles à coefficients dans $(U\mathcal{G})^{\otimes 3}$).

En conclusion, *la représentation* T_λ *de* B_n *par des opérateurs dans* $W = V^{\otimes n}$ *est équivalente*[1] *à la représentation de* B_n *qui applique le générateur* σ_i *sur l'opérateur*

$$\rho^{\otimes n}(\underbrace{1 \otimes \cdots \otimes 1}_{i-1} \otimes R(\lambda) \otimes \underbrace{1 \otimes \cdots \otimes 1}_{n-i-1}) \ .$$

Par exemple, si $\mathcal{G} = s\ell(N, \mathbf{C})$ avec la représentation naturelle ρ dans $\mathbf{C}^N$, on a

$$t(x \otimes y) = \frac{1}{2N}\,(y \otimes x) - \frac{1}{2N^2}\,(x \otimes y) \ . \tag{4.22}$$

Si l'on pose $q = e^{\pi i \lambda / N}$, la représentation obtenue est celle liée à $\mathcal{H}_n(q)$, à torsion près par une représentation de degré 1 de B_n (voir le n° 2.2).

(1) Au sens des séries formelles en λ ; il faudrait établir la convergence !

5. CATÉGORIES ASSOCIÉES AUX TRESSES ET AUX CABLAGES

5.1. Turaev et Reshetikhin, après Freyd et Yetter, ont introduit un calcul graphique, lié aux tresses, et aux cablages qui les généralisent. Cela leur a permis de donner dans [C19] une construction rigoureuse des invariants associés par Witten aux variétés de dimension 3 ; pour ces invariants, je renvoie à la brillante description donnée dans ce même Séminaire par M. Atiyah. La méthode de Turaev et Reshetikhin fournit aussi un traitement graphique du calcul tensoriel classique, très proche de celui de Penrose dans [G8].

5.2. Le point de départ est que *les tresses colorées forment une catégorie.* Introduisons un ensemble $\mathcal{X}$ de "couleurs". Les objets de la catégorie $Tr(\mathcal{X})$ sont les suites $(x_1, \cdots, x_n)$ d'éléments de $\mathcal{X}$; les morphismes sont les tresses "colorées", chaque brin étant associé à un élément de $\mathcal{X}$. Une telle coloration des n brins détermine évidemment une coloration des extrémités supérieures, donnant une suite $(x_1, \cdots, x_n)$ qui est l'objet de $Tr(\mathcal{X})$ dont part la tresse colorée ; définition analogue du but par les extrémités inférieures. Avec ces conventions, la composition des tresses est telle qu'un brin garde la même couleur tout au long. De plus, on définit un foncteur strictement associatif Φ dans $Tr(\mathcal{X})$: sur les objets, on a $\Phi(x, x') = (x_1, \cdots, x_n, x'_1, \cdots, x'_{n'})$ si $x = (x_1, \cdots, x_n)$ et $x' = (x'_1, \cdots, x'_{n'})$; sur les flèches, on juxtapose une tresse à n brins t à gauche et une tresse à n' brins t' à droite. Notation $x \times x'$ pour $\Phi(x, x')$ et $t \times t'$ pour $\Phi(t, t')$. Il y a une contrainte de commutativité qu'on laisse au lecteur le soin de décrire graphiquement.

Supposons alors qu'à chaque couleur $x \in \mathcal{X}$ on associe un espace vectoriel V_x et qu'on se donne des opérateurs linéaires $R_{x,y} : V_x \otimes V_y \to V_x \otimes V_y$. On suppose que, pour tout triplet de couleurs x, y, z , on a la relation de Yang-Baxter

$$R_{12}\, R_{13}\, R_{23} = R_{23}\, R_{13}\, R_{12}$$

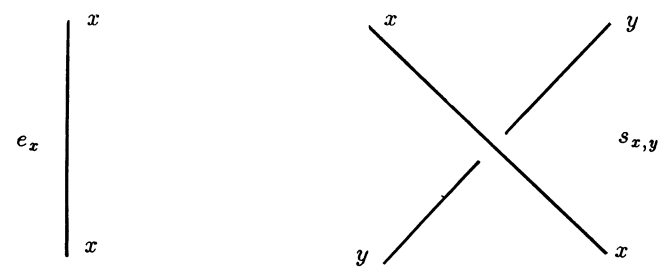
entre opérateurs sur $V_x \otimes V_y \otimes V_z$; par exemple, on a $R_{12} = R_{x,y} \otimes \mathrm{Id}_{V_z}$, etc...

On peut alors généraliser la construction du n° 2.1. Si t est une tresse colorée, de source $x = (x_1, \cdots, x_n)$ et de but $y = (y_1, \cdots, y_n)$, on lui associe une application linéaire $H(t)$ de $H(x) = V_{x_1} \otimes \cdots \otimes V_{x_n}$ dans $H(y) = V_{y_1} \otimes \cdots \otimes V_{y_n}$. On obtient ainsi un foncteur H de la catégorie $Tr(\mathcal{X})$ dans celle des espaces vectoriels sur $\mathbf{C}$. Il est caractérisé par les propriétés suivantes :

a) *on a* $H(x \times y) = H(x) \otimes H(y)$ *pour les objets et les flèches* ;

b) *si* $s_{x,y}$ *est la tresse colorée à 2 brins ci-dessous, on a* $H(S_{x,y}) = \sigma_{x,y} R_{x,y}$, *où* $\sigma_{x,y}$ *est la symétrie usuelle de* $V_x \otimes V_y$ *sur* $V_y \otimes V_x$;

c) *si* e_x *est la tresse à 1 brin ci-dessous,* $H(e_x)$ *est l'application identique de* V_x.



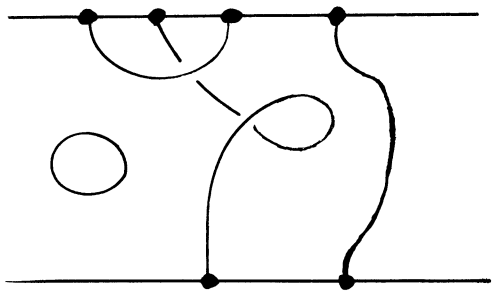
5.3. On généralise la notion de tresse en celle de *cablage.* Supposons donc donnés deux plans parallèles Π et Π' , une suite de points distincts $P_1, \cdots, P_n$ dans Π et de même $P'_1, \cdots, P'_{n'}$ dans Π'. Un cablage M ayant les extrémités $P_1, \cdots, P_n, P'_1, \cdots, P'_{n'}$ sera réunion d'un nombre fini d'arcs ou de lacets (différentiables par morceaux) ; on fait les hypothèses suivantes :

a) ces arcs et lacets sont deux à deux disjoints ;

b) les extrémités des arcs appartiennent à l'ensemble $\{P_1, \cdots, P_n, P'_1, \cdots, P'_{n'}\}$ et chacun de ces points intervient exactement une fois ;

c) si C est l'un des arcs ou lacets, il est transverse à tous les plans parallèles à Π et Π' sauf éventuellement un nombre fini ;

d) M est entièrement contenu dans la région H comprise entre les plans Π et Π'.



Une projection plane d'un cablage

On remarquera qu'un entrelac n'est autre qu'un cablage dont l'ensemble des extrémités est vide. De plus, on supposera chaque arc ou lacet *orienté*, et *muni d'une couleur* appartenant à un ensemble $\mathcal{X}$. Deux telles configurations sont équivalentes s'il existe un homéomorphisme de $\mathbf{R}^3$, conservant l'orientation et transformant l'une en l'autre.

Ces cablages colorés forment les flèches d'une catégorie $Cab(\mathcal{X})$ *dont les objets sont les suites* $(x_1, \varepsilon_1, \cdots, x_n, \varepsilon_n)$ *formées de couleurs* $x_1, \cdots, x_n$ *et de nombres* $\varepsilon_1, \cdots, \varepsilon_n$ *égaux à* 1 *ou* -1 . Les conventions de source et de but sont figurées ci-dessous

A côté des configurations fournies par les tresses, apparaissent deux situations élémentaires nouvelles

5.4. Décrivons maintenant une méthode très générale pour fabriquer des invariants d'isotopie des entrelacs. On reprend les hypothèses du n° 3.5. Soit $(A, \Delta, \varepsilon, S)$ une algèbre de Hopf ; on note $\mathcal{A}_n$ l'algèbre duale de la

coalgèbre $A^{\otimes n}$ et l'on suppose donné un élément R de $\mathcal{A}_2$ satisfaisant aux relations (3.12) à (3.15) de Drinfeld. On considère des comodules sur la coalgèbre A , de dimension finie comme espaces vectoriels sur $\mathbf{C}$; ce sont des $\mathcal{A}_1$-modules. Si M et N sont deux tels comodules, R définit un opérateur $R_{M,N}$ dans l'espace vectoriel $M \otimes N$. De plus, l'antipodisme S de A permet d'associer à tout comodule M (à gauche sur A) un comodule $M^\vee$ (à gauche sur A) dont l'espace vectoriel sous-jacent est le dual de M . On note aussi $\mathbf{1}$ le A-module ayant $\mathbf{C}$ pour espace vectoriel sous-jacent avec le coproduit $\lambda \mapsto 1 \otimes \lambda$ de $\mathbf{C}$ dans $A \otimes \mathbf{C}$. Il existe alors deux homomorphismes de comodules

$$e_M : \mathbf{1} \longrightarrow M \otimes M^\vee \qquad , \qquad \varepsilon_M : M^\vee \otimes M \longrightarrow \mathbf{1}$$

définis par

$$e_M(1) = \sum_{i=1}^{N} v_i \otimes v^i \qquad , \qquad \varepsilon_M(x \otimes y) = \langle x, y \rangle$$

($v_1, \cdots, v_N$ forment une base de M sur $\mathbf{C}$, et $v^1, \cdots, v^N$ la base duale de $M^\vee$).

Supposons qu'on ait associé à chaque couleur $x \in \mathcal{X}$ un comodule M_x. Grâce aux opérateurs de Yang-Baxter R_{M_x,M_y} , on peut définir comme au n° 5.2 un foncteur H de la catégorie $Tr(\mathcal{X})$ dans celle des A-comodules. On peut alors étendre ce foncteur en un foncteur $\widetilde{H}$ de la catégorie $Cab(\mathcal{X})$ vers celle des comodules sur A . Il suffit d'ajouter les règles suivantes aux règles a), b) et c) du n° 5.2 :

d) *A un objet* $(x_1, \varepsilon_1, \cdots, x_n, \varepsilon_n)$ *de* $Cab(\mathcal{X})$, *on associe le comodule* $M_{x_1}^{\varepsilon_1} \otimes \cdots \otimes M_{x_n}^{\varepsilon_n}$ (par convention, on a $M^+ = M$ et $M^- = M^\vee$) ; *en particulier, l'objet vide de* $Cab(\mathcal{X})$ *donne par* $\widetilde{H}$ *le comodule* $\mathbf{1}$.

e) *Le foncteur* $\widetilde{H}$ *associe à la configuration* a_x *ci-dessous le morphisme* e_{M_x} *de* $\mathbf{1}$ *dans* $M_x \otimes M_x^\vee$ *et à* b_x *il associe le morphisme* ε_{M_x} *de* $M_x^\vee \otimes M_x$ *dans* $\mathbf{1}$.

Le point crucial est que *deux cablages isotopes fournissent le même morphisme de comodules. En particulier, un entrelac coloré et orienté L fournit un endomorphisme de* **1** *, c'est-à-dire un nombre complexe $e(L)$. Ce nombre ne dépend que de la classe d'isotopie de L* . On comparera ce résultat aux théories quantiques des champs topologiques de Witten et Atiyah. Il restera à expliciter les invariants ainsi obtenus !!

BIBLIOGRAPHIE RAISONNÉE

A. Ouvrages généraux

Voici d'abord les textes fondateurs :

[1] E. ARTIN - *Collected papers* (édités par S. Lang et J. Tate), Addison-Wesley, 1965. [Voir en particulier la partie consacrée à la Topologie (p. 416-498) qui contient les articles célèbres : *Theorie der Zöpfe* (1925), *Theory of braids* (1947), *Braids and permutations* (1947).]

[2] W. BURAU - *Über Zopfinvarianten*, Hamburg Abh. **9** (1932), p. 117-124.

[3] A.A. MARKOV - *Über die freie Equivalenz der geschlossenen Zöpfe*, Recueil Soc. Math. Moscou **43** (1936), p. 73-78.

[4] R.H. FOX - *Free differential calculus* I : *Derivations in the free group ring*, Ann. of Math. **57** (1953), p. 547-560.

[5] E. FADELL and L. NEUWIRTH - *Configuration spaces*, Math. Scand. **10** (1962), p. 111-118.

[6] R.H. FOX and L. NEUWIRTH - *The braid groups*, Math. Scand. **10** (1962), p. 119-126.

Nous donnons maintenant une sélection de manuels consacrés essentiellement aux nœuds et tresses.

[7] K. REIDEMEISTER - *Knotentheorie*, Erg. Math. Vol. 1, Springer (1932).

[8] R.H. CROWELL and R.H. FOX - *Introduction to knot theory*, Ginn Co. (1963) (réimprimé dans GTM, vol. 57, Springer (1977)).

[9] L. NEUWIRTH - *Knot groups*, Annals Math. Studies **56**, Princeton Univ. Press (1965).

[10] W. MAGNUS, A. KARASS, D. SOLITAR - *Combinatorial group theory*, Interscience/Wiley (1966).

[11] J. BIRMAN - *Braids, links and mapping class groups*, Annals Math. Studies **82**, Princeton Univ. Press (1974).

[12] J. ROLFSEN - *Knots and links*, Publish or Perish (1976).

[13] L. KAUFFMAN - *Formal knot theory*, Math. Notes **30**, Princeton Univ. Press (1983).

[14] G. BURDE and H. ZIESCHANG - *Knots*, W. de Gruyter (1985).

Mentionnons également deux rapports au Séminaire N. Bourbaki qui ont conservé une certaine actualité :

[15] A. GRAMAIN - *Rapport sur la théorie classique des nœuds* (1ère partie), Sém. Bourbaki, exp. n° 485, juin 1976, Springer, Lect. Notes Math. **567** (1977), p. 222-237.

[16] A. DOUADY - *Nœuds et structures de contact en dimension* 3 [*d'après D. Bennequin*], Sém. Bourbaki, exp. n° 604 (février 1983), Astérisque **105-106**, 1983, p. 129-148.

Pour terminer, mentionnons un ouvrage récent explorant la plupart des aspects liés aux groupes de tresses :

[17] J. BIRMAN and A. LIBGOBER (éditeurs) - *Braids*, Proceedings of a Research Conference, Contemporary Math. vol. 78, American Math. Soc. (1988).

B. Catégories et dualité

Articles fondamentaux sur les conditions de cohérence dans les catégories :

[1] S. MACLANE - *Natural associativity and commutativity*, Rice Univ. Studies, **49** (1963), p. 28-46.

[2] S. EILENBERG and G.M. KELLY - *Closed categories*, in Proc. Conf. Categorical Algebra, Springer (1966).

[3] S. MACLANE - *Categories for the working mathematician*, GTM vol. 5, Springer (1974).

[4] G.M. KELLY and M.L. LAPLAZA - *Coherence for compact closed categories*, J. Pure Appl. Alg. **19** (1980), p. 193-213.

Pour la dualité de Tannaka "classique" des groupes compacts, les articles de base :

[5] T. TANNAKA - *Über den Dualitätssatz der nicktkommutativen topologischen Gruppen*, Tohoku Math. J. **45** (1939), p. 1-12.

[6] M.G. KREIN - *A principle of duality for a bicompact group and a square block algebra*, Dokl. Akad. Nauk SSSR **69** (1949), p. 725-728.

[7] M. TAKESAKI - *A characterization of group algebras as a converse of Tannaka-Stinespring-Tatsuuma duality theorem*, Amer. J. Math. **91** (1969), p. 529-564.

[8] S. DOPLICHER and J. ROBERTS - *Duals of compact Lie groups realized in the Cuntz algebras and their actions on C^*-algebras*, J. Funct. Anal. **74** (1987), p. 96-120.

[9] S. DOPLICHER and J. ROBERTS - *Endomorphisms of C^*-algebras, cross products and duality for compact groups*, Ann. of Math. **130** (1989), p. 78-119.

[10] S. DOPLICHER and J. ROBERTS - *A new duality theory for compact groups*, Invent. Math. **98** (1989), p. 157-218.

Pour une extension dans le cas des groupes quantiques :

[11] P. GHEZ, R. LIMA and J. ROBERTS - *W^*-categories*, Pacific J. Math. **120** (1985), p. 79-109.

[12] S.L. WORONOWICZ - *Duality in the C*-algebra theory*, Proc. Int. Cong. Math., Varsovie 1983, vol. 2, p. 1347-1350.

[13] S.L. WORONOWICZ - *Compact matrix pseudo-groups*, Comm. Math. Phys. **111** (1987), p. 613-665.

[14] S.L. WORONOWICZ - *Tannaka-Krein duality for compact matrix pseudo-groups. Twisted SU(N)*, Invent. Math. **93** (1988), p. 35-76.

Enfin, l'extension de la dualité de Tannaka-Krein aux groupes algébriques :

[15] C. CHEVALLEY - *Théorie des groupes de Lie, tome* II : *groupes algébriques*, Hermann (1951).

[16] P. CARTIER - *Dualité de Tannaka et algèbres de Lie*, C.R. Acad. Sci. Paris, **242** (1956), p. 322-325.

[17] S. SAAVEDRA - *Catégories tannakiennes*, Lect. Notes Math. vol. 265, Springer (1972).

[18] P. DELIGNE et J.S. MILNE - *Tannakian categories* in *Hodge cycles, Motives and Shimura varieties*, Lect. Notes Math. vol. 900, Springer (1982).

[19] P. DELIGNE - *Catégories tannakiennes*, in Grothendieck's Festschrift, Prog. in Math., Birkhäuser (1990), à paraître.

C. Invariants polynomiaux des nœuds

Voici les articles originaux pour le polynôme de Jones :

[1] V. JONES - *Index for subfactors*, Invent. Math. **72** (1983), p. 1-25.

[2] V. JONES - *A polynomial invariant for knots via von Neumann algebras*, Bull. Amer. Math. Soc. **12** (1985), p. 103-112.

[3] V. JONES - *Braid groups, Hecke algebras and type* II_1 *factors*, in "Geometric methods in operator algebras", Proc. U.S.-Japan Symposium, Wiley, 1986, p. 242-273.

[4] V. JONES - *On a certain value of the Kauffman polynomial*, Comm. Math. Phys.

[5] V. JONES - *Hecke algebra representations of braid groups and link polynomials*, Ann. of Math. **126** (1987), p. 335-388.

[6] V. JONES - *Notes on subfactors and statistical mechanics*, in "Braid group, knot theory and statistical mechanics" (C.N. Yang et M.L. Ge, éditeurs), World Scientific, 1989, p. 1-25.

[7] A. OCNEANU - *Quantized groups, string algebras and Galois theory for algebras*, prépublication Penn. State Univ., 1985.

[8] A. OCNEANU - *A polynomial invariant for knots : a combinatorial and an algebraic approach*, à paraître.

[9] H. WENZL - *Representations of Hecke algebras and subfactors*, Thèse, Univ. of Pennsylvania, 1985.

[10] H. WENZL - *Hecke algebras of type A_n and subfactors*, Invent. Math. **92** (1988), p. 349-383.

[11] H. WENZL - *Braid group representations and the quantum Yang-Baxter equation*, à paraître.

La généralisation en un polynôme à deux variables est contenue dans l'article-annonce :

[12] P. FREYD, D. YETTER, J. HOSTE, W. LICKORISH, K. MILLETT, A. OCNEANU - *A new polynomial invariant of knots and links*, Bull. Amer. Math. Soc. **12** (1985), p. 239-246.

Les articles suivants fournissent un exposé général et des extensions des résultats précédents :

[13] A. CONNES - *Indice des sous-facteurs, algèbres de Hecke et théorie des nœuds*, Sém. Bourbaki, exp. n° 647, juin 1985, Astérisque **133-134** (1986), p. 289-308.

[14] F. GOODMAN, P. DE LA HARPE et V. JONES - *Coxeter-Dynkin diagrams and towers of algebras*, M.S.R.I. Publ. vol. 14, Springer (1989).

[15] P. DE LA HARPE, M. KERVAIRE et C. WEBER - *On the Jones polynomial*, Ens. Math. **32** (1986), p. 271-335.

[16] P. VOGEL - *Représentations et traces des algèbres de Hecke, polynôme de Jones-Conway*, Ens. Math. **34** (1988), p. 333-356.

Voici la référence de base sur les représentations des algèbres de Hecke :

[17] P.N. HOEFSMIT - *Representations of Hecke algebras of finite groups with BN pairs of classical type*, Thèse, Univ. of British Columbia, 1974.

Enfin, l'approche tridimensionnelle est contenue dans les travaux suivants :

[18] M. ATIYAH - *Topological quantum field theories*, Publ. I.H.E.S. **68** (1988), p. 175-186.

[19] N. RESHETIKHIN and V. TURAEV - *Invariants of 3-manifolds via link polynomial and quantum groups*, à paraître.

[20] E. WITTEN - *Quantum field theory and the Jones polynomial*, Comm. Math. Phys. **121** (1989), p. 351-399.

D. Groupes quantiques et invariants des nœuds

Références de base sur les groupes quantiques :

[1] V. DRINFELD - *Hopf algebras and the quantum Yang-Baxter equation*, Sov. Math. Dokl. **32** (1985), p. 254-258.

[2] V. DRINFELD - *Quantum groups*, Proc. Int. Cong. Math., Berkeley 1986, vol. 1, p. 798-820.

Y joindre un compte-rendu à Bourbaki :

[3] J.-L. VERDIER - *Groupes quantiques [d'après V. Drinfeld]*, Sém. Bourbaki, exp. n° 685, juin 1987, Astérisque **152-153** (1987), p. 305-319.

Sur les représentations des groupes quantiques :

[4] J. JIMBO - *A q-analogue of $U(g\ell(N+1))$, Hecke algebras and the Yang-Baxter equation*, Lett. Math. Phys. **11** (1986), p. 247-252.

[5] A. KIRILLOV and N. RESHETIKHIN - *Representations of the algebra $U_q(s\ell(2))$, q-orthogonal polynomials and invariants of links*, LOMI preprint, Leningrad, 1988.

[6] G. LUSZTIG - *Quantum deformations of certain simple modules over enveloping algebras*, Adv. Math. **70** (1988), p. 237-249.

[7] M. ROSSO - *Finite dimensional representations of the quantum analog of the enveloping algebra of a complex simple Lie algebra*, Comm. Math. Phys. **117** (1988), p. 581-593. [Corrections dans la thèse de l'auteur.]

Pour conclure, voici une liste de travaux de l'École de Léningrad (applications des groupes quantiques aux invariants des nœuds) :

[8] V. DRINFELD - *Sur les algèbres de Hopf presque cocommutatives*, à paraître dans "Algebra and Analysis", Leningrad, 1989 (en russe).

[9] V. DRINFELD - *Quasi-algèbres de Hopf*, Algebra and Analysis, vol. 1, n° 2 (1989), p. 30-46 (en russe).

[10] N. RESHETIKHIN - *Quantized universal enveloping algebras, the Yang-Baxter equation and invariants of links*, I, II, LOMI preprint, Léningrad, 1988.

[11] N. RESHETIKHIN - *Algèbres de Hopf quasi-triangulaires et invariants des nœuds*, Algebra and Analysis, vol. 1, n° 2 (1989), p. 169-188 (en russe).

[12] N. RESHETIKHIN, L. TAKHTADJAN et L. FADDEEV - *Groupes de Lie quantiques et algèbres de Lie*, Algebra and Analysis, vol. 1, n° 2 (1989), p. 178-205 (en russe).

[13] V. TURAEV - *The Yang-Baxter equation and invariants of links*, Invent. Math. **92** (1988), p. 527-553.

[14] V. TURAEV - *Algebra of loops on surfaces, algebra of knots, and quantization*, LOMI preprint, Léningrad, 1988.

Référence supplémentaire :

[15] C.M. RINGEL - *Hall algebras and quantum groups*, à paraître (Bielefeld, RFA).

E. Topologie des espaces de configuration

Le point de départ est fourni par les travaux d'Arnold et Brieskorn :

[1] V.I. ARNOLD - *The cohomology ring of the colored braid group*, Mat. Zametki **5** (1969), p. 227-231.

[2] V.I. ARNOLD - *Topological invariants of algebraic functions* II, Funct. Anal. Appl. **4** (1970), p. 91-98.

[3] E. BRIESKORN - *Die Fundamentalgruppe des Raumes der regulären Orbits einer endlichen komplexen Spiegelungsgruppe*, Invent. Math. **12** (1971), p. 57-61.

Il y a eu déjà deux rapports au Séminaire Bourbaki sur ce sujet :

[4] E. BRIESKORN - *Sur les groupes de tresses [d'après V.I. Arnold]*, Sém. Bourbaki, exp. n° 401, novembre 1971, Springer, Lect. Notes Math. **317** (1973), p. 21-44.

[5] P. CARTIER - *Arrangements d'hyperplans : un chapitre de Géométrie combinatoire*, Sém. Bourbaki, exp. n° 582, novembre 1980, Springer, Lect. Notes Math. **901** (1982), p. 1-22.

Quant à la structure des groupes de tresses, elle est élucidée dans ce qui suit :

[6] F.A. GARSIDE - *The braid groups and other groups*, Quart. J. Math. Oxford **20**, (1969), p. 235-254.

[7] E. BRIESKORN and K. SAITO - *Artin-Gruppen und Coxeter-gruppen*, Invent. Math. **17**, (1972), p. 245-271.

[8] P. DELIGNE - *Les immeubles des groupes de tresses généralisés*, Invent. Math. **17**, (1972), p. 273-302.

[9] M. FALK and R. RANDELL - *Pure braid groups and products of free groups*, in "Braids", Contemporary Math., Amer. Math. Soc. (1988), vol. 78, p. 217-228.

F. Équations différentielles et monodromie

Pour un rapport général sur la monodromie, voir mon exposé récent :

[1] P. CARTIER - *Jacobiennes généralisées, monodromie unipotente et intégrales itérées*, Sém. Bourbaki, exp. n° 687, novembre 1987, Astérisque **161–162** (1988), p. 31-52.

Voici quelques références complétant la bibliographie de cet exposé :

[2] A.A. BELAVIN and V. DRINFELD - *Solution of the classical Yang-Baxter equation for simple Lie algebras*, Funct. Anal. Appl. **16** (1982), p. 1-29.

[3] T. KOHNO - *Homology of a local system on the complement of hyperplanes*, Proc. Japan Acad. Sci. **62**, série A (1986), p. 144-147.

[4] T. KOHNO - *One-parameter family of linear representations of Artin's braid groups*, Adv. Stud. in Pure Math. **12** (1987), p. 189-200.

[5] T. KOHNO - *Linear representations of braid groups and classical Yang-Baxter equations*, in "Braids", Contemporary Math., Amer. Math. Soc. (1988), vol. 78, p. 339-363.

[6] A.B. GIVENTAL and V.V. SHEKHTMAN - *Monodromy groups and Hecke algebras*, Usp. Math. Nauk **12** n° 4 (1987), p. 138- .

[7] K. AOMOTO - *A construction of integrable differential system associated with braid groups*, in "Braids", Contemporary Math., Amer. Math. Soc. (1988), vol. 78, p. 1-11.

[8] A.B. GIVENTAL - *Twisted Picard-Lefschetz formulas*, Funct. Anal. Appl. **22** (1988), p. 10-18.

Donnons enfin quelques articles fondamentaux provenant de la théorie conforme des champs quantiques :

[9] A.A. BELAVIN, A.N. POLYAKOV and A.B. ZAMOLODCHIKOV - *Infinite dimensional symmetries in two-dimensional quantum field theory*, Nucl. Phys. **B 241** (1984), p. 333-380.

[10] V.G. KNIZHNIK and A.B. ZAMOLODCHIKOV - *Current algebras and Wess-Zumino models in two dimensions*, Nucl. Phys. **B 247** (1984), p. 83-103.

[11] A. TSUCHIYA and Y. KANIE - *Vertex operators in conformal field theory on* $\mathbf{P}^1$ *and monodromy representations of braid group*, Adv. Studies in Pure Math. **12** (1988), p. 297-372.

G. Mécanique statistique et théorie des nœuds

Deux collections d'articles sur le sujet viennent de paraître :

[1] C.N. YANG and M.L. GE (éditeurs) - *Braid group, knot theory and statistical mechanics*, Adv. Series Math. Phys. vol. 9, World Scientific (1989).

[2] M.L. GE and N.C. SONG (éditeurs) - *Conformal field theory and braid group* (Nankai lectures in mathematical physics, 1988), World Scientific (1989).

On doit à Kauffman trois exposés de synthèse sur l'interprétation des invariants des nœuds :

[3] L. KAUFFMAN - *Statistical mechanics and the Jones polynomial*, in "Braids", Contemporary Math., Amer. Math. Soc. (1988), vol. 78, p. 263-297.

[4] L. KAUFFMAN - *New invariants in the theory of knots*, Astérisque **163-164** (1988), p. 137-219.

[5] L. KAUFFMAN - *Knots, abstract tensors and the Yang-Baxter equation*, prépublication IHES/M/89/24 (avril 1989).

Deux références classiques, de physiciens, sur les modèles de Mécanique Statistique :

[6] R.J. BAXTER - *Exactly solved models in statistical mechanics*, Acad. Press (1982).

[7] F.Y. WU - *The Potts model*, Rev. Mod. Phys. vol. 54, n° 1, Janvier 1982.

Sur l'approche par les "modèles à vertex", voir :

[8] R. PENROSE - *Applications of negative dimensional tensors*, in Comb. Math. and its Appl. (Welsch éditeur), Acad. Press (1971).

[9] L. KAUFFMAN - *State models and the Jones polynomial*, Topology **26** (1987), p. 395-407.

[10] V. JONES - *On knot invariants related to statistical mechanics models*, Pac. J. Math. **138** (1989), p. .

[11] M. ROSSO - *Groupes quantiques et modèles à vertex de V. Jones en théorie des nœuds*, C.R. Acad. Sci. Paris, Série I, vol. 307 (1988), p. 207-210.

H. Applications des tresses à la physique

Voici un échantillon, portant surtout sur les travaux de l'école de Zü rich :

[1] V. DOTSENKO and V. FATEEV - *Conformal algebra and multipoint correlation functions in 2D statistical mechanics*, Nucl. Phys. **B240** (1984), p. 312-.

[2] J. FRÖHLICH - *Statistics of fields, the Yang-Baxter equation and the theory of braids and links*, Cargèse lectures 1987, G.'t Hooft (éditeur), Plenum Press (1988).

[3] J. FRÖHLICH - *Statistics and monodromy in two- and three-dimensional quantum field theory*, in "Differential geometrical methods in mathematical physics", K. Bleuler et M.Werner (éditeurs), Dordrecht (1988).

[4] K.H. REHREN and B. SHROER - *Einstein causality and Artin braids*, prépublication, Freie Universität Berlin, 1988.

[5] J. FRÖHLICH and C. KING - *Two-dimensional conformal field theory and three-dimensional topology*, prépublication ETH/TH/89-9, Zürich, 1989.

[6] G. FELDER, J. FRÖHLICH and G. KELLER - *Braid matrices and structure constants for minimal conformal models*, Comm. Math. Phys. **124** (1989), p. 647-664.

[7] J. FRÖHLICH, G. GABBIANI and P.A. MARCHETTI - *Braid statistics in three-dimensional local quantum theory*, in the Proceedings of the Banff Summer School in Theoretical physics (août 1989) on "Physics, Geometry and Topology", à paraître.

I. Applications arithmétiques des groupes de tresses

[1] A. GROTHENDIECK - *Esquisse d'un programme*, Notes miméographiées, Univ. Montpellier, 1982.

[2] R. COLEMAN - *Dilogarithms, regulators and p-adic L-functions*, Invent. Math. **69** (1982), p. 171-208.

[3] Y. IHARA - *Profinite braid groups, Galois representations and complex multiplication*, Ann. of Math. **123** (1986), p. 3-106.

[4] Y. IHARA - *On Galois representations arising from towers of coverings of* $\mathbf{P}^1\backslash\{0,1,\infty\}$, Invent. Math. **86** (1986), p. 427-459.

[5] B.H. MATZAT - *Konstruktive Galois Theorie*, Lect. Notes Math. **1284**, Springer (1987).

[6] T. KOHNO and T. ODA - *The lower central series of the pure braid group of an algebraic curve*, Adv. Studies in Pure Math. **12** (1988).

[7] P. DELIGNE - *Le groupe fondamental de la droite projective moins trois points*, in "Galois groups over **Q**", M.S.R.I. Publ. vol. 16, Springer, 1989.

Pierre CARTIER
École Normale Supérieure
Département de Mathématique
et Informatique
45 rue d'Ulm
F-75230 PARIS CEDEX 05

Astérisque

BERNADETTE PERRIN-RIOU

Travaux de Kolyvagin et Rubin

Astérisque, tome 189-190 (1990), Séminaire Bourbaki,
exp. n° 717, p. 69-106

<http://www.numdam.org/item?id=SB_1989-1990__32__69_0>

© Société mathématique de France, 1990, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Séminaire BOURBAKI Novembre 1989
42e année, 1989/90, n° 717

TRAVAUX DE KOLYVAGIN ET RUBIN

par Bernadette PERRIN-RIOU

Soit F un corps de nombres. Le théorème de Dirichlet détermine le rang du groupe des unités $\mathfrak{E}_F$ de l'anneau des entiers de F. Construire effectivement des unités est un problème beaucoup plus difficile. Cela est possible dans deux cas particuliers. Lorsque F est une extension abélienne de $\mathbb{Q}$ ou d'un corps quadratique imaginaire K, on construit un sous-groupe $\mathfrak{C}_F$ des unités (appelé groupe des unités cyclotomiques dans le premier cas et groupe des unités elliptiques dans le second cas) dont l'indice est fini et à peu près égal au nombre de classes de F, c'est-à-dire au cardinal du groupe des classes C_F de F. On peut alors se demander quel est le rapport entre les deux modules galoisiens $\mathfrak{E}_F/\mathfrak{C}_F$ et C_F.

Soit E une courbe elliptique sur $\mathbb{Q}$ paramétrée par des fonctions modulaires (conjecturalement, c'est toujours le cas). Grâce au théorème de Mordell-Weil, on sait que le groupe $E(F)$ des points de E rationnels sur F est de rang fini. Mais le calcul du rang est beaucoup plus difficile. Cependant, Birch (en reprenant une idée de Heegner) a construit de manière systématique des points sur E rationnels sur certaines extensions abéliennes d'un corps quadratique imaginaire (soumis à des conditions supplémentaires). Engendrent-ils un sous-groupe d'indice fini et si oui cet indice est-il relié au cardinal du groupe de Shafarevich-Tate qui est dans cette situation l'analogue du groupe des classes d'idéaux?

Rappelons que jusqu'aux travaux de Kolyvagin et Rubin, aucun exemple de courbe elliptique ayant un groupe de Shafarevich-Tate fini n'avait été trouvé.

Les travaux de Kolyvagin et Rubin apportent une réponse aux problèmes qui viennent d'être évoqués. Ils permettent aussi de redémontrer de manière élémentaire la conjecture principale d'Iwasawa sur $\mathbb{Q}$ (démontrée par Mazur et Wiles [38]) et de prouver la conjecture principale de Coates-Wiles sur un corps quadratique imaginaire. Disons seulement pour l'instant que ces conjectures relient l'arithmétique des extensions abéliennes de $\mathbb{Q}$ avec les fonctions L p-adiques construites par interpolation de valeurs de fonctions L complexes.

Nous allons d'abord donner un résultat de formulation aussi simple que possible pour chacune de ces trois situations. Puis, après un bref historique, nous parlerons des conjectures principales et des conséquences sur les courbes elliptiques sur $\mathbb{Q}$ en direction de la conjecture de Birch et Swinnerton-Dyer. Nous essaierons ensuite de donner quelques idées des techniques de démonstration utilisées.

Notations. Soit $\overline{\mathbb{Q}}$ la fermeture algébrique de $\mathbb{Q}$ dans $\mathbb{C}$; tous les corps de nombres considérés sont supposés contenus dans $\overline{\mathbb{Q}}$. Si F est un corps de nombres, on note C_F son groupe de classes d'idéaux et $\mathfrak{G}_F$ le groupe des unités de l'anneau des entiers de F. Si G est un groupe abélien fini, si M est un $\mathbb{Z}[G]$-module fini et si χ est un caractère de G, on pose

$$M^{(\chi)} = \{m \in M \otimes_{\mathbb{Z}} \mathbb{Z}[\chi] \text{ tel que } gm = \chi(g)m \text{ pour } g \in G\}$$

où $\mathbb{Z}[\chi]$ est l'anneau engendré par les valeurs de χ. Si p est un nombre premier, on note M(p) la composante p-primaire de M. Soit μ_n le groupe des racines n-ièmes de l'unité.

1. Présentation des résultats.

1.1. Premiers résultats.

Regardons d'abord le cas cyclotomique. Soit F une extension abélienne réelle de $\mathbb{Q}$. Le groupe des unités cyclotomiques de F est défini de la manière suivante: si L est une sous-extension de F cyclique sur $\mathbb{Q}$ de conducteur f, soit $\mathfrak{H}_L$ le sous-groupe de $L^\times$ engendré par les conjugués de $N_{\mathbb{Q}(\mu_f)/L}(1-\zeta_f)$ où ζ_f est une racine de l'unité d'ordre f. Le groupe des unités cyclotomiques de F est défini par

$$\mathfrak{C}_F = \mathfrak{E}_F \cap (\prod \mathfrak{H}_L)$$

où L parcourt les sous-extensions cycliques de $F/\mathbb{Q}$.

Théorème 1.1. Soient F une extension abélienne réelle de $\mathbb{Q}$ et χ un caractère de $\mathrm{Gal}(F/\mathbb{Q})$. Alors, pour tout nombre premier p ne divisant pas $2[F:\mathbb{Q}]$,

$$\#((\mathfrak{E}_F/\mathfrak{C}_F)(p)^{(\chi)}) = \#(C_F(p)^{(\chi)}).$$

Passons au cas elliptique. Soient K un corps quadratique imaginaire. On suppose pour simplifier que l'anneau des entiers $\mathfrak{O}_K$ de K est principal. On peut alors trouver une courbe elliptique E définie sur K et à multiplication complexe par $\mathfrak{O}_K$. Soit

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

une équation minimale de E sur $\mathfrak{O}_K$ et $\Delta(E)$ son discriminant. On considère la coordonnée x comme une fonction rationnelle sur E. Soit $\mathfrak{a}=(\alpha)$ un idéal de K premier à 6. On sait [45] que $\Delta(E)^{N\alpha-1}$ est une puissance 12-ième dans K. On considère la fonction rationnelle sur E

$$\Theta_0(z,\mathfrak{a}) = \Delta(E)^{(N\alpha-1)/12}\alpha^{-1}\prod_{b\in E_\alpha-\{0\}}(x(z)-x(b))^{-6}$$

(elle est définie à une racine de l'unité de K près). Soit ψ le caractère de Hecke de K associé à E et $\mathfrak{F}$ son conducteur. Si $\mathfrak{M}$ est un idéal de K, on note

$$I(\mathfrak{M})=\{\text{idéaux entiers de K premiers à } 6\mathfrak{F}\mathfrak{M}\},$$

$$J_0(\mathfrak{M})=\{\mu: I(\mathfrak{M}) \to \mathbb{Z} \ , \ \mu(\mathfrak{Q}) = 0 \text{ pour presque tout } \mathfrak{Q}, \ \sum \mu(\mathfrak{Q})(N\mathfrak{Q}-1)=0\}.$$

Pour $\mu \in J_0(\mathfrak{M})$, on pose

$$\Theta_0(z,\mu)=\prod_{\mathfrak{Q}} \Theta_0(z,\mathfrak{Q})^{\mu(\mathfrak{Q})}$$

Si L est une extension abélienne de K de conducteur $\mathfrak{M}$ premier à $6\mathfrak{F}$, on note Ω_L le sous-groupe engendré par les $N_{L(E_{\mathfrak{F}\mathfrak{M}})/L}(\Theta_0(a,\mu))$ pour $\mu \in J_0(\mathfrak{M})$ et a un point de $\mathfrak{F}\mathfrak{M}$-torsion. Enfin, si F est une extension abélienne de K, on définit le groupe des unités elliptiques $\mathfrak{C}_F$ comme étant le groupe des unités de F engendré par les $\Omega_L^{\cdot}$ pour toute sous-extension cyclique L de F/K et par le groupe des racines de l'unité de F.

Théorème 1.2. Soient F une extension abélienne de K et χ un caractère de Gal(F/K). Alors, pour tout nombre premier p ne divisant pas [F:ℚ] et tel que F ne contienne pas μ_p,

$$\#((\mathfrak{E}_F/\mathfrak{C}_F)(p)^{(\chi)})=\#(C_F(p)^{(\chi)}).$$

Enfin, introduisons le cas modulaire : une courbe elliptique E définie sur ℚ est dite de Weil [35] s'il existe un entier N et un morphisme non nul φ de $X_0(N)$ dans E qui envoie la pointe ∞ de $X_0(N)$ sur l'origine de E. Soit K un corps quadratique imaginaire tel que les facteurs premiers de N se décomposent dans K. Choisissons un idéal $\mathfrak{N}$ de l'anneau des entiers $\mathfrak{O}$ de K tel que $\mathfrak{O}/\mathfrak{N} \simeq \mathbb{Z}/N\mathbb{Z}$. Alors, l'isogénie cyclique de degré N

$$\mathbb{C}/\mathfrak{O} \to \mathbb{C}/\mathfrak{N}^{-1}$$

définit un point de $X_0(N)$ qui est rationnel sur le corps de Hilbert K(1) de K. Soit τ_1 son image par φ dans E(K(1)). On note τ_K la trace de K(1) à K de τ_1. Le sous-groupe de E(K) engendré par τ_K et par le sous-groupe de torsion de E(K) est indépendant des choix faits, on l'appelle groupe des points de Heegner de E(K). D'autre part, le groupe de Shafarevich-Tate Ш(E/K) est défini comme le

sous-groupe de $H^1(\mathrm{Gal}(\overline{K}/K),E(\overline{K}))$, noyau des applications de localisation

$$H^1((\mathrm{Gal}(\overline{K}/K),E(\overline{K}))\to\prod_v H^1((\mathrm{Gal}(\overline{K}_v/K_v),E(\overline{K}_v))\,.$$

Soit S_E l'ensemble suivant de nombres premiers : si E n'est pas à multiplication complexe, $p\in S_E \Leftrightarrow p=2$ ou le groupe de Galois de $\mathbb{Q}(E_p)/\mathbb{Q}$ est différent de $GL_2(\mathbb{Z}/p\mathbb{Z})$; si E a multiplication complexe par un ordre $\mathcal{O}$, $p\in S_E \Leftrightarrow$ $p=2$ ou p divise le discriminant de $\mathcal{O}$ ou p divise le cardinal du sous-groupe de torsion de E(K) ou le groupe de Galois de $\mathbb{Q}(E_p)/\mathbb{Q}$ est différent de $(\mathcal{O}/p\mathcal{O})^\times$

Théorème 1.3. Supposons τ_K d'ordre infini dans E(K). Alors,

(i) le groupe E(K) est de rang 1 et $Ш(E/K)$ est fini;

(ii) si $p\notin S_E$, l'ordre de $Ш(E/K)(p)$ divise $[E(K):\mathbb{Z}\tau_K]^2$ et $[E(K):\mathbb{Z}\tau_K]$ annule $Ш(E/K)(p)$.

Remarques. a) Le théorème 1.3 démontre une partie de la conjecture suivante. On note m_p le nombre de Tamagawa de $E/\mathbb{Q}$ en p [55] et c est le rationnel positif défini de la manière suivante: si ω est l'unique forme différentielle de E sur $\mathbb{Q}$ telle que $\varphi^*\omega$ soit la forme différentielle $\sum a_n q^n dq/q$ associée à une forme modulaire normalisée ($a_1=1$), $c\omega$ est une forme différentielle de Néron sur E.

Conjecture 1.4. Supposons que τ_K est d'ordre infini dans E(K). Alors,

(i) le groupe E(K) est de rang 1 ;

(ii) le groupe de Shafarevich-Tate $Ш(E/K)$ est fini et l'on a

$$\#(Ш(E/K))=([E(K):\mathbb{Z}\tau_K]/c\textstyle\prod_{p|N} m_p)^2\,.$$

Cette conjecture est l'analogue dans le cas modulaire des théorèmes 1.1 et 1.2 pour le caractère trivial. On peut énoncer une conjecture plus générale pour un caractère de Gal(K(n)/K) d'ordre premier à p.

b) Soit $L(E/\mathbb{Q},s)=\sum_n a_n n^{-s}$ la fonction L complexe de $E/\mathbb{Q}$ et

$L(E/K,s)$ la fonction L complexe de E/K. Gross et Zagier [26] ont établi une formule liant la dérivée de la fonction L de E/K avec la hauteur de Néron-Tate de τ_K. En particulier, ils montrent que si $L'(E/K,1)$ est non nul, le point τ_K est d'ordre infini.

c) Rappelons enfin l'énoncé de la conjecture de Birch et Swinnerton-Dyer pour une courbe elliptique E définie sur $\mathbb{Q}$ [55].

Conjecture 1.5. La fonction $L(E/\mathbb{Q},s)$ a un zéro en $s=1$ de multiplicité $g_{E(\mathbb{Q})}$ égale au rang de $E(\mathbb{Q})$. Le groupe de Shafarevich-Tate est fini et on a

$$L^{(g_{E(\mathbb{Q})})}(E/\mathbb{Q},1) = (\prod_{p|N} m_p)\#(Ш(E/\mathbb{Q}))R_\infty(E)\Omega_\infty$$

où $R_\infty(E)$ est le volume de $E(\mathbb{Q})$ pour la forme bilinéaire de Néron-Tate et où Ω_∞ est la période réelle positive de E.

1.2. Intermède.

En s'appuyant sur des calculs numériques, Gras [19] a conjecturé que les facteurs de Jordan-Hölder des modules galoisiens $\mathfrak{S}_F/\mathfrak{T}_F$ et C_F d'ordre premier à $2[F:\mathbb{Q}]$ sont les mêmes et ont la même multiplicité, ce qui équivaut au théorème 1.1. En reprenant une idée de Ribet [43], Mazur et Wiles [38] ont montré ce théorème en utilisant la géométrie des courbes modulaires pour construire des extensions non ramifiées d'extensions cyclotomiques de $F(\mu_p)$ dans la partie - du groupe de classes et en utilisant la théorie d'Iwasawa (voir plus loin). Dans [56], Thaine montre que $\#((\mathfrak{S}_F/\mathfrak{T}_F)(p)^{(\chi)})$ annule $C_F(p)^{(\chi)}$ de manière directe et élémentaire. Rubin [50] adapte sa démonstration au cas elliptique; il peut alors montrer la finitude du groupe de Shafarevich-Tate pour les courbes elliptiques à multiplication complexe définies sur le corps de multiplication complexe telles que $L(E/\mathbb{Q},1)$ est non nul (paragraphe 1.5).

D'autre part, des calculs numériques ont permis à Birch et Stephens [4]

de suggérer une forme de la conjecture 1.4 . Celle-ci a été ensuite écrite sous une forme définitive par Gross et Zagier [26] à la lumière de leur travail sur la dérivée de la fonction L de E/K et de la conjecture de Birch et Swinnerton-Dyer. Kolyvagin démontre d'abord une partie du théorème 1.3 ([31],[32]) et trouve un annulateur d'une partie du groupe de Shafarevich-Tate. Il se rend alors compte que sa méthode et celle de Thaine sont de fait similaires et une itération de cette méthode permet à Kolyvagin de démontrer les trois théorèmes.

L'idée est la suivante. Dans tous les cas précédents, les sous-groupes spéciaux de $\mathfrak{C}_F$ ou de E(K) n'arrivent pas tous seuls. A tout entier n sont associés une extension abélienne K(n) de $\mathbb{Q}$ ou de K et un élément spécial τ_n (unité cyclotomique, elliptique ou point de Heegner) de "niveau n" , défini sur cette extension . Ces points sont reliés entre eux par des formules. C'est ce que Kolyvagin appelle un système d'Euler. L'utilisation de ce système d'Euler permet de trouver des relations dans le groupe des classes ou le groupe de Shafarevich-Tate. L'idée fondamentale de Kolyvagin est alors de construire à partir d'un système d'Euler d'autres systèmes d'Euler qu'il appelle systèmes d'Euler dérivés paramétrés par des suites de nombres premiers $\ell_1,\ldots,\ell_s$ et qui fournissent d'autres relations dans le groupe des classes d'idéaux ou dans le groupe de Shafarevich-Tate. Le théorème de Cebotarev permet de choisir les ℓ_i de manière à avoir le plus de relations indépendantes possibles. On obtient ainsi une divisibilité de l'indice par le cardinal de la χ-partie du groupe de classes. L'égalité est alors obtenue en utilisant la formule donnant le nombre de classes de F .

Kolyvagin explique de plus comment la connaissance du système d'Euler des unités cyclotomiques ou elliptiques détermine complètement la structure des groupes de classes en tant que groupe abélien et en particulier son rang.

Les théorèmes 1.1 et 1.2 admettent des généralisations à des caractères de conducteur une puissance de p , que l'on appelle conjectures principales cyclotomique et elliptique. La conjecture cyclotomique d'Iwasawa a été démon-

trée par Mazur et Wiles [38]. L'utilisation des systèmes d'Euler dérivés de Kolyvagin et les techniques de la théorie d'Iwasawa ont permis à Rubin de redémontrer la conjecture principale dans le cas cyclotomique [34] et de la démontrer dans le cas elliptique [50]. On obtient ainsi une démonstration élémentaire de ces conjectures dont nous allons maintenant rappeler l'énoncé.

1.3. Conjectures principales (cas cyclotomique et elliptique)

On fixe ici un nombre premier p impair. On note $\mathbb{Q}_\infty$ l'unique sous-corps de $\mathbb{Q}(\mu_{p^\infty})$ tel que $\Gamma = Gal(\mathbb{Q}_\infty/\mathbb{Q}) \simeq \mathbb{Z}_p$ et pour tout n, $\mathbb{Q}_n$ la sous-extension de $\mathbb{Q}_\infty/\mathbb{Q}$ de degré p^n. Soit F une extension abélienne réelle de $\mathbb{Q}$ de degré premier à p; on pose $\Delta = Gal(F/\mathbb{Q})$, $F_\infty = F\mathbb{Q}_\infty$, $G_n = Gal(F_n/\mathbb{Q})$ et $G_\infty = Gal(F_\infty/\mathbb{Q}) = \Gamma \times \Delta$. On choisit une clôture algébrique $\bar{\mathbb{Q}}_p$ de $\mathbb{Q}_p$ contenant $\bar{\mathbb{Q}}$. Fixons un caractère de Δ dans $\bar{\mathbb{Q}}_p^*$. Si M est un $\mathbb{Z}_p[[\Delta]]$-module, on note

$$M^{(\chi)} = \{m \in M \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\chi] \text{ tel que } gm = \chi(g)m \text{ pour } g \in \Delta\}.$$

Soient $\mathfrak{C}_{F_n}$ le groupe des unités cyclotomiques de F_n et A_{F_n} le p-groupe de Sylow de C_{F_n}. Soient $\bar{\mathfrak{E}}_{F_n}$ et $\bar{\mathfrak{C}}_{F_n}$ les séparés complétés de $\mathfrak{E}_{F_n}$ et $\mathfrak{C}_{F_n}$ pour la toplogie p-adique. On note A_{F_∞} (resp. $\bar{\mathfrak{E}}_{F_\infty}$, resp. $\bar{\mathfrak{C}}_{F_\infty}$) la limite projective des A_{F_n} (resp. $\bar{\mathfrak{E}}_{F_n}$, resp. $\bar{\mathfrak{C}}_{F_n}$) relativement aux homomorphismes induits par la norme. Tous ces $\mathbb{Z}_p$-modules sont de manière naturelle des $\mathbb{Z}_p[[G_\infty]]$-modules. L'anneau $\mathbb{Z}_p[[G_\infty]]^{(\chi)}$ s'identifie à $\mathbb{Z}_p[\chi][[\Gamma]]$ (qui est isomorphe à $\mathbb{Z}_p[\chi][[T]]$). Rappelons que, pour tout module M de type fini et de torsion sur $B = \mathbb{Z}_p[\chi][[\Gamma]]$ (ou plus généralement un anneau local complet régulier), il existe des éléments non nuls $f_1, \ldots, f_d$ de B et un homomorphisme injectif de B-modules de $\oplus_{1 \leqslant i \leqslant d} B/(f_i)$ dans M dont le conoyau est fini (resp. annulé par un idéal de hauteur $\geqslant 2$) ; l'idéal de B engendré par $f_1 \ldots f_d$ ne dépend que de M, c'est l'idéal caractéristique de M. Les $\mathbb{Z}_p[\chi][[\Gamma]]$-modules $(A_{F_\infty})^{(\chi)}$ et $(\bar{\mathfrak{E}}_{F_\infty}/\bar{\mathfrak{C}}_{F_\infty})^{(\chi)}$ sont de type fini et de torsion

([29],[34], le second est même monogène à un groupe fini près).

Théorème 1.6 (conjecture principale pour $\mathbb{Q}$). Les idéaux caractéristiques de $(A_{F_\infty})^{(\chi)}$ et de $(\overline{\mathfrak{C}}_{F_\infty}/\overline{\mathfrak{C}}_{F_\infty})^{(\chi)}$ sont égaux.

D'habitude, ce théorème est énoncé en faisant intervenir les fonctions L p-adiques. Si χ est un caractère de Dirichlet p-adique primitif non trivial, on notera de la même manière le caractère galoisien associé. La fonction L complexe attachée à χ est $L(\chi,s)=\sum_n \chi(n)n^{-s}$. Soit ω le caractère de Teichmüller (en tant que caractère galoisien, il est donné par l'action sur μ_p). Soit ν le caractère de $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ dans $1+p\mathbb{Z}_p$ tel que $\omega\nu$ donne l'action du groupe de Galois sur μ_{p^∞}. Il existe [28] une unique fonction $L_p(\chi,s)$ continue pour $s\in\mathbb{Z}_p$ telle que pour tout entier $k\geqslant 1$

$$L_p(\chi,1-k)=(1-\chi_k(p)p^{k-1})L(\chi_k,1-k)$$

où χ_k est le caractère primitif associé à $\chi\omega^{-k}$. C'est la fonction L p-adique de Kubota-Leopoldt (si χ est impair (i.e. $\chi(-1)=-1$), elle est identiquement nulle). On peut de plus lui associer un unique élément $G_p(\chi)$ de $\mathbb{Z}_p[\chi][\![\Gamma]\!]$: un élément de cet anneau peut être considéré comme une fonction sur le groupe $\mathrm{Hom}_{\mathrm{cont}}(\Gamma,\mathbb{C}_p^*)$ (où $\mathbb{C}_p$ est la complétion de $\overline{\mathbb{Q}}_p$) et $G_p(\chi)$ est caractérisé par

$$G_p(\chi)(\nu^k)=L_p(\chi,1-k) \text{ pour tout entier } k\geqslant 1.$$

Soient M_{F_n} la plus grande p-extension abélienne de F_n non ramifiée au dehors de p, M_{F_∞} la réunion des M_{F_n} et X_{F_∞} le groupe de Galois de M_{F_∞}/F_∞. C'est encore un $\mathbb{Z}_p[\![\mathrm{Gal}(F_\infty/\mathbb{Q})]\!]$-module de type fini. La théorie du corps de classes permet de construire une suite exacte

$$0\to U_{F_\infty}/\overline{\mathfrak{C}}_{F_\infty}\to X_{F_\infty}\to A_{F_\infty}\to 0\,.$$

où U_{F_∞} est la limite projective relativement aux normes des unités semi-locales en p de F_n congrues à 1 modulo les places au dessus de p. On peut donc

relier les idéaux caractéristiques des χ-composantes de X_{F_∞}, A_{F_∞}, $U_{F_\infty}/\overline{\mathcal{C}}_{F_\infty}$ et $\overline{\mathcal{C}}_{F_\infty}/\overline{\mathcal{C}}_{F_\infty}$. D'autre part, Iwasawa a montré qu'une série caractéristique de $(U_{F_\infty}/\overline{\mathcal{C}}_{F_\infty})^{(\chi)}$ est $G_p(\chi)$ si χ est non trivial [34, Th. 5.2]. Le théorème 1.6 est alors équivalent au théorème suivant.

Théorème 1.7. Soit χ un caractère de $\mathrm{Gal}(F/\mathbb{Q})$ non trivial. Alors, l'idéal caractéristique de $X_{F_\infty}^{(\chi)}$ est engendré par $G_p(\chi)$.

Donnons-en une dernière formulation. Supposons maintenant que F est une extension abélienne de $\mathbb{Q}$ contenant μ_p de degré premier à p (c'est donc une extension quadratique imaginaire d'une extension réelle). Soit $\mathcal{A}_{F_\infty}$ la limite inductive des A_{F_n} et $\hat{\mathcal{A}}_{F_\infty}=\mathrm{Hom}_{\mathbb{Z}_p}(\mathcal{A}_{F_\infty}, \mathbb{Q}_p/\mathbb{Z}_p)$ son dual de Pontryagin. En utilisant la théorie de Kummer, Iwasawa a montré [29] qu'il existe un homomorphisme injectif à conoyau fini de A_{F_∞} dans $(\hat{\mathcal{A}}_{F_\infty})^*$ (le point indique que l'action de $\mathrm{Gal}(F_\infty/\mathbb{Q})$ est modifiée par $\gamma.m=\gamma^{-1}m$)); de plus, si χ est un caractère pair non trivial, $X_{F_\infty}^{(\chi)}$, et $\mathrm{Hom}_{\mathbb{Z}_p}(\mathcal{A}_{F_\infty}, \mu_{p^\infty})^{(\chi)}$ sont des $\mathbb{Z}_p[\chi][[\Gamma]]$-modules de torsion isomorphes.

Théorème 1.8. Si χ est un caractère impair de $\mathrm{Gal}(F/\mathbb{Q})$ différent de ω^{-1}, l'idéal caractéristique de $\hat{\mathcal{A}}_{F_\infty}^{(\chi)}$ est engendré par la fonction $\rho \mapsto G_p(\chi\omega)(\nu\rho)$.

La conjecture principale (maintenant théorème) dans le cas elliptique s'énonce de manière analogue. Soient F une extension abélienne de K de degré premier à p, K_∞ une $\mathbb{Z}_p$- ou $\mathbb{Z}_p^2$-extension de K et $F_\infty=K_\infty F$. On remplace unités cyclotomiques par unités elliptiques. Rubin a annoncé le théorème suivant [50] :

Théorème 1.9 (Rubin). Les idéaux caractéristiques de $(A_{F_\infty})^{(\chi)}$ et de $(\overline{\mathcal{C}}_{F_\infty}/\overline{\mathcal{C}}_{F_\infty})^{(\chi)}$

sont égaux dans chacun des cas suivants

(i) lorsque $p=\mathfrak{P}\mathfrak{P}^*$ se décompose dans K et que K_∞ est la $\mathbb{Z}_p$-extension de K non ramifiée en dehors de $\mathfrak{P}$, pour tout caractère χ de $\mathrm{Gal}(F/K)$,

(ii) lorsque p se décompose dans K, que K_∞ est l'unique $\mathbb{Z}_p^2$-extension de K et que, soit μ_p n'est pas contenu dans F, soit $\chi\chi^g\neq\omega$ pour tout $g\in\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$,

(iii) lorsque p est inerte dans K.

Ce théorème a une traduction en termes de fonctions L p-adiques lorsque p se décompose dans K ([13],[60],[54]). Nous ne rappelons ici que le cas où K_∞ est l'unique $\mathbb{Z}_p^2$-extension de K. Soit E la courbe elliptique utilisée pour construire le groupe des unités elliptiques. Soit $L(\psi,s)$ la fonction L du caractère de Hecke ψ de K associé à E. La fonction L de E/K est donnée par

$$L(E/K,s)=L(\psi,s)L(\overline{\psi},s).$$

Si E est définie sur $\mathbb{Q}$, la fonction L de $E/\mathbb{Q}$ est donnée par $L(E/\mathbb{Q},s)=L(\psi,s)$.

Choisissons un idéal premier $\mathfrak{P}$ de K au dessus de p. Soit $\overline{W}$ l'anneau des entiers du complété de l'extension maximale non ramifiée de $K_{\mathfrak{P}}$. Rappelons ([12], [14], [30], [61]) qu'il existe un unique élément $G_{\mathfrak{P}}(\chi)$ de $\overline{W}[[\mathrm{Gal}(F_\infty/F)]]$ tel que pour tout caractère ρ d'ordre fini de $\mathrm{Gal}(F_\infty/F)$

$$G_{\mathfrak{P}}(\chi)(\rho)/\Omega_{\mathfrak{P}}(\rho)=(1-\psi\rho(\mathfrak{P})/p)(1-\overline{\psi}(\mathfrak{P}^*)\rho^{-1}(\mathfrak{P}^*)/p)L(\psi\rho,1)/\Omega_\infty(\rho)$$

(ici, $\Omega_\infty(\rho)$ et $\Omega_{\mathfrak{P}}(\rho)$ sont des périodes respectivement complexes et $\mathfrak{P}$-adiques attachées à ψ et à ρ que l'on peut explicitement décrire).

Soit M_{F_n} la plus grande p-extension abélienne de F_n non ramifiée en dehors de $\mathfrak{P}$, M_{F_∞} la réunion des M_{F_n} et X_{F_∞} le groupe de Galois de M_{F_∞}/F_∞. Grâce au théorème de Coates-Wiles [14] et de Yager [60], le théorème 1.9 (ii) est équivalent au théorème suivant.

Théorème 1.10. Soit χ un caractère de $\mathrm{Gal}(F/K)$. On suppose que F ne contient

pas μ_p ou que $\chi\chi^g \neq \omega$ pour tout $g \in Gal(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. L'idéal caractéristique de $X_{F_\infty}^{(\chi)}$ dans $\overline{W}[[\Gamma]]$ est engendré par $G_{\mathfrak{P}}(\chi)$.

1.4. Courbes elliptiques sur $\mathbb{Q}$.

Les résultats qui précèdent (à la fois dans le cas elliptique et modulaire) permettent d'avancer en direction de la conjecture de Birch et Swinnerton-Dyer. Nous aurons besoin des deux résultats suivants sur les fonctions L complexes attachées aux courbes elliptiques de Weil.

Théorème 1.11. (i) Supposons $L(E/\mathbb{Q},1)=0$. Il existe une infinité de caractères quadratiques imaginaires χ tels que $\chi(\ell)=1$ pour $\ell | N$ et $L(E/\mathbb{Q},\chi,1)\neq 0$.
(ii) Supposons $L(E/\mathbb{Q},1)\neq 0$. Il existe une infinité de caractères quadratiques imaginaires χ tels que $\chi(\ell)=1$ pour $\ell | N$ et que $L(E/\mathbb{Q},\chi,s)$ a un zéro d'ordre 1 en $s=1$.

La partie (i) a été montrée par Waldspurger (citée dans [57]). La partie (ii) vient d'être montrée indépendamment par Bump, Friedberg et Hoffstein [8] et par M. Ram Murty et V. Kumar Murty [39]. Si E est une courbe elliptique de Weil sur $\mathbb{Q}$, on obtient alors le théorème suivant.

Théorème 1.12. Si $L(E/\mathbb{Q},1)$ est non nul, alors $E(\mathbb{Q})$ et $Ш(E/\mathbb{Q})$ sont finis. Si $L(E/\mathbb{Q},s)$ a un zéro simple en $s=1$, $E(\mathbb{Q})$ est de rang 1 et $Ш(E/\mathbb{Q})$ est fini.

Démonstration. La valeur propre ε de l'involution d'Atkin-Lehner w_N sur f vaut -1 si $L(E/\mathbb{Q},1)\neq 0$ (resp. $+1$ si $L(E/\mathbb{Q},s)$ a un zéro simple en $s=1$). Soit K le corps quadratique imaginaire associé à un caractère χ donné par (ii) (resp. (i)) du théorème 1.11. Alors $L(E/K,s)$ a un zéro simple en $s=1$. Grâce au résultat de [26] rappelé dans 1.1, τ_K est un point d'ordre infini et si σ est la conjugai-

son complexe, on a $\sigma\tau_K=\varepsilon\tau_K$ modulo torsion. Il n'appartient donc pas (resp. appartient) à $E(\mathbb{Q})$ modulo torsion. On déduit alors le résultat du théorème 1.3 .

Supposons maintenant que E est une courbe elliptique à multiplication complexe par l'anneau des entiers $\mathcal{O}$ d'un corps quadratique imaginaire k et est définie sur k . Soit $w_k\in\{2,4,6\}$ le nombre de racines de l'unité de k. Les résultats dans le cas elliptique (avec $K=k$) permettent d'obtenir des résultats plus précis sur la conjecture de Birch et Swinnerton-Dyer.

Théorème 1.13. Si $L(E/k,1)\neq 0$, alors $E(k)$ et $Ш(E/k)$ sont finis et la conjecture de Birch et Swinnerton-Dyer est vraie à multiplication par une unité de $\mathcal{O}[1/w_k]$ près .

Théorème 1.14. Si $L(E/k,1)=0$, soit $E(k)$ est infini, soit la composante $\mathfrak{P}$-primaire de $Ш(E/k)$ est infinie pour tout idéal $\mathfrak{P}$ de k ne divisant pas w_k .

La démonstration de ces deux théorèmes utilise des techniques de descente. Lorsque p se décompose dans k, on utilise [40] et le théorème 1.10 (Kolyvagin-Rubin + Coates-Wiles). Lorsque p est inerte dans k, Rubin utilise de plus la loi explicite de réciprocité de Wiles [58].

Théorème 1.15. Si E est définie sur $\mathbb{Q}$ et si $L(E/\mathbb{Q},s)$ a un zéro simple en $s=1$, alors $E(\mathbb{Q})$ est de rang 1 , $Ш(E/\mathbb{Q})$ est fini; si p est premier à w_k et se décompose dans k , la conjecture de Birch et Swinnerton-Dyer est vraie à multiplication par une unité de $\mathbb{Z}_p$ près.

Démonstration. On utilise dans la démonstration la fonction L p-adique $L_p(E/\mathbb{Q})$ construite par Mazur et Swinnerton-Dyer [37] qui coincide avec une spécialisation de la fonction L p-adique attachée au caractère de Hecke ψ (paragraphe

1.3). Soit χ un caractère quadratique imaginaire tel que $\chi(\ell)=1$ pour tout ℓ divisant N et $L(E/\mathbb{Q},\chi,1)\neq 0$. On déduit de [26] et de [42] que la fonction L p-adique $L_p(E/\mathbb{Q})$ de $E/\mathbb{Q}$ a un zéro simple en 1. Le théorème 1.10 implique qu'il en est de même de la série caractéristique du dual de Pontryagin du groupe de Selmer $S(\mathbb{Q}_\infty)$ (on a une suite exacte

$$0 \to E(\mathbb{Q}_\infty)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p/\mathbb{Z}_p \to S(\mathbb{Q}_\infty) \to Ш(E/\mathbb{Q}_\infty)(p) \to 0;$$

voir [40] pour le lien avec X_{F_∞}). Le corollaire 1.9 de [42] (qui dépend lui-même du théorème de Gross-Zagier, de son analogue p-adique et de [40]) implique alors le théorème.

Ainsi, ces théorèmes relient un invariant analytique (l'ordre du zéro de la fonction L complexe) avec un invariant arithmétique (le rang de $E(\mathbb{Q})$). Le premier résultat dans cette direction a été celui de Coates et Wiles [13] dans le cas des courbes elliptiques à multiplication complexe: si $E(\mathbb{Q})$ est infini, alors $L(E/\mathbb{Q},1)$ est nul.

Théorème 1.16. Le groupe $E(\mathbb{Q}_\infty)$ est un $\mathbb{Z}$-module de type fini (conjecture de Mazur).

En effet, Rohrlich [46] a montré que la fonction L p-adique $L_p(E/\mathbb{Q})$ est non nulle. On en déduit par le théorème 1.10 que le dual de Pontryagin du $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}]]$-module $S(\mathbb{Q}_\infty)$ est de torsion (voir démonstration du théorème 1.15), ce qui permet de conclure [40].

Par manque de place, nous avons choisi de ne pas donner la démonstration des conjectures principales. Nous donnons dans le paragraphe 3 une idée de la démonstration des théorèmes 1.1 et 1.3 en suivant Kolyvagin [33] (des modifications ont été faites dans [25] et dans l'appendice de [34]). Dans le paragraphe 2, nous parlerons d'un outil essentiel de la démonstration de Kolyvagin, les sys-

tèmes d'Euler.

2. Systèmes d'Euler.

Dans la suite, p est un nombre premier fixé et M, M',... désigneront des puissances de p. Si L/F est une extension galoisienne, on note

$$H^i(L/F,\blacksquare)=H^i(\mathrm{Gal}(L/F),\blacksquare) \text{ et } H^i(F,\blacksquare)= H^i(\bar{\mathbb{Q}}/F,\blacksquare).$$

Si x est un élément de $H^i(\blacksquare/\blacksquare, C_M)$ et si $M'|M$, on note $x(M')$ l'image de x dans $H^i(\blacksquare/\blacksquare,C_{M'})$ par l'application induite par la multiplication par M/M'. Si $x \in H^1(F,\blacksquare)$ et si v est une place de F, on note x_v l'image de x dans $H^1(F_v,\blacksquare)$.

En suivant Kolyvagin, nous allons construire à partir d'unités des familles d'éléments de F^*/F^{*M} qui sont des unités en dehors d'un ensemble fini de places et dont on peut décrire la valuation. On fait une construction analogue dans le cas modulaire (cas d'une courbe elliptique). Le résultat utile pour la démonstration des théorèmes 1.1 et 1.3 (démonstration esquissée dans le paragraphe 3) est le théorème 2.1 . On explique ensuite dans ce paragraphe la manière dont Kolyvagin l'obtient. Pour ne pas alourdir d'avantage le texte, nous ne considèrerons que le cas de représentations p-adiques sur $\mathbb{Q}$ (dans le cas elliptique, la représentation p-adique associée à la situation est une représentation de $\mathrm{Gal}(\bar{\mathbb{Q}}/K)$, il faut remplacer les nombres premiers ℓ de $\mathbb{Q}$ par des idéaux premiers...).

2.1. Représentations p-adiques.

Donnons quelques définitions relatives aux représentations p-adiques aussi générales que possibles bien que les applications que nous ayons en vue soient le cas des modules de Tate $\mathbb{Z}_p$, $\mathbb{Z}_p(1)$ et $T_p(E)$ de $\mathbb{Q}_p/\mathbb{Z}_p$, μ_{p^∞} et de E_{p^∞}.

Soit $T_p(X)$ un $\mathbb{Z}_p$-module libre de type fini de dimension d muni d'une action linéaire et continue de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. On note X le groupe p-divisible (au

sens des groupes abéliens) associé ($X_M = T_p(X)/MT_p(X)$). On considère le groupe p-divisible X' défini par

$$T_p(X') = \mathrm{Hom}_{\mathbb{Z}_p}(T_p(X), \mathbb{Z}_p(1)).$$

On suppose que $T_p(X)$ est une représentation de de Rham en p [15]. Soit $\mathfrak{N}$ le produit (supposé fini) des nombres premiers de $\mathbb{Q}$ où $T_p(X)$ a mauvaise réduction (si ℓ ne divise pas p (resp. $\ell=p$), $T_p(X)$ a bonne réduction en ℓ si l'action du sous-groupe d'inertie en ℓ est triviale (resp. si $T_p(X)$ est cristalline en p [15]). Si ℓ est un nombre premier ne divisant pas $\mathfrak{N}p$, soit P_ℓ le polynôme caractéristique du Frobenius (arithmétique) Fr_ℓ sur $T_p(X)$. Si L une extension de $\mathbb{Q}$ et v une place de L, on associe à $T_p(X)$ un sous-groupe $H^1_f(L_v, X_M)$ de $H^1(L, X_M)$ défini par $H^1_f(L_v, X_M) = H^1(L_v^{nr}/L_v, X_M)$ si v ne divise pas $\mathfrak{N}p$ (où L_v^{nr} est la plus grande extension de L_v non ramifiée) et en utilisant les méthodes de Greenberg et Bloch-Kato en général ([6],[23]).

Exemples. Si $X = \mu_{p^\infty}$, $H^1(L_v, X_M) = L_v^\times/L_v^{\times M}$ par la théorie de Kummer et $H^1_f(L_v, X_M) = U(L_v)/U(L_v)^M$ (où $U(L_v)$ est le groupe des unités de L_v); si $X = \mathbb{Q}_p/\mathbb{Z}_p$, $H^1(L_v, X_M) = \mathrm{Hom}_{\mathbb{Z}_p}(\mathrm{Gal}(\bar{L}_v/L_v), \mathbb{Z}/M\mathbb{Z})$ et $H^1_f(L_v, X_M) = \mathrm{Hom}_{\mathbb{Z}_p}(\mathrm{Gal}(L_v^{nr}/L_v), \mathbb{Z}/M\mathbb{Z})$. Si $X = E_{p^\infty}$, $H^1_f(L_v, E_M)$ est l'image réciproque de $H^1(L_v^{nr}/L_v, E(L_v^{nr}))_M$ dans $H^1(L_v, E_M)$ et on a la suite exacte

$$0 \to E(L_v)/ME(L_v) \to H^1_f(L_v, E_M) \to H^1(L_v^{nr}/L_v, E(L_v^{nr}))_M \to 0.$$

L'accouplement naturel $[\blacksquare,\blacksquare]_M : X_M \times X'_M \to \mu_M$ induit un accouplement local non dégénéré $\langle \blacksquare, \blacksquare \rangle_v$

$$H^1(L_v, X_M) \times H^1(L_v, X'_M) \to H^2(L_v, \mu_M) = \mathbb{Z}/M\mathbb{Z} ;$$

Si x (resp. y) est un élément de $H^1(L, X_M)$ (resp. $H^1(L, X'_M)$), on a

$$\sum_v \langle x, y \rangle_v = 0. \tag{2.1}$$

Les sous-groupes $H_f^1(L_v, X_M)$ et $H_f^1(L_v, X'_M)$ sont exactement orthogonaux ([6], [52]). On en déduit un isomorphisme

$$H^1(L_v, X'_M)/H_f^1(L_v, X'_M) \simeq \mathrm{Hom}_{\mathbb{Z}_p}(H_f^1(L_v, X_M), \mu_M).$$

Soit v une place de L au dessus de ℓ première à $\mathfrak{n}p$ totalement décomposée dans $L(X_M)/L$ et non ramifiée sur $\mathbb{Q}$ de degré résiduel f. Choisissons une racine de l'unité $\zeta_{M,v}$ d'ordre M. L'application de $H_f^1(L_v, X_M)$ dans X_M donnée par $x \mapsto x(\mathrm{Fr}_\ell^f)$ est un isomorphisme. On en déduit un isomorphisme $\mathfrak{C}_v$ de $H^1(L_v, X'_M)/H_f^1(L_v, X'_M)$ sur X'_M (dépendant de $\zeta_{M,v}$) caractérisé par

$$[x(\mathrm{Fr}_\ell^f), \mathfrak{C}_v(y)]_M = \zeta_{M,v}^{\langle x,y\rangle_v}.$$

Remarque. Si $X = E_{p^\infty}$, l'accouplement de Weil permet d'identifier X et X' (on le note encore $[\blacksquare,\blacksquare]_M$). L'accouplement $\langle .,. \rangle_v$ induit alors l'accouplement local de Tate $E(L_v)/ME(L_v) \times H^1(L_v, E_M) \to \mathbb{Z}/M\mathbb{Z}$. Si $X = \mathbb{Z}_p$ et $X' = \mu_{p^\infty}$, on a $\mathfrak{C}_v(y) = \zeta_{M,v}^{\mathrm{ord}_v(y)}$ si ord_v est la valuation de L_v normalisée par $\mathrm{ord}_v(L_v) = \mathbb{Z}$.

Si T est un ensemble fini de places de L, on note $S_T(X/L)^{(M)} = S_T(T_p(X)/L)^{(M)}$ le sous-$\mathbb{Z}_p$-module de $H^1(L, X_M)$ formé des éléments dont l'image dans $H^1(L_v, X_M)$ appartient à $H_f^1(L_v, X_M)$ pour toute place v de L ne divisant aucune place de T. On pose $S(T_p(X)/L)^{(M)} = S(X/L)^{(M)} = S_\emptyset(X/L)^{(M)}$. C'est le "groupe de Selmer". Lorsque $X = E_{p^\infty}$, on retrouve le groupe de Selmer classique attaché à la courbe elliptique E. On vérifie facilement que $S(\mathbb{Z}_p/L)^{(M)} = \mathrm{Hom}_{\mathbb{Z}_p}(A_L, \mathbb{Z}/M\mathbb{Z})$ où A_L est le p-groupe de Sylow du groupe C_L des classes d'idéaux de L. Si T est un ensemble de places finies, $S_T(\mathbb{Z}_p(1)/L)^{(M)} = \mathfrak{C}_{L,T}/\mathfrak{C}_{L,T}^M$ où $\mathfrak{C}_{L,T}$ est le groupe des T-unités de L.

2.2. Théorème clé.

On se donne maintenant une extension abélienne K de $\mathbb{Q}$, un ensemble fini de places S_0 et pour chaque entier m non nul, une extension abélienne $K(m)$ de K vérifiant les propriétés suivantes:

(i) si $n|m$, alors $K(n)\subset K(m)$; $K(n)\cap K(m)=K(pgcd(n,m))$; $K(n)K(m)=K(ppcm(n,m))$;

(ii) pour ℓ premier, $K(\ell)/K(1)$ est de degré premier à ℓ ;

(iii) $K(\ell)/K$ est non ramifiée en dehors des places au dessus de ℓ et de S_0.

En fait, nous ne considèrerons que l'un des deux cas particuliers suivants:

(2.2) (i) si $X=\mu_{p^\infty}$, on prend $K=\mathbb{Q}$ et $\mathbb{Q}(m)=\mathbb{Q}(\mu_m)$; (ii) si $X=E_{p^\infty}$, K est un corps quadratique imaginaire tel que tout nombre premier divisant le conducteur de E est décomposé dans K ; $K(m)$ est l'extension de K associée par le corps de classes à l'ordre $\mathfrak{O}_m$ de $\mathfrak{O}_K$ de conducteur m.

On se fixe un entier $\mathfrak{N}_0$ divisible par $2\mathfrak{N}$ et par les nombres premiers ramifiés dans $K/\mathbb{Q}$. On suppose désormais que <u>tous les nombres premiers ℓ considérés sont premiers à</u> $\mathfrak{N}_0$. On note M_ℓ la plus grande puissance de p divisant $[K(\ell):K(1)]$ telle que les éléments de X_M sont rationnels sur K_v où v est une place de K au dessus de ℓ.

On définit inductivement [1] un ensemble $\mathfrak{P}^{(k)}$ de l'ensemble des $k+1$-uples $[m;\ell_1,\dots,\ell_k]$ où m est un entier et où les ℓ_i sont des nombres premiers distincts : $\mathfrak{P}^{(0)}=\{[m],m\in\mathbb{N}\}$, $\mathfrak{P}^{(k)}$ est l'ensemble des $[m;\ell_1,\dots,\ell_k]$ où $[m;\ell_1,\dots,\ell_{k-1}]$ est un élément de $\mathfrak{P}^{(k-1)}$ et où ℓ_k est un nombre premier ne divisant pas $\mathfrak{N}_0 mp\ell_1\dots\ell_{k-1}$, inerte dans K, totalement décomposé dans $K(m\ell_1\dots\ell_{k-1})/K$ et tel que si $M_0(m,\ell_1,\dots,\ell_{k-1})$ est le ppcm des annulateurs de $X_{p^\infty}(K(m\ell_1\dots\ell_{k-1}))$ et des

[1] Une méthode légérement différente permet d'enlever certaines des conditions techniques de la définition de cet ensemble, voir [49], [50] et article en préparation de Kolyvagin.

$X_{p^\infty}(K(m\ell_1..\ell_{k-2}/\ell_j)_v)$ pour $j=1,...,k-2$ et pour toute place v au dessus de ℓ_j, $M_0(m,\ell_1,...,\ell_{k-1})M_{\ell_{k-1}}$ divise M_{ℓ_k}.

Dans le cas (2.2),(i), pour tout entier m, on choisit des racines de l'unité ζ_m d'ordre m vérifiant $\zeta_{nm}=\zeta_n^m$. On pose $\tau_m=1-\zeta_m$. Dans le cas (2.2),(ii), rappelons la définition des points de Heegner de niveau quelconque. Si m est un entier positif, notons $\mathcal{O}_m$ l'ordre de $\mathcal{O}$ de conducteur m. Fixons un idéal $\mathfrak{N}$ de $\mathcal{O}$ tel que $\mathcal{O}/\mathfrak{N}\simeq\mathbb{Z}/N\mathbb{Z}$. La classe d'isomorphismes de l'isogénie cyclique de degré N

$$\mathbb{C}/\mathcal{O}_m \to \mathbb{C}/(\mathfrak{N}\cap\mathcal{O}_n)^{-1}.$$

définit un élément de $X_0(N)(K(m))$. On note τ_m son image dans $E(K(m))$ ou dans $E(K(m))\otimes_{\mathbb{Z}}\mathbb{Z}_p$.

Théorème 2.1(Kolyvagin). Supposons (2.2). On se donne un entier m, un entier $k\geq 1$, une puissance M de p. Alors, il existe pour $j=1,...,k$ des nombres premiers ℓ_j et des éléments $\tau_{[m;\ell_1,...,\ell_j]}$ de $S_{\{\ell_1,...,\ell_j\}}(X/K(m))^{(M_{\ell_1})}$ avec $\tau_{[m]}=\tau_m$ tels que $M|M_{\ell_1}$, $[m;\ell_1,...,\ell_k]\in\mathcal{P}^{(k)}$ et tel que pour tous $j\leq i$ et pour v_{ℓ_j} une place de $K(m)$ au dessus de ℓ_j, on ait (2.3)

$$\mathfrak{G}_{v_{\ell_j}}(\tau_{[m;\ell_1,...,\ell_i]}(M))=Fr_{\ell_j}^{-1}(\tau_{\varepsilon_j([m;\ell_1,...,\ell_i])}(M)(Fr_{\ell_j}^d))=Fr_{\ell_j}^{-1}(Fr_{\ell_j}^d-1)(\tau_{\varepsilon_j([m;\ell_1,...,\ell_i])}(M)/M)$$

dans X_M si $\varepsilon_j([m;\ell_1,...,\ell_i])=[m;\ell_1,...\ell_{j-1},\ell_{j+1},...,\ell_i]$.

De plus, une fois trouvés $\ell_1,...,\ell_{k-1}$ et les éléments $\tau_{[m;\ell_1,...,\ell_j]}$ pour $j\leq k-1$, si M' est une puissance de p divisible par $M_{\ell_{k-1}}$, si L est une extension finie de $K(m)(X_{M'})$ et si h est un élément de $Gal(L/K(m)(X_{M'}))$, on peut choisir ℓ_k tel que $h=Fr_{\ell_k}$.

On indique dans les paragraphes 2.3 et 2.4 une idée de la démonstration de Kolyvagin.

2.3. Construction auxiliaire: la corestriction de Kolyvagin.

La situation générale est la suivante. Soit G un groupe, H un sous-groupe distingué de G tel que G/H est cyclique d'ordre fini D. On choisit un générateur δ de G/H. Si C est un G-module discret, on note $H^1_G(H,C)$ le noyau de l'homomorphisme de corestriction

$$cor_{H,G}: H^1(H, C) \to H^1(G, C).$$

Soit c un entier tel que cD annule C et tel que $cC^G \subset (\delta-1)(cC)^H$ (par exemple tel que cC^G est nul). On définit alors un homomorphisme

$$cor'_{H,G}: H^1_G(H,C) \to H^1(G, cC)$$

de la manière explicite suivante. Soit $\tilde{\delta}$ un relèvement de δ à G. Soit φ un cocycle représentant x. La corestriction de x est représentée par l'unique cocycle φ_1 de G à valeurs dans C vérifiant

$$\varphi_1(h)=\sum_{i=0}^{D-1}\delta^i(\varphi)(h) \text{ si } h\in H \text{ et } \varphi_1(\tilde{\delta})=\varphi(\tilde{\delta}^D)$$

Si $x \in H^1_G(H,C)$, il existe donc un élément e de C tel que $\varphi_1(g)=(g-1)e$ pour tout $g \in G$. Considérons le polynôme $P(X)$ vérifiant

$$X^{D-1}+X^{D-2}+\ldots+X+1=(X-1)P(X)+D$$

Le fait que cD annule C implique qu'il existe un et un seul cocycle ψ de G à valeurs dans cC tel que

$$\psi(h)= cP(\delta)(\varphi)(h) \text{ si } h\in H \text{ et } \psi(\tilde{\delta}) = ce .$$

La condition imposée sur C^G implique que la classe $cores'_{H,G}(x)$ dans $H^1(F,cC)$ ne dépend pas du choix du relèvement $\tilde{\delta}$ de δ, du représentant φ de x, ni du choix de e.

Remarque. Lorsque C^G est nul, $H^i(L/F, C^H)=0$ pour $i=1,2$; la restriction

$$H^1(F,C) \to H^1(L,C)^{Gal(L/F)}$$

est alors un isomorphisme. Il est d'autre part clair que $P(\delta)x$ est un élément de $H^1(L,C)^{Gal(L/F)}$. Donc, $cores'_{H,G}(x)$ est alors simplement l'image réciproque de

$P(\delta)x$ dans $H^1(F,C)$ par la restriction.

Nous appliquerons cette construction au cas où $G=Gal(\bar{\mathbb{Q}}/F)$ avec F un corps de nombres, où $H = Gal(\bar{\mathbb{Q}}/L)$ avec L/F une extension cyclique de degré divisible par M et où $C=X_{cM}$ (on a $cX_{cM} = X_M$). On écrira alors $cor'_{L/F}$. On a la proposition suivante.

Proposition 2.2. Soit F un corps de nombres, L/F une extension cyclique de degré D. Soit $Ram(L/F)$ l'ensemble des places de ramification de L/F. On suppose que M est un diviseur de D et que $c=c(F)$ est un entier tel que $cX_{cM}^{Gal(\bar{F}/F)}=0$. Si T est un ensemble fini de places de F et si x appartient à l'intersection de $H^1_F(L,X_{cM})$ et de $S_T(X/L)^{(cM)}$, alors $cor'_{L/F}(x)$ appartient à $S_{T\cup Ram(L/F)}(X/F)^{(M)}$.

2.4. Systèmes d'Euler.

Plaçons-nous de nouveau dans la situation (2.2). Pour tout ℓ, on se donne un élément y_ℓ appartenant à l'algèbre de groupe du groupe de Galois sur $\mathbb{Q}$ de la plus grande extension non ramifiée en ℓ contenue dans $UK(m)$: si K est différent de $\mathbb{Q}(\sqrt{-3})$ et de $\mathbb{Q}(\sqrt{-1})$, on prend

$$y_\ell = Fr_{\ell'}^{-1}([K(\ell):K(1)]+ (-1)^{d-1} P_\ell(Fr_{\ell'}))$$

(ℓ' est au dessus de ℓ dans K ; si ℓ est inerte dans K, $y_\ell=a_\ell$ si $X=E_{p^\infty}$ et $y_\ell= 1-Fr_\ell^{-1}$ si $X=\mu_{p^\infty}$).

Soit T un ensemble fini de nombres premiers. Une famille d'Euler non ramifiée en dehors de T est la donnée pour tout entier m premier à T d'une puissance de p, éventuellement infinie, $M(m)$ et d'un élément $\tau_m=(\tau_m(M))_{M|M(m)}$ de $\lim proj_{M|M(m)} S_T(X/K(m))^{(M)}$ vérifiant pour ℓ premier à T et à $\mathfrak{N}_0 p$, non ramifié dans $K(m)/K$ et pour M divisant $M(m)$ et $M(m\ell)$

$$cores_{K(\ell m)/K(m)}(\tau_{\ell m}(M))=y_\ell \tau_m(M).$$

Un système d'Euler d'ordre k est la donnée pour toute suite $[\ell_1,\ldots,\ell_k]$ de

nombres premiers distincts d'une famille d'Euler $(M(m;\ell_1,\dots,\ell_k),\tau_{m,[\ell_1,\dots,\ell_k]})_m$ non ramifiée au dehors de $\{\ell_1,\dots,\ell_k\}$.

Si $\pi=[m;\ell_1,\dots,\ell_k]$, on notera $\tau_\pi=\tau_{m,[\ell_1,\dots,\ell_k]}$, $M(\pi)=M(m;\ell_1,\dots,\ell_k)$. L'entier m est le niveau de π et de τ_π. On pose $\ell.\pi=[\ell m;\ell_1,\dots,\ell_k]$.

On fixe désormais pour tout nombre premier ℓ un générateur δ_ℓ du groupe cyclique $Gal(K(\ell)/K(1))$. Pour tout entier n premier à ℓ, il détermine un générateur (noté toujours δ_ℓ) de $Gal(K(n\ell)/K(n))$ grâce à l'isomorphisme $Gal(K(n\ell)/K(n)) \to Gal(K(\ell)/K(1))$. Les applications cor' seront définies à l'aide de ces choix. Le groupe des points d'ordre une puissance de p contenus dans $X(K(m))$ pour n premier à p est fini. On note son cardinal $c_p(m)$.

Soient $k\geq 1$ et τ_π un système d'Euler d'ordre $k-1$. Remarquons que si π est de niveau m, lorsque la place de K au dessus de ℓ se décompose totalement dans $K(m)$ et que $Mc_p(m)$ divise M_ℓ, on a $cores_{K(\ell m)/K(m)}(\tau_{\ell.\pi}(Mc_p(m)))=0$; $cores'_{K(\ell m)/K(m)}(\tau_{\ell.\pi})$ est donc définie dans $H^1(K(m),X_M)$. Si $\ell_1,\dots,\ell_k$ sont tous distincts, inertes dans K et totalement décomposés dans $K(m)/K$, posons

$$\tau_{[m;\ell_1,\dots,\ell_k]}(M) = cor'_{K(m\ell_1)/K(m)}(\tau_{[m\ell_1;\ell_2,\dots,\ell_k]})(M)$$

pour M divisant $M_{\ell_1}/c_p(m)$ et $M(m;\ell_2,\dots,\ell_k)/c_p(m)$. Sinon, posons $M(m;\ell_1,\dots,\ell_k)=1$ et $\tau_{[m;\ell_1,\dots,\ell_k]}=0$. On obtient ainsi un système d'Euler d'ordre k tel que si $\ell_1,\dots,\ell_k$ sont inertes dans K et totalement décomposés dans $K(m)/K$,

$$M(m;\ell_1,\dots,\ell_k)\geq pgcd(M_{\ell_1}/c_p(m),\ M(\ell m;\ell_2,\dots,\ell_k)/c_p(m), M(m;\ell_2,\dots,\ell_k)/c_p(m)).$$

En étant plus soigneux, on peut en fait prendre

$$M(m;\ell_1,\dots,\ell_k)\geq pgcd(M_{\ell_1},\ M(\ell m;\ell_2,\dots,\ell_k)/c_p(m), M(m;\ell_2,\dots,\ell_k)/c_p(m)).$$

Théoréme 2.3. Soit τ_m une famille d'Euler non ramifiée vérifiant $M(m)=p^\infty$. Alors, la construction précédente itérée fournit un système d'Euler d'ordre k vérifiant

$$M(m;\ell_1,\dots,\ell_k)\geq pgcd(M_{\ell_1},\ M(\ell m;\ell_2,\dots,\ell_k)/c_p(m), M(m;\ell_2,\dots,\ell_k)/c_p(m)).$$

Si de plus, τ_m vérifie pour tout ℓ premier à $pm\mathfrak{N}_0$

$$(2.4)_\ell \qquad \tau_{\ell m,w}=Fr_\ell^{-1}(\tau_{m,v})$$

pour toute place v de $K(m)$ au dessus de ℓ (ℓ' étant la place de K au dessus de ℓ et w l'unique place de $K(\ell m)$ au dessus de v) et si $\pi=[m;\ell_1,\dots,\ell_k]\in\mathfrak{P}^{(k)}$, alors $M(\pi)\geqslant M_{\ell_1}$ et pour toute place v_{ℓ_j} au dessus de ℓ_j, l'image $\tau_{\pi,v_{\ell_j}}(M)$ de $\tau_\pi(M)$ par localisation en v_{ℓ_j} appartient à

$$\mathrm{Hom}_{\mathbb{Z}_p}(\mathrm{Gal}(K(\ell_j m)_{v_{\ell_j}}/K(m)_{v_{\ell_j}}), X_M(K(m)_{v_{\ell_j}}))$$

et est donnée par la formule

$$(2.5) \qquad \tau_{\pi,v_{\ell_j}}(M)(\delta_{\ell_j})= Fr_{\ell_j}^{-1}\tau_{\varepsilon_j(\pi),v_{\ell_j}}(M)(Fr_{\ell_j}^{d})=Fr_{\ell_j}^{-1}(Fr_{\ell_j}^{d}-1)(\tau_{\varepsilon_j(\pi),v_{\ell_j}}(M)/M)$$

où $\varepsilon_j(\pi)=[m;\ell_1,\dots,\ell_{j-1},\ell_{j+1},\dots\ell_k]$.

Remarquons que si L'/L est une extension totalement ramifiée en v et v' la place de L' au dessus de v, la restriction induit un isomorphisme de $H_f^1(L_v, X_M)$ sur $H_f^1(L'_{w'}, X_M)$ et que le Frobenius agit sur ces modules, ce qui donne un sens aux conditions (2.4). Les conditions imposées dans la définition de $\mathfrak{P}^{(k)}$ impliquent que les applications de Kolyvagin locales cor'_v pour v divisant ℓ_j sont bien définies et que des relations du type $(2.4)_{\ell_j}$ sont vraies pour le système d'Euler d'ordre k. Cela permet de faire le calcul local de τ_π et de montrer (2.5).

On démontre le théorème 2.1 à partir du théorème 2.3 en appliquant le théorème de Cebotarev. En effet dans les deux cas particuliers envisagés, on a exhibé une famille d'Euler non ramifiée ($M(m)=p^\infty$) vérifiant les relations $(2.4)_\ell$. Il s'agit des $(\tau_m)_m$ avec $\tau_m=1-\zeta_m$ (système des unités cyclotomiques: il est en fait non ramifié en dehors de ℓ si m est une puissance de ℓ mais cela se corrige lorsque l'on prend les χ-composantes) et τ_m point de Heegner de niveau m dans le cas modulaire (système des points de Heegner). Pour passer de la formule (2.5) à la formule (2.3), on choisit $\zeta_{M,v}=\zeta_{\delta_\ell}^{(\ell^d-1)/M}$ comme racine de l'unité d'or-

dre M intervenant dans la définition de $\mathfrak{E}_v$ où ζ_{δ_ℓ} est la racine de l'unité d'ordre ℓ^d-1 corespondant à δ_ℓ par l'isomorphisme d'Artin.

Enfin, remarquons que le théorème 2.3 peut se généraliser à une représentation p-adique comme en 2.1. Il ne resterait plus qu'à exhiber une famille d'Euler non ramifiée vérifiant $M(m)=p^\infty$, ce qui est beaucoup plus difficile.

3. Démonstrations des théorèmes 1.1 et 1.3.

3.1. Généralités.

Commençons par donner l'idée générale commune aux démonstrations des théorèmes 1.1, 1.3 (et 1.2). Soit $T_p(X)$ une représentation p-adique comme en 2.1. On désire étudier le groupe de Selmer $S(X'/L)^{(M)}$. Il est facile de construire des caractères de ce groupe: si v est une place de L au dessus de ℓ non ramifiée sur $\mathbb{Q}$ de degré résiduel f et totalement décomposée dans $L(X_M)/L$, si e est un élément de X_M, on note $\xi_{v,e}$ l'élément de $\mathrm{Hom}_{\mathbb{Z}_p}(S(X'/L)^{(M)},\mu_M)$ défini par $\xi_{v,e}(x)=[e, x_v(\mathrm{Fr}_\ell^f)]_M$. La formule du produit (2.1) permet d'associer à tout élément de $S_T(X/L)^{(M)}$ une relation entre les caractères $\xi_{v,e}$: choisissons une base (e_i) de $T_p(X)$ et soit $e_i^{(M)}$ la projection de e_i dans X_M ; choisissons une racine de l'unité ζ d'ordre M et posons $(\zeta_{M,v})^{u_v}=\zeta$ (u_v est une unité de $\mathbb{Z}_p$); si τ est un élément de $S_T(X/L)^{(M)}$, posons $\mathfrak{E}_v(\tau)=\sum_{i=1}^d E_{v,i}(\tau)e_i^{(M)}$; on a alors

$$\prod_{i=1}^d \prod_{v\in T} (\xi_{v,e_i})^{u_v E_{v,i}(\tau)} = 1. \tag{3.1}$$

Nous allons utiliser les éléments fabriqués dans le théorème 2.1 pour un choix convenable de k. En reprenant les notations du théorème 2.1, on a ainsi une suite croissante d'ensembles $T_s=\{\ell_1,\dots,\ell_s\}$ et des éléments $\tau_{[m;\ell_1,\dots,\ell_s]} \in S_{T_s}(X/K(m))^{(M)}$ pour $s\leqslant k$. En choisissant bien l'élément h du théorème 2.1, on peut prendre $E_{v_{\ell_s},j}(\tau_{[m;\ell_1,\dots,\ell_s]})$ de valuation p-adique minimale. Remarquons que

les τ_m et τ_π peuvent être divisibles par p dans $S_T(X/L)^{(M)}$.; c'est ce qui fait intervenir l'indice que l'on trouve dans les théorèmes du paragraphe 1 .

3.2. Cas cyclotomique.

Soit χ un caractère pair non trivial de conducteur f ; pour simplifier, on suppose qu'il est à valeurs dans $\mathbb{Z}_p^*$ et on note e_χ le projecteur associé. On peut d'autre part supposer que F est le corps (réel) fixe par le noyau de χ . Kolyvagin démontre alors la proposition suivante.

Proposition 3.1. $\#(A_F^{(\chi)})$ divise $[\mathfrak{C}_F^{(\chi)}: \mathbb{Z}_p e_\chi(N_{\mathbb{Q}(\zeta_f)/F}(1-\zeta_f))]$.

Ici, $N_{\mathbb{Q}(\zeta_f)/F}(1-\zeta_f))=\tau_{F,f}$ est la norme sur F d'un point du système d'Euler que l'on a décrit. On peut facilement voir que $\mathbb{Z}_p e_\chi(N_{\mathbb{Q}(\zeta_f)/F}(1-\zeta_f))$ est égal à $\mathfrak{C}_F^{(\chi)}$. Pour montrer le théorème 1.1, c'est-à-dire l'égalité dans la proposition 3.1, on utilise la formule du nombre de classes que l'on rappelle dans le cas où p ne divise pas $2[F:\mathbb{Q}]$ [34].

Proposition 3.2. On a $\#(A_F)= \prod_{\chi\neq 1} [\mathfrak{C}_F^{(\chi)}: \mathfrak{C}_F^{(\chi)}]$ où le produit est pris sur les caractères χ de $Gal(F/\mathbb{Q})$ non triviaux.

Dans le cas elliptique, la formule analogue est montrée dans [18]

Revenons à la démonstration de la proposition 3.1. Le choix d'une racine de l'unité ζ permet d'identifier $Hom_{\mathbb{Z}_p}(S(\mathbb{Z}_p/F)^{(M)}, \mu_M)$ et $A_F = C_F(p)$ (si v est une place de F, la classe [v] de l'idéal associé à v correspond au caractère $\xi_{v,\zeta}$). Soient $p^{n_1(\chi)},\ldots, p^{n_r(\chi)}$ les invariants de $A_F^{(\chi)}$ avec $n_1(\chi)\geq\ldots\geq n_r(\chi)$ et soient $c_1,\ldots c_r$ des éléments de $A_F^{(\chi)}$ tels que c_i soit d'ordre $p^{n_i(\chi)}$ dans $A_F^{(\chi)}/\mathbb{Z}_p c_1 +\ldots \mathbb{Z}_p c_{i-1}$. Si

x appartient à F^*/F^{*M}, on note $J(x,M)$ l'annulateur de x et

$$J'(x,M)=\{a\in\mathbb{Z}_p \text{ tel que } aJ(x,M)\subset M\mathbb{Z}_p\}.$$

Pour M assez grand et $x\in F^*$, la valuation p-adique $C(x)$ de $J'(x,M)$ est le plus grand entier C tel que $x\in F^{*p^C}$. Lorsque $x\in\mathfrak{C}^{(\chi)}$, l'indice de $\mathbb{Z}_p x$ dans $\mathfrak{C}^{(\chi)}$ est égal à $p^{C(x)}$.

On définit $\alpha_v(x)\in\mathbb{Z}/M\mathbb{Z}$ par $(\zeta_{M,v})^{\alpha_v(x)}=(1-Fr_\ell^{-1})(x/M)$. Il s'agit maintenant d'appliquer plusieurs fois le théorème 2.1 en faisant un choix convenable de l'élément h qui assure les propriétés désirées de $[v_{\ell_k}]$ et de la valuation p-adique de $\alpha_{v_k}(e_\chi\tau_{\pi_k})$. Nous ne le faisons pas en détail ici et donnons simplement la suite logique de la démonstration. On choisit $\tilde{M}$ divisible par $\#(A_F)$, $M=\tilde{M}^3$ et $k=r$.

On choisit ℓ_1 tel que $e_\chi[v_{\ell_1}]=c_1$ et tel que

$$\mathrm{ord}_p(\alpha_{v_{\ell_1}}(e_\chi\tau_f))=C(e_\chi\tau_f)=_{\text{déf}}C_0(\chi)$$

et on pose $\pi_1=[f;\ell_1]$ et $C_1=C(e_\chi\tau_{\pi_1})$. On a donc $C_1\leqslant C_0(\chi)$ et la relation dans $A_F^{(\chi)}/A_F^{(\chi)M}=A_F^{(\chi)}$

$$p^{-C_1}\alpha_{v_1}(e_\chi\tau_f)e_\chi[v_{\ell_1}]=0,$$

d'où l'inégalité $C_0(\chi)-C_1\geqslant n_1(\chi)$. Supposons choisis $\ell_2,\ldots,\ell_{s-1}$ comme dans le théorème 2.1 tels que $e_\chi[v_{\ell_j}]=c_j$ et $C_{j-1}-C_j\geqslant n_j(\chi)$ avec $\pi_j=[f;\ell_1,\ldots\ell_j]$ et $C_j=C(e_\chi\tau_{\pi_j})$. On choisit ℓ_s tel que $e_\chi[v_{\ell_s}]=c_s$ et tel que $\mathrm{ord}_p(\alpha_{v_{\ell_s}}(e_\chi\tau_{\pi_{s-1}}))=C_{s-1}$. On pose $C_s=C(e_\chi\tau_{\pi_s})$. On a alors dans $A_F^{(\chi)}/\mathbb{Z}_pc_1+\ldots+\mathbb{Z}_pc_{s-1}$

$$p^{-C_s}\alpha_{v_{\ell_s}}(e_\chi\tau_{\pi_{s-1}})[v_{\ell_s}]^{(\chi)}=0$$

d'où $C_{s-1}-C_s\geqslant n_s(\chi)$. On en déduit que $C_0(\chi)\geqslant n_1(\chi)+\ldots+n_r(\chi)=\#(A_F^{(\chi)})$.

Kolyvagin caractérise un certain sous-ensemble de suites $[f;\ell_1,\ldots,\ell_r]$ à partir desquelles on peut déterminer le rang et les invariants du groupe abélien $A_F^{(\chi)}$. Ce sous-ensemble est construit par récurrence en même temps qu'une suite

d'entiers $C_0(\chi)>\ldots> C_r(\chi)$. L'entier $C_0(\chi)$ est celui déjà défini. Choisissons M suffisamment grand ($\geqslant 3C_0(\chi)$ par exemple). Supposons construits les $C_i(\chi)$ et les ℓ_i pour $i\leqslant s$. On note $\pi_i=[f;\ell_1,\ldots\ell_i]$. Pour tout nombre premier ℓ ne divisant pas $pf\ell_1..\ell_s$ totalement décomposé dans $F(\mu_M)$, on pose

$$C(\pi_s,\ell)= \mathrm{ord}_p(J'(e_\chi \tau_{[\pi_s,\ell]}(M),M)).$$

On montre qu'il existe un nombre premier ℓ totalement décomposé dans $F(\mu_M)$ et tel que

$$\mathrm{ord}_p(\alpha_{v_\ell}(e_\chi \tau_{\pi_s}(M)))=C_s(\chi) \text{ et } \mathrm{ord}_p(\alpha_{v_\ell}(e_\chi \tau_{\pi_j}(M)))>C_j(\chi) \text{ pour } 0\leqslant j\leqslant s-1 .$$

On note $C_{s+1}(\chi)$ la borne inférieure des $C(\pi_s,\ell)$ pour ℓ vérifiant ces conditions et on choisit pour ℓ_{s+1} n'importe lequel des nombres premiers ℓ pour lesquels la borne inférieure est atteinte. Nous avons alors les propriétés suivantes

(i) $C_{s+1}(\chi)\leqslant C_s(\chi)$;

(ii) si $C_{s+1}(\chi)<C_s(\chi)$, alors $n_{s+1}(\chi)=C_s(\chi)-C_{s+1}(\chi)$

(iii) si $C_{s+1}(\chi)=C_s(\chi)$, alors s est le $\mathbb{Z}/p\mathbb{Z}$-rang de $A_F^{(\chi)}/A_F^{(\chi)p}$ $(s=r)$ et l'on a

$$n_1(\chi)=C_0(\chi)-C_1(\chi),\ n_2(\chi)=C_1(\chi)-C_2(\chi),\ n_s(\chi)=C_{s-1}(\chi)-C_s(\chi);$$

De plus si v_{ℓ_i} est une place de F au dessus de ℓ_i, l'homomorphisme

$$\mathbb{Z}^s \to A_F^{(\chi)}$$

$$(\alpha_1,\ldots,\alpha_s) \mapsto \sum \alpha_i\ e_\chi[v_{\ell_i}]$$

a comme noyau $p^{n_1}\mathbb{Z}\times\ldots p^{n_s}\mathbb{Z}$ et est surjectif pour $s=r$. Enfin, on peut écrire $e_\chi \tau_{\pi_i}(M)=y_i^{p^{C_i(\chi)}}$ dans F^*/F^{*M} et les $y_1,\ldots,y_r$ sont linéairement indépendants dans F^*/F^{*p}.

3.3. Démonstration du théorème 1.3.

Soit $c=\#(E(K)_{tors})$. Soit t_p la p-partie du nombre de Tamagawa. Si P est un point d'ordre infini de $E(K)$, soit $C(P)$ le plus grand entier qui divise P

dans $E(K)/E(K)_{tors}$. Lorsque $E(K)$ est de rang 1, $C(P)$ est l'indice de $\mathbb{Z}P$ dans $E(K)/E(K)_{tors}$.

Lemme 3.3. Il existe un entier a tel que, pour tout nombre premier p et pour tous entiers n et m, le groupe $H^1(K(E_{p^{n+m}})/K, E_{p^n})$ est annulé par a. Il existe un entier b' tel que $b'A$ est nul pour tout sous-module galoisien A de E_{p^n} tel que $(\sigma+1)A=0$ ou $(\sigma-1)A=0$ (on posera $b=2b'$).

La démonstration utilise la théorie de la multiplication complexe et le résultat suivant dû à Serre [53]: si E n'est pas à multiplication complexe, le groupe de Galois de $\mathbb{Q}(E_p)/\mathbb{Q}$ est isomorphe à $Gl_2(\mathbb{Z}/p\mathbb{Z})$ pour p suffisamment grand. Les facteurs premiers de ab appartiennent à S_E (th. 1.3).

Rappelons que le groupe de Selmer $S(F)^{(M)} = S(T_p(E)/F)^{(M)}$ est lié au groupe de Shafarevich-Tate par la suite exacte

$$0 \to E(F)/ME(F) \to S(F)^{(M)} \to Ш(E/F)_M \to 0.$$

On note $S(K)^{(M)(\pm)}$, $Ш(E/K)^{(\pm)}$ les espaces propres relatifs à ± 1 pour la conjugaison complexe σ de $S(K)^{(M)}$ et de $Ш(E/K)$. On choisit une base $e_\pm$ de $2T_p(E)$ telle que $\sigma e_\pm = \pm e_\pm$ et on note $e_\pm^{(M)}$ leurs projections dans $E_M^\pm$. Si ℓ est inerte dans K totalement décomposé dans $K(E_M)/K$, on note $\xi_{\alpha\ell}$ (pour $\alpha \in \{+,-\}$) le caractère $\xi_{\ell,e}$ pour $e = e_{-\alpha}^{(M)} \in E_M$ défini dans le paragraphe 3.1 (on a ici $f=2$) : $\xi_{\pm\ell} \in \mathrm{Hom}_{\mathbb{Z}_p}(S(K)^{(M)(\pm)}, \mu_M)$.

Plus généralement, si x est un élément de $H^1(K, E_M)$, on pose pour $\alpha \in \{+,-\}$

$$\eta_\ell^\alpha(x) = [X_v(Fr_\ell^2), e_{-\alpha}^{(M)}]_M .$$

La restriction de $\eta_\ell^\pm$ à $S(K)^{(M)(\pm)}$ est donc $\xi_{\pm\ell}$. On note ξ_0 le caractère trivial.

Soient $\ell_1, \ldots, \ell_{k-1}$ des nombres premiers inertes dans K totalement dé-

composés dans $K(E_M)/K$. On note $Y_M(\ell_1,\dots,\ell_{k-1})$ le sous-groupe de $\mathrm{Hom}_{\mathbb{Z}_p}(S(K)^{(M)((-1)^k\varepsilon)}, \mu_M)$ engendré par les caractères $\xi_{(-1)^k\varepsilon\ell_{k-1}},\dots,\xi_{(-1)^k\varepsilon\ell_1},\xi_0$ et on pose

$$\cdot\ Z_M(\ell_1,\dots,\ell_{k-1})=\mathrm{Hom}_{\mathbb{Z}_p}(S(K)^{(M)((-1)^k\varepsilon)},\mu_M)/Y_M(\ell_1,\dots,\ell_{k-1}).$$

Si ξ est un élément de $\mathrm{Hom}_{\mathbb{Z}_p}(S(K)^{(M)((-1)^k\varepsilon)},\mu_M)$, on note $\mathrm{ord}_{p,Z_M(\ell_1,\dots,\ell_{k-1})}(\xi)$ la valuation p-adique de l'ordre de ξ dans $Z_M(\ell_1,\dots,\ell_{k-1})$.

Enfin, donnons quelques propriétés des points de Heegner et du système d'Euler associé. Si π est de niveau 1, τ_π est défini sur $K(1)$. Si σ est la conjugaison complexe et si ε est la valeur propre de l'involution d'Atkin-Lehner agissant sur la forme modulaire f associée à E, on a

$$\sigma(\mathrm{cores}_{K(1)/K}(\tau_\pi))=(-1)^k\varepsilon\,\mathrm{cores}_{K(1)/K}(\tau_\pi) \text{ modulo torsion}$$

où $\pi=[1;\ell_1,\dots,\ell_k]$ (le cas des points de Heegner est bien connu [24], le cas d'ordre quelconque s'en déduit par récurrence en revenant à la définition de τ_π). Le point $\tau_{\pi,K}=(\sigma+(-1)^k\varepsilon)\mathrm{cores}_{K(1)/K}(\tau_\pi)$ est défini sur K et vérifie

$$\sigma\tau_{\pi,K}=(-1)^k\varepsilon\tau_{\pi,K}.$$

En particulier, $\tau_{1,K}=\tau_{[1],K}$ est un point de $E(K)$.

Théorème 3.4. <u>On suppose que le point de Heegner</u> $\tau_{1,K}$ <u>est d'ordre infini. Fixons un entier</u> r. <u>Soit</u> $M=p^n$ <u>une puissance de</u> p <u>telle que</u>

$$n\geqslant \mathrm{ord}_p(C(\tau_{1,K}))+r\,\mathrm{ord}_p(abc)+2\mathrm{ord}_p(2c)+1.$$

<u>Il existe des nombres premiers</u> $\ell_1,\dots,\ell_r$ <u>inertes dans</u> K <u>totalement décomposés dans</u> $K(E_M)/K$ <u>tels que</u> $[1;\ell_1,\dots,\ell_r]\in\mathcal{P}^{(r)}$ <u>et</u> $M^3t_p\mid M_{\ell_1}$ <u>et des entiers</u> n_k <u>vérifiant</u>

$$n_0=\mathrm{ord}_p(C(\tau_{1,K})),\quad 0\leqslant n_k\leqslant n,\quad -\mathrm{ord}_p(abc)\leqslant n_{k-1}-n_k \text{ pour } k\geqslant 1$$

<u>tels que l'on ait les inégalités</u>

(3.2) $$0\leqslant \mathrm{ord}_p(\mathrm{exposant}(Z_M(\ell_1,\ell_2,\dots,\ell_{k-1})))-\mathrm{ord}_{p,Z_M(\ell_1,\dots,\ell_{k-1})}(\xi_{(-1)^k\varepsilon\ell_k})\leqslant \mathrm{ord}_p(ab)$$

(3.3) $$\mathrm{ord}_{p,Z_M(\ell_1,\dots,\ell_{k-1})}(\xi_{(-1)^k\varepsilon\ell_k}) \leqslant n_{k-1}-n_k+2\mathrm{ord}_p(2abc).$$

L'ordre de $\tau_{[1;\ell_1,\dots,\ell_j],K}(M)$ est égal à M/p^{n_j} et il existe un élément $\tau'_{[1;\ell_1,\dots,\ell_j]}(M)$ de $S_{\{\ell_1,\dots,\ell_j\}}(K)^{(M)}$ tel que

(3.4) $$c\tau_{[1;\ell_1,\dots,\ell_j],K}(M) = p^{n_j}\tau'_{[1;\ell_1,\dots,\ell_j]}(M)$$

et tel que $\eta_{(-1)^{k-1}\varepsilon\ell_k}(\tau'_{[1;\ell_1,\dots,\ell_{k-1}]}(M))$ soit une racine de l'unité d'ordre p^β avec

(3.5) $$n-\mathrm{ord}_p(abc)\leqslant\beta\leqslant n-\mathrm{ord}_p(c).$$

On déduit facilement du théorème 3.4 les résultats annoncés.

Corollaire 3.5. Si le point de Heegner $\tau_{1,K}$ est d'ordre infini, $Ш(E/K)^{(-\varepsilon)}$ est fini et annulé par $4(ab)^3c^2C(\tau_{1,K})$.

Démonstration. On utilise le théorème 3.4 avec $r=1$. Le groupe $Z_M = S(K)^{(M)(-\varepsilon)}$ est annulé par $2p^{n_0-n_1}(ab)^3c^2$ et donc par $2(ab)^3c^2\,C(\tau_{1,K})$. On en déduit que $4(ab)^3c^2\,C(\tau_{1,K})$ annule $Ш(E/K)^{(-\varepsilon)}$. Comme $Ш(E/K)^{(-\varepsilon)}$ est de type fini sur $\mathbb{Z}$, il est donc fini.

Corollaire 3.6. Si le point de Heegner $\tau_{1,K}$ est d'ordre infini, $E(K)$ est de rang 1, $Ш(E/K)$ est fini et annulé par $4d(ab)^5c^2C(\tau_{1,K})$.

Démonstration. On utilise ici le théorème 3.4 avec $r=2$ afin de contrôler $Ш(E/K)^{(\varepsilon)}$. Ainsi $2p^{n_1-n_2}(ab)^3c^2$ (donc $2(ab)^4c^2\,C(\tau_{1,K})$) annule $Z_M(\ell_1) = \mathrm{Hom}_{\mathbb{Z}_p}(S(K)^{(M)(\varepsilon)},\mu_M)/(\chi_{\varepsilon\ell_1})$ et donc $\ker\xi_{\varepsilon\ell_1}$. Mais $\xi_{\varepsilon\ell_1}(\tau'_1)$ est d'ordre p^γ avec $n-\mathrm{ord}_p(abc)\leqslant\gamma\leqslant n-\mathrm{ord}_p(c)$. On en déduit que $S(K)^{(M)(\varepsilon)}/\langle\ker\xi_{\varepsilon\ell_1},\tau'_1\rangle$ est un groupe cyclique annulé par abc et que $2(abc)(ab)^4c^2C(\tau_{1,K})$ annule $S(K)^{(M)}/\langle\tau'_1\rangle$. Donc $S(K)^{(M)\varepsilon}$ est de rang 1. On voit (lemme 3.8) qu'il existe $\tau\in E(K)$ tel que $c\tau=\tau'_1$

et on a alors $E(K)=E(K)_{tor}+\mathbb{Z}\tau$. Donc $S(K)^{(M)}/<\tau>+E(K)_{tor}$ est égal à $Ш(E/K)_M$. Ainsi, $4(ab)^5c^3C(\tau_{1,K})$ annule $Ш(E/K)$ qui est en particulier un groupe fini.

Corollaire 3.7. Supposons que p ne divise pas 2abc. Si le point de Heegner $\tau_{1,K}$ est d'ordre infini, le cardinal de $Ш(E/K)$ divise $C(\tau_{1,K})^2$.

Démonstration. On applique le théorème avec r supérieur à 2 fois le rang sur $\mathbb{Z}/p\mathbb{Z}$ de $Ш(E/K)^{(\pm)}$.

On peut déduire du théorème 3.4 une estimation du cardinal de $Ш(E/K)$ pour les nombres premiers p divisant 2abc.

On démontre facilement le lemme suivant qui est en fait le cas r=0 du théorème.

Lemme 3.8. Si $n\geq ord_p(cC(\tau_{1,K}))+1$, l'annulateur de $\tau_{1,K}$ modulo $p^nE(K)$ est de valuation p-adique $n-ord_p(C(\tau_{1,K}))$, c'est-à-dire que $n_0=ord_p(C(\tau_{1,K}))$. Il existe un point τ'_1 de $E(K)$ tel que $c\tau_{1,K}=p^{n_0}\tau'_1$.

Commençons la démonstration du théorème 3.4 en supposant p impair. Elle se fait par récurrence sur r. Supposons le théorème vrai pour r-1. On pose $\pi_{r-1}=[1;\ell_1,\ldots,\ell_{r-1}]$ et lorsque ℓ_r sera choisi, $\pi_r=[1;\ell_1,\ldots,\ell_r]$. Il s'agit de bien choisir le h du théorème 2.1. Il est facile de vérifier que $\tau'_{\pi_{r-1}}(M)$ est d'ordre $Mp^{-ord_p(c)}=p^{n-ord_p(c)}$.

On définit un sous-groupe $S_\pm$ de $S_{(\ell_1,\ldots\ell_{r-1})}(K)^{(M)(\pm)}$ par

$$S_{(-1)^{r-1}\varepsilon}=\mathbb{Z}_p\tau'_{\pi_{r-1}}(M) \text{ et } S_{(-1)^r\varepsilon}=S(K)^{(M)((-1)^r\varepsilon)}.$$

On pose $Y_{M,r}=Y_M(\ell_1,\ldots,\ell_{r-1})$ et $Z_{M,r}=Z_M(\ell_1,\ldots,\ell_{r-1})$.

On choisit un entier M' assez grand (tel que M^3t_p (resp.

$M_0(m,\ell_1,\dots\ell_k)M_{\ell_k}$) divise M' si $r=1$ (resp. $r>1$)).

Soit $S'_\pm$ l'image de $S_\pm$ dans $H^1(K(E_{M'}), E_M)$ par l'homomorphisme de restriction. Comme M divise M', ce dernier groupe est isomorphe à $\mathrm{Hom}_{\mathbb{Z}_p}(\mathrm{Gal}(\overline{K}/K(E_{M'})), E_M)$. Soit $F_\pm$ la plus petite extension de $K(E_{M'})$ telle que $S'_\pm$ soit contenu dans $\mathrm{Hom}_{\mathbb{Z}_p}(\mathrm{Gal}(F_\pm/K(E_{M'})), E_M)$. On pose

$$F=F_+F_-\ ,\ H_\pm=\mathrm{Gal}(F_\pm/K(E_{M'}))\ ,\ H=\mathrm{Gal}(F/K(E_{M'}))\ .$$

On a donc

$$S'_\pm \subset \mathrm{Hom}_{\mathbb{Z}_p}(H_\pm,E_M) \subset \mathrm{Hom}_{\mathbb{Z}_p}(H,E_M).$$

On définit un homomorphisme $\varphi_\pm : H \to \mathrm{Hom}_{\mathbb{Z}_p}(S'_\pm,\mu_M)$ par

$$\varphi_\alpha(h)(x)=[x(hh^\sigma),e_{-\alpha}^{(M)}]_M\ .$$

Soit $\psi_\pm$ le composé de $\varphi_\pm$ avec l'homomorphisme induit par la restriction

$$\mathrm{Hom}_{\mathbb{Z}_p}(S'_\pm,\mu_M) \to \mathrm{Hom}_{\mathbb{Z}_p}(S_\pm,\mu_M).$$

Le lemme suivant utilise le lemme 3.3.

Lemme 3.9. $\varphi_\pm(H) \supset b\,\mathrm{Hom}_{\mathbb{Z}_p}(S'_\pm,\mu_M)$ et ab annule $\mathrm{Hom}_{\mathbb{Z}_p}(S_\pm,\mu_M)/\psi_\pm(H)$.

Lemme 3.10. Il existe un élément η de H tel que l'ordre de $\psi_{(-1)^r\varepsilon}(\eta)$ (resp. $\psi_{(-1)^{r-1}\varepsilon}(\eta)$) dans $\psi_{(-1)^r\varepsilon}(H)/Y_{M,r}\cap\psi_{(-1)^r\varepsilon}(H)$ (resp. dans $\psi_{(-1)^{r-1}\varepsilon}(H)$) soit égal à l'exposant de $\psi_{(-1)^r\varepsilon}(H)/Y_{M,r}\cap\psi_{(-1)^r\varepsilon}(H)$ (resp. de $\psi_{(-1)^{r-1}\varepsilon}(H)$).

Pour montrer l'existence de η, on utilise la propriété que la réunion de deux sous-groupes de H distincts de H est strictement contenue dans H.

Corollaire 3.11. On a les inégalités

$$n-\mathrm{ord}_p(abc)\leqslant \mathrm{ord}_p(\text{ordre } \psi_{(-1)^{r-1}\varepsilon}(\eta))\leqslant n-\mathrm{ord}_p(c)$$

$$\mathrm{ord}_p(\text{exposant } Z_{M,r})-\mathrm{ord}_p(ab)\leqslant \mathrm{ord}_{p,Z_{M,r}}(\psi_{(-1)^r\varepsilon}(\eta))\ .$$

Fixons maintenant un tel η et posons $h=\eta\sigma$. Choisissons un nombre premier ℓ_r comme dans le théorème 2.1 tel que le Frobenius de ℓ_r dans $F/\mathbb{Q}$ soit h. Comme $\eta\eta^{\sigma}=(\eta\sigma)^2=Fr_{\ell}^2$ (σ est d'ordre 2), $\psi_{(-1)^r\varepsilon}(\eta)$ et $\xi_{(-1)^r\varepsilon\ell_r}$ coincident et on a

$$\psi_{(-1)^{r-1}\varepsilon}(\eta)(\tau'_{\pi_{r-1}})=\eta_{(-1)^{r-1}\varepsilon\ell_r}(\tau'_{\pi_{r-1}}).$$

L'ordre p^{β} de ce dernier élément vérifie donc

$$n\text{-}ord_p(abc)\leqslant\beta\leqslant n\text{-}ord_p(c).$$

Cela montre les propriétés (3.2) et (3.5).

L'ordre de $\tau_{\pi_r}(M)$ est par définition M/p^{n_r}. Il est facile de voir que $\tau_{\pi_r}(M')$ est divisible par p^{n_r} dans $H^1(K,E_{M'})$: $\tau_{\pi_r}(M')=p^{n_r}\tau'_{\pi_r}(M'p^{-n_r})$. On vérifie que par projection dans $H^1(K,E_M)$, $\tau'_{\pi_r}(M)$ appartient à $S_{\{\ell_1,\ldots\ell_j\}}(K)^{(M)}$.

Nous allons maintenant montrer que $n_{r-1}-n_r\geqslant -ord_p(abc)$. Rappelons que l'on a

$$\psi_{(-1)^{r-1}\varepsilon}(\eta)(x)=[(Fr_{\ell_r}^2-1)(x/M),e^{(M)}_{(-1)^r\varepsilon}]_M$$

pour tout x appartenant au sous-groupe engendré par $\tau'_{\pi_{r-1}}(M)$ et que d'après le corollaire 3.11,

$$n\text{-}ord_p(abc)\leqslant ord_p(\text{ordre } \psi_{(-1)^{r-1}\varepsilon}(\eta))\leqslant n\text{-}ord_p(c).$$

On en déduit que $(Fr_{\ell_r}^2-1)(\tau'_{\pi_{r-1}}(M)/M)$ est d'ordre p^{β} avec

$$n\text{-}ord_p(abc)\leqslant\beta\leqslant n\text{-}ord_p(c).$$

En utilisant les relations (2.3) du théorème 2.1 et le fait que Fr_{ℓ_r} et la conjugaison complexe coincident sur K, on trouve que si v_r est la place de K au dessus de ℓ_r

$$p^{n_r}\mathfrak{S}_{v_r}(\tau'_{\pi_r}(M))=(-1)^r\varepsilon p^{n_{r-1}}(Fr_{\ell_r}^2-1)(\tau'_{\pi_{r-1}}(M)/M).$$

Les deux termes sont des multiples de $e^{(M)}_{(-1)^{r-1}\varepsilon}$. On en déduit que

$n_r \leqslant n_{r-1} + n - \beta$ (car p^{n_r} divise M). D'où $n_{r-1} - n_r \geqslant -\mathrm{ord}_p(abc)$. La relation précédente devient alors

$$\mathfrak{e}_{v_r}(abc\tau'_{\pi_r}(M)) = (-1)^r \varepsilon (Fr_{\ell_r}^2 - 1)(abcp^{n_{r-1}-n_r}\tau'_{\pi_{r-1}}(M)/M).$$

Si l'on pose

$$\mathfrak{e}_{v_k}(abc\tau'_{\pi_r}(M)) = E_k e_{(-1)^{r-1}\varepsilon},$$

on a $\mathrm{ord}_p(E_r) \leqslant (n_{r-1} - n_r) + 2\mathrm{ord}_p(abc)$. La relation (3.1) pour $\tau = abc\tau'_{\pi_r}(M)$ devient

$$\prod_{k=1}^{r} (\xi_{(-1)^r \varepsilon \ell_k})^{u_k E_k} = 1$$

et on en déduit que $\mathrm{ord}_{p, Z_M(\ell_1, \ldots, \ell_{r-1})}(\xi_{(-1)^r \varepsilon \ell_r}) \leqslant n_{r-1} - n_r + 2\mathrm{ord}_p(abc)$ (relation (3.3)). Cela termine la démonstration du théorème 3.4.

Références

[1] B. Birch. Diophantine analysis and modular functions, Proceedings of Bombay Colloquium on Algebraic Geometry (1968), 35-42.

[2] B. Birch. Elliptic curves and modular functions, Symposia Mathematica (1970), 27-32.

[3] B. Birch. Heegner points of elliptic curves, Symposia Mathematica (1975), 441-445.

[4] B. Birch et N. Stephens. Heegner's construction of points on the curve $y^2 = x^3 - 1728e^3$. Séminaire de théorie des nombres. Paris 1981-1982, Progress in Math. 38. Birkhäuser (1983), 1-19.

[5] B. Birch et H. Swinnerton-Dyer. Notes on elliptic curves II J. reine u. Angew. Math. 218 (1965), 79-108.

[6] S. Bloch et K. Kato. L-functions and Tamagawa nombers of motives, Grothendieck Festschrift, Progress in Math., Birkhaüser Boston.

[7] A. Brumer. Travaux récents d'Iwasawa et Leopoldt, Séminaire Bourbaki n° 325 (1966/1967).

[8] D. Bump, S. Friedberg et J. Hoffstein. A non vanishing theorem for derivatives of automorphic L-functions with applications to elliptic curves, Bull.

AMS. Math. Soc. 21 (1989), 89-93.

[9] J. Coates. p-adic L functions and Iwasawa's theory, in Algebraic Number Fields, édité par A. Fröhlich, Academic Press (1977), 269-353.

[10] J. Coates. The work of Mazur and Wiles on cyclotomic fields, Séminaire Bourbaki, n° 574 (1980-1981).

[11] J. Coates. On p-adic L-functions, Séminaire Bourbaki, n° 701 (1988-1989).

[12] J. Coates et C. Goldstein. Some remarks on the main conjecture for elliptic curves with complex multiplication, Am. Journal of Math. 105 (1983), 337-366.

[13] J. Coates et A. Wiles. On the conjecture of Birch and Swinnerton-Dyer, Invent. Math. 39 (1977), 223-251.

[14] J. Coates et A. Wiles. On p-adic L-functions and elliptic units, J. Austral. Math. Soc. (Series A) 26 (1978), 1-25.

[15] J.-M. Fontaine. Représentations p-adiques, Proc. Int. Cong. Math, Varszawa (1983), 475-486.

[16] R. Gillard. Unités cyclotomiques, unités semi-locales et $\mathbb{Z}_\ell$-extensions, Ann. Inst. Fourier 29,1 (1979), 49-79 et 29,4 (1979), 1-15.

[17] R. Gillard. Unités elliptiques et unités cyclotomiques, Math. Ann. 243 (1979), 181-189.

[18] R. Gillard et G. Robert. Groupes d'unités elliptiques, Bull. SMF 107 (1979), 305-317.

[19] G. Gras. Classes d'idéaux des corps abéliens et nombres de Bernoulli généralisés, Ann. Inst. Fourier 27 (1977), 1-66.

[20] R. Greenberg. On p-adic L-functions and cyclotomic fields, Nagoya Math. J. 56 (1975), 61-77 et 67 (1977), 139-158.

[21] R. Greenberg. Iwasawa's theory and p-adic L-functions for imaginary quadratic fields, dans Number theory related to Fermat's last theorem, édité par N. Koblitz, Progress in Math. 26, Birkhäuser (1982), 275-285.

[22] R. Greenberg. On the Birch et Swinnerton-Dyer conjecture, Invent. Math. 72 (1983), 241-265.

[23] R. Greenberg. Iwasawa theory for p-adic representations, Adv. Stud. Pure Math. 17 (1989).

[24] B.H. Gross. Heegner points on $X_0(N)$, dans Modular forms, édité par R.A. Rankin, Ellis Horwood Limited (1984), 87-105.

[25] B.H. Gross. Kolyvagin's work on modular elliptic curves (prépublication).

[26] B.H. Gross et D. Zagier. Heegner points et derivatives of L-series, Invent. Math. 84 (1986), 225-320.

[27] K. Iwasawa, On p-adic L functions, Ann. of Math. 89, (1969), 198-205.

[28] K. Iwasawa. Lectures on p-adic L-functions, Ann. Math. Studies 74, Princeton University Press (1972)

[29] K. Iwasawa, On $\mathbb{Z}_\ell$-extensions of algebraic number fields, Ann. of Math. 98 (1973), 246-326.

[30] N. Katz. p-adic L-functions for C.M. fields, Invent. Math. 49 (1978),199-297.

[31] V.A. Kolyvagin. Finiteness of $E(\mathbb{Q})$ and $Ш(E/\mathbb{Q})$ for a subclass of Weil curves, Izv. Akad. Nauk. SSSR Ser Mat. 52 (3) (1988), 522-540; Math. USSR Izvestiya 32 (1989), 523-541.

[32] V.A. Kolyvagin. On the Mordell-Weil group and the Shafarevich-Tate group of Weil elliptic curves, Izv. Akad. Nauk. SSSR Ser Mat. 52 (6) (1988),1154-1179.

[33] V.A. Kolyvagin. Euler systems, Grothendieck Festschrift, Progress in Math., Birkhaüser Boston.

[34] S. Lang. Cyclotomic fields I-II avec appendice de K. Rubin. GTM 121 ($2^{ième}$ édition) (1989), Springer Berlin.

[35] B. Mazur. Courbes elliptiques et symbole modulaire, Séminaire Bourbaki 414 (1971/1972), dans L. N. in Math. 317, Springer Berlin.

[36] B. Mazur. Modular curves and arithmetic, Proc. Int. Congress Math. (1983), Warszawa, 185-211.

[37] B. Mazur et P. Swinnerton-Dyer. Arithmetic of Weil curves, Invent. Math. 25 (1974), 1-61.

[38] B. Mazur et A. Wiles. Class fields of abelian extensions of $\mathbb{Q}$, Invent. Math. 76 (1984), 179-330.

[39] M. Ram Murty et V. Kumar Murty. Mean values of derivatives of modular L-series, prépublication (1989).

[40] B. Perrin-Riou. Arithmétique des courbes elliptiques et théorie d'Iwasawa, Mémoire de de la S.M.F. n° 17. Suppl. au Bull. de la S.M.F. 112 (1984).

[41] B. Perrin-Riou. Fonctions L p-adiques, théorie d'Iwasawa et points de Heegner, Bull. Soc. Math. France, 115 (1987), 399-456.

[42] B. Perrin-Riou. Dérivées de fonctions L p-adiques et points de Heegner, Invent. Math. 89 (1987), 456-510.

[43] K. Ribet. A modular construction of unramified p-extensions of $\mathbb{Q}(\mu_p)$, Invent. Math. 34 (1976), 151-162.

[44] G. Robert. Unités elliptiques, Bull. Soc. Math. France, mémoire 36 (1973).

[45] G. Robert. Nombres de Hurwitz et unités elliptiques, Ann. Sc. ENS (4) 11 (1978), 297-389.

[46] D. E. Rohrlich. On L-functions of elliptic curves and cyclotomic towers, Invent. Math. 75 (1984), 383-408 et 409-423.

[47] K. Rubin. Global units and ideal class groups, Invent. Math. 89 (1987), 511-526.

[48] K. Rubin. Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication, Invent. Math. 89 (1987), 527-560.

[49] K. Rubin. On the main conjecture of Iwasawa theory for imaginary quadratic fields, Invent. 93 (1988) 701-719 .

[50] K. Rubin. The "main conjectures" of Iwasawa theory for imaginary quadratic fields (1990).

[51] J.-P. Serre. Classes des corps cyclotomiques, d'après Iwasawa, Séminaire Bourbaki 174 (1958/1959).

[52] J.-P. Serre. Cohomologie galoisienne, Lectures Notes in Math 5 (1973), Springer Berlin.

[53] J.-P. Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. Invent. Math. 15 (1972), 259-331.

[54] E. de Shalit. The Iwasawa theory of elliptic curves with complex multiplication, Perspec. in Math. 3, Orlando: Academic Press (1987).

[55] J. Tate. The arithmetic of elliptic curves, Invent. Math. 23 (1974), 179-206.

[56] F. Thaine. On the ideal class groups of real number fields, Ann. of Math. 128 (1987), 1-18.

[57] J.-L. Waldspurger. Sur les valeurs de certaines fonctions L automorphes en leur centre de symétrie, Comp. Math. 54 (1985), 173-242.

[58] A. Wiles. Higher explicit reciprocity laws, Ann. Math. 107 (1978), 235-254.

[59] A. Wiles. On p-adic representations for totally real fields, Ann. Math. 123 (1986), 407-456.

[60] R. Yager. On two variables p-adic L functions, Ann. Math. 115 (1982), 411-449.

[61] R. Yager. p-adic measures on Galois groups, Invent. Math. 76 (1984), 331-343.

Bernadette PERRIN-RIOU
Université Pierre et Marie Curie
UFR 21, LMF 45-46, 3ième étage
4 place Jussieu
F-75230 PARIS CEDEX 05

Astérisque

BERNARD TEISSIER

Résultats récents d'algèbre commutative effective

Astérisque, tome 189-190 (1990), Séminaire Bourbaki,
exp. n° 718, p. 107-131

<http://www.numdam.org/item?id=SB_1989-1990__32__107_0>

© Société mathématique de France, 1990, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Séminaire BOURBAKI Novembre 1989
42ème année, 1989-90, n° 718

RÉSULTATS RÉCENTS D'ALGÈBRE COMMUTATIVE EFFECTIVE

par **Bernard TEISSIER**

Introduction

Beaucoup des résultats fondamentaux de l'algèbre commutative sont des résultats d'existence non effectifs: le théorème de Lasker-Noether affirmant l'existence pour tout idéal I d'un anneau noetherien A d'une décomposition $I = \mathcal{Q}_1 \cap \ldots \cap \mathcal{Q}_s$ en idéaux primaires, le théorème de normalisation de Noether, etc.. Le problème est de déterminer effectivement, lorsque l'on a des données précises, le cran auquel une suite croissante d'idéaux va stationner, ou bien une décomposition primaire d'un idéal donné, et bien sûr en premier lieu si un élément donné de l'anneau appartient à un idéal donné.

Le premier cadre naturel dans lequel on peut se poser de tels problèmes est celui des idéaux de l'algèbre des polynomes à coefficients dans un corps k dans lequel on sait faire des calculs effectifs, comme c'est le cas si k est une extension finie de son corps premier.

Ces problèmes ont déjà été attaqués au début du siècle, essentiellement au moyen de la théorie de l'élimination, et en ce qui concerne le dernier cité, par Macaulay au moyen de sa théorie des "systèmes inverses" qui est devenue la théorie de la dualité en algèbre et en géométrie algébrique (*cf* [35] et ses références). La donnée consiste en un nombre fini de polynomes, et l'on cherche des renseignements sur la décomposition primaire de l'idéal qu'ils engendrent; nombre des idéaux primaires, degré de leurs générateurs, taille de leurs coefficients, etc...

Soient k un corps et $I = (f_1, \ldots, f_m)$ un idéal de l'anneau de polynomes $k[x_1, \ldots, x_n]$. Etant donné un polynome g dont l'on suppose qu'il est dans I, comment écrire explicitement une relation $g = \sum_{i=1}^{m} g_i f_i$?. Il faut d'abord avoir une borne des degrés en dessous desquels on est sûr trouver des polynomes g_i. Dans le cas où $g = 1$, c'est le problème de l'identité de Bézout. Si D est le plus grand des degrés des polynomes $(f_1, \ldots, f_m)$, la théorie de l'élimination (*cf* [2] p.140, [26], [38],) montre que l'on peut trouver des g_i tels que $\deg g_i f_i \leq \deg g + 2(2D)^{2^{n-1}}$. Lorsque $(f_1, \ldots, f_m)$ est une intersection complète, on sait depuis Macaulay que l'on a une borne en $\deg g + D^m$. Un exemple de Mayr-Meyer ([18], [39]) a mis fin aux espoirs de trouver une borne simplement exponentielle dans le cas général : Ils ont montré comment construire pour tout entier $D \geq 5$, en prenant $n = 10n'$, une famille de $n+1$ polynomes $f_1, \ldots, f_{n+1}$ engendrant un idéal I qui contient z_1 mais tel que si l'on écrit

$$z_1 = g_1 f_1 + \cdots + g_{n+1} f_{n+1}$$

alors $\max_j(\deg g_j) > (D-2)^{2^{n'-1}}$. Ceci montre que le problème de l'appartenance est doublement exponentiel en le nombre de variables.

Le problème, analogue, du théorème des zéros effectif est celui de trouver, pour un polynome $g \in \sqrt{(f_1, \ldots, f_m)}$, des bornes pour s et le degré de polynomes en dessous desquelles on soit sûr de trouver des polynomes $g_1, \ldots, g_m$ tels que $g^s = \sum_{i=1}^{m} f_i g_i$. Dans le cas homogène, il suffit bien sûr de borner l'entier s.

Des problèmes de cette nature, dans des cas très particuliers, ont joué un rôle important en théorie de la transcendance depuis les travaux de Gel'fond, mais depuis une dizaine d'années, à la suite en particulier des travaux de Nesterenko (*cf* [40]), les spécialistes de la transcendance les ont remis à l'ordre du jour dans les cas les plus généraux (voir [10]).

Ainsi, c'est au travail fondamental (*cf* [12], [13]) de Brownawell que l'on doit de savoir que contrairement au problème de l'appartenance, le théorème des zéros effectif, lui, est simplement exponentiel en le nombre de variables.

D'autre part les recherches de calcul formel et de géométrie algébrique effective ont aussi, depuis une dizaine d'années, fait surgir des problèmes

d'effectivité de calculs dans les anneaux de polynomes. En ce qui concerne le calcul formel, mis à part les travaux de Lazard ([32], [33]), et plus récemment de Heintz et ses collaborateurs (*cf* [16], qui donna la première borne simplement exponentielle pour l'identité de Bézout valable sur un corps quelconque, [17] et [19]), l'attention s'était concentrée sur les calculs de bases standard d'idéaux, qui sont des systèmes de générateurs très particuliers permettant de décider effectivement par un algorithme de division de l'appartenance d'un élément à l'idéal qu'ils engendrent. Mais il semble que pour le moment ces méthodes "trop générales" ne savent pas distinguer entre les problèmes, comme celui de l'appartenance, qui sont doublement exponentiels, et les problèmes, comme ceux dont il est question ici, qui sont simplement exponentiels. Je ne parlerai pas ici de bases standard et renvoie le lecteur à [44] pour un panorama récent de cet aspect. De même, je renvoie à [17] et [25] pour les liens avec le calcul formel, et suis obligé de passer sous silence d'autres jolis résultats, comme la version effective du théorème de Serre-Quillen-Souslin sur les modules projectifs sur un anneau de polynomes ([19]).

On va considérer d'abord le cas "géométrique", où l'on ne retient des polynomes, outre le nombre des variables, que leur degré, alors que des calculs effectifs nécéssitent de considérer aussi la taille de leurs coefficients, ce dont nous nous occuperons ensuite, d'abord par des méthodes analytiques dues à Berenstein et Yger puis par des méthodes algébriques dues à Philippon.

Je remercie Daniel Bertrand, André Galligo, et Joos Heintz pour l'aide qu'ils m'ont apportée dans la préparation de ce texte.

§1 La géométrie

1. Le résultat

Soit k un corps. Posons $R = k[x_0, \ldots, x_n]$ et soit $I = (f_1, \ldots, f_m)$ un idéal de R engendré par des polynomes homogènes; posant $d_i = \deg f_i$,

ordonnons les générateurs de telle façon que l'on ait $d_2 \geq d_3 \geq \ldots \geq d_m \geq d_1 > 0$, et notons μ l'entier $\min(m,n)$. Le résultat de Kollár ([29]) raffiné par Brownawell ([11]) s'énonce comme la version effective suivante de l'égalité $\sqrt{I} = \mathcal{P}_1 \cap \cdots \cap \mathcal{P}_r$:

Théorème 1.- *Supposons $d_i \geq 3$ pour $i > 1$ et soient $\mathcal{P}_1, \ldots, \mathcal{P}_r$ les idéaux premiers minimaux associés à l'idéal $I = \mathcal{Q}_1 \cap \ldots \cap \mathcal{Q}_s$. Il existe des entiers e_i tels que l'on ait*

$$\mathcal{P}_1^{e_1} \ldots \mathcal{P}_r^{e_r} \subset I$$

et

$$\sum_{i=1}^{r} e_i \leq d_1 \ldots d_\mu.$$

Lorsque $(f_1, \ldots, f_m)$ est une intersection complète, d'après un théorème de Macaulay ([37]), toutes les composantes de la variété projective définie par I sont de la même dimension $n-m$, il n'y a pas de composantes immergées et il résulte alors très facilement du théorème de Bézout que l'on a l'égalité

$$\sum_{i=1}^{r} \mathrm{long}\mathcal{Q}_i \deg \mathcal{P}_i = d_1 \ldots d_m$$

où $\mathrm{long}\mathcal{Q}_i$ désigne la longueur dans l'anneau local $R_{\mathcal{P}_i}$ de l'idéal engendré par $\mathcal{Q}_i$, c'est-à-dire la longueur du $R_{\mathcal{P}_i}$-module $R_{\mathcal{P}_i}/\mathcal{Q}_i R_{\mathcal{P}_i}$; c'est la multiplicité avec laquelle la composante correspondant à l'idéal $\mathcal{P}_i$ intervient dans l'intersection des m hypersurfaces $f_i = 0$ dans $\mathbf{P}^n$. L'entier $\deg \mathcal{P}_i \geq 1$ est le degré de la variété projective correspondant à $\mathcal{P}_i$. Il n'est pas difficile de vérifier (*cf* [11]) que l'on a $\mathcal{P}^{\mathrm{long}\mathcal{Q}_i} \subset \mathcal{Q}_i$ et on a donc, en posant $e_i = \mathrm{long}\mathcal{Q}_i$ les inclusions $\mathcal{P}_1^{e_1} \ldots \mathcal{P}_r^{e_r} \subset \mathcal{Q}_1 \ldots \mathcal{Q}_r \subset \mathcal{Q}_1 \cap \ldots \cap \mathcal{Q}_r = I$ et le résultat dans ce cas, sans hypothèse sur les degrés. La difficulté dans le cas général vient des intersections non propres des hypersurfaces, qui détruisent l'équidimensionalité et surtout font apparaître des composantes immergées. L'idée de la démonstration est, après avoir, comme dans [11], par des combinaisons linéaires générales n'affectant pas trop les degrés remplacé la suite de polynomes donnée par une suite $(h_1, \ldots, h_l)$ aussi proche que possible d'une intersection complète, de construire l'idéal en ajoutant

une fonction après l'autre, en examinant à chaque pas les nouvelles composantes immergées qui apparaissent. Une construction voisine apparait dans la démonstration du théorème de Bézout général due à W. Vogel ([49]). L'idée de Kollár est de borner la méchanceté des composantes immergées à chaque étape au moyen d'un argument de cohomologie locale et le point est que cela permet d'obtenir le résultat optimal. Comme nous le verrons, l'hypothèse $d_i \geq 3$ provient de ce que la cohomologie locale naît de suites exactes à trois termes.

1) Préparation de l'idéal.

Rappelons que la hauteur $\mathrm{ht}\mathcal{P}$ d'un idéal premier $\mathcal{P}$ d'un anneau A est la longueur d'une suite croissante maximale d'idéaux premiers emboités de A contenus dans $\mathcal{P}$. La hauteur d'un idéal I est la plus petite des longueurs des idéaux premiers associés à I. Lorsque $A = k[x_0, \ldots, x_n]$, la hauteur correspond à la codimension de la sous-variété de l'espace affine (ou projectif si I est homogène) définie par I.

D'après Brownawell ([11]) une suite *assez régulière* d'éléments d'un idéal I d'un anneau A est une suite $(h_1, \ldots, h_l)$ d'éléments de I telle que pour chaque $i, 1 \leq i < l$, si nous notons $\mathcal{B}_i$ l'idéal de A engendré par $(h_1, \ldots, h_i)$, on ait :

a) Si h_{i+1} appartient à un des idéaux premiers isolés associés à $\mathcal{B}_i$, cet idéal premier contient I (et est donc un idéal premier isolé associé à I).

b) Au moins un des idéaux premiers isolés associés à I ne contient pas h_{i+1}.

Lemme 1.- (*cf* [11], lemma 0, [16], prop.3) *Si A est l'anneau $k[x_0, \ldots, x_n]$ des polynomes à coefficients dans un corps k infini et $I = (f_1, \ldots, f_m)$, il existe une suite assez régulière $(h_1, \ldots, h_l)$ d'éléments de I tels que pour $1 \leq i \leq l$ on ait $\deg h_i = \deg f_{j(i)}$, où les $j(i)$ sont tous distincts, et telle que l'idéal $\mathcal{B} \subset I$ engendré par les h_i ait les mêmes idéaux premiers isolés que I. De plus, la suite $(h_1, \ldots, h_{\mathrm{ht}I})$ est régulière.*

On prend $h_1 = f_1$ et, supposant avoir construit $(h_1, \ldots, h_i)$, on considère le plus grand entier j tel que, pour tout idéal premier isolé $\mathcal{R}$ de $\mathcal{B}_i$ qui n'est pas associé à I, l'un au moins des éléments $f_j, \ldots, f_m$ n'appartienne pas à $\mathcal{R}$. On choisit une combinaison linéaire assez générale Y des coordonnées x_i n'appartenant à aucun idéal premier $\mathcal{R}$ et la règle de Cramèr

montre qu'une combinaison linéaire générale

$$h_{i+1} = f_j + \sum_{k=j+1}^{m} c_k Y^{\deg f_j - \deg f_k} f_k$$

n'appartient à aucun des idéaux $\mathcal{R}$ qui ne sont pas associés à I. Le reste est facile.

Un argument de hauteur montre l'inégalité $l \leq n+1$. Comme le remarque Brownawell, le résultat qu'il démontre avec k infini prouve , par passage à $k[T]$, que le lemme est aussi valable sur un corps fini, et donc que le résultat final est vrai sur tout corps.

2) La cohomologie locale.

Si nous notons D_i le degré de h_i, nous avons $d_2 \geq D_i \geq d_1$ et pour montrer l'inclusion $\mathcal{P}_1^{e_1} \ldots \mathcal{P}_r^{e_r} \subset I$ il suffit de montrer $\mathcal{P}_1^{e_1} \ldots \mathcal{P}_r^{e_r} \subset (h_1, \ldots, h_l)$, mais à cause des différences de degrés, cela ne signifie pas que l'on puisse tout ramener *a priori* au cas où I est engendré par une suite assez régulière.

Nous pouvons supposer que la hauteur de l'idéal I est > 1; sinon les générateurs f_i ont un facteur commun, et il suffit de diviser par ce facteur pour se ramener au cas où la hauteur est > 1; on peut ensuite remultiplier par le facteur commun les deux côtés de l'inclusion du théorème. Fixons une suite assez régulière $(h_1, \ldots, h_l)$ dans I, posons $I_0 = (0)$ et définissons par récurrence des idéaux I_i, K_i et E_i par les égalités

$$(I_{i-1}, h_i) = I_i \cap K_i \cap E_i$$

où E_i est la partie immergée d'une décomposition primaire du membre de gauche, K_i désigne l'intersection des idéaux primaires de cette décomposition dont le radical est isolé et contient h_{i+1} (et donc I tout entier par définition des h_i), et enfin I_i est l'intersection des idéaux primaires dont le radical est isolé et ne contient pas h_{i+1}. Puisque par construction h_i n'est dans aucun des idéaux premiers isolés de I_{i-1}, il résulte du théorème de l'idéal principal que l'idéal $I_i \cap K_i$ est pur et de hauteur i (c'est-à-dire que toutes ses composantes ont la même dimension, qui vaut $n-i$), et il en

est donc de même de I_i et K_i. Notons que puisque la hauteur de I est > 1, les h_i n'ont pas de facteur commun et $K_1 = A$, et puisqu'une hypersurface n'a pas de composantes immergées, $E_1 = A$. L'idée est de démontrer pour $i = 1, \ldots, \lambda = min(l, n)$ l'inclusion

$$(*) \qquad (K_1^{3^{i-2}} K_2^{3^{i-3}} \ldots K_{i-1}^{3^0})(I_i \cap K_i) \subset (I_{i-1}, h_i)$$

Cela va résulter essentiellement du lemme suivant.
Rappelons que, pour des idéaux I et J tels que $\sqrt{I} \subset \sqrt{J}$ et que I soit pur, on note $\mathrm{codim}_I J$ pour $\mathrm{ht}J - \mathrm{ht}I$.

Lemme-clé (Kollár [29], revu par Brownawell [11]).-*Soient R un anneau noetherien de Cohen-Macaulay, I un idéal pur de R et h un élement de R hors de tous les idéaux premiers associés à I. Ecrivons $(I, h) = J \cap E$, où J est la partie d'une décomposition primaire de l'idéal (I, h) dont les idéaux premiers sont minimaux, et E celle dont les idéaux premiers sont immergés. Soit F un idéal réduit contenant J et considérons la cohomologie locale $H_F^*(M)$ des R-modules M.*

Si un idéal N de R annihile les espaces de cohomologie locale de R/I par rapport à F et à $\sqrt{E}$ en degré $< \mathrm{codim}_I F$ et $< \mathrm{codim}_I \sqrt{E}$ respectivement, c'est-à-dire si $N.H_F^i(R/I) = 0$ pour $i < \mathrm{codim}_I F$ et $N.H_{\sqrt{E}}^i(R/I) = 0$ pour $i < \mathrm{codim}_I \sqrt{E}$, alors on a $N^3.H_F^i(R/J) = 0$ pour $i < \mathrm{codim}_J F$ et si l'idéal (I, h) est pur, on a même $N^2.H_F^i(R/J) = 0$ pour $i < \mathrm{codim}_J F$.

Notons d'abord que l'idéal J est pur de hauteur $\mathrm{ht}I+1$ puisque d'après le théorème de l'idéal principal de Krull, l'idéal $h.R/I$ est de hauteur 1, donc $\mathrm{ht}(I, h) = \mathrm{ht}J = \mathrm{ht}I + 1$. Considérons les suites exactes

$$0 \longrightarrow R/I \xrightarrow{\times h} R/I \longrightarrow R/(I, h) \longrightarrow 0$$

et

$$0 \longrightarrow J/(I, h) \longrightarrow R/(I, h) \longrightarrow R/J \longrightarrow 0$$

qui donnent naissance aux suites exactes de cohomologie

$$(1) \ldots \rightarrow H_F^i(R/I) \longrightarrow H_F^i(R/(I, h)) \longrightarrow H_F^{i+1}(R/I) \rightarrow \ldots$$

et

$$(2)\ldots \to H^i_F(J/(I,h)) \longrightarrow H^i_F(R/(I,h)) \longrightarrow H^i_F(R/J) \longrightarrow H^{i+1}_F(J/(I,h)) \to ..$$

Puisque N annihile $H^i_F(R/I)$, il résulte de la suite exacte (1) que N^2 annihile $H^i_F(R/(I,h))$ pour $i+1 < \mathrm{codim}_J F$, c'est-à-dire pour $i < \mathrm{codim}_J F$.

Il résulte facilement des définitions que si (I,h) a effectivement des composantes immergées, c'est-à-dire si $E \neq R$, alors $H^0_{\sqrt{E}}(R/I) = 0$ et il en résulte par la première suite de cohomologie que l'on a une injection $H^0_{\sqrt{E}}(R/(I,h)) \to H^1_{\sqrt{E}}(R/I)$. Mais par ailleurs le $R/(I,h)$-module $J/(I,h)$ a pour support $\sqrt{E}$ et par conséquent $J/(I,h) = H^0_{\sqrt{E}}(J/(I,h))$ et ce dernier espace est un sous-module de $H^0_{\sqrt{E}}(R/(I,h))$. Finalement on a une injection de R/I-modules $J/(I,h) \to H^1_{\sqrt{E}}(R/I)$. Puisque $\mathrm{codim}_I \sqrt{E} > 1$, d'après l'hypothèse N annule $H^1_{\sqrt{E}}(R/I)$ et donc aussi $J/(I,h)$ ainsi que tous ses groupes de cohomologie. La suite exacte (2) nous montre que du fait que N^2 annihile les groupes $H^i_F(R/(I,h))$ pour $i < \mathrm{codim}_J F$ et que N annule tous les $H^j_F(J/(I,h))$ il résulte que $N^3.H^i_F(R/I) = 0$ pour $i < \mathrm{codim}_J F$. Si (I,h) est pur alors $J/(I,h)$ est nul ainsi que tous ses groupes de cohomologie, et en fait $N^2.H^i_F(R/I) = 0$ pour $i < \mathrm{codim}_J F$.

Corollaire.- *Pour tout entier* $i \leq \mu = \min(m,n)$ *l'idéal* $N_i = K_1^{3^{i-1}} K_2^{3^{i-2}} \ldots K_i$ *annihile les groupes de cohomologie locale* $H^j_F(R/I_i)$ *pour* $j < \mathrm{codim}_{I_i} F$.

On raisonne par récurrence sur i; pour $i = 1$, l'idéal $I_1 = (h_1)$ est contenu dans un idéal intersection complète de hauteur $htF = 1 + \mathrm{codim}_{I_1} F$ contenu dans F et d'après la seconde propriété fondamentale de la cohomologie locale tous les groupes de cohomologie $H^j_F(R/I_1)$ sont nuls pour $j < \mathrm{codim}_{I_1} F$. Ensuite on utilise le lemme-clé avec $I = I_{i-1}$, $f = h_i$, $J = I_i \cap K_i$. Puisque la multiplication par K_i annihile $I_i/I_i \cap K_i$ et par conséquent tous ses groupes de cohomologie, la suite exacte de cohomologie déduite de la suite exacte

$$0 \longrightarrow I_i/I_i \cap K_i \longrightarrow R/I_i \cap K_i \longrightarrow R/I_i \longrightarrow 0$$

montre que la multiplication par K_i envoie $H^j(R/I_i)$ dans le sous module de $H^j(R/I_i)$ image de $H^j(R/I_i \cap K_i)$.

D'après l'hypothèse de récurrence, on a $N_{i-1}.H_F^j(R/I_{i-1}) = 0$ pour $j < \text{codim}_{I_{i-1}} F$ et donc par le lemme-clé $N_{i-1}^3.H_F^j(R/I_i \cap K_i) = 0$ pour $j < \text{codim}_{I_i} F$.

En combinant cela avec ce qui précède, on obtient $N_{i-1}^3 K_i.H_F^j(R/I_i) = 0$ pour $j < \text{codim}_{I_i} F$, et le résultat.

Une récurrence aisée utilisant le fait que si $E_i \neq R$ on a l'inclusion $(K_i \cap E_i)/(I_{i-1}, h_i) \subset H^1_{\sqrt{E}}(R/I_{i-1})$ donne alors pour $1 \leq i \leq \lambda = \min(l, n)$ l'inclusion de nature géométrique

$$(3) \quad (K_1^{3^{i-2}} K_2^{3^{i-3}} \dots K_{i-1})(I_i \cap K_i) \subset (I_{i-1}, h_i)$$

et de cette inclusion on déduit, cette fois-ci par une récurrence descendante depuis $\lambda = min(l, n)$ les inclusions

$$(\prod_{j=i-1}^{\lambda} N_{j-1} K_j).I_\lambda \subset (I_{i-1}, h_i, h_{i+1}, \dots, h_\lambda)$$

d'où l'on tire

$$(4) \quad (K_1^{(\frac{3^{\lambda-1}+1}{2})} K_2^{(\frac{3^{\lambda-2}+1}{2})} \dots K_{\lambda-1}^2)(K_\lambda I_\lambda) \subset (h_1, \dots, h_\lambda) \ .$$

3) La fin de la preuve

On termine maintenant à l'aide essentiellement du théorème de Bézout; une récurrence directe donne pour $1 \leq i \leq \lambda = \min(n, l)$ les égalités

$$(5) \quad \deg I_i + \textstyle\sum_{j=0}^{i} (\deg K_j) D_{j+1} \dots D_i = D_1 \dots . D_i \ .$$

Montrons maintenant comment l'on conclut la preuve du théorème dans le cas $l \leq n$

On écrit une décomposition primaire de chacun des idéaux K_i, soit $K_i = \bigcap_{\sigma \in S_i} \mathcal{Q}_\sigma^{(i)}$; on pose $\sqrt{\mathcal{Q}_\sigma^{(i)}} = \mathcal{P}_\sigma^{(i)}$ et pour chaque $\mathcal{Q}_\sigma^{(i)}$ il existe un entier $t_\sigma^{(i)} \leq \text{long}\mathcal{Q}_\sigma^{(i)}$ tel que $(\mathcal{P}_\sigma^{(i)}))^{t_\sigma^{(i)}} \subset \mathcal{Q}_\sigma^{(i)}$. En utilisant l'inclusion (4), on obtient puisque $I_l = R$ des entiers $s_\sigma^{(i)}$ tels que l'on ait les inclusions

$$\prod_{i=1}^{l} \prod_{\sigma \in S_i} (\mathcal{P}_\sigma^{(i)})^{s_\sigma^{(i)}} \subset (K_1^{(\frac{3^{l-1}+1}{2})} K_2^{(\frac{3^{l-2}+1}{2})} \dots K_{l-1}^2) K_l \subset (h_1, \dots, h_l).$$

La première inclusion implique l'inégalité

$$(6) \qquad \sum_{i=1}^{l} \sum_{\sigma \in S_i} s_\sigma^{(i)} \deg \mathcal{P}_\sigma^{(i)} \leq \sum_{i=1}^{l} (\deg K_i)(\tfrac{3^{l-i}+1}{2})$$

et par ailleurs il faut remarquer que puisque $h_1, \ldots, h_{\mathrm{ht}I}$ est une intersection complète, on a $K_i = R$, donc $\deg K_i = 0$, pour $i < \mathrm{ht}I$. Il résulte de l'égalité (5) que l'on a alors

$$(7) \qquad \sum_{i=\mathrm{ht}I}^{l} (\deg K_i) D_{i+1} \ldots D_l \leq D_1 \ldots . D_l$$

et nous allons montrer l'inégalité

$$\sum_{i=1}^{l} \sum_{\sigma \in S_i} s_\sigma^{(i)} \deg \mathcal{P}_\sigma^{(i)} \leq d_1 \ldots . d_\mu$$

Pour cela, il suffit au vu de (6) et (7) de prouver l'inégalité

$$(8) \qquad \sum_{i=htI}^{l} (\deg K_i)(\tfrac{d_1 \ldots . d_\mu}{D_1 \ldots . D_i} - \tfrac{3^{l-i}+1}{2}) \geq 0 \ .$$

Or on a clairement $l \leq \mu$ et les D_i étant les degrés de polynomes $f_{j(i)}$ distincts, on a l'inégalité $d_1 \ldots . d_\mu \geq D_1 \ldots . D_l$ d'où résulte

$$\frac{d_1 \ldots . d_\mu}{D_1 \ldots . D_i} \geq D_{i+1} \ldots . D_l \geq 3^{l-i} \geq \frac{3^{l-i}+1}{2}$$

d'après l'hypothèse $d_j \geq 3$ pour $j > 1$. En fait si l'on voulait se passer de cette hypothèse, on pourrait, en notant κ le nombre des D_i $(1 \leq i \leq l)$ qui sont égaux à 2, utiliser l'inégalité $(\frac{3}{2})^\kappa D_{i+1} \ldots . D_l \geq 3^{l-i}$, et dans le résultat final le produit $d_1 \ldots . d_\mu$ serait affecté d'un facteur $(\frac{3}{2})^\kappa$.

Ainsi nous avons montré, dans le cas $l \leq n$, l'existence d'une famille d'idéaux premiers homogènes $\mathcal{P}_\sigma^{(i)}$ contenant les idéaux premiers isolés de I, et d'une famille d'entiers $s_\sigma^{(i)}$ vérifiant

$$\prod (\mathcal{P}_\sigma^{(i)})^{s_\sigma^{(i)}} \subset (h_1, \ldots, h_l) \subset I$$

et

$$\sum s_\sigma^{(i)} \deg \mathcal{P}_\sigma^{(i)} \leq d_1 \ldots d_\mu$$

donc en particuler

$$\sum s_\sigma^{(i)} \leq d_1 \dots d_\mu \ .$$

Le cas où $l = n+1$ est analogue et un peu plus compliqué; on utilise la généralisation suivante, due à Kollár et Philippon, d'un résultat de Macaulay (*cf* [37], p.67) et Lazard (*cf* [32]):

Lemme .- *Notons $\mathcal{M}$ l'idéal $(x_0, \dots, x_n)R$. Si h_{n+1} ne s'annule sur aucun des zéros de I_n, alors*

i) Pour $d \geq deg I_n - 1$ on a $\mathcal{M}^{D_{n+1}+d} \subset (I_n, h_{n+1})$

ii) Si $(h_1, \dots, h_n)$ est une suite régulière, pour $d \geq \Sigma_{i=1}^n (D_i - 1)$ on a

$$\mathcal{M}^{D_{n+1}+d} \cap (K_n, h_{n+1}) = \mathcal{M}^{D_{n+1}+d} \cap (I_n \cap K_n, h_{n+1})$$

Ici on est essentiellement en dimension zéro, et la démonstration se ramène à un décompte de dimensions d'espaces vectoriels, comme chez Macaulay.

Par une récurrence descendante analogue à celle qui prouve (4), en partant de l'inclusion $\mathcal{M}^{D_{n+1}+d} \subset (I_n, h_{n+1})$, on prouve

$$(9) \qquad (K_1^{(\frac{3^{n-1}+1}{2})} K_2^{(\frac{3^{n-2}+1}{2})} \dots K_{n-1}^2) K_n \mathcal{M}^{D_{n+1}+d} \subset (h_1, \dots, h_{n+1})$$

et on en déduit de la même manière que précédemment l'existence d'une famille d'idéaux premiers homogènes $\mathcal{P}_\sigma^{(i)}$ distincts de $\mathcal{M}$ contenant les idéaux premiers isolés de I, et d'une famille d'entiers $(s_0,\ s_\sigma^{(i)})$ vérifiant

$$\mathcal{M}^{s_0} \prod (\mathcal{P}_\sigma^{(i)})^{s_\sigma^{(i)}} \subset (h_1, \dots, h_l) \subset I$$

et

$$s_0 + \sum s_\sigma^{(i)} \deg \mathcal{P}_\sigma^{(i)} \leq d_1 \dots d_\mu$$

donc en particuler

$$s_0 + \sum s_\sigma^{(i)} \leq d_1 \dots d_\mu \ .$$

Le théorème annoncé en résulte aussitôt.

2. Théorèmes de Bézout et théorème de Hilbert

1) Identité de Bézout et théorème des zéros.

Soient $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$ et supposons qu'il n'ont aucun zéro commun dans $\overline{k}^n$. Il résulte du théorème des zéros de Hilbert qu'il existe des polynomes $g_1, \ldots, g_m \in k[x_1, \ldots, x_n]$ tels que l'on ait *l'identité de Bézout*

$$\sum_1^m f_i g_i = 1$$

si en effet on ajoute une variable x_0 et considère les polynomes homogenes $\tilde{f}_i = x_0^{d_i} f_i(x_1/x_0, \ldots, x_n/x_0)$ ils ont tous leurs zéros communs dans l'hyperplan à l'infini $x_0 = 0$ et donc il existe un entier e et des polynomes homogènes $\tilde{g}_1, \ldots, \tilde{g}_m$ tel que l'on ait $x_0^e = \Sigma_{i=1}^m \tilde{f}_i \tilde{g}_i$, d'où le résultat en faisant $x_0 = 1$. Inversement, Rabinowitsch (*cf* [43]) a montré que si l'on connait l'identité de Bézout, on peut en déduire le théorème de Hilbert: si un polynome g s'annule sur tous les zéros communs de $f_1, \ldots, f_m$, on ajoute une variable x_{n+1} et on considère les polynomes $f_1, \ldots, f_m, 1 - x_{n+1}g$; ils n'ont aucun zéro commun dans $\overline{k}^n$, donc on peut écrire $1 = \sum_{i=1}^m f_i g_i + h(1 - x_{n+1}g)$. En remplaçant x_{n+1} par g^{-1} et en chassant les dénominateurs, on obtient $g^s = \Sigma_{i=1}^m f_i g_i'$, c'est-à-dire le théorème des zéros.

La technique que nous venons d'exposer a permis à Kollár de donner le résultat optimal en ce qui concerne l'identité de Bézout et le théorème des zéros.

Etant donnés un corps k et des entiers positifs $n, d_1, \ldots, d_m$ notons $N_B(k; n, d_1, \ldots, d_m)$ le plus petit entier s tel que pour tout choix de polynomes $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$ tels que $\deg f_i = d_i$ et sans zéro commun dans $\overline{k}^n$, il existe des polynomes $g_1, \ldots, g_m \in k[x_1, \ldots, x_n]$ tels que $\Sigma_1^m f_i g_i = 1$ et $\sup_i(\deg f_i g_i) \leq s$, et notons $N_H(k; n, d_1, \ldots, d_m)$ le plus petit entier s tel que pour tout choix de polynomes *homogènes* $f_1, \ldots, f_m \in k[x_0, \ldots, x_n]$ tels que $\deg f_i = d_i$ on ait l'inclusion d'idéaux $(\sqrt{(f_1, \ldots, f_m)})^s \subset (f_1, \ldots, f_m)$.

Etant donnés des entiers positifs n et $d_1 \geq d_2 \cdots \geq d_m$, notons $P(n, d_1, \ldots, d_m)$

le nombre défini ainsi:

$$P(n, d_1, \ldots, d_m) = \begin{cases} d_1 \ldots . d_m & \text{si } m \leq n; \\ d_1 \ldots . d_{n-1} . d_m & \text{si } m > n > 1 \ ; \\ d_1 + d_m - 1 & \text{si } m > n = 1. \end{cases}$$

On étend la définition de $P(n, d_1, \ldots, d_m)$ aux suites quelconques d'entiers en rangeant $d_1, \ldots, d_m$ par ordre décroissant avant d'appliquer la définition précédente. On a alors

Théorème 2 (Kollár [29]).- *Si tous les d_i sont différents de 2, on a les égalités*

$$N_B(k; n, d_1, \ldots, d_m) = N_H(k; n, d_1, \ldots, d_m) = P(n, d_1, \ldots, d_m).$$

Les inégalités $\leq$ sont essentiellement un corollaire de ce que nous avons vu au paragraphe précédent. Il faut remarquer que puisqu'il s'agit de déterminer en fin de compte si des systèmes d'équations linéaires entre les coefficients ont des solutions, on peut librement faire grossir le corps k et en particulier le supposer algébriquement clos.

Kollár a adapté un exemple de Masser et Philippon pour montrer que les inégalités déduites du paragraphe précédent sont optimales :

Exemple([29]).-Etant donnés des entiers positifs $n, d_1, \ldots, d_n$, considérons les polynomes suivants de $k[x_0, \ldots, x_n]$:

$$x_1^{d_1}, x_1 x_n^{d_2 - 1} - x_2^{d_2}, \ldots, x_{n-2} x_n^{d_{n-1} - 1} - x_{n-1}^{d_{n-1}}, x_{n-1} x_n^{d_n - 1} - x_0^{d_n}$$

Notons f_i le i-ième; il est de degré d_i. Les zéros communs des f_i sont les points de la droite $x_0 = \cdots = x_{n-1} = 0$ et un calcul rapide montre que $k[x_0, \ldots, x_n]/(f_1, \ldots, f_n, x_n - 1) \simeq k[x_0]/(x_0)^{\Pi d_i}$. Ainsi x_0 est dans le radical de l'idéal $(f_1, \ldots, f_n)$, mais $(x_0)^{\Pi d_i - 1} \notin (f_1, \ldots, f_n)$. En arrangeant les d_i de telle façon que d_n soit le plus petit et ajoutant aux f_i des multiples convenables de f_n, on obtient la borne du théorème pour $m > n$ et en regardant cet exemple avec m variables parmi n, on obtient la borne pour $m < n$. En déshomogeneisant x_0, on obtient la borne pour $N_B(k; n, d_1, \ldots, d_m)$.

Il faut remarquer que dans un anneau euclidien il est très facile de démontrer l'identité de Bézout avec de bonnes bornes pour les degrés et la

taille des coefficients, et on peut donc espérer que des méthodes de division en dimension quelconque seront utiles. Comme il a été dit, le théorème de division général de Hironaka et l'algorithme de Buchberger (*cf* [44]) ne semblent pas aider pour le moment, mais nous allons voir au paragraphe suivant que l'on peut obtenir par l'analyse des substituts à la division.

2)Théorème de Bézout sur les intersections et théorème de Hilbert.

La théorie des intersections de Vogel dans [49] (voir aussi [48]) associe à l'intersection de $m \leq n$ hypersurfaces V_i de $\mathbf{P}^n$ des sous-variétés réduites $C_1, \ldots, C_t$ de l'intersection $\bigcap_{i=1}^m V_i$ et des entiers $j_b \geq 1$ de telle façon que, posant $d_i = \deg V_i$, on ait $d_1 \ldots d_m = \sum_{b=1}^t j_b \deg C_b$. Du point de vue de Fulton et MacPherson dans [20], il existe des sous-variétés (dites distinguées) $Z_1, \ldots, Z_u$, des entiers $m_1, \ldots, m_u$ et sur chaque Z_c un cycle α_c tels que l'on ait pour le cycle intersection l'égalité $V_1 \cdots V_m = \sum_{c=1}^u m_c \alpha_c$. Ces résultats décrivent l'intersection $\bigcap_{i=1}^m V_i$ par un cycle algébrique, qui coincide avec certaines des composantes de l'intersection au point générique de celles-ci. Au contraire, la version effective du théorème des zéros du No. 1 est vraiment géométrique et pas seulement numérique ou "cycliste", puisqu'elle décrit un sous-schéma et pas un cycle, et que ce sous-schéma contient effectivement, et pas seulement au voisinage de points génériques, l'intersection $\bigcap_{i=1}^m V_i$. On peut donc la voir, en éxagérant un peu, comme un "théorème de Bézout géométrique".

§2 L'analyse

De ce point de vue, l'histoire remonte au problème de la couronne résolu par Carleson et aux généralisations de Hörmander ([27]) et Kelleher-Taylor ([28]).

On se donne un sous-ensemble ouvert Ω de $\mathbf{C}^n$ et une fonction s plurisousharmonique non négative sur Ω. On note $A_s(\Omega)$ l'algèbre des fonctions f analytiques sur Ω et telles qu'il existe des constantes C_1 et C_2 telles que l'on ait, pour $z \in \Omega$,

$$|f(z)| \leq C_1 \exp(C_2 s(z))$$

et le problème est de déterminer si des éléments $f_1, \ldots, f_m$ de $A_s(\Omega)$ tels

qu'il existe des nombres positifs c_1, c_2 tels que pour $z \in \Omega$ on ait

$$|f_1(z)| + \cdots + |f_m(z)| \geq c_1 \exp(-c_2 s(z))$$

engendrent l'algèbre $A_s(\Omega)$.

Remarquons que la condition est nécessaire, comme on le voit en écrivant

$$1 = \sum_1^m f_i(z) g_i(z)$$

dans $A_s(\Omega)$.

On reprend donc les problèmes du §1 dans cette classe d'algèbres. L'algèbre des polynomes $\mathbf{C}[x_1, \ldots, x_n]$ correspond, d'après le théorème de Liouville, au cas $\Omega = \mathbf{C}^n$, $s(z) = \log(1 + \|z\|)$. On trouve dans [7] la motivation suivante:

Un signal, représenté par une distribution σ sur $\mathbf{R}^n$, est analysé par m instruments de mesure, qui sont représentés par m distributions à support compact $\mu_1, \ldots, \mu_m$ sur $\mathbf{R}^n$, tandis que le résultat de chaque analyse est représenté par la convolution $\gamma_i = \mu_i * \sigma$. Le problème est de reconstituer explicitement σ à partir des γ_i, c'est-à-dire de trouver explicitement des distributions à support compact ν_i telles que l'on ait $\sigma = \sum_{i=1}^m \nu_i * \mu_i * \sigma$; il s'agit donc de résoudre dans l'algèbre de convolution, dont l'unité est la distribution de Dirac δ_0 en 0, l'équation

$$\delta_0 = \sum_{i=1}^m \nu_i * \mu_i \ .$$

La transformation de Fourier $\mathcal{F}$ établit un isomorphisme entre l'algèbre de convolution des distributions à support compact sur $\mathbf{R}^n$ et l'algèbre $A_s(\mathbf{C}^n)$ où $s(z) = \log(1+\|z\|)+\|\mathrm{Im} z\|$. Il s'agit donc de résoudre dans cette algèbre de fonctions entières le problème de Bézout

$$1 = \sum_{i=1}^m \mathcal{F}(\nu_i)\mathcal{F}(\mu_i) \ .$$

Plus généralement, on peut se demander si une condition nécessaire et suffisante pour qu'une fonction $g \in A_s(\Omega)$ appartienne à l'idéal de $A_s(\Omega)$ engendré par $f_1, \ldots, f_m$ est qu'il existe des constantes non négatives c_1, c_2

telles que l'on ait pour $z \in \Omega$, en posant $f = (f_1, \ldots, f_m)$ et $\|f\| = (\sum_1^m |f_i(z)|^2)^{\frac{1}{2}}$, les inégalités

$$|g(z)| \leq c_1 \|f\| \exp(c_2 s(z)).$$

Skoda a démontré dans [47] un théorème très général dans cette direction, qui était d'ailleurs utilisé par Brownawell dans sa démonstration (voir [12] et [14]) d'une identité de Bézout effective pour les polynomes.

Les progrès récents dus à Berenstein et Yger s'appuient sur une formule de représentation qui se substitue à une formule de division pour permettre d'écrire explicitement des solutions de l'équation $g = \sum_{i=1}^m f_i g_i$. Berenstein et Yger commencent par montrer l'existence d'un courant résidu associé à une famille de polynomes $f_1, \ldots, f_n$ définissant une sous-variété discrète de $\mathbf{C}^n$. Ils utilisent le théorème d'Atiyah ([3]) et Bernstein ([9]).

Théorème 3 (Berenstein-Yger [5]).-*Etant données p fonctions $f_1, \ldots, f_p$ holomorphes sur un ouvert Ω de $\mathbf{C}^n$ et y définissant une intersection complète V, soit ϕ une forme différentielle $\mathcal{C}^\infty$ sur $\mathbf{C}^n$ à support compact de type $(n, n-p)$ et $\overline{\partial}$-fermée au voisinage de V. La fonction*

$$\lambda \mapsto \frac{(-1)^{\frac{p(p-1)}{2}}}{(2\pi i)^p} \int_\Omega \frac{|f_1 \ldots f_p|^{2p\lambda}}{(|f_1|^2 + \cdots + |f_p|^2)^{\frac{1}{2}}} \overline{\partial} f_1 \wedge \ldots \wedge \overline{\partial} f_p \wedge \phi$$

est méromorphe dans tout le plan complexe. De plus, elle a en $\lambda = 0$ un pôle simple en lequel son résidu est égal à

$$\left\langle \bar{\partial} \frac{1}{f_1} \wedge \ldots \wedge \bar{\partial} \frac{1}{f_p} \ , \ \phi \right\rangle = \lim_{\epsilon \to 0} \frac{1}{(2\pi i)^p} \int_{\Gamma_\epsilon} \frac{\phi}{f_1 \ldots f_p}$$

où Γ_ϵ est le cycle analytique réel orienté $(z \in \Omega / |f_1(z)| = \cdots = |f_p(z)| = \epsilon)$.

Supposons donnés m polynomes $(p_1, \ldots, p_m)$ de $\mathbf{C}[x_1, \ldots, x_n]$, et quand nous voudrons distinguer les n premiers, notons les $(f_1, \ldots, f_n, p_{n+1}, \ldots, p_m)$ (c'est-à dire que nous noterons, pour $i \leq n$, f_i ou p_i).

Notons $F = f_1 \ldots f_n$, $f^a = f_1^{a_1} \ldots f_n^{a_n}$, $\|F\| = \left(\sum_{i=1}^n |f_i(z)|^2\right)^{\frac{1}{2}}$ et $\partial f = \bigwedge_1^n \partial f_i$, $\bar{\partial} f = \bigwedge_1^n \bar{\partial} f_i$ et $df = \bigwedge_1^n df_i$ (dans l'ordre croissant). Supposons que les n premiers d'entre eux satisfont une inégalité à la Łojasiewicz:

Il existe un rayon r et des constantes $c > 0$ et $d \in \mathbf{R}$ telles que pour $\|z\| > r$ on ait

$$(Ł(d)) \qquad \left(\sum_{i=1}^{n} |f_i(z)|^2\right)^{\frac{1}{2}} \geq c\|z\|^d$$

Par ailleurs, choisissons, pour chaque fonction f_i, n polynomes en $2n$ variables $g_{j,\ell}$ de degré $\leq d_j$ en chaque paquet de variables et tels que l'on ait

$$f_j(z) - f_j(\zeta) \equiv \sum_{\ell=1}^{n} g_{j,\ell}(z,\zeta)(z_\ell - \zeta_\ell)$$

On peut prendre par exemple

$$g_{j,\ell} = \frac{f_j(\zeta_1, \ldots, \zeta_{\ell-1}, z_\ell, \ldots, z_n) - f_j(\zeta_1, \ldots, \zeta_\ell, z_{\ell+1}, \ldots, z_n)}{z_\ell - \zeta_\ell}$$

Dans ces conditions, étant donné un polynome q appartenant à l'idéal $(f_1, \ldots, f_m)$ et des fonctions holomorphes $u_1, \ldots, u_m$ dans un voisinage Ω de V telles que l'on ait $q = u_1 p_1 + \cdots + u_m p_m$ dans Ω, considérons les polynomes en z, ζ définis par

$$W_j(z,\zeta) = \det \begin{pmatrix} g_{1,1}(z,\zeta) & g_{2,1}(z,\zeta) & \ldots & g_{n,1}(z,\zeta) & g_{j,1}(z,\zeta) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ g_{1,n}(z,\zeta) & g_{2,n}(z,\zeta) & \ldots & g_{n,n}(z,\zeta) & g_{j,n}(z,\zeta) \\ f_1(z) - f_1(\zeta) & f_2(z) - f_2(\zeta) & \ldots & f_n(z) - f_n(\zeta) & p_j(z) \end{pmatrix}$$

Notons $a + \underline{1} = (a_1 + 1, \ldots, a_n + 1)$ et $\bar{\partial}\frac{1}{f^{a+\underline{1}}} = \bar{\partial}\frac{1}{f_1^{a_1+1}} \wedge \ldots \wedge \bar{\partial}\frac{1}{f_n^{a_n+1}}$.

On a alors le

Théorème 4 (Berenstein-Yger [5]).- *Posons* $D = \max_{1 \leq j \leq n} \deg f_j$ *et soit* d *l'exposant apparaissant dans l'inégalité (Ł(d)). Si* r *est un entier tel que* $dr > \deg q + (n-1)(2D-1) + 1$, *on a l'identité*

$$(B\text{-}Y) \qquad q(z) = \sum_{|a| \leq r-n} \left\langle \bar{\partial}\frac{1}{f^{a+\underline{1}}(\zeta)} \, , \, \sum_{j=1}^{m} u_j(\zeta) W_j(z,\zeta) d\zeta \right\rangle f^a(z)$$

On vérifie que ceci donne bien une identité de Bézout $q = \sum_1^m A_i p_i$. Le seul terme qui pose un problème est le terme en $a = 0$, mais on développe

les déterminants W_j et on utilise le fait que le courant résidu $\overline{\partial}\frac{1}{f}$ annule le sous-module $(f_1,\ldots,f_n)\Omega^{n,0}$ du module $\Omega^{n,0}$ des n-formes différentielles de type $(n,0)$.

La convergence des intégrales est assurée par (L(d)) et le nombre d qui y apparaît est borné en fonction des données au moyen du résultat suivant, qui est une amélioration due à Kollár d'un résultat de Brownawell.

Proposition (Kollár, (*cf* [29]) *Soient* $p_1,\ldots,p_m \in \mathbf{C}[x_1,\ldots,x_n]$ *des polynomes n'ayant qu'un nombre fini de zéros communs dans* $\mathbf{C}^n$*; posons* $d_i = \deg p_i$ *et supposons* $n \geq 2$. *Alors il existe une constante* $C > 0$ *telle que pour* $\|z\|$ *assez grand on ait*

$$\max_i(\|z\|^{-d_i}|p_i(z)|) \geq C\|z\|^{-P(n,d_1,\ldots,d_m)}$$

La démonstration consiste à utiliser le fait que le problème est local au voisinage des points à l'infini, et se ramène donc à prouver que si $p_1,\ldots,p_m \in \mathbf{C}[x_1,\ldots,x_n]$, avec $m \leq n$ sont des polynomes dont les zéros communs sont contenus dans $x_1 = 0$, alors près de l'origine on a pour une constante $C' > 0$

$$\max_i |p_i(z)| \geq C'|x_1|^{\Pi d_i}.$$

Kollár remarque qu'il suffit de vérifier qu'une au moins des fonctions $p_i \circ \pi$ s'annule avec un ordre $< \Pi d_i$ le long de chaque composante du diviseur exceptionnel de l'éclatement $\pi: Z \to \mathbf{C}^n$ de l'idéal engendré par les p_i, et cela résulte d'un simple argument de degré.

Le miracle est que cette identité (B-Y) d'apparence fort compliquée permet de borner les degrés et , si l'on est parti de polynomes à coefficients dans $\mathbf{Z}$, la taille des coefficients de l'identité de Bézout.

Etant donné un polynome $p(z) = \sum p_\alpha z^\alpha \in \mathbf{Z}[x_1,\ldots,x_n]$, on appelle hauteur (*) de p le nombre $\mathrm{H}(p) = \mathrm{Max}_\alpha|p_\alpha|$ et hauteur logarithmique le nombre $\mathrm{h}(p) = \log\mathrm{H}(p)$. Il faut remarquer qu'une borne sur les degrés

(*) cette notion de hauteur, qui s'étend aux idéaux, (*cf* [40], [41]) est sans rapport avec celle que nous avons utilisée au §1; le mot *taille* serait préférable, mais telle est malheureusement la terminologie reçue.

dans l'identité de Bézout implique par l'algèbre linéaire une borne sur les hauteurs, mais cette borne est bien mauvaise; elle est en $c(n)D^{n^2}(h+\log m+ n^2\log D)$. La méthode de Berenstein et Yger donne le

Théorème 5 (Berenstein-Yger [5]).- *Soient $p_1,\dots,p_m$ des polynomes de $\mathbf{Z}[x_1,\dots,x_n]$ tous de degré $\leq D$ et tels que $\mathrm{h}(p_j) \leq h$ $(1 \leq j \leq m)$, et sans zéro commun dans $\mathbf{C}^n$. Il existe un entier δ et des polynomes $g_1(z),\dots,g_m(z) \in \mathbf{Z}[x_1,\dots,x_n]$ tels que l'on ait*

$$\delta = \sum_1^m f_j(z)g_j(z)$$

et pour tout j

$$\deg g_j \leq 10(n+1)^5(2D+1)^{2n},$$

$$\mathrm{h}(g_j(z)) \leq \kappa(n)D^{9n+3}(h+\log m + D\log D)$$

$$\log\delta \leq \kappa(n)D^{9n+3}(h+\log m + D\log D)$$

où $\kappa(n)$ est une constante effective.

On prend $\Omega = \mathbf{C}^n$. La borne sur les degrés se voit directement sur (B-Y), mais les bornes sur les hauteurs sont bien plus délicates. Berenstein et Yger utilisent une version effective du théorème de normalisation de Noether pour préparer de meilleurs p_i et le point est qu'au bout du compte il suffit de trouver une borne pour le p.g.c.d. des dénominateurs des nombres rationnels

$$\left\langle \bar\partial \frac{1}{f^{a+\underline{1}}(\zeta)}\ , \frac{\zeta^b d\zeta}{f_{n+1}(\zeta)} \right\rangle,\ |b| \leq 3(n+1)^2(2D+1)^n,\quad |a| \leq r-n$$

où f_{n+1} est un nouveau générateur bien choisi et à hauteur controlée pour l'idéal $(p_1,\dots,p_m)$.(*)

(*) Dans [8], Berenstein et Yger annoncent obtenir, par un raffinement de leur méthode et en utilisant les résultats de Philippon présentés ci-après, des bornes

$$\deg g_j \leq 10n^2D^n,$$

$$\max(\log\delta, \mathrm{h}(g_1(z)),\dots,\mathrm{h}(g_m(z))) \leq \kappa(n)D^{8n+3}(h+D\log D).$$

§3 L'arithmétique

Philippon se propose de majorer les degrés et la taille des coefficients dans le théorème des zéros dans le cadre plus général des polynomes à coefficients dans un anneau A muni d'une fonction "taille", mais nous nous restreindrons ici au cas de $\mathbf{Z}$. Comme on le fait depuis Nesterenko ([40]), Philippon estime la taille arithmétique de l'idéal engendré par des polynomes homogènes $p_i \in \mathbf{Z}[x_0, \ldots, x_n]$ au moyen des coefficients de la forme de Cayley-Chow associée. Il appelle *rang restreint* d'un idéal $I \subset \mathbf{Z}[x_0, \ldots, x_n]$ la plus petite des hauteurs des idéaux premiers $\mathcal{P}$ associés à I et tels que $x_0 \notin \mathcal{P}$ *et* $\mathcal{P} \cap \mathbf{Z} = (0)$. On rappelle qu'un élément g d'un anneau A est dit *entier* sur un idéal J de A s'il satisfait une relation algébrique $g^t + a_1 g^{t-1} + \cdots + a_t = 0$ avec $a_i \in J^i$. En géométrie algébrique la dépendance intégrale se traduit par des inégalités valuatives et en géométrie analytique locale par des inégalités de Łojasiewicz (*cf* [36]). L'ensemble des éléments de A qui sont entiers sur J est un idéal, que l'on note $\overline{J}$. Par des méthodes valuatives (donc complètement algébriques), Philippon démontre le résultat suivant:

Théorème 6 (Philippon [41]).- *Soient $p_1, \ldots, p_m \in \mathbf{Z}[x_0, \ldots, x_n]$ des polynomes homogènes de degrés $d_1 \leq d_m \leq \ldots \leq d_2$ et tels que $\mathrm{h}(p_j) \leq h$. On pose $\mu = \min(m, n)$ et $\nu = \min(m, n+1)$. Si l'idéal I engendré par les p_j est de rang restreint $\geq n+1$, il existe un élément $\gamma \in \mathbf{Z}$ tel que*

$$\gamma x_0^{d_1 \ldots d_\mu} \in \overline{I} \ , \text{ et}$$

$$\log \gamma \leq C(n) h d_1 \ldots d_\nu \left(\frac{1}{h} + \sum_{j=1}^{\nu} \left(\frac{1}{d_j}\right)\right)$$

où $C(n)$ est effectivement calculable.

Il déduit alors de ([36], Theorem 2.1), qui joue ici le rôle du théorème de Skoda, que *pour tout nombre premier p il existe un entier a_p premier avec p et tel que, posant $q = \gamma x_0^{d_1 \ldots d_\mu}$, on ait*

$$a_p q^{n+2} \in I.$$

Il vient alors assez facilement

Théorème 7 (Philippon [41]).-*Soient* $p_1, \ldots, p_m \in \mathbf{Z}[x_1, \ldots, x_n]$ *des polynomes de degrés* $d_1 \leq d_m \leq \ldots \leq d_2$ *et tels que* $\mathrm{h}(p_j) \leq h$. *Si* $p_1, \ldots, p_m$ *n'ont pas de zéro commun dans* $\mathbf{C}^n$. *Il existe un entier* δ *tel que*

$$\log\delta \leq (n+2)C(n)hd_1 \ldots d_\nu(\frac{1}{h} + \sum_{j=1}^{\nu}(\frac{1}{d_j}))$$

et des polynomes $g_1, \ldots, g_m \in \mathbf{Z}[x_1, \ldots, x_n]$ *tels que*

$$\delta = \sum_{j=1}^{m} p_j g_j$$

$$\text{avec} \quad \deg(p_j g_j) \leq (n+2)d_1 \ldots d_\mu.$$

L'hypothèse sur les zéros implique que la hauteur réduite est $\geq n+1$. Puisque les a_p sont premiers entre eux dans leur ensemble, le théorème précédent implique, en posant $\delta = \gamma^{n+2}$ et en homogéneisant les polynomes p_j en $\tilde{p}_j$, que l'on a

$$q^{n+2} = \delta x_0^{(n+2)d_1 \ldots d_\mu} \in (\tilde{p}_1, \ldots, \tilde{p}_m)$$

On peut donc écrire

$$\delta x_0^{(n+2)d_1 \ldots d_\mu} = \sum_{j=1}^{m} \tilde{g}_i \tilde{p}_i$$

et l'on conclut en faisant $x_0 = 1$. Tout récemment Philippon a donné une démonstration de résultats équivalents par une méthode différente consistant à faire fonctionner sur $\mathbf{Z}$ la démonstration de Kollár revue par Brownawell qui a été exposée au paragraphe 1. Selon sa préférence, (*cf* [42]), la cohomologie locale y est présentée sous la forme de complexes de Koszul, plus maniables lorsqu'il s'agit de surveiller les hauteurs des éléments. Pour le moment, ces méthodes ne donnent pas les bornes sur la hauteur des polynomes g_j qu'obtiennent Berenstein et Yger.

§4 Conclusion

Considérer le résultat du §1 comme un théorème d'intersection géométrique conduit à espérer que le bon cadre pour ce type de problème est la géométrie arithmétique d'Arakelov ([1]), que ces résultats sont les prémices d'une théorie géométrique de l'intersection sur les variétés arithmétiques. Cela permettrait en particulier de remplacer par de la théorie des intersections à la Gillet-Soulé (*cf* [21], [22], [23]) les lourds calculs sur les formes de Cayley-Chow que j'ai cachés (*).

Un thème commun aux trois paragraphes est "résidus et dualité"; au §1, ce thème apparaît dans l'utilisation des propriétés en cohomologie locale des suites (assez) régulières, au §2 il est tout-à-fait explicite, et au §3 il est présent par l'utilisation d'un résultat de [36] qui est une conséquence de la dualité locale de Grothendieck. On peut aussi espérer que les trois approches présentées ci-dessus constituent les prémices d'une résonnance de ce thème en Géométrie d'Arakelov.

Références

[1] S.Ju. Arakelov, Intersection theory of divisors on an arithmetic surface, *Izv. Akad. Nauk. SSSR* **38** (1974), No.6, 1167-1180.

[2] Jean-Marie Arnaudiès, *Elimination et théorie de Galois.* Thèse, Université Paul Sabatier de Toulouse, Janvier 1989.

[3] Michael Atiyah, Resolution of singularities and division of distributions, *Comm. Pure and App. Math*, **23**, (1970), 145-150.

[4] David A. Bayer, *The division algorithm and the Hilbert Scheme* , Thèse, Université Harvard, 1982.

[5] Carlos A. Berenstein and Alain Yger, *Effective Bézout identities in* $\mathbf{Q}[z_1, \ldots, z_n]$, Preprint University of Maryland, Sept.1988.

(*) En fait la construction de cette théorie est déjà entamée; voir les prépublications *Hauteurs alternatives* de P. Philippon (Institut Henri Poincaré, 1990) et *Géométrie d'Arakelov et théorie des nombres transcendants* de C. Soulé (Institut des hautes Études scientifiques, 1990).

[6] Carlos A. Berenstein and Daniele Struppa, On explicit solutions to the Bézout equation, *Syst. Control Letters* **4** (1984), 33-39.

[7] Carlos A. Berenstein and Alain Yger, Le problème de la déconvolution, *J. Funct. Anal.* **54** (1983), 113-160.

[8] Carlos A. Berenstein and Alain Yger, Une formule de Jacobi et ses conséquences, à paraître dans *Annales sci. E.N.S.*

[9] I.N. Bernstein, The analytic continuation of generalized functions with respect to a parameter, *Funct. An. Appl.* **6** (1972), 273-285.

[10] Daniel Bertrand, Lemmes de zéros et nombres transcendants, *Séminaire Bourbaki*, exposé No. 652, Nov. 1985. Astérisque No. 145-146, (1987) p.21-44.

[11] W. Dale Brownawell, A prime power version of the Nullstellensatz. Preprint 1989.

[12] W. Dale Brownawell, Bounds for the degree in the Nullstellensatz. *Annals of Math.***126** (1987), 577-591.

[13] W. Dale Brownawell, Bornes effectives pour l'exposant dans le théorème des zéros. *C.R.A.S.*, Paris t.305, série 1 (1987), 287-290.

[14] W. Dale Brownawell, Local diophantine nullstellen inequalities. *J.A.M.S.* **1**, No.2 (1988), 311-322.

[15] W. Dale Brownawell and D.W. Masser, Multiplicity estimates for analytic functions, II, *Duke Math. J.* **47**, No.2, June 1980.

[16] L. Caniglia, A. Galligo, J. Heintz, Borne simple exponentielle pour les degrés dans le théorème des zéros sur un corps de caractéristique quelconque. *C.R.A.S. , Paris* **307** (1988), 255-258.

[17] L. Caniglia, A. Galligo, J. Heintz, Some new effectivity bounds in computational geometry. *6th International Conference on applied algebra* (AAECC-6) Springer LNCS No. 357 (1989), 131-151.

[18] Michel Demazure, Le théorème de complexité de Mayr-Meyer, *Géométrie algébrique et applications,*Travaux en cours No.22, Hermann 1987.

[19] Noaï Fitchas et André Galligo: Nullstellensatz effectif et conjecture de Serre, in *Séminaire "Structures algébriques ordonnées"* 1987-88, Université Paris 7.

[20] William Fulton: *Intersection theory*, Ergebnisse der Mathematik, Springer 1984.

[21] Henri Gillet and Christophe Soulé: Arithmetic intersection theory. Preprint IHES 1988.

[22] Henri Gillet and Christophe Soulé: Amplitude arithmetique. *CRAS* Paris **307** (1988), 887-890.

[23] Henri Gillet and Christophe Soulé: Characteristic classes for algebraic vector bundles with hermitian metrics. A paraître dans Annals of Math.

[24] Alexander Grothendieck, *Local cohomology* (Notes by R. Hartshorne), Springer L.N.M. No. 41, Springer 1967.

[25] J. Heintz, M.-F. Coste-Roy, P.Solernó, On the complexity of semi-algebraic sets. A paraître dans *Proc. IFIP, World Computer congress*, San Francisco 1989.

[26] Greta Hermann, Die Frage der endliche vielen Schritte in der Theorie der Polinomideale, *Math. Ann.* **95** (1926), p.736-788.

[27] Lars Hörmander, Generators for some rings of analytic functions, *Bull. A.M.S.*, **73** (1967), 943-949.

[28] J.J.Kelleher and B.A.Taylor, Finitely generated ideals in rings of analytic functions, *Math. Ann.* **193** (1971), 225-237.

[29] János Kollár, Sharp effective Nullstellensatz. *J.A.M.S.* **1** (1988), 963-975.

[30] János Kollár, A Łojasiewicz-type inequality for Algebraic Varieties, Preprint, University of Utah, 1990.

[31] E. Lasker, Zur Theorie der Moduln und Ideale, *Math. Ann.* **60**, (1905), 20-116, Errata p.607-608.

[32] Daniel Lazard, Algorithmes fondamentaux en algèbre commutative, *Astérisque* No. 38-39.

[33] Daniel Lazard, Algèbre linéaire sur $k[x_1, \ldots, x_n]$ et élimination, *Bull. S.M.F.* **105** (1977), 165-190.

[34] Monique Lejeune-Jalabert, *Effectivité de calculs polynomiaux*, Cours de DEA, Institut Fourier, 1984-85. A paraître.

[35] Monique Lejeune-Jalabert, Liaison et résidus, *Algebraic Geometry*, Springer LNM No. 961, 1982, p.233.

[36] Joseph Lipman and Bernard Teissier, Pseudo-rational local rings and a theorem of Briançon-Skoda, *Mich. Math. J.* **28** (1981), 97-116.

[37] F.S. Macaulay, *The algebraic theory of modular systems*, Cambridge

tracts in Math. No.19, Cambridge 1916, et Stechert-Hafner, New York 1964.

[38] D.W. Masser and G. Wüstholz, Fields of large transcendance degree generated by values of elliptic functions, *Invent. Math.* **72** (1983), 407-464.

[39] E.W. Mayr and A.R. Meyer, The complexity of the word problems for commutative semi-groups and polynomial ideals, *Adv. in Math.* **46** (1982), 305-329.

[40] Yu.V. Nesterenko, Estimates for the order of zeros of functions of a certain class and their applications in the theory of transcendental numbers, *Izv. Akad. Nauk USSR* **41** (1977)= *Math. USSR Izv.*, **11** (1977), 239-270.

[41] Patrice Philippon, Dénominateurs dans le théorème des zéros de Hilbert, *Prépublications, Institut Henri Poincaré*, 1989. (soumis à Acta arithmetica)

[42] Patrice Philippon, Théorème des zéros effectif d'après J. Kollár, *Problèmes diophantiens*, Publ. Math. Univ. Paris 6, No.88, 1988-89.

[43] J.L. Rabinowitsch, Zum Hilbertschen Nullstellensatz, *Math. Ann.* **102** (1929), p.520.

[44] Lorenzo Robbiano (Ed.) *Computational aspects of commutative algebra*, Academic Press 1989.

[45] Pierre Samuel, *Méthodes d'algèbre abstraite en Géométrie algébrique.* Springer, Ergebnisse der Math. No.4, 1967.

[46] Bernard Schiffman, Degree bounds for the division problem in polynomial ideals, *Mich. Math. Journ.* **36**, (1989), 163-171.

[47] Henri Skoda, Application des techniques L^2 à l'étude des idéaux d'une algèbre de fonctions holomorphes avec poids, *Ann. sci. E.N.S.* **5** (1972), 545-579.

[48] Leendert Van Gastel: *Excess intersections*, Thèse, Université d'Utrecht, 1989.

[49] W. Vogel: *Lectures on results on Bézout's theorem*, Tata Institute Lecture notes, Bombay 1984.

Bernard TEISSIER
D.M.I., École normale supérieure
45 rue d'Ulm, F-75230 Paris Cedex 05.

Astérisque

JEAN-PAUL THOUVENOT

La convergence presque sûre des moyennes ergodiques suivant certaines sous-suites d'entiers

Astérisque, tome 189-190 (1990), Séminaire Bourbaki,
exp. n° 719, p. 133-153

<http://www.numdam.org/item?id=SB_1989-1990__32__133_0>

© Société mathématique de France, 1990, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Séminaire BOURBAKI novembre 1989
42ème année, 1989-90, n° 719

LA CONVERGENCE PRESQUE SÛRE DES MOYENNES ERGODIQUES SUIVANT CERTAINES SOUS-SUITES D'ENTIERS

[d'après **Jean Bourgain**]

par **Jean-Paul THOUVENOT**

1. INTRODUCTION

Étant donné un système dynamique $(X, \mathcal{A}, m, T)$ où T est une bijection bimesurable préservant la mesure de l'espace probabilisé $(X, \mathcal{A}, m)$, le théorème de Birkhoff dit que si $f \in L^1(X)$ alors $\frac{1}{N} \sum_{k=1}^{N} f(T^k x)$ converge p.s. quand $N \to +\infty$.

De nombreuses généralisations de ce résultat ont été données, notamment pour l'action de groupes plus généraux que $\mathbf{Z}$, ou pour des sous-suites des entiers de densité positive, avec des restrictions sur la nature de T (à spectre discret ou à spectre de Lebesgue, voir [B-K] et [B-L]). Mais on n'avait aucun exemple où le théorème était valable pour des sous-suites de densité supérieure nulle, notamment parce que les méthodes combinatoires utilisées sur les orbites pour établir le lemme maximal semblaient inadaptées à traiter cette situation. L'exemple le plus naturel à étudier dans ce cadre était la suite des carrés, car on savait, par la théorie spectrale, que si $f \in L^2$, $\frac{1}{N} \sum_{k=1}^{N} f(T^{k^2} x)$ converge L^2 quand $N \to +\infty$. La question se trouve explicitement posée dans [B] et [F2].

Bourgain, dans [B 1], a démontré d'abord le lemme maximal dans la situation précédente en introduisant une technique absolument nouvelle, la transformation de Fourier sur le modèle des orbites. Il a ensuite, dans [B 3], produit par la même technique suffisamment de fonctions f pour lesquelles il y avait convergence *p.s.* (les fonctions L^∞) et a étendu ses résultats à la suite n^d, $d \geq 2$ et aux nombres premiers.

Pour la suite n^d , il a montré [B 2] ensuite la convergence *p.s.* pour des fonctions $f \in L^p$, $p > \frac{1+\sqrt{5}}{2}$.

Il a considérablement développé sa méthode jusqu'à lui donner la forme d'un outil capable de s'adapter au cas de différentes suites de type arithmétique. Il a prouvé en particulier dans [B 6]

THÉORÈME.— *Soit* $(X, \mathcal{A}, m, T)$ *un système dynamique et* $p(n)$ *un polynôme à coefficients entiers. Soit* $r > 1$ *et* $f \in L^r(X)$. *Alors* $\frac{1}{N} \sum_{k=1}^{N} f(T^{p(k)}x)$ *converge p.s. quand* $N \to +\infty$. *Le même résultat est valable si* $p(n)$ *désigne le n-ième nombre premier.*
(Le cas des nombres premiers pour $f \in L^r$, $r > 1$, avait été résolu auparavant dans [W].)

Nous donnons une présentation de son travail en nous restreignant cependant au cas $f \in L^2(X)$ et $p(n) = n^d$, $d \geq 2$ et nous indiquons comment traiter le cas des nombres premiers (Théorème 5 et Théorème 6).

Dans la partie 6, nous donnons une liste des autres résultats de Bourgain qui ressortissent de la même théorie.

1. L'INÉGALITÉ MAXIMALE

THÉORÈME 1.— *Soit d un entier* ≥ 2 . *Soit* $f \in \ell^2(\mathbf{Z})$ *et* Mf *défini par*

$$Mf(n) = \sup_{N>0} \left| \frac{1}{N} \sum_{k=1}^{N} f(n + k^d) \right| .$$

Alors il existe une constante C telle que

$$\|Mf\|_2 \leq C\|f\|_2$$

(C ne dépend que de d).

THÉORÈME 2.— *Soit* $(X, \mathcal{A}, m, T)$ *un système dynamique. Soit* $d \geq 2$. *Soit* $f \in L^2(X)$. *Soit* $f^*(x) = \sup_{N>0} \left| \frac{1}{N} \sum_{k=1}^{N} f(T^{k^d}x) \right|$. *Alors* $\|f^*\|_2 \leq C\|f\|_2$. *(C est exactement la constante du Théorème 1.)*

Démonstration du théorème 2 *à partir du théorème* 1 : Soit $\bar{N}$ un entier positif et

$$f^*_{\bar{N}}(x) = \sup_{\bar{N} \geq N > 0} \left| \frac{1}{N} \sum_{k=1}^{N} f(T^{k^d} x) \right| .$$

Il suffit de démontrer $\|f^*_{\bar{N}}\|_2 \leq C\|f\|_2$ (indépendamment de $\bar{N}$). Soit $J \gg \bar{N}$. Soit $x \in X$ et $\varphi_x \in \ell^2(\mathbf{Z})$ défini par $\varphi_x(n) = f(T^n x)$, $n \in [0, J]$, $\varphi_x(n) = 0$ si $n \notin [0, J]$. Alors si on définit $M_{\bar{N}} f(n) = \sup_{\bar{N} \geq N > 0} \left| \frac{1}{N} \sum_{k=1}^{N} f(n+k^d) \right|$, $\|M_{\bar{N}}\, \varphi_x\|_2 \leq \|M\, \varphi_x\|_2 \leq C\|\varphi_x\|_2$ (d'après le Théorème 1), ce qui se lit :

$$\sum_{k=0}^{J-\bar{N}} \left| f^*_{\bar{N}}(T^k x) \right|^2 \leq C^2 \sum_{k=0}^{J} \left| f(T^k x) \right|^2$$

et en intégrant, comme T préserve la mesure,

$$(J - \bar{N})\|f^*_{\bar{N}}\|_2^2 \leq C^2\ J\|f\|_2^2 .$$

D'où le résultat puisque J peut être choisi arbitrairement grand.

Ce passage du modèle d'une seule orbite ($\mathbf{Z}$, le shift S) à une transformation apparaît dans [C]. L'inégalité maximale (le théorème 2) entraîne que pour tout système $(X, \mathcal{A}, m, T)$, l'ensemble des fonctions $f \in L^2(X)$ pour lesquelles il y a convergence presque sûre des sommes $S_N f(x) = \frac{1}{N} \sum_{k=1}^{N} f(T^{k^d} x)$ est fermé dans L^2 . Tandis que, pour les sommes de Birkhoff usuelles, il est facile de produire une classe dense de fonctions pour lesquelles on a convergence *p.s.*, il n'y a aucune classe naturelle dans le cas des sommes $S_N f(x)$.

Cependant pour des transformations spécifiques, on a des classes denses naturelles : par exemple si T a un spectre de Lebesgue (les fonctions dont la densité spectrale est bornée), ou si T est isomorphe à une rotation irrationnelle (les fonctions continues).

2. SUFFISAMMENT DE FONCTIONS POUR LESQUELLES ON A UNE CONVERGENCE PRESQUE SÛRE

THÉORÈME 3.— *Soit* $f \in \ell^2(\mathbf{Z})$. *Soit* $\varepsilon > 0$. *Soit* $d \geq 2$. *Posons* $\mathbf{Z}_\varepsilon = [(1+\varepsilon)^n]$, $n \in \mathbf{N}$ ([ ] *désigne la partie entière). Soit* N_j *une suite d'entiers telle que* $N_{j+1} > 2N_j$ *et soit*

$$M_j^\varepsilon f(n) = \sup_{\substack{N \in \mathbf{Z}_\varepsilon \\ N_j \leq N \leq N_{j+1}}} \left| \frac{1}{N} \sum_{k=1}^{N} f(n+k^d) - \frac{1}{N_j} \sum_{\ell=1}^{N_j} f(n+\ell^d) \right| .$$

Alors $\sum_{1 \leq j \leq J} \| M_j^\varepsilon f \|_2 \leq A(J) \|f\|_2$ *où* $\frac{A(J)}{J}$ *tend vers 0 avec une vitesse qui ne dépend que de* ε *(et pas de la suite* N_j *).*

THÉORÈME 4.— *Le théorème* 3 *entraîne que si* $(X, \mathcal{A}, m, T)$ *est un système dynamique et si* $f \in L^\infty(X)$, *alors*

$$S_N f(x) = \frac{1}{N} \sum_{k=1}^{N} f(T^{k^d}(x)) \quad \text{converge p.s. quand} \quad N \to +\infty .$$

Démonstration : Exactement la même démonstration que celle du théorème 2 dit que si on pose

$$M_j^\varepsilon f(x) = \sup_{\substack{N_j \leq N \leq N_{j+1} \\ N \in \mathbf{Z}_\varepsilon}} \left| S_N f(x) - S_{N_j} f(x) \right|$$

$$\text{alors} \quad (1) \quad \frac{1}{J} \sum_{1 \leq j \leq J} \| M_j^\varepsilon f \|_2 \to 0 .$$

Mais si $S_N f$ ne converge pas p.s. suivant $\mathbf{Z}_\varepsilon$, il y a un nombre $a > 0$ et un ensemble E de X , $m(E) = a$, tels que $\overline{\lim}_{N \in \mathbf{Z}_\varepsilon} S_N f(x) - \underline{\lim}_{N \in \mathbf{Z}_\varepsilon} S_N f(x) > a$ pour tout x de E , et on peut alors choisir une suite N_j , satisfaisant $N_{j+1} \geq 2N_j$ telle que $\sup_{N_j < N \leq N_{j+1}} \left| S_N f(x) - S_{N_j} f(x) \right| > \frac{a}{2}$ pour tous les x d'une partie de E de mesure plus grande que $\frac{a}{2}$. Mais ceci contredit (1). Quand f est dans L^∞ , pour tout N , il existe N' dans $\mathbf{Z}_\varepsilon$ tel que $\left| S_N f(x) - S_{N'} f(x) \right| \leq 2\varepsilon \|f\|_\infty$ et par conséquent

$\overline{\lim} S_N f - \underline{\lim} S_N f \leq 4\varepsilon \|f\|_\infty$ *p.s.* et le résultat puisque (1) est vrai pour tout ε .

Comme corollaire des Théorèmes 2 et 4, on a le

THÉORÈME 5.— *Soit* $(X, \mathcal{A}, m, T)$ *un système dynamique* $d \geq 2$ *et* $f \in L^2(X)$. *Alors*

$$S_N f(x) = \frac{1}{N} \sum_{k=1}^{N} f(T^{k^d} x) \quad \text{converge p.s. quand} \quad N \to +\infty \ .$$

Si le système est totalement ergodique (toutes les puissances de T *ergodiques), la limite est* $\int f dm$.

Ce dernier point se voit en remarquant que, d'après le théorème de Bochner, la convergence L^2 des sommes $S_N f(x)$ est équivalente à la convergence dans $L^2_{d\nu_f}$ sur $S_1 = \{z \in \mathbf{C} \ |z| = 1\}$ des polynômes $\frac{1}{N} \sum_{k=1}^{N} z^{k^d}$ où $d\nu_f$ est la mesure sur S_1 définie par $\int f T^n f dm = \int e^{inx} \ d\nu_f(x) \ \forall n \in \mathbf{Z}$, $d\nu_f\{0\} = \int f dm$. Si T est totalement ergodique, $d\nu_f$ n'a pas de masse ponctuelle sur les points $e^{2i\pi \frac{p}{q}}$, $\frac{p}{q}$ rationnel différent de 0 , et $\frac{1}{N} \sum_{k=1}^{N} e^{2i\pi k^d \theta}$ converge vers 0 pour tout θ irrationnel d'après le théorème de Weyl.

3. DÉMONSTRATION DU THÉORÈME 1

Comme f peut être supposée positive,

$$2 \ M_{2^{p+1}} f(n) \geq M_N f(n) \quad 2^p \leq N \leq 2^{p+1} \ , \ \left(M_N f(n) = \frac{1}{N} \sum_{k=1}^{N} f(n + k^d) \right)$$

et si $\bar{\mathbf{Z}} = \{2^k \ k \in \mathbf{N}\}$ il suffit de prouver le théorème pour

$$M f(n) = \sup_{N \in \bar{\mathbf{Z}}} |M_N f(n)| \ .$$

(1) Si K_N est la mesure sur $\mathbf{Z}$ définie par $K_N = \frac{1}{N} \sum_{k=1}^{N} \delta_{\{k^d\}}$, alors $M_N f = f * K_N$.

La méthode, comme dans l'étude du problème de Waring par Hardy et Littlewood, est d'utiliser la transformation de Fourier. Soit $\hat{f}(\alpha) = \sum_{n\in\mathbf{Z}} f(n)\, e^{-2i\pi n\alpha}$, $\hat{K}_N(\alpha) = \frac{1}{N}\sum_{k=1}^{N} e^{-2i\pi\alpha k^d}$. Alors $M_N f(n) = \int_0^1 e^{2i\pi n\alpha}\hat{f}(\alpha)\,\hat{K}_N(\alpha)\,d\alpha$ et en utilisant la relation de Parseval, le théorème à démontrer devient :
Si $\hat{f}(\alpha) \in L^2[0,1]$

$$\text{(I)} \qquad \left\| \sup_{N\in\bar{\mathbf{Z}}} \left| \int_0^1 e^{2i\pi n\alpha}\,\hat{f}(\alpha)\,\hat{K}_N(\alpha)\,d\alpha \right| \right\|_{\ell^2(dn)} \leq C\|\hat{f}\|_2 \ .$$

(2) Nous introduisons un lemme qui sera démontré par la suite.

Lemme 5.— *Soient* $\lambda_1, \lambda_2, \cdots \lambda_K$ K *points sur le cercle* $S_1 = \mathbf{R}/\mathbf{Z}$ *et pour* j *un entier positif,* $Rj = \{\lambda | \lambda \in S_1$ et il existe $1 \leq r \leq k$ tel que $|\lambda - \lambda_r| < \frac{1}{2^j}\}$. *Soit* $s > 0$ *tel que* $|\lambda_i - \lambda_j| > \frac{1}{2^{s-1}}$ $\forall i \neq j$. *Soit* $\hat{f} \in L^2[0,1]$ *et*

$$f^*(n) = \sup_{j\geq s} \left| \int_{R_j} e^{2i\pi n\alpha}\,\hat{f}(\alpha)d\alpha \right| .$$

Alors il existe une constante absolue C_2 *telle que*

$$\|f^*\|_{\ell^2(dn)} \leq C_2(\text{Log } K)^3\ \|\hat{f}\|_2 \ .$$

Le but maintenant est de remplacer $\hat{K}_N(\alpha)$ par des approximations convenables auxquelles on pourra appliquer le lemme 5.

(3) Soit s un entier positif et

$$R_s = \left\{\theta \in Q \cap [0,1] \mid \theta = \frac{a}{q}\ 2^s \leq q < 2^{s+1}\ (a,q) = 1\right\}$$

et soit ζ une fonction C^∞ définie sur $\mathbf{R}$, $|\zeta| \leq 1$, $\zeta = 1$ sur $\left[-\frac{1}{10}, \frac{1}{10}\right]$ et $\zeta = 0$ en dehors de $\left[-\frac{1}{5}, \frac{1}{5}\right]$.

Soit $\theta = \frac{a}{q}$; on pose $S(\theta) = \frac{1}{q}\sum_{k=1}^{q} e^{2i\pi k^d\theta}$. Pour β réel, et N entier positif, on pose

$$V_N(\beta) = \int_0^1 e^{-2i\pi\beta N^d y^d}\,dy$$

et on définit enfin pour $\alpha \in S^1 = \mathbf{R}/\mathbf{Z}$

$$\psi_{s,N}(\alpha) = \sum_{\theta \in R_s} S(\theta) V_N(\alpha - \theta) \zeta(10^s(\alpha - \theta)) \ . \tag{4}$$

Remarquons que les fonctions intervenant dans la somme ont des supports disjoints puisque si θ_1 et θ_2 sont dans R_s , $\theta_1 \neq \theta_2$; alors $|\theta_1 - \theta_2| > \frac{1}{2^{2s}}$. De l'estimation de H. Weyl ([V], p. 11), dès que $\left|\alpha - \frac{a}{q}\right| < \frac{1}{q^2}$, $(a,q) = 1$,

$$\left| \sum_{m=1}^{n} e^{2i\pi\alpha m^d} \right| \leq C_\varepsilon \ n^{(1+\varepsilon)} \left[\frac{1}{q} + \frac{1}{n} + \frac{q}{n^d} \right]^{\frac{1}{2^{d-1}}} \tag{5}$$

on va déduire qu'il existe un nombre $\delta_1 > 0$ tel que

$$\left| \hat{K}_N(\alpha) - \sum_{s \geq 0} \psi_{s,N}(\alpha) \right| < \frac{C_3}{N^{\delta_1}} \tag{6}$$

(les constantes ou bien sont absolues ou bien ne dépendent que de d). Soit $\delta' = \frac{1}{1002^{d-1}}$, $\delta = \frac{1}{100}$. Soit un rationnel $\frac{p}{q}$, $(p,q) = 1$, $q < N^\delta$; l'ensemble

$$\mathcal{M}_N\left(\frac{p}{q}\right) = \left\{ \alpha \,\middle|\, \left|\alpha - \frac{p}{q}\right| < \frac{1}{N^{d-\delta}} \right\}$$

est appelé un arc majeur.

On appelle $\mathcal{M}_{N,\delta}$ la réunion de tous les arcs majeurs qui sont deux à deux disjoints et on a les estimations classiques suivantes (7), (8) et (9) :

(7) Si $\alpha \in \mathcal{M}_{N,\delta}^c$, $|\hat{K}_N(\alpha)| < \frac{C_4}{N^{\delta'}}$ (une conséquence facile de (5) et du lemme des tiroirs de Dirichlet qui dit qu'il existe a et q , $(a,q) = 1$, tels que $\left|\alpha - \frac{a}{q}\right| < \frac{1}{N^{d-\delta} q}$, $q < N^{d-\delta}$, et comme α n'est pas dans un arc majeur, $q > N^\delta$).

(8) Si $\alpha \in \mathcal{M}_{N,\delta}$, alors $\alpha = \frac{p}{q} + \beta$, $(p,q) = 1$, $|\beta| < \frac{1}{N^{d-\delta}}$ et $\hat{K}_N(\alpha) = S\left(\frac{p}{q}\right) V_N(\beta) + 0\left(\frac{1}{\sqrt{N}}\right)$ (on utilise les notations de (3)) par un calcul élémentaire utilisant uniquement que si $m = qs + r$ $\left(s < \frac{N}{q},\ 0 \leq r < q\right)$, $\left|\{\alpha m^d\} - \left(\frac{p}{q}\right) r^d - \beta (qs)^d\right| < \frac{d}{N^{1-2\delta}}$ et $\left|e^{2i\pi\beta q^d s^d} - e^{2i\pi\beta q^d y^d}\right| < \frac{C}{N^{d-2\delta}}$ dès que $|s - y| \leq 1$.

(9) Il y a trois minorations évidentes
(M1) $|V_N(\beta)| < \frac{C_5}{N|\beta|^{\frac{1}{d}}}$.
(M2) $|1 - V_N(\beta)| < C_6\,|\beta|\,N^d$.
(M3) Si $(p,q) = 1$, $2^s \le q < 2^{s+1}$, $S\left(\frac{p}{q}\right) < C_7\ 2^{-s\delta'}$
((M3) est une conséquence de (5)).

(10) On peut maintenant démontrer (6).

(A) $\alpha \in \mathcal{M}_{N,\delta}$. Alors $\left|\alpha - \frac{p}{q}\right| < \frac{1}{N^{d-\delta}}$, $q < N^\delta$ et $\theta = \frac{p}{q} \in R_{s_0}$ avec $2^{s_0} < N^\delta$. Soit s_1 tel que $2^{s_1} \sim N^\delta$

$$\left|\hat{K}_N(\alpha) - \sum_{s\ge 0} \psi_{s,N}(\alpha)\right| \le \sum_{\substack{s\le s_1 \\ s\ne s_o}} \sup_{\theta' \in R_s} |V_N(\alpha - \theta')| + \frac{C_8}{2^{s_1\delta}} .$$

(On a utilisé (8) et (M3).) Comme pour tout $\theta' \in R_s$ $(s \le s_1\ ,\ s \ne s_0)$ $|\alpha - \theta'| > \frac{1}{2N^\delta}$, (M1) entraîne que la somme est bornée par $C_5 \frac{\mathrm{Log}\,N}{N^{1-2\delta}}$.

(B) Si $\alpha \notin \mathcal{M}_{N,\delta}$, conservant la définition de s_1 donnée en (A) ,

$$\left|\sum_{s\ge 0} \psi_{s,N}(\alpha)\right| \le \sum_{s\le s_1} |\psi_{s,N}| + \frac{C_9}{2^{s_1\delta}}$$

et comme pour tout $\frac{p}{q} \in R_s$, on a $\left|\frac{p}{q} - \alpha\right| > \frac{1}{N^{d-\delta}}$, (M1) entraîne encore $\sum_{s\le s_1} |\psi_{s,N}| \le C_{10}\,\frac{\mathrm{Log}\,N}{N^{\frac{\delta}{d}}}$.

(10) (A), (B) et (7) entraînent bien (6) $\delta_1 = (\delta')^2$.

(11) On pose $\psi_N(\alpha) = \sum_{s\ge 0} \psi_{s,N}(\alpha)$ et on montre qu'il suffit de prouver (I) en changeant $\hat{K}_N(\alpha)$ en $\psi_N(\alpha)$. En effet

$$\sup_{N\in\overline{\mathbf{Z}}}\left|\int_0^1 e^{2i\pi n\alpha}\ \hat{f}(\alpha)\,\hat{K}_N(\alpha)\,d\alpha\right| \le \sup_{N\in\overline{\mathbf{Z}}}\left|\int_0^1 e^{i\pi n\alpha}\ \hat{f}(\alpha)\,\psi_N(\alpha)\,d\alpha\right|$$
$$+ \left\{\sum_{N\in\overline{\mathbf{Z}}}\left|\int_0^1 e^{2i\pi n\alpha}\,\hat{f}(\alpha)\left(\hat{K}_N(\alpha) - \psi_N(\alpha)\right)d\alpha\right|^2\right\}^{\frac{1}{2}}$$

et prenant les normes $\| \ \|_{\ell^2}$, on obtient

$$\left\| \sup_{N\in\bar{\mathbf{Z}}} \left| \int_0^1 e^{2i\pi n\alpha}\ \hat{f}(\alpha)\,\hat{K}_N(\alpha)\,d\alpha \right| \right\|_{\ell^2(dn)}$$

$$\leq \left\| \sup_{N\in\bar{\mathbf{Z}}} \left| \int_0^1 e^{2i\pi n\alpha}\ \hat{f}(\alpha)\,\psi_N(\alpha)\,d\alpha \right| \right\|_{\ell^2(dn)}$$

$$+ \left\{ \sum_{N\in\bar{\mathbf{Z}}} \int_0^1 |\hat{f}(\alpha)|^2 \left|\hat{K}_N(\alpha) - \psi_N(\alpha)\right|^2 d\alpha \right\}^{\frac{1}{2}} .$$

La dernière expression se majore par

$$\left(\sum_{N\in\bar{\mathbf{Z}}} \|\hat{K}_N(\alpha) - \psi_N(\alpha)\|_\infty^2 \right)^{\frac{1}{2}} \|\hat{f}\|_2 \leq C_{11}\,\|\hat{f}\|_2 \ .$$

(On a utilisé (6).)

(12) On introduit les fonctions $\widetilde{\psi}_{N,s}(\alpha) = \sum_{\theta\in R_s} S(\theta)\ \chi[N^d(\alpha-\theta)]$ $\times\zeta(10^s(\alpha-\theta))$ (χ la fonction caractéristique de l'intervalle $[-1,1]$) et on prouve l'estimation

$$S_s(\alpha) = \sum_{N\in\bar{\mathbf{Z}}} \left|\widetilde{\psi}_{N,s} - \psi_{N,s}\right| \leq C_{12}\ 2^{-s\delta} \ . \tag{13}$$

Comme d'après (4) il n'y a au plus qu'un θ de R_s qui donne une contribution, on a

$$S_s(\alpha) \leq \sum_{\substack{N\in\bar{\mathbf{Z}} \\ |\beta|\,N^d\leq 1}} \sup_{\theta\in R_s} |S(\theta)|\,|1 - V_N(\beta)| + \sum_{\substack{|\beta|\,N^d>1 \\ N\in\bar{\mathbf{Z}}}} \sup_{\theta\in R_s} |S(\theta)|\,|V_N(\beta)|$$

($\beta = \alpha-\theta$) et on a la majoration en utilisant (M3) et (M2) pour la première somme, (M3) et (M1) pour la deuxième.

$$\left\| \sup_{N\in\bar{\mathbf{Z}}} \left| \int_0^1 e^{2i\pi n\alpha}\,\hat{f}(\alpha)\,\psi_N(\alpha)\,d\alpha \right| \right\|_{\ell^2(dn)} \tag{14}$$

$$\leq \sum_{s\geq 0} \left\| \sup_{N\in\bar{\mathbf{Z}}} \left| \int_0^1 e^{2i\pi n\alpha}\,\hat{f}(\alpha)\,\psi_{N,s}(\alpha)\,d\alpha \right| \right\|_{\ell^2(dn)}$$

le même argument que (11), utilisant (13), donne

$$\left\| \sup_{N\in\bar{\mathbf{Z}}} \left| \int_0^1 e^{2i\pi n\alpha}\, \hat{f}(\alpha)\, \psi_{N,s}(\alpha)\, d\alpha \right| \right\|_{\ell^2(dn)}$$

$$\leq \left\| \sup_{N\in\bar{\mathbf{Z}}} \left| \int_0^1 e^{2i\pi n\alpha}\, \hat{f}(\alpha)\, \widetilde{\psi}_{N,s}(\alpha) \right| \right\|_{\ell^2(dn)} \tag{15}$$

$$+ C_{12} 2^{-s\delta} \|\hat{f}(\alpha)\|_2 \ .$$

Soit $\hat{f}_s(\alpha) = \sum_{\theta\in R_s} \hat{f}(\alpha)\, S(\theta)\, \zeta(10^s(\alpha-\theta))$. On peut appliquer le lemme 5. En prenant $\{\lambda_1, \lambda_2 \cdots, \lambda_K\} = R_s$, et en remarquant que, pour $N \in \bar{\mathbf{Z}}$, $\frac{1}{N^d} = \frac{1}{2^j}$, on obtient, notant $R_{s,u}$ le u voisinage de R_s ,

$$(15) = \left\| \sup_{N\in\bar{\mathbf{Z}}} \left| \int_{R_{s,\frac{1}{N^d}\wedge\frac{1}{5\,10^s}}} e^{2i\pi n\alpha}\, \hat{f}_s(\alpha)\, d\alpha \right| \right\|_{\ell^2(dn)}$$

$$\leq \left\| \sup_{j\geq 2s} \left| \int_{R_{s,\frac{1}{2^j}}} e^{2i\pi n\alpha}\, \hat{f}_s(\alpha)\, d\alpha \right| \right\|_{\ell^2(dn)}$$

$$\leq C_2 (\mathrm{Log}\, \mathrm{Card}(R_s))^3\, \|\hat{f}_s\|_2$$

$$\leq C_2\, s^3\, 2^{-s\delta}\, \|\hat{f}\|_2 \ . \tag{16}$$

(On a utilisé (M3)).
La sommation de (11), (14) et (16) donne (I).

4. DÉMONSTRATION DU LEMME 5

On utilise maintenant certains résultats de la théorie des martingales.

DÉFINITION.— *Soit* $a = \{a_n\}$, $n \in \mathbf{N}$, *une suite. Soit* $s > 0$. *On pose*

$$\|\{a_n\}\|_{v_s} = \sup_{\substack{J \\ n_1<n_2\cdots<n_J}} \left(\sum_{k=1}^{J-1} \left| a_{n_{k+1}} - a_{n_k} \right|^s \right)^{\frac{1}{s}} .$$

Le lemme suivant est dû à Lépingle [Lep].

Lemme 6.— *Soit* $(X, \mathcal{A}, m)$ *un espace probabilisé,* $f \in L^2(X)$, *et* $\mathcal{A}_n \uparrow \mathcal{A}$. *Soit* $s > 2$. *Alors il existe une constante absolue* C *telle que*

$$\| \| \{E^{\mathcal{A}_n} f\} \|_{v_s} \|_{L^2} \stackrel{\text{def}}{=} \| \{E^{\mathcal{A}_n} f\} \|_{L^2_{v_s}} \leq \frac{C}{s-2} \|f\|_2 .$$

Nous ne démontrerons pas ce lemme que Bourgain obtient par interpolation à partir des estimations de Doob sur l'espérance du nombre de sauts d'amplitude donnée dans une martingale.

La généralisation au cas continu est immédiate (avec l'extension évidente de la définition de $\| \|_{v_s}$ à ce cas). Si f est une fonction réelle, on pose $f_t(x) = \frac{1}{t} f\left(\frac{x}{t}\right)$, $\left(\hat{f}_t(\lambda) = \hat{f}(t\lambda)\right)$.

Une opération "classique" de passage des martingales aux convolutions donne le

Lemme 7.— *Soit* $s > 2$ *et* $f \in L^2(\mathbf{R})$. *Alors* $\left\| \{f * \chi_t\} \,|\, t > 0 \right\|_{L^2_{v_s}} \leq \frac{C}{s-2} \|f\|_2$ *(où* χ *est la fonction indicatrice de l'intervalle* $[0,1]$ *).*

La démonstration de ce lemme repose sur le fait que si P_t désigne le semi-groupe de Poisson sur $\mathbf{R}$, le lemme de dilatation de Rota et le lemme précédent entraînent $\left\| \{P_t f \,|\, t > 0\} \right\|_{L^2_{v_s}} \leq \frac{C}{s-2} \|f\|_2$. Posant $K = \chi - P_1$ qui vérifie $|\lambda| \, |(\hat{K})'(\lambda)| < C_1$, $|(\hat{K})(\lambda)| < C_2 \min(|\lambda|, |\lambda|^{-1})$, ces deux dernières propriétés suffisent pour entraîner $\left\| \{f * K_t \,|\, t > 0\} \right\|_{L^2_{v_2}} \leq C \|f\|_2$.

Nous ne donnons pas les détails de cette preuve.

La version discrète de ce résultat pour $f \in \ell^2(\mathbf{Z})$, $\|f * \frac{1}{N} \chi[0\,N]\|_{\ell^2_{v_s}} \leq \frac{C}{s-2} \|f\|^2$ sera aussi utilisée dans la suite.

Soit φ une fonction différentiable sur $[0, \infty[$ tendant vers 0 à l'∞ . Alors

$$\varphi(x) = -\int_0^\infty \chi_t(x)\; t\varphi'(t)\, dt .$$

Comme corollaire du lemme 7, par convexité, on a, si φ vérifie les hypothèses ci-dessus le

Lemme 9.— $\|\{f * \varphi_t \,|\, t > 0\}\|_{L^2_{v_s}} \leq \frac{C}{s-2} \left(\int_0^\infty |x| \, |\varphi'(x)| \, dx\right) \|f\|_2$.

On pose $\frac{C}{s-2}\int_0^\infty |x|\,|\varphi'(x)|\,dx = C_\varphi$.

Si E est une partie d'un espace métrique et $\lambda > 0$, on définit $M_\lambda(E)$ comme le cardinal du plus petit ensemble de boules de rayon λ qui recouvrent E . Si $\operatorname{diam}(E) < \lambda$, on pose $M_\lambda(E) = 0$.

Lemme 10.— *Soit φ comme ci-dessus, H un espace de Hilbert, $f \in L^2_{\mathbf{R}}(H)$, $s > 2$. Alors* $\left\|\sup_{\lambda>0}\left(\lambda\, M_\lambda^{\frac{1}{s}}(x)\right)\right\|_2 \le \frac{C_\varphi}{s-2}\,\|f\|_2$ *où* $M_\lambda(x) = M_\lambda\left(\{f * \varphi_t(x) \mid t > 0\}\right)$.

Démonstration.— Si on définit par récurrence $t_j = \min t > t_{j-1}$ tels que $\left\|f * \varphi_t(x) - f * \varphi_{t_{j-1}}(x)\right\|_H > \lambda$, alors $\lambda\, M_\lambda(x)^{\frac{1}{s}} \le \left\{\sum_j \|f * \varphi_{t_j}(x) - f * \varphi_{t_{j-1}}(x)\|_H^s\right\}^{\frac{1}{s}} \le \|\{f * \varphi_t(x)\}\|_{v_s}$. Si e_n est une base orthogonale de H , $f = \sum_n (f \mid e_n)\, e_n$ et $\left\|\sup_{\lambda>0}\left(\lambda\, M_\lambda^{\frac{1}{s}}\right)\right\|_2 \le \left[\sum_n \left\|\{(f \mid e_n) * \varphi_t\}\right\|^2_{L^2_{v_s}}\right]^{\frac{1}{2}} \le \frac{C_\varphi}{s-2}\,\|f\|_2$ d'après le lemme 9.

Conservant les mêmes hypothèses et les mêmes notations, on a le

Corollaire 11.— *Si $f \in L^2_H(\mathbf{R})$, et si $K > 0$, alors*

$$\text{(M)} \qquad \left\|\int_0^\infty \min\left(K, M_\lambda(x)\right)^{\frac{1}{2}} d\lambda\right\|_2 \le C'_\varphi\,(\operatorname{Log} K)^2\,\|f\|_2 \ .$$

Démonstration.— Soit $f_n = (f \mid e_n)$ et $f_n^* = \sup_{t>0}|f_n * \varphi_t|$, $\|f_n^*\|_2 \le C_\varphi\,\|f_n\|_2$ (Inégalité maximale de Hardy-Littlewood). Si $F(x) = \left[\sum_n (f_n^*)^2\right]^{\frac{1}{2}}$, $F(x) > \operatorname{diam}\{f * \varphi_t(x) \mid t > 0\}$ et

$$\begin{aligned}
\int_0^\infty \min\left(K, M_\lambda(x)\right)^{\frac{1}{2}} d\lambda &= \int_0^{F(x)} \min\left(K, M_\lambda(x)\right)^{\frac{1}{2}} d\lambda \\
\text{(s>2)} \qquad &\le \int_0^{\frac{F(x)}{\sqrt{K}}} \sqrt{K}\, d\lambda + \int_{\frac{F(x)}{\sqrt{K}}}^{F(x)} K^{\frac{1}{2}-\frac{1}{s}}\, M_\lambda^{\frac{1}{s}}(x)\, d\lambda \\
&\le F(x) + 2^{-1}\, K^{\frac{1}{2}-\frac{1}{s}} \operatorname{Log} K \sup_{\lambda>0} \lambda\, M_\lambda^{\frac{1}{s}}(x) \ .
\end{aligned}$$

Prenant les normes $\|\ \|_2$, choisissant s vérifiant $\frac{1}{2} - \frac{1}{s} = \frac{1}{\operatorname{Log} K}$, le lemme 10 donne (M).

Lemme 12.— *Soient* $\lambda_1, \lambda_2, \cdots \lambda_K \in \mathbf{R}$, $(\lambda_1 < \lambda_2 \cdots < \lambda_K)$. *Soient* $f_1, f_2, \cdots f_K$, K *fonctions de* $L^2(\mathbf{R})$. *Soit* $\tau > 0$ *tel que* $|\lambda_{k+1} - \lambda_k| > \tau$, $k = 1, 2 \cdots K-1$. *Soit* φ *une fonction différentiable telle que* $\hat{\varphi}$ *ait son support dans* $[-1, 1]$. *Alors*

$$(1) \qquad \left\| \sup_{t > \frac{1}{\tau}} \left| \sum_{k=1}^{K} e^{2i\pi\lambda_k x} \left(f_k * \varphi_t\right) \right| \right\|_2 < C \left(\operatorname{Log} K\right)^3 \left(\sum_{k=1}^{K} \|f_k\|_2^2 \right)^{\frac{1}{2}}$$

(C ne dépend que de φ*).*

Démonstration.— Comme $|\lambda_k - \lambda_\ell| > |k - \ell|\,\tau$, $\int_0^{\frac{1}{\tau}} e^{2i\pi(\lambda_k - \lambda_\ell)u}\, du$ est $0\left(\frac{1}{|k-\ell|}\right)$ et

$$(2) \qquad \left\| \sum_{k \leq K} a_k\, e^{2i\pi\lambda_k u} \right\|_{L^2\left[0, \frac{1}{\tau}\right]} \leq \frac{C'}{\sqrt{\tau}} \operatorname{Log} K \left(\sum_{k=1}^{K} |a_k|^2 \right)^{\frac{1}{2}} .$$

Il y a une meilleure constante $B < +\infty$ telle que (1) soit vraie ($C_\varphi \sqrt{K}$ convient d'après le lemme maximal de Hardy-Littlewood). Soit $u > 0$. On pose $\sigma_u f(x) = f(x+u)$. Alors

$$\left\| \sup_{t > \frac{1}{\tau}} \left| \sum_{k=1}^{K} e^{2i\pi\lambda_k x} \left(f_k * \varphi_t\right) \right| \right\|_2$$

$$(S_1)(u) \qquad \leq \left\| \sup_{t > \frac{1}{\tau}} \left| \sum_{k=1}^{K} e^{2i\pi\lambda_k x} \sigma_u \left(f_k * \varphi_t\right) \right| \right\|_2$$

$$(S_2) \qquad + \left\| \sup_{t > \frac{1}{\tau}} \left| \sum_{k=1}^{K} e^{2i\pi\lambda_k x} \left((f_k - \sigma_u f_k) * \varphi_t \right) \right| \right\|_2$$

l'hypothèse sur φ et $t > \frac{1}{\tau}$ entraînent qu'on peut supposer $\operatorname{supp} \hat{f}_k \subset [-\tau, \tau]$, $1 \leq k \leq K$ et on a par Parseval une estimation uniforme

$$\left\| f_k - \sigma_u f_k \right\|_2 < \frac{1}{2} \left\| f_k \right\|_2 \quad k = 1, 2 \cdots K \quad |u| < \frac{1}{100\,\tau} .$$

(S_2) est alors majorée par $\frac{1}{2} B \left(\sum \|f_k\|_2^2 \right)^{\frac{1}{2}}$.

Pour estimer (S_1), on regarde l'ensemble $A_x = \{f_1 * \varphi_t(x), f_2 * \varphi_t(x), \cdots f_K * \varphi_t(x) \,|\, t > 0\}$ et on remarque qu'on peut décrire tout point de cet ensemble par une somme

$$\sum_{s\in\mathbf{Z}} b_s \qquad b_s \in \mathbf{R}^K \quad , \qquad |b_s| = \left(\sum_{i=1}^{K} |b_{s,i}|^2\right)^{\frac{1}{2}} ,$$

où $|b_s| < 2^{s+1}$, et où chaque b_s appartient à un ensemble B_s (qui dépend de $b_{s'}$, $s' > s$ tel que $\mathrm{Card}(B_s) < M_{2^s}(x)$ et où presque sûrement il n'y a qu'un nombre fini de b_s , $s > 0$ non nuls). (On a utilisé les notations du lemme 10 et du corollaire 11 où H est de dimension K et $f = (f_1, f_2, \cdots f_K)$.)

Alors : (on n'a plus besoin de se restreindre à $t > \frac{1}{\tau}$)

$$\sup_{t>0} \left|\sum_{k=1}^{K} e^{-2i\pi\lambda_k(u-x)}\, f_k * \varphi_t(x)\right|$$

$$\leq \sum_{s\in\mathbf{Z}} \operatorname*{Max}_{b\in B_s} \left|\sum_{k=1}^{K} e^{-2i\pi\lambda_k(u-x)}\, b_k\right| \quad (b = (b_1, b_2, \cdots b_K)) .$$

$$(3) \quad \operatorname*{Max}_{b\in B_s} \left|\sum_{k=1}^{K} e^{-2i\pi\lambda_k(u-x)}\, b_k\right|$$

$$< \min\left(\sqrt{K}\, 2^{s+1}, \left(\sum_{b\in B_s} \left|\sum_{k=1}^{K} e^{-2i\pi\lambda_k(u-x)}\, b_k\right|^2\right)^{\frac{1}{2}}\right) .$$

On peut remplacer $(S_1)(u)$ par

$$10\sqrt{\tau}\, \left\|S_1(u)\right\|_{L^2\left(0,\frac{1}{100\tau}\right)}$$

$$\leq \left\| 10 \sum_{s} \min\left(2^{s+1}\sqrt{K}, C' \operatorname{Log} K\, 2^{s+1}\, M_{2^s}^{\frac{1}{2}}(x)\right)\right\|_{L^2(dx)}$$

(on a changé l'ordre des intégrations, et utilisé (3) et (2)). Par le corollaire 11, cette dernière expression est majorée par $10\, C'\, C'_\varphi (\operatorname{Log} K)^3 \left(\sum_{k=1}^{K} \|f_k\|_2^2\right)^{\frac{1}{2}}$, d'où $B \leq \frac{1}{2}\, B + 10\, C'\, C'_\varphi\, (\operatorname{Log} K)^3$, ce qui donne (1).

On a maintenant une version $L^2(\mathbf{R})$ du lemme 5.

Lemme 13.— *Soient* $\lambda_1 < \lambda_2 \cdots < \lambda_K \in \mathbf{R}$ *avec* $|\lambda_{k+1} - \lambda_k| > 2^{-s}$. *Soit* R_j *le* $\frac{1}{2^j}$ *voisinage de l'ensemble* $\{\lambda_1, \lambda_2, \cdots \lambda_K\}$. *Alors, si* $f \in L^2(\mathbf{R})$

$$(1) \qquad \left\| \sup_{j \geq s} \left| \int_{R_j} e^{2i\pi\lambda x} \hat{f}(\lambda)\, d\lambda \right| \right\|_2 \leq C(\operatorname{Log} K)^3 \, \|\hat{f}\|_2$$

(C est absolu).

Pour démontrer ce lemme, on prend une fonction φ telle que $\operatorname{Supp} \hat{\varphi} \subset [-1, 1]$, $\hat{\varphi} = 1$ sur $\left[-\frac{1}{2}, \frac{1}{2}\right]$ et l'inégalité (1) s'obtient en appliquant le lemme 12 avec $f_k = \left(f \,.\, e^{-2i\pi\lambda_k x}\right) * \varphi_{2^{s-1}}$ et en remarquant que $\sup_{\lambda \in \mathbf{R}} \left[\sum_{j \geq s} |\chi_{R_j}(\lambda) - \sum_{i=1}^{K} \hat{\varphi}\left(2^j(\lambda - \lambda_i)\right)\right]$ est fini.

Fin de la démonstration du lemme 5.— Soit $B = C\,(\operatorname{Log} K)^3$. Le lemme 13 dit que

$$\left(\int_{-\infty}^{\infty} \sup_j \left| \int_{R_j} e^{2i\pi x\alpha} \hat{f}(\alpha)\, d\alpha \right|^2 dx \right)^{\frac{1}{2}} \leq B \, \|\hat{f}\|_2 \ ,$$

$R_j \subset [0, 1]$ et $\hat{f}(\alpha)$ considérée comme une fonction sur $\mathbf{R}$ de support $[0, 1[$.

On veut montrer qu'il y a une constante C telle que

$$\left(\sum_{n \in \mathbf{Z}} \sup_j \left| \int_{R_j} e^{2i\pi n\alpha} \hat{f}(\alpha)\, d\alpha \right|^2 \right)^{\frac{1}{2}} \leq CB \, \|\hat{f}\|_2 \ .$$

On montre en fait qu'il existe C indépendante de N telle que

$$(1) \qquad \left(\sum_{|n| < N} \sup_j \left| \int_{R_j} e^{2i\pi n\alpha} \hat{f}(\alpha)\, d\alpha \right|^2 \right)^{\frac{1}{2}} \leq CB \, \|\hat{f}\|_2 \ .$$

Soit C_N la meilleure constante telle que (1) soit vraie $\left(C_N \leq \sqrt{2N+1}\right)$.

Soit ρ un nombre < 1 et $0 < u < \rho$, alors

$$\int_{R_j} e^{2i\pi n\alpha} \hat{f}(\alpha)\, d\alpha = \int_{R_j} e^{2i\pi(n+u)\alpha} \hat{f}(\alpha)\, d\alpha + \int_{R_j} e^{2i\pi n\alpha} \left[1 - e^{+2i\pi u\alpha}\right] \hat{f}(\alpha)\, d\alpha \ .$$

$$\left(\sum_{|n|<N} \sup_j \left|\int_{R_j} e^{2i\pi n\alpha}\, \hat{f}(\alpha)\, d\alpha\right|^2\right)^{\frac{1}{2}}$$

$$(S_1)(u) \qquad \leq \left(\sum_{|n|<N} \sup_j \left|\int_{R_j} e^{2i\pi(n+u)\alpha}\, \hat{f}(\alpha)\, d\alpha\right|^2\right)^{\frac{1}{2}}$$

$$(S_2) \qquad + \left(\sum_{|n|<N} \sup_j \left|\int_{R_j} e^{2i\pi n\alpha}\left(1 - e^{2i\pi u\alpha}\right)\hat{f}(\alpha)\, d\alpha\right|^2\right)^{\frac{1}{2}}$$

(S_2) est majorée par $C_N\, C_1\, \rho\, \|\hat{f}\|_2$, tandis que $\frac{1}{\sqrt{\rho}}\, \|S_1(u)\|_{L^2(0,\rho)} \leq \frac{1}{\sqrt{\rho}}\, B\, \|\hat{f}\|_2$, $C_N \leq \frac{B}{\sqrt{\rho}} + C_N\, C_1\, \rho$ et le résultat en prenant ρ assez petit.

5. DÉMONSTRATION DU THÉORÈME 3

$$\|M_j^\varepsilon\, f\|_2 = \left\| \sup_{\substack{N_j < N \leq N_{j+1} \\ N \in \mathbf{Z}_\varepsilon}} \left|\int_0^1 e^{2i\pi n\alpha}\, \hat{f}(\alpha)\big(\hat{K}_N(\alpha) - \hat{K}_{N_j}(\alpha)\big)\, d\alpha\right| \right\|_{\ell^2(dn)}$$

l'estimation (6) du théorème 1 permet de remplacer $\hat{K}_N(\alpha) - \hat{K}_{N_j}(\alpha)$ par $\psi_N(\alpha) - \psi_{N_j}(\alpha)$ et l'estimation (16), en considérant maintenant M_j^ε défini par ψ_N , pour $s_0 > 0$, donne

$$\|M_j^\varepsilon\, f\|_2 \leq \sum_{s \leq s_0} \left\| \sup_{\substack{N_j < N \leq N_{j+1} \\ N \in \mathbf{Z}_\varepsilon}} \left|\int_0^1 e^{2i\pi n\alpha}\, \hat{f}(\alpha)\big(\psi_{N,s}(\alpha) - \psi_{N_j,s}(\alpha)\big)\, d\alpha\right| \right\|_2 + \frac{C}{\varepsilon}\, 2^{-\delta s_0}\, \|f\|_2$$

Redéfinissant

$$(1) \qquad M_j^\varepsilon\, f(n) = \sup_{\substack{N_j < N \leq N_{j+1} \\ N \in \mathbf{Z}_\varepsilon}} \left|\int_0^1 e^{2i\pi n\alpha}\, \hat{f}(\alpha)\big(V_N(\alpha) - V_{N_j}(\alpha)\big)\, d\alpha\right|$$

on ne modifie pas le comportement de $\frac{1}{J} \sum_{j=1}^{J} \|M_j^\varepsilon\, f\|_2$.

Si χ est la fonction indicatrice de $[0,1]$, (M1) et (M2) donnent $|V_N(\alpha) - \hat{\chi}(N^d\alpha)| < C(\min(|\alpha| N^d, \frac{1}{N(\alpha)^{\frac{1}{d}}})$ et $\sup_\alpha \sum_{N\in\mathbf{Z}_\epsilon} |V_N(\alpha) - \hat{\chi}(N^d\alpha)|^2 < C_\varepsilon$. Par conséquent, si on définit $\bar{M}_j f(n) = \sup_{N_j<N\le N_{j+1}} \left| f * (\chi_{N^d} - \chi_{N_j^d}) \right|$, où $\chi_N = \frac{1}{N}\chi_{[0,N]}$, on aura

$$\sum_{j=1}^{J} \|M_j^\varepsilon f\|_2^2 \le C_\varepsilon \|f\|_2^2 + \sum_{j=1}^{J} \|\bar{M}_j f\|_2^2 . \tag{2}$$

Mais $\left|\sum_{j=1}^{J} (\bar{M}_j f)^2\right|^{\frac{1}{2}} \le J^{\frac{1}{4}} \|\{f * \chi_N \mid N > 1\}\|_{v_4}$ et le lemme 7 donne

$$\sum_{j=1}^{J} \|\bar{M}_j f\|_2^2 < C\sqrt{J}\, \|f\|_2^2 \tag{3}$$

et (2) et (3) entraînent le Théorème 3.

La méthode est assez souple pour s'appliquer avec des modifications convenables et donner le

THÉORÈME 6.— *Soit $(X, \mathcal{A}, m, T)$ un système dynamique. Soit $f \in L^2(X)$ si p_n désigne le n-ième nombre premier $\frac{1}{N}\sum_{k=1}^{N} f(T^{p_k}x)$ converge p.s. quand $N \to +\infty$.*

Si toutes les puissances de T sont ergodiques, la limite est $\int f\, dm$.

La démonstration se fonde sur deux estimations de $S_N(\alpha) = \sum_{n\le N} \Lambda(n)\, e^{2i\pi n\alpha}$ ($\Lambda(n) = \operatorname{Log} p$ si n est une puissance du nombre premier p, $\Lambda(n) = 0$ sinon) (voir [V], p. 26, 29).

1) Si $\left|\alpha - \frac{a}{q}\right| < \frac{1}{q^2}$, où $(a,q) = 1$

$$\left|S_N(\alpha)\right| < C\left(\frac{N}{\sqrt{q}} + N^{\frac{4}{5}} + N^{\frac{1}{2}} q^{\frac{1}{2}}\right)(\operatorname{Log} N)^4 .$$

2) Si $\left|\alpha - \frac{a}{q}\right| \le \frac{(\operatorname{Log} N)^c}{N}$ où $(a,q) = 1$ et $q \le (\operatorname{Log} N)^c$, alors

$$S_N(\alpha) = \frac{\mu(q)}{\phi(q)} \sum_{1\le k\le N} e^{2i\pi k\left(\alpha - \frac{a}{q}\right)} + O\left(N\, e^{-c\sqrt{\operatorname{Log} N}}\right) ,$$

valable pour $c > 0$ où $\mu(q)$ désigne la fonction de Möebius et $\phi(q)$ le nombre d'entiers plus petits que q premiers avec q .

On considère P l'ensemble des nombres premiers ; on pose $P_N = P \cap [1, N]$ et $K_N = \frac{1}{|P_N|} \sum_{p \in P_N} \delta_{\{p\}}$.

Il y a une estimation

$$\left\| \frac{\operatorname{Log} N}{N} \sum_{p \in P_N} \delta_{\{p\}} - \frac{1}{N} \sum_{k \leq N} \Lambda(k)\, \delta_{\{k\}} \right\|_1 < \frac{C}{\operatorname{Log} N} ,$$

ce qui entraîne

$$\left| \hat{K}_N(\alpha) - \frac{1}{N} S_N(-\alpha) \right| < \frac{C}{\operatorname{Log} N} . \tag{3}$$

On peut remplacer $\hat{K}_N(\alpha)$ par $\frac{1}{N} S_N(-\alpha)$ et on utilise (1) et (2) exactement de la même manière que (5) et (8) dans la démonstration du Théorème 1.

6. LES AUTRES RÉSULTATS

Dans le même travail [B6], Bourgain démontre le

THÉORÈME 6.1.— *Soit $(X, \mathcal{A}, m, T)$ un système dynamique et $p(n)$ un polynôme à coefficients réels dont le terme de plus haut degré a un coefficient positif. Soit $f \in L^r(X)$, $r > 1$.*

Alors $\frac{1}{N} \sum_{k=1}^{N} f\left(T^{[p(k)]} x\right)$ converge p.s. quand $N \to +\infty$.

Il y a aussi une version de son théorème pour le cas d'une action de $\mathbf{Z}^\ell$ ([B1], [B6]).

THÉORÈME 6.2.— *Soient $T_1, T_2, \cdots T_\ell$ ℓ transformations préservant la mesure sur $(X, \mathcal{A}, m)$ et commutant deux à deux, et soient $p_1(n), p_2(n), \cdots p_\ell(n)$ ℓ polynômes à coefficients entiers. Soit $f \in L^r(X)$, $r > 1$. Alors*

$$\frac{1}{N} \sum_{n=1}^{N} T_1^{p_1(n)} T_2^{p_2(n)} \cdots T_\ell^{p_\ell(n)} f \quad \text{converge p.s. quand} \quad N \to +\infty .$$

Dans le cas de suites de densité positive où on a facilement le lemme maximal, sa technique peut être utilisée pour produire suffisamment de fonctions .

THÉORÈME 6.3 [B4][B5][B6].— *Soit* $(X, \mathcal{A}, m, T)$ *un système dynamique et* $A \in \mathcal{A}$, $m(A) > 0$. *Soit* $x \in X$ *et* $\Lambda_x = \{n \in \mathbf{N} \mid T^n x \in A\}$. *Alors, pour presque tout* x , Λ_x *est une suite sommante universelle i.e. : si* $\Lambda_x^N = \Lambda_x \cap [1, N]$, *pour tout système dynamique* $(Y, \mathcal{B}, \mu, S)$ *pour tout* $g \in L^1(Y)$

$$\frac{1}{|\Lambda_x^N|} \sum_{k \in \Lambda_x^N} g(S^k y) \quad \text{converge p.s. quand} \quad N \to +\infty \ .$$

Une démonstration "élémentaire" a été donnée par la suite par Furstenberg, Katznelson et Ornstein et se trouve en appendice dans [B6].

Répondant à une question de Furstenberg [F1], Bourgain a montré dans [B7] le

THÉORÈME 6.4.— *Si* T_1 *et* T_2 *sont deux puissances d'une même transformation* T *de* $(X, \mathcal{A}, m)$ *et* f_1 *et* f_2 *deux fonctions de* $L^2(X)$, *alors*

$$(1) \qquad \frac{1}{N} \sum_{1}^{N} f_1(T_1^n x)\, f_2(T_2^n x) \quad \text{converge p.s. quand} \quad N \to +\infty \ .$$

(Dans [Les], Lesigne avait démontré (1) dans les deux cas extrêmes où T est un K-système et où T est à spectre discret.)

BIBLIOGRAPHIE

[B] A. BELLOW - *Two problems in* Measure Theory, Oberwolfach 1981, Springer L.N.M., Vol. 945, 429-431.

[B-L] A. BELLOW and V. LOSERT - *The weighted pointwise ergodic theorem and the individual ergodic theorem along subsequences*, T.A.M.S. 1985, Vol. 288, 307-345.

[B1] J. BOURGAIN - *On the maximal ergodic theorem for certain subsets of the integers*, Israel Journal of Mathematics, Vol. 61, n° 1, 1988, 39-72.

[B2] J. BOURGAIN - *On the pointwise ergodic theorem on L^p for arithmetic sets*, Israel Journal of Mathematics, Vol. 61, n° 1, 1988, 73-84.

[B3] J. BOURGAIN - *An approach to pointwise ergodic theorems*, Springer L.N.M., Vol. 1317, 204-223.

[B4] J. BOURGAIN - *Return time sequences of dynamical systems*, preprint I.H.E.S., 1988.

[B5] J. BOURGAIN - *Temps de retour pour les systèmes dynamiques*, C.R.A.S., t. 306, Série I, 1988, 483-485.

[B6] J. BOURGAIN - *Pointwise ergodic theorems on arithmetic sets, with an appendix on return time sequences (jointly with H. Furstenberg, Y. Katznelson, D. Ornstein)*, Publications Mathématiques de l'I.H.E.S. n° 69, 1989, 5-45.

[B7] J. BOURGAIN - *Double recurrence and almost sure convergence*, preprint, 1988.

[C] R.P. CALDERON - *Ergodic theory and translation invariant operators*, Proc. Nat. Acad. Sci. U.S.A. 59, 1968, 349-353.

[B-K] A. BRUNEL and M. KEANE - *Ergodic theorems for operator sequences*, Z.F.W. 12 , 1969, 231-240.

[F1] H. FURSTENBERG - *Recurrence in ergodic theory and combinatorial number theory*, Princeton U.P., 1981.

[F2] H. FURSTENBERG - Proceedings of the Durham Conference, June 1982.

[Lep] D. LÉPINGLE - *La variation d'ordre p des semi-martingales*, Z.F.W. 36, 1976, 295-316.

[Les] E. LESIGNE - *Sur la convergence ponctuelle de certaines moyennes ergodiques*, C.R.A.S., Paris, t. 298, série I (1984).

[V] R.C. VAUGHAN - *The Hardy-Littlewood circle method*, Cambridge University Press, 1981.

[W] M. WIERDL - *Pointwise ergodic theorem along the prime numbers*, Israel Journal of Mathematics, Vol. 64, n° 3, 1988, 315-336.

Jean-Paul THOUVENOT

U.A. 224 du C.N.R.S.
Université Pierre et Marie Curie
Laboratoire de Probabilités
Tour 56 (3e étage)
4 place Jussieu
F-75252 PARIS CEDEX 05

Astérisque

JEAN-MARC DESHOUILLERS

L'étude des formes cubiques rationnelles via la méthode du cercle

Astérisque, tome 189-190 (1990), Séminaire Bourbaki, exp. n° 720, p. 155-177

<http://www.numdam.org/item?id=SB_1989-1990__32__155_0>

© Société mathématique de France, 1990, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Séminaire BOURBAKI mars 1990
42ème année, 1989-90, n° 720

L'ÉTUDE DES FORMES CUBIQUES RATIONNELLES VIA LA MÉTHODE DU CERCLE

[d'après **D.R. HEATH-BROWN, C. HOOLEY** et **R.C. VAUGHAN**](*)

par **Jean-Marc DESHOUILLERS**

On doit à Hardy, Littlewood et Ramanujan un outil puissant, la **méthode du cercle**, pour étudier les problèmes diophantiens de la forme $P(x_1, \cdots, x_s) = 0$ lorsque le nombre de variables est grand par rapport au degré du polynôme P. Les derniers avatars de cette méthode ont notamment permis à Heath-Brown de montrer que toute forme cubique rationnelle non-singulière en 10 variables représente 0, à Hooley de réduire le nombre de variables à 9 s'il n'y a pas d'obstruction locale, à Vaughan de donner une évaluation asymptotique du nombre de représentations d'un entier en sommes de 8 cubes, et une bonne minoration pour les représentations en sommes de 7 cubes.

SOMMAIRE

Introduction

§1. Abord heuristique : l'intégrale singulière

1.1 Expérimentation
1.2 Etude du nombre de représentations
1.3 Ecriture intégrale du nombre de représentations
1.4 Ordre de grandeur heuristique de $r_s(N)$

(*) The author thanks the Séminaire Bourbaki and the Séminaire de Théorie des Nombres de Bordeaux for allowing him to publish the English version of this text in the latter publication.

§2. Abord-p-adique : la série singulière

2.1 Nombre de solutions de la congruence $m_1^k + \cdots + m_s^k \equiv N \pmod{q}$

2.2 Interprétation de la série singulière

§3. Dissection de Farey classique : arcs majeurs, série et intégrale singulières

3.1 Contribution du premier arc majeur (α proches de 0)

3.2 Contribution des arcs majeurs : répartition des puissances dans les progressions arithmétiques

§4. Dissection de Farey classique : arcs mineurs

4.1 Majoration de Weyl : 13 cubes

4.2 Relation de Parseval : 9 cubes

4.3 Nombre de représentations en somme de huit cubes, d'après Vaughan

4.4 Nombre de représentations en somme de sept cubes

§5. Formes cubiques non diagonales

5.1 Une situation atypique : le cas des formes normiques

5.2 Le prolongement des arcs majeurs, d'après Vaughan

5.3 Intermède : la dissection de Farey-Kloosterman

5.4 Formes cubiques en 10 variables, d'après Heath-Brown

5.5 Formes cubiques en 9 variables, d'après Hooley

INTRODUCTION

Le problème de savoir si tout entier positif est somme de quatre carrés, peut-être soulevé par les Grecs, a été considéré par plusieurs mathématiciens aux XVII et XVIIIème siècles et finalement résolu par Lagrange en 1770. L'intérêt ainsi que la difficulté de cette question proviennent du mélange entre les lois d'addition et de multiplication des entiers.

Si des conjectures de ce type sont faciles à proposer, elles sont en revanche le plus souvent hors d'atteinte, mais source de développements mathématiques. D'importance historique sont le problème de Goldbach (1742), **tout entier pair est somme de deux nombres premiers** (le nombre 1 était alors décompté comme premier), et le problème de Waring

(1770), **tout entier est somme d'au plus 4 carrés, 9 cubes ou 19 bicarrés**, avec adjonction de points de suspension en 1782.

La Théorie additive des Nombres traite de ces questions ; notre propos est ici de présenter la **méthode du cercle** introduite en 1917 par Hardy et Ramanujan et perfectionnée quelques années plus tard par Hardy et Littlewood. Cet outil septuagénaire n'a rien perdu de sa vigueur ; on l'utilise toujours avec profit, tant pour obtenir des estimations asymptotiques, comme nous le verrons ici, que des évaluations numériques effectives et efficaces. C'est à travers l'étude -limitée- des formes diagonales (et principalement des formes cubiques diagonales), que nous effectuons cette présentation en suggérant quelques étapes de la démonstration des résultats suivants

Théorème 1.— *(D.R. Heath-Brown, 1982) Soit* $F(\mathbf{x}) = F(x_1, \cdots x_s)$ *une forme cubique non singulière à coefficients rationnels. Si* s *est au moins égal à 10, il existe* $\mathbf{x}$ *dans* $\mathbf{Q}^s \backslash \{0\}$ *tel que* $F(\mathbf{x}) = 0$.

Théorème 2.— *(C. Hooley, 1987) Soit* $F(\mathbf{x})$ *une forme cubique non singulière à coefficients rationnels en 9 variables. L'équation* $F(\mathbf{x}) = 0$ *a une solution rationnelle non triviale dans* $\mathbf{Q}$ *si et seulement si elle a une solution non triviale dans chaque corps p-adique* $\mathbf{Q}_p$.

Théorème 3.— *(R.C. Vaughan, 1985) Soit* $r_8(N)$ *le nombre de représentations de l'entier* N *en sommes de huit cubes d'entiers positifs. Lorsque* N *tend vers l'infini, on a*

$$r_8(N) = \mathfrak{S}(N) \frac{\Gamma(4/3)^8}{\Gamma(8/3)} N^{5/3} (1 + o(1)).$$

où

$$\mathfrak{S}(N) = \sum_{q=1}^{\infty} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \left\{ q^{-1} \sum_{m=1}^{q} \exp(2\pi i (am^3/q)) \right\}^8 \exp(-2\pi i a N/q).$$

On conjecture que la condition de non-singularité peut être levée dans l'énoncé du Théorème 1. Davenport a établi en 1963 que toute forme cubique rationnelle en au moins 16 variables représente 0 ; même dans le

cas des formes non singulières, c'était le meilleur résultat connu avant le travail de Heath-Brown. La condition locale est indispensable dans le cas des formes nonaires, comme l'a montré Mordell en 1936. Le Théorème 3 était une conjecture favorite de Davenport qui, m'a-t-on dit, la proposait systématiquement à ses élèves.

Pour clore cette introduction, signalons les travaux de Colliot-Thélène, Sansuc et Swinnerton-Dyer, 1986 (on pourra consulter Colliot-Thélène, 1986, pour une présentation générale). Abordant le problème par la géométrie algébrique, ils parviennent notamment aux meilleurs résultats actuellement connus sur les systèmes de formes quadratiques. Pour ce qui est des formes cubiques, ce type de méthode permet d'établir le résultat suivant, que l'on comparera avec profit au Théorème 2 (moins de variables, mais des conditions géométriques plus subtiles).

Théorème 4.— *(J.-L. Colliot-Thélène et P. Salberger, 1988). Soit K un corps de nombres et $X \subset \mathbf{P}^n_K$ une hypersurface cubique définie sur K, avec $(n \geq 3)$. Si X contient un ensemble de 3 points singuliers conjugués, et si X admet des points rationnels sur tous les complétés de K, alors X admet un point rationnel sur K.*

§1 ABORD HEURISTIQUE : L'INTÉGRALE SINGULIÈRE

1.1 Expérimentation

Observons une table donnant, pour chaque entier N jusqu'à 40 000 le nombre minimal de termes intervenant dans la décomposition de N en somme de cubes positifs : les nombres 23 et 239 sont les seuls à nécessiter 9 cubes ; quinze autres entiers, dont le plus grand est 8402, nécessitent 8 cubes, et tous les autres au plus 7 cubes. Si l'on poursuivait cette table jusque vers 10^{15}, on en retirerait l'impression qu'à partir d'un certain rang, 4 cubes seulement sont suffisants !... Ainsi, il semble plus facile de représenter les grands entiers que les petits.

1.2 Étude du nombre des représentations

Cet aspect n'était pas pris en compte dans les travaux développés dans la seconde moitié du XIXème siècle, de Liouville qui montre en 1859 que tout nombre est somme d'au plus 53 bicarrés, à Hilbert qui montre en 1909 que tout entier est somme d'un nombre fini (ne dépendant que de k) de puissances k-ièmes et à Kempner qui complète un travail de Wieferich et établit en 1912 que tout nombre est somme d'au plus 9 cubes.

La méthode du cercle, introduite par Hardy et Littlewood dans le contexte du problème de Waring, prend en compte cette plus grande facilité à représenter de grands entiers : pour savoir si l'entier N est représentable comme somme de s puissances k-ièmes, ils cherchent à déterminer le **comportement asymptotique du nombre de représentations** de N comme somme de s puissances k-ièmes. De ce point de vue, ils ne s'intéressent qu'aux entiers assez grands, et de là provient le succès de leur méthode.

1.3 Ecriture intégrale du nombre de représentations

Commençons par fixer quelques notations :

k désigne un entier supérieur ou égal à 2. On pourra se limiter à ne considérer que la valeur 3 pour k.

N désigne un entier, qui sera amené à tendre vers l'infini.

Pour s entier positif, on note $r_s(N)$ le nombre de représentations de N en somme de s puissances k-ièmes.

$e(\cdot)$ désigne l'exponentielle complexe $\exp(2\pi i\cdot)$

Le lecteur n'aura aucune peine à donner une démonstration de la relation

$$1.3.a \qquad r_s(N) = \int_{\mathbf{R}/\mathbf{Z}} \Big(\sum_{0 \le n^k \le N} e(\alpha n^k) \Big)^s e(-\alpha N) d\alpha$$

en se fondant soit sur l'orthogonalité des caractères $e(h\cdot)$, soit sur la formule intégrale de Cauchy. Nous en donnons ici une présentation probabiliste, dont nous ne mentionnons que pour mémoire l'intérêt pour certain calcul explicite (Deshouillers, 1985).

On considère s variables aléatoires indépendantes $X_1, \cdots, X_s$ de loi commune $\lambda \sum_{n \leq N^{1/k}} \delta(n)$, où $\delta(a)$ désigne la mesure de Dirac en a, et le facteur de normalisation λ vaut $[N^{1/k}+1]^{-1}$. Chaque variable aléatoire X_i^k a pour loi $\lambda \sum_{n \leq N^{1/k}} \delta(n^k)$. La loi de la variable aléatoire $X := X_1^k + \cdots + X_s^k$ est la puissance s-ième de convolution de la loi commune de X_i^k ; elle vaut donc $\lambda^s \sum_m r_s^*(m)\delta(m)$, où $r_s^*(m)$ est le nombre de façons d'écrire m comme somme de s puissances k-ièmes au plus égales à N ; le coefficient $r_s^*(m)$ s'obtient de façon classique à partir de la fonction génératrice (ou série de Fourier) de X, qui est la puissance s-ième de celle de X_1^k. La formule 1.3.a découle de cela et de l'égalité banale de $r_s(N)$ et $r_s^*(N)$.

1.4 Ordre de grandeur heuristique de $r_s(N)$

On donne une approximation continue du problème considéré : on considère s variables aléatoires indépendantes $Z_1, \cdots, Z_s$ de loi uniforme sur $[0, N^{1/k}]$ et on note Z la somme $Z_1^k + \cdots + Z_s^k$. La fonction caractéristique (alias transformée de Fourier) de Z est la puissance s-ième de celle de Z_1^k ; par transformation de Fourier inverse, on obtient la densité $\rho_s(t)$ de Z au point t :

$$\rho_s(t) = \int_{-\infty}^{\infty} \Big(\int_0^{N^{1/k}} e(\beta x^k) dx \Big)^s e(-\beta t) d\beta \tag{1.4.a}$$

Le membre de droite s'appelle l'**intégrale singulière**. Par changement de variables, on obtient dans le cas où t vaut N :

$$\rho_s(N) = \frac{\Gamma(1+1/k)^s}{\Gamma(s/k)} N^{s/k-1}, \tag{1.4.b}$$

car on a

$$\int_{-\infty}^{\infty} \Big(\int_0^1 e(\gamma \xi^k) d\xi \Big)^s e(-\gamma) d\gamma = \frac{\Gamma(1+1/k)^s}{\Gamma(s/k)}. \tag{1.4.c}$$

Ainsi, la valeur moyenne de $r_s(N)$ est-elle $N^{s/k-1}$ à un facteur eulérien près. On notera la présence de l'intégrale singulière dans la formule asymptotique pour le nombre de représentations en somme de 8 cubes (cf. Théorème 3).

§2 ABORD p-ADIQUE : LA SÉRIE SINGULIÈRE

Après avoir expliqué la présence de l'intégrale singulière dans le théorème 3, nous allons interpréter la **série singulière** $\mathfrak{S}(N)$, selon la terminologie introduite par Hardy et Littlewood.

2.1 Nombre de solutions de la congruence $m_1^k + \cdots + m_s^k \equiv N \pmod{q}$

Notons $M(q)$ le nombre de solutions de la congruence considérée. L'égalité

$$2.1.a \qquad M(q) = \frac{1}{q} \sum_{r=1}^{q} \left(\sum_{m=1}^{q} e(rm^k/q) \right)^s e(-rN/q)$$

qui s'obtient aisément à partir des relations d'orthogonalité

$$\frac{1}{q} \sum_{r=1}^{q} e(rh/q) = \begin{cases} 1 & \text{si} \quad q \mid h \\ 0 & \text{si} \quad q \nmid h, \end{cases}$$

est l'équivalent, dans $\mathbf{Z}/q\mathbf{Z}$, de l'expression intégrale 1.3.a . En réordonnant les termes du membre de droite de 2.1.a en fonction de la valeur de (r, q), on a

$$M(q) = \frac{1}{q} \sum_{d \mid q} \sum_{\substack{a=1 \\ (a,d)=1}}^{d} \left(\frac{q}{d} \sum_{m=1}^{d} e(am^k/d) \right)^s e(-aN/d),$$

ou encore

$$2.1.b \qquad M(q) = q^{s-1} \sum_{d \mid q} G(d) \ ,$$

où

$$G(d) = \sum_{\substack{a=1 \\ (a,d)=1}}^{d} \{d^{-1} \sum_{m=1}^{d} e(am^3/d)\}^s e(-aN/d).$$

Voilà qui commence à fleurer le théorème 3 !

2.2 Interprétation de la série singulière

La multiplicativité de la fonction G (qui découle directement du théorème chinois, ou indirectement via la relation 2.1.b), permet d'écrire la série singulière

$$\mathfrak{S}(N) = \sum_{q=1}^{\infty} G(q)$$

comme un produit eulérien

$$\mathfrak{S}(N) = \prod_{p} \sum_{h=0}^{\infty} G(p^h) \ .$$

Par la relation 2.1.b, on a donc

2.2.a $$\mathfrak{S}(N) = \prod_{p} \lim_{\ell \to \infty} p^{\ell(1-s)} M(p^\ell) \ .$$

En remarquant que $p^{\ell(s-1)}$ est le cardinal d'un hyperplan dans $(\mathbf{Z}/p^\ell\mathbf{Z})^s$, on interprète chaque facteur de $\mathfrak{S}(N)$ comme une densité des solutions de $x_1^k + \cdots + x_s^k = N$ dans $\mathbf{Z}_p$.

Le lecteur sera peut-être tenté d'aller plus loin dans cette direction : nous lui recommandons la lecture de Lachaud, 1982, pour une présentation adélique de la méthode du cercle.

§3 DISSECTION DE FAREY CLASSIQUE : ARCS MAJEURS, SÉRIE ET INTÉGRALE SINGULIÈRES

Nous abordons maintenant le calcul de $r_s(N)$ à partir de la représentation intégrale 1.3.a . L'expression cruciale figurant dans l'intégrande est la somme exponentielle

3.0.a $$S(\alpha) := \sum_{n \le P-1} e(\alpha n^k) \quad , \quad \text{où} \quad P := \lfloor N^{1/k} + 1 \rfloor$$

Son module est clairement maximal lorsque α est entier ; nous commencerons par étudier la contribution à $r_s(N)$ des α proches de 0 dans $\mathbf{R}/\mathbf{Z}$, ou encore proches de 0 dans $\mathbf{R}$ en identifiant $\mathbf{R}/\mathbf{Z}$ à un voisinage de 0.

3.1 Contribution du premier arc majeur (α proches de 0)

Puisque $S(\alpha)$ est une fonction continue de α et que $S(\alpha) = P$ (cette égalité justifie la gaucherie de la définition de P), l'analyse nous permet d'évaluer $S(\alpha)$ pour α proche de 0.

Supposons effectivement que $|\alpha| \leq \varepsilon N^{-1}$, où ε est n'importe quelle fonction de N tendant vers 0 à l'infini. Par la formule de Taylor, on a :

$$S(\alpha) = P + o(P) \quad \text{et} \quad e(-\alpha N) = 1 + o(1), \quad \text{d'où}$$

$$\int_{-\varepsilon N^{-1}}^{\varepsilon N^{-1}} S(\alpha)^s e(-\alpha N) d\alpha = 2\varepsilon N^{-1} P^s (1 + o(1))$$

$$= 2\varepsilon N^{s/k-1}(1 + o(1)).$$

Il est remarquable que la contribution à $r_s(N)$ d'un tel intervalle autour de 0 soit de l'ordre de grandeur de la valeur heuristique.

En fait, nous avons utilisé la formule de Taylor qui est quelque peu sommaire (ne l'enseignons-nous pas à nos étudiants dès la première année ?). La formule sommatoire de Poisson (quand l'enseignons-nous à nos étudiants ?) est un outil beaucoup plus efficace. Posons

$$f(x) := \begin{cases} e(\alpha x^k) & \text{pour} \quad 0 \leq x \leq P \\ 0 & \text{sinon} \end{cases}$$

et notons $\hat{f}$ sa transformée de Fourier ($\hat{f}(t) = \int_{-\infty}^{\infty} f(x) e(xt) dx$) ; on a

$$\sum_{n \in \mathbf{Z}} f(x) = \sum_{\nu \in \mathbf{Z}} \hat{f}(\nu) + \mathrm{O}(1) \ ,$$

et donc

$$3.1.a \qquad S(\alpha) = \sum_{\nu \in \mathbf{Z}} \int_0^P e(\alpha x^k + \nu x) dx + \mathrm{O}(1).$$

Lorsque $|\alpha|$ est assez petit ($k|\alpha|P^{k-1} \leq 1/2$), la fonction $e(\alpha x^k + \nu x)$ oscille sur l'intervalle $[0, P]$ pour $\nu \neq 0$, et l'intégrale $\int_0^P e(\alpha x^k + \nu x) dx$ est petite,

comme on le voit en intégrant par parties ; il n'est pas difficile de montrer que l'on a

3.1.*b* $$S(\alpha) = \int_0^P e(\alpha x^k)dx + \mathrm{O}(1)$$

c'est alors un calcul de routine de vérifier que, pour $s \geq k+1$, la contribution de l'intervalle

3.1.*c* $$\mathfrak{M}_{0,1} := \{\alpha/|\alpha| \leq (2kP^{k-1})^{-1}\}$$

est équivalente à $\rho_s(N)$, le nombre moyen de représentations. (cf. 1.4.a et 1.4.b) !

3.2 Contribution des arcs majeurs : répartition des puissances dans les progressions arithmétiques

Dans le paragraphe 2.2, nous avons réécrit la série singulière en terme du nombre de solutions des congruences $x_1^k + \cdots + x_s^k \equiv N \pmod q$. Nous voulons ici expliquer comment la moyenne des sommes de Gauss que nous avons notée $G(q)$ intervient lorsque l'on étudie la contribution à $r_s(N)$ de petits intervalles centrés aux rationnels de dénominateur q.

Commençons par évaluer $S(a/q)$; on a

$$S(a/q) = \sum_{n\leq P-1} e(an^k/q) = \sum_{m=1}^{q} \sum_{\substack{n\leq P-1 \\ n\equiv m (\mathrm{mod} q)}} e(an^k/q)$$

$$= \sum_{m=1}^{q} e(am^k/q) \sum_{\substack{n\leq P-1 \\ n\equiv m (\mathrm{mod} q)}} 1 = \frac{P}{q} \sum_{m=1}^{q} e(am^k/q) + \mathrm{O(q)}$$

Or la somme de Gauss $\sum_{m=1}^{q} e(am^k/q)$ n'a aucune raison d'être nulle (ainsi, pour $k = 3$ et $a/q = 1/4$, elle vaut 2) ; cela correspond aux irrégularités de répartition des puissances k-ièmes dans les progressions arithmétiques. Il en résulte que $S(a/q)$ a (parfois) un ordre de grandeur comparable à $S(0)$. On étudie alors le comportement local de S en a/q comme en 0 : on introduit les **arcs majeurs**

3.2.*a* $$\mathfrak{M}_{a,q} := \{\alpha/|\alpha - \frac{a}{q}| \leq (2kP^{k-1}q)^{-1}\} ,$$

où $0 < a < q$, $(a,q) = 1$ et $q \leq Q$. Disons à ce stade que le choix de Q n'a pas une très grande importance ; on prend généralement une puissance de P, e.g. P lui même. Notons dès maintenant que le choix d'un Q supérieur à P est possible, mais demande beaucoup de délicatesse : cela revient à étudier la répartition d'un ensemble de P entiers dans les classes modulo un entier supérieur à P.

La formule sommatoire de Poisson permet d'approcher

$$S(\alpha) \quad \text{par} \quad \left(\frac{1}{q}\sum_{m=1}^{q} e(am^k/q)\right)\int_0^P e((\alpha - \frac{a}{q})x^k)dx \quad \text{sur} \quad \mathfrak{M}_{a,q} .$$

En regroupant les contributions des différents arcs majeurs (on note $\mathfrak{M}$ leur réunion) on a

Proposition.— *Pour $s \geq 4k$ (et $s \geq 4$ dans le cas des cubes), il existe un réel A strictement positif, tel que l'on ait, lorsque N tend vers l'infini*

$$3.2.b \quad \int_{\mathfrak{M}} S(\alpha)^s e(-\alpha N)d\alpha = (1 + o(1))\rho_s(N).\mathfrak{S}(N) \quad \textit{avec} \quad \mathfrak{S}(N) \geq A .$$

On rappelle que $\rho_s(N) = \frac{\Gamma(1+1/k)^s}{\Gamma(s/k)} N^{s/k-1}$.

§4 DISSECTION DE FAREY CLASSIQUE : ARCS MINEURS

Bien qu'elle soit la substance d'une mise en oeuvre traditionnelle de la méthode du cercle, nous traitons sommairement cette partie qui dépend fondamentalement de la nature diagonale des formes impliquées dans le problème de Waring.

La réunion des arcs majeurs ne peut recouvrir tout $\mathbf{R}/\mathbf{Z}$; une façon simple de le voir est de mesurer la longueur totale des arcs majeurs. Considérons le cas des cubes, on a

$$|\mathfrak{M}| = \sum_{q \leq Q} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \frac{1}{3P^2 q} \leq \frac{Q}{3P^2} ;$$

non seulement la longueur des arcs majeurs est inférieure à 1, mais encore elle tend vers 0 quand N tend vers l'infini ! On appelle **arcs mineurs** le complémentaire des arcs majeurs et on le note $\mathfrak{m}$.

4.1 Majoration de Weyl : 13 cubes

La somme $S(\alpha)$, pour α irrationnel, a été considérée sous un angle "dual" par Weyl en 1916 : pour α donné et P tendant vers l'infini, il a montré que la quantité $S(\alpha)/P$ tend vers 0. De ce point de vue que nous ne développons pas ici, cela correspond au fait que les nombres αn^3 sont "uniformément répartis" dans $\mathbf{R}/\mathbf{Z}$. La méthode de Weyl pour majorer $|S(\alpha)|$ conduit à la majoration valable dans le cas des cubes et pour tout $\varepsilon > 0$:

$$4.1.a \qquad |S(\alpha)| = O_\varepsilon(P^{3/4+\varepsilon}) \quad \text{uniformément pour} \quad \alpha \in \mathfrak{m}$$

(Pour les puissances k-ièmes, l'exposant est $1 - 2^{1-k}$).

De la majoration 4.1.a, on déduit aisément

$$4.1.b \qquad \Big| \int_{\mathfrak{m}} (S(\alpha))^s e(-\alpha N) d\alpha \Big| = O_\varepsilon(P^{3s/4+\varepsilon}) \ .$$

En regroupant ce résultat avec 3.2.b (contribution des arcs majeurs), on obtient un équivalent pour le nombre de représentations en somme de s cubes dès que

$$s - 3 > 3s/4 \ ,$$

c'est-à-dire dès que s est strictement supérieur à 12. On obtient de même un équivalent pour le nombre de représentations en somme de $k2^{k-1} + 1$ puissances $k$ièmes.

4.2 Relation de Parseval : 9 cubes

La force de la relation 4.1.a ne réside pas tant dans l'exposant (on aimerait bien remplacer 3/4 par 1/2, majoration probabiliste de la marche aléatoire des $e(\alpha n^3)$), que dans son uniformité sur $\mathfrak{m}$. Or cette uniformité est gaspillée dans l'application que l'on en donne en 4.1.b, où la norme ℓ^s est recherchée. La relation de Parseval nous donne l'exposant $s/2$ dans la relation 4.1.b, au moins pour $s = 2$, ce qui est banal, et $s = 4$, ce qui est un peu plus subtil : l'identité $x^3 + y^3 = (x + y)(x^2 - xy + y^2)$ permet de majorer $r_2(n)$ par le nombre de diviseurs de n, d'où la majoration

4.2.*a* $$r_2(n) = \mathrm{O}_\varepsilon(\mathrm{n}^\varepsilon) \ .$$

On peut alors écrire, pour $s \geq 4$:

$$\int_{\mathfrak{m}} |S(\alpha)|^s d\alpha \leq \max_{\alpha \in \mathfrak{m}} |S(\alpha)|^{s-4} \int_0^1 |S(\alpha)|^4 d\alpha$$

d'où l'on déduit un équivalent pour le nombre de représentations en somme de s cubes dès que

$$s - 3 > \frac{3}{4}(s-4) + \frac{4}{2} \ ,$$

c'est-à-dire dès que s est strictement supérieur à 8, et puisque s est entier, cela signifie seulement $s \geq 9$.

Dans le cas des puissances k-ièmes, Hua a généralisé la relation de Parseval et obtenu la majoration

4.2.*b* $$\int_0^1 |S(\alpha)|^{2^k} d\alpha = \mathrm{O}_{\varepsilon,\mathrm{k}}(\mathrm{P}^{2^\mathrm{k}-\mathrm{k}+\varepsilon}) \ .$$

d'où un équivalent pour $r_s(N)$ lorsque $s \geq 2^k + 1$. C'est seulement pour mémoire que nous mentionnons ici les améliorations de Vinogradov (amélioration du Lemme de Weyl pour $k \geq 12$), de Heath-Brown (amélioration de l'inégalité de Hua pour $k \geq 6$), de Vinogradov, Davenport, Vaughan et autres (résolubilité de $x_1^k + \cdots + x_s^k = N$, sans équivalent de $r_s(N)$).

4.3 Nombre de représentations en somme de huit cubes : le théorème 3

Reprenons l'inégalité de Hua 4.2.b pour les cubes. Elle implique

$$\int_0^1 |S(\alpha)|^8 d\alpha = \mathrm{O}_\varepsilon(\mathrm{P}^{5+\varepsilon}) ,$$

alors que la contribution des arcs majeurs est de l'ordre de P^5. Comme Hooley l'a remarqué, la considération en moyenne des fonctions de diviseurs permettent de remplacer le terme P^ε par une puissance de $\log P$; un résultat de Hall et Tenenbaum conduit même à

4.3.*a* $$\int_0^1 |S(\alpha)|^8 d\alpha = \mathrm{O}_\varepsilon(\mathrm{P}^5(\log \mathrm{P})^\varepsilon),$$

et donc à

4.3.*b* $$r_8(N) = \mathrm{O}_\varepsilon(\mathrm{N}^{5/3}(\log \mathrm{N})^\varepsilon) .$$

Le théorème 3 découle directement de l'existence d'un réel $C > 0$ tel que l'on ait

4.3.*c* $$\int_{\mathfrak{m}} |S(\alpha)|^8 d\alpha = \mathrm{O}(\mathrm{P}^5(\log \mathrm{P})^{-c})$$

On notera combien faible est la marge entre les majorations 4.3.a et 4.3.b. Pour la franchir, Vaughan introduit plusieurs dissections : sur $\mathfrak{m}$, selon les propriétés diophantiennes des α, et sur les entiers de 0 à P (sur lesquels est effectuée la somme $S(\alpha)$), selon leurs propriétés arithmétiques. Il se ramène alors à de nouvelles équations diophantiennes avec un gain global d'un logarithme si l'on sait évaluer le nombre de leurs solutions ; des majorations du type 4.3.b sont alors suffisantes pour conserver les avantages acquis : on peut ainsi prendre pour c tout réel inférieur à 1 dans 4.3.c .

4.4 Nombre de représentations en somme de sept cubes

Cette méthode itérative est à la base de la minoration

4.4.*a* $$r_7(N) \geq cN^{4/3},$$

pour un réel $C > 0$ et tout entier N assez grand, obtenue par Vaughan, 1987. R.C. Baker et J. Brüdern ont récemment étendu ce résultat aux formes diagonales en 7 variables.

Linnik, 1942 a démontré la positivité de $r_7(N)$, pour tout N assez grand, par des considérations différentes (formes quadratiques ternaires, répartition des nombres premiers dans les progressions arithmétiques).

L'évaluation asymptotique de $r_7(N)$ a été conditionnellement établie par Hooley, 1984 sous l'hypothèse de Riemann pour certaines fonctions L globales de Hasse-Weil.

§5 FORMES CUBIQUES NON DIAGONALES

5.1 Une situation atypique : le cas des formes normiques

Comme nous venons de le voir, ce n'est que très récemment que l'on a su adapter la méthode du cercle pour démontrer que tout entier assez grand est somme de sept cubes. Le résultat de Davenport sur les formes cubiques en 16 variables, mentionné dans l'introduction, et les théorèmes 1 et 2 laissent penser que les formes générales sont plus délicates à manipuler. Le théorème 4 montre l'utilisation qui peut être faite de certaines particularités géométriques. Il est également possible de tenir compte de certaines particularités algébriques, comme en témoigne le résultat suivant qui concerne des formes cubiques en 7 variables (et plus généralement des formes de degré k en $2k+1$ variables).

Théorème 5.— *(B.J. Birch, H. Davenport, D.J. Lewis, 1962) Soient K_1 (resp. K_2) un corps cubique et $N_1(x_1, y_1, z_1)$ (resp. $N_2(x_2, y_2, z_2)$) la forme normique par rapport à une base d'entiers donnée. Si l'équation*

$$N_1(x_1, y_1, z_1) + N_2(x_2, y_2, z_2) + t^3 = N$$

admet une solution non singulière pour tout nombre premier p qui divise $d(K_1)d(K_2)$ (produit des discriminants de K_1 et K_2), alors elle admet une infinité de solutions en entiers rationnels.

Par des méthodes de crible, H. Iwaniec a même obtenu des résultats sur le nombre de représentations par certaines formes cubiques en 6 variables. Pour la simplicité, nous ne citons qu'un corollaire de son résultat :

Théorème 6.— *(H. Iwaniec, 1977) Soit $K/\mathbf{Q}$ une extension cubique galoisienne ; on note N_K la forme normique par rapport à une base d'entiers donnée. (Il existe un entier D et une famille H de classes modulo D tels qu'un nombre premier p se décompose totalement dans K si et seulement si p est congru à un élément de H modulo D).*

Tout entier pair assez grand et congru modulo D à la somme de deux éléments de H, est représentable par la forme $N_K(x_1, y_1, z_1)+N_K(x_2, y_2, z_2)$.

5.2 Le prolongement des arcs majeurs, d'après Vaughan

Dans les quatre premiers chapitres, nous n'avons considéré que des formes **diagonales**. Toute la partie concernant les arcs majeurs peut en fait s'étendre aux formes non diagonales, via la transformation de Fourier sur $\mathbf{Z}^s$. La première utilisation vraiment cruciale de l'aspect diagonal n'est intervenue que dans l'inégalité de Weyl (formule 4.1.a).

A la fin des années 1970, Vaughan a remarqué que le choix de l'arc majeur $\mathfrak{M}_{0,1}$ effectué en 3.1.c n'était commandé que par le souci de négliger le nombre maximal de termes dans la formule sommatoire de Poisson 3.1.a et obtenir la relation 3.1.b . Si l'on choisit un arc majeur plus grand, la fonction $e(\alpha x^k + \nu x)$ n'oscille plus nécessairement, et il faut conserver d'autant plus de termes que l'arc majeur est prolongé. Un agrandissement raisonnable permet encore de contrôler la somme $\sum_{N_1<\nu<N_2} \int_0^P e(\alpha x^k + \nu x)dx$, dans laquelle chaque terme est traité par la méthode de la phase stationnaire (développement limité autour du point où $k\alpha x^{k-1}+\nu$ s'annule, conduisant à une intégrale de Fresnel). Bilan : dans le cas des cubes, on récupère exactement l'exposant 3/4 de la majoration de Weyl, tandis que pour les puissances supérieures, on trouve un exposant supérieur ou égal à 1, ce qui présente peu d'intérêt. Signalons tout de même une utilisation de l'idée de Vaughan pour les bicarrés, dans un contexte où une certaine subtilité numérique était recherchée (Deshouillers, 1985). Autre avantage, la méthode de Vaughan permet d'écrire $S(\alpha)$ comme une somme

trigonométrique qui, traitée trivialement, conduit à la majoration de Weyl ; mais rien n'interdit de conserver explicite ladite somme exponentielle, en vue de futures compensations. Le lecteur, je le remercie d'être encore du voyage, devrait être désormais convaincu que, de même que "13 cubes" provient de la seule majoration de Weyl, on doit pouvoir démontrer le Théorème 1 pour une forme non-singulière en 13 variables à partir d'une bonne connaissance des sommes de Gauss généralisées (Théorème de Deligne !).

Avant d'expliquer d'où vient le gain de 3 variables supplémentaires, je signale l'utilisation faite par Cherly, 1989 de la méthode de Vaughan pour obtenir une inégalité du type Weyl pour les sommes trigonométriques cubiques sur $\mathbf{F}_2[X]$, impossible à obtenir par la méthode classique, puisque dans $\mathbf{F}_2$, on a $3! = 0$.

5.3 Intermède : la dissection de Farey-Kloosterman

Si l'on tient à garder explicites les sommes trigonométriques considérées, pour tout $\alpha \in \mathbf{R}/\mathbf{Z}$, il faut obtenir une **partition** de $\mathbf{R}/\mathbf{Z}$ en arcs majeurs. En étudiant les formes quadriques diagonales en quatre variables, Kloosterman a rencontré la même difficulté il y a un peu plus de soixante ans. La solution qu'il y a apportée se trouvera être une des clefs des Théorèmes 1 et 2. Elle mérite d'autant plus d'être présentée que Kloosterman lui-même l'a réutilisée pour obtenir la première majoration non triviale des coefficients de Fourier de formes modulaires paraboliques holomorphes ; repolie par Petersson, cette idée devait ultérieurement se développer dans les travaux de Selberg, Kuznecov, Iwaniec *et al.* pour étudier les sommes de Kloosterman en moyenne (via les formes modulaires non holomorphes), mettant en oeuvre ce que Hooley redécouvre dans un contexte différent et nomme "double Kloosterman reffinement".

A la suite de Farey d'ordre Q, c'est-à-dire l'ensemble des rationnels $\frac{a}{q}$ de $\mathbf{R}/\mathbf{Z}$, avec $(a,q) = 1$ et $q \leq Q$, Kloosterman associe la partition

5.3.a
$$\mathbf{R}/\mathbf{Z} = \coprod_{q \leq Q} \coprod_{\substack{a=1 \\ (a,q)=1}}^{q} \mathfrak{M}'_{a,q} ,$$

où

5.3.*b* $$\mathfrak{M}'_{a,q} = \left]\frac{a+a'}{q+q'}\ ,\ \frac{a+a''}{q+q''}\right] \ ;$$

on a noté $\frac{a'}{q'}$ et $\frac{a''}{q''}$ les voisins de $\frac{a}{q}$ dans la suite de Farey d'ordre Q.

Le défi consiste à déterminer les extrémités de $\mathfrak{M}'_{a,q}$ connaissant seulement a et q ! Pour cela, on utilise la propriété fondamentale de la suite de Farey :

5.3.*c* $$aq' - a'q = 1$$

Cela implique que l'on a

$$\mathfrak{M}'_{a,q} = \left]\frac{a}{q} - \frac{1}{q(q+q')}, \frac{a}{q} + \frac{1}{q(q+q'')}\right],$$

où la référence à a' et a'' a disparu.

Il reste à exprimer q' (et de même q'') en terme de a et q uniquement. On commence par remarquer que q' est bien localisé dans un intervalle de longueur q ; on a en effet

5.3.*d* $$Q < q + q' \leq Q + q$$

(la minoration provient de ce que $\frac{a}{q}$ et $\frac{a'}{q'}$ sont voisins dans la suite de Farey d'ordre Q, et donc $\frac{a+a'}{q+q'}$ n'appartient à cette suite).

Kloosterman remarque alors que la relation 5.3.c permet de localiser q' modulo q ; en notant $\bar{a}$ l'inverse de a modulo q, on a

5.3.*e* $$q' \equiv \bar{a} (\mathrm{mod} q)$$

Les deux relations 5.3.d et 5.3.e déterminent parfaitement q', et donc l'extrémité gauche de $\mathfrak{M}'_{a,q}$, en terme de a et q uniquement. On procède de même pour l'extrémité droite.

On notera que la partition de $\mathbf{R}/\mathbf{Z}$ considérée (5.3.a) présente cet aspect désagréable que les arcs $\mathfrak{M}'_{a,q}$ relatifs au même q ont des longueurs

différentes. Pour pouvoir cependant les surperposer, Kloosterman développe leurs fonctions indicatrices en série de Fourier, introduisant un terme $\psi_q(\bar{a})$, où ψ_q est un caractère additif modulo q. Le cas le plus simple conduit aux sommes de Kloosterman

5.3.f $$K(m,n;q) := \sum_{a \bmod q}^{*} e(\frac{m\bar{a}+na}{q})$$

pour lesquelles il donne une majoration non triviale.

5.4 Formes cubiques en 10 variables, d'après Heath-Brown

Les acteurs sont maintenant en place ! Soit F une forme cubique et P un nombre réel positif. L'intégrale

5.4.a $$r_F(P) = \int_0^1 (\sum_{\|\mathbf{x}\|_\infty \leq P} e(\alpha F(\mathbf{x})))d\alpha$$

donne le nombre de solutions de l'équation $F(\mathbf{x}) = 0$, sous la condition $\|\mathbf{x}\|_\infty \leq P$. Si l'on montre que $r_F(P) > 1$ pour un certain P (par exemple en obtenant un équivalent, ou une minoration asymptotique de $r_F(P)$), on en déduit que l'équation $F(\mathbf{x}) = 0$ admet une solution non triviale.

On utilise alors la partition de Farey-Kloosterman (5.3.a), d'ordre $P^{3/2}$ (on se souviendra de la remarque introduite après la définition 3.2.a) : sur chaque arc majeur, on transforme la somme $\sum_{\|\mathbf{x}\|_\infty \leq P} e(\alpha F(\mathbf{x}))$ par la formule sommatoire de Poisson. Les contributions des arcs majeurs de même dénominateur sont alors regroupées par la méthode de Kloosterman. Bilan de l'opération : yaka évaluer les sommes

5.4.b $$S_u(q;\mathbf{b}) := \sum_{s=1}^{q}{}^{*} \sum_{\mathbf{c} \bmod q} e(\bar{s}F(\mathbf{c}) + us - \mathbf{b}.\mathbf{c}).$$

Si la voie est clairement tracée sur la carte (à nous Deligne !), la situation sur le terrain est bien plus rocailleuse et embroussaillée. Voici les deux obstacles majeurs que doit contourner Heath-Brown :

- Avec l'aide de Katz, il majore $|S_u(p;\mathbf{b})|$ par $O(p^{(n+1)/2})$, ce qui est la compensation maximale espérée. La difficulté provient du terme $\bar{s}$ dans

5.4.b, ce qui complique la nature de la variété sur laquelle est effectuée la sommation (prisme à base hyperbolique), et donc la majoration de S_u, même dans la meilleure hypothèse où F est non-singulière.

- Le traitement des sommes $S_u(p^\ell; \mathbf{b})$, pour $\ell > 1$, est en principe plus simple ; malheureusement, la compensation maximale espérée pour $S_u(p^\ell; \mathbf{b})$ n'a pas toujours lieu. Heath-Brown montre que ce cas n'est pas très fréquent (on pourra aussi consulter S. Cohen, 1979) ce qui prouve qu'en moyenne, on peut majorer $|S_u(q; \mathbf{b})|$ par $O(q^{(n+1)/2+\varepsilon})$.

De fait, ce n'est pas l'intégrale 5.4.a qui est considérée, mais une version pondérée

$$\int_0^1 (\sum_{\|\mathbf{x}\|} w(\mathbf{x}) e(\alpha F(\mathbf{x}))) d\alpha \ ,$$

où le poids lisse w fait bien meilleur ménage avec la transformation de Fourier que la fonction indicatrice de la boite $\|\mathbf{x}\| \leq P$.

5.5 Formes cubiques en 9 variables, d'après Hooley

Cette section entretient avec la précédente une relation similaire à celle qui connecte la section 4.3 (somme de 8 cubes) à la section 4.2 (somme de s cubes pour $s > 8$).

Un premier effort consiste à poursuivre la méthode de Heath-Brown pour traiter les sommes $S_u(k; \mathbf{b})$ avec autant d'efficacité lorsque k est le carré d'un nombre sans facteur carré, que lorsque k est lui-même sans facteur carré ; le cas des puissances d'exposant supérieur à 2 peut alors être traité de façon élémentaire dans la plupart des cas. On gagne ainsi un facteur de l'ordre d'une puissance de P.

Quelques puissances du logarithme de P sont également économisées : les unes en choisissant un poids w à support compact, les autres par un lissage des extrémités des arcs $\mathfrak{M}'_{aq}$ définis en 5.3.b.

L'estocade est portée avec la complicité de Katz. Une estimation délicate des moments d'ordre 4 de sommes trigonométriques permet d'obtenir pour une famille de nombre premiers de densité positive des majorations

dont la forme générale est

$$\sum_{\mathbf{a} \bmod p} \Big| \sum_{\substack{\mathbf{x} \bmod p \\ f(\mathbf{x}) \equiv 0 (p)}} e(\mathbf{a}.\mathbf{x}/P)| \leq (1-\delta) p^{(3n-1)/2}$$

avec une constante miraculeusement inférieure à 1 ! En moyenne sur les dénominateurs q des points de Farey (cf. l'alinea introductif de la section 5.3), on économise une puissance du logarithme de P, faible, mais décisive.

Pour terminer, signalons les travaux en cours de Hooley concernant le cas de formes nonaires dont les lieux singuliers de dimension zéro ne sont que des points doubles linéairement indépendants.

BIBLIOGRAPHIE

[1] R.C. BAKER, 1988 - *Diagonal cubic equations*, II, Acta Arithmetica 53 (1989) 217-250

[2] B.J. BIRCH, H. DAVENPORT, D.J. LEWIS, 1962 - *The addition of norm forms* Mathematika 9 (1962) 75-82.

[3] J. CHERLY, 1989 - *Sommes d'exponentielles cubiques dans l'anneau des polynômes en une variable sur le corps à deux éléments, et application au problème de Waring*, Thèse de Doctorat d'Etat, Univ. Bordeaux I, 1989.

[4] S.D. COHEN, 1979 - *The distribution of Galois groups and Hilbert's irreducibility theorem*, Proc. London Math. Soc. (3), 43 (1981) 227-250.

[5] J.-L. COLLIOT-THÉLÈNE, 1986 - *Arithmétique des variétés rationnelles et problèmes birationnels*, Proc. Int. Congress Math., (1987) 641-653.

[6] J.-L. COLLIOT-THÉLÈNE, J. SANSUC, Sir P. SWINNERTON-DYER, 1986 - *Intersection of two quadrics and Châtelet surfaces, II*, J. reine ang. Math. 374 (1987) 72-168.

[7] J.-L. COLLIOT-THÉLÈNE, P. SALBERGER, 1988 - *Arithmetic on some singular cubic hypersurfaces*. Proc. London Math. Soc. (3), 58 (1989) 519-549.

[8] H. DAVENPORT, 1962 - *Analytic methods for Diophantine equations and Diophantine inequalities*, Univ. Michigan, 1962.

[9] H. DAVENPORT - *Cubic forms in sixteen variables*, Proc. Roy. Soc. London ser. A, 272 (1963) 285-303.

[10] P. DELIGNE - *La conjecture de Weil, I*, Pub. Math. 43 (IHES, Paris, 1974) 273-307.

[11] J.-M. DESHOUILLERS, 1985 - *Problème de Waring pour les bicarrés*, Sem. Th. Nb. Bordeaux (1984-1985), exposé 14, 47 p.

[12] R.R. HALL, G. TENENBAUM, 1988 - *Divisors*, Cambridge University Press.

[13] G.H. HARDY, J.E. LITTLEWOOD, 1919-1928 - cf. Several papers on Partitio Numerorum, in G.H. HARDY's collected papers, Oxford, 1966.

[14] G.H. HARDY, S. RAMANUJAN, 1917 - *Asymptotic formulae in combinatory analysis*, Proc. London Math. Soc. (2), 17 (1918) 75-115.

[15] D.R. HEATH-BROWN, 1982 - *Cubic forms in ten variables*, Proc. London Math. Soc. (3), 47 (1983) 225-257.

[16] C. HOOLEY, 1977 - *On a new technique and its applications to the theory of numbers*, Proc. London Math. Soc. (3), 38 (1979) 115-151.

[17] C. HOOLEY, 1984 - *On Waring's problem*, Acta Math. 157 (1986) 49-97.

[18] C. HOOLEY, 1987 - *On nonary cubic forms*, J. reine ang. Math. 386 (1988), 32-98.

[19] H. IWANIEC, 1977 - *On sums of two norms from cubic fields*, in *Journées de théorie additive des nombres* (Université de Bordeaux I, 1977)

[20] N.M. KATZ, - *Perversity and exponential sums*, à paraître.

[21] H.D. KLOOSTERMAN, 1925 - *On the representation of numbers in the form* $ax^2 + by^2 + cz^2 + dt^2$. Acta Math. 49 (1926) 407-464.

[22] H.D. KLOOSTERMAN, 1925 - *On the representation of numbers in the form* $ax^2 + by^2 + cz^2 + dt^2$. Proc. London Math. Soc. (2), 25 (1926) 143-173.

[23] G. LACHAUD, 1982 - *Une présentation adéligne de la série singulière et du problème de Waring*, Ens. Math. 28 (1982) 139-169.

[24] Ju.V. LINNIK - *On the representation of large numbers as sums of seven cubes.* Doklady Akad. Nauk SSSR 35 (1942), 162 and Mat. Sbornik 12 (1943) 218-224.

[25] L.J. MORDELL 1936 - *A remark on indeterminate forms in several variables*, J. London Math. Soc. 12 (1937) 127-129.

[26] H. RADEMACHER, 1969 - *Topics in Analytic Number Theory*, Springer-Verlag, 1973.

[27] R.G. VAUGHAN, 1981 - *Some remarks on Weyl sums*, Coll. Math. Soc. Janos Bolyai 34 (Halasz ed.) Amsterdam, 1984, 1585-1602.

[28] R.G. VAUGHAN, 1981 - *The Hardy-Littlewood method*, Cambridge, 1981.

[29] R.G. VAUGHAN, 1985 - *On Waring's problem for cubes*, J. reine ang. Math. 365 (1986) 122-170.

[30] R.G. VAUGHAN, 1987 - *On Waring's problem for cubes, II*, J. London Math. Soc. 39 (1989) 205-218.

[31] H. WEYL, 1914 - *Über die Gleichverteilung von Zahlen mod. Eins*, Math. Ann. 77 (1916) 313-352.

Jean-Marc DESHOUILLERS

Centre de Recherche en Mathématiques
Université Bordeaux I
351, cours de la Libération
F-33405 TALENCE CEDEX

dezou at frbdx11.bitnet

Astérisque

CHRISTIAN GÉRARD

Complétude asymptotique des systèmes à N corps à courte portée

Astérisque, tome 189-190 (1990), Séminaire Bourbaki,
exp. n° 721, p. 179-201

<http://www.numdam.org/item?id=SB_1989-1990__32__179_0>

© Société mathématique de France, 1990, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Séminaire BOURBAKI Mars 1990
42éme année, 1989/90, n° 721

COMPLÉTUDE ASYMPTOTIQUE DES SYSTÈMES À N CORPS À COURTE PORTÉE
[d'après I.M.Sigal et A.Soffer]

par Christian Gérard

1. INTRODUCTION

Le Problème à N corps quantique concerne les propriétés d'un système de N particules *non relativistes* en interaction. Ce système de N particules est décrit par un Hamiltonien de Schrödinger de la forme suivante:

$$H = \sum_{i=1}^{N} -\frac{\Delta_{x_i}}{2m_i} + \sum_{i<j} V_{ij}(x_i - x_j). \tag{1}$$

Ici m_i est la masse de la particule i, x_i est sa position qui est un point dans $\mathbf{R}^\nu$,($\nu = 3$ dans le cas physique) et $V_{ij}(x_i - x_j)$ est le potentiel d'interaction entre les particules i et j. H agit donc sur l'espace de Hilbert $L^2(\mathbf{R}^{N\nu})$. Un autre exemple important est celui des Hamiltoniens *atomiques*, où certaines particules sont supposées de masse infinie et donc fixes (comme par exemple les noyaux des atomes ou des molécules) :

$$\widetilde{H} = \sum_{i=1} -\frac{\Delta_{x_i}}{2m_i} + \sum_{i,k} \frac{e_i e_k}{|x_i - X_k|} + \sum_{i<j} \frac{e_i e_j}{|x_i - x_j|}. \tag{2}$$

Ici e_i désigne la charge de la particule i et X_k la position de la particule k de masse infinie. Ce type de Hamiltoniens a posé beaucoup de problèmes aux physiciens depuis la naissance de la Mécanique Quantique. Le premier est que dès que N est plus grand que 2 (ou que 1 pour les Hamiltoniens atomiques, c'est à dire dès l'atome d'Hélium !) il n'existe plus

de solutions explicites de l'équation de Schrödinger, même si les potentiels d'interaction sont de type Coulombien. Ceci a donné lieu à un grand nombre d 'approximations permettant de calculer le niveau fondamental $\inf_{\psi \in L^2(\mathbf{R}^{3N})} < \widetilde{H}\psi, \psi >$ (approximations de Hartree-Fock et de Thomas -Fermi par exemple cf. Landau-Lifschitz [LL]). On peut en mentionner un autre, qui est de définir H comme un opérateur autoadjoint non borné sur $L^2(\mathbf{R}^{N\nu})$ avec un domaine $D(H)$. Il est assez surprenant de constater que ce problème n'a été résolu rigoureusement que dans les années cinquante par Kato [Ka] pour l'atome d'Hélium et par Combes [Com] dans les années soixante-dix pour le cas général. D'un point de vue plus théorique, il est important de comprendre, ne serait-ce que pour justifier *a posteriori* l' introduction de ces Hamiltoniens, comment établir rigoureusement certaines propriétés de base des systèmes quantiques formés d'un grand nombre de particules. La propriété la plus fondamentale est certainement la *stabilité de la matière* , qui se traduit mathématiquement par le fait que le Hamiltonien atomique $\widetilde{H}$ est borné inférieurement (uniformément sur toutes les positions des noyaux) par $-C_0(N+K)$, où N est le nombre d'électrons et K le nombre de noyaux. Cette propriété est démontrée rigoureusement depuis les années soixante-dix (Dyson-Lenard [DL], Lieb-Thirring [LT]). Nous renvoyons à l'article de revue très récent de Lieb [L] pour une introduction à ces problèmes. A noter qu'il y a beaucoup de propriétés physiquement tout à fait raisonnables des systèmes Coulombiens que l'on ne sait pas démontrer mathématiquement.

Une autre classe de problèmes concerne l'évolution d'un système quantique à N particules pour des temps grands. Cette évolution est décrite par l'équation de Schrödinger dépendant du temps:

$$i\partial_t u_t = Hu_t \tag{3}$$

$$u_{|t=0} = u. \tag{4}$$

On note symboliquement cette évolution par $e^{-itH}u$. Si H admet une réalisation autoadjointe, cette équation a une solution pour tous temps. C' est le cas par exemple si:

$$V_{ij} \in L^r(\mathbf{R}^\nu) + L^\infty_\epsilon(\mathbf{R}^\nu)$$

pour $r > \nu/2$ (cf. Reed-Simon [RS]). Ici l'indice ϵ veut dire que la composante dans L^∞ doit être prise de norme arbitrairement petite. H est alors autoadjoint sur l'espace de Sobolev $H^2(\mathbf{R}^{N\nu})$. En particulier pour des interactions Coulombiennes, l'évolution est définie pour tous temps: il n'y a pas de trajectoires de collision pour le problème quantique. Cette différence importante avec le problème à N corps *classique* peut être vue comme une manifestation du principe d'incertitude.

Si u est dans l'espace spectral ponctuel de H, $\mathcal{H}_{pp}(H)$, l'évolution $e^{-itH}u$ est une évolution triviale: la composante de u sur chaque vecteur propre ϕ_j de H est simplement multipliée par $e^{-it\lambda_j}$, où λ_j est la valeur propre associée à ϕ_j. Le problème central de la théorie du *scattering* consiste à décrire l'évolution d'un état u qui appartient à l'espace spectral continu $\mathcal{H}_c(H) = \mathcal{H}_{pp}(H)^\perp$. L'intuition physique suggère que le système de N particules va se désintégrer en des amas de particules stables qui se déplacent chacun comme des particules libres. Aucun autre type de comportement n'a encore été observé dans la réalité. La traduction de cette propriété en des termes mathématiques est ce qu'on appelle la *complétude asymptotique* . Cette propriété n'est pas aussi évidente qu'elle le parait. Elle est par exemple liée à l'absence de spectre *singulier continu*, c'est à dire d'états dont la probabilité de présence dans un compact tend vers 0 seulement *en moyenne*. En d'autres termes les particules décrites par un tel état quantique peuvent se rapprocher les unes des autres à des temps arbitrairement grands. On connaît pour les problème à deux corps des exemples de potentiels dus à Pearson (cf . [Pe]) dans $C_0^\infty(\mathbf{R}^\nu \backslash \{0\})$ tel que le spectre de H soit purement singulier continu dans $]0, +\infty[$.

2. LES OPÉRATEURS D'ONDE

La première réduction à faire pour étudier le Hamiltonien H est de séparer le mouvement du centre de masse des particules. En effet H est invariant par les translations d'ensemble du système. L'espace de configuration du mouvement (classique) dans le référentiel du centre de masse est

l'espace :

$$X = \{x \in \mathbf{R}^{N\nu} \mid \sum_i m_i x_i = 0\}.$$

Une première difficulté est qu'il n'y a plus de coordonnées naturelles sur X. On peut tourner cette difficulté en introduisant la forme quadratique sur $\mathbf{R}^{N\nu}$ suivante :

$$q(x,y) = \sum_i 2m_i x_i.y_i.$$

On remarque que $\sum_{i=1}^{N} -\frac{\Delta_{x_i}}{2m_i}$ est en fait l'opérateur de Laplace-Beltrami sur $\mathbf{R}^{N\nu}$ associé à q, que l'on notera dans la suite simplement $-\Delta_{|X}$ et qui est complètement intrinsèque. L'espace X est simplement l'orthogonal pour q de l'espace de configuration du mouvement du centre de masse:

$$X^{\perp} = \{x \in \mathbf{R}^{N\nu} | x_i = x_j \, \forall \, i,j\}.$$

Si on pose $V(x) = \sum_{i<j} V_{ij}(x_i - x_j)$, V est en fait une fonction sur X, et on peut écrire, en décomposant $L^2(\mathbf{R}^{N\nu})$ comme $L^2(X) \otimes L^2(X^{\perp})$:

$$H = \mathbf{1}_{|X} \otimes -\Delta_{|X^{\perp}} + (-\Delta_{|X} + V(x)) \otimes \mathbf{1}_{|X^{\perp}}. \tag{5}$$

Le premier terme correspond à l'énergie cinétique du centre de masse. C'est le deuxième terme $-\Delta_{|X} + V(x)$ que l'on notera dorénavant H.

La principale difficulté d'un Hamiltonien à N corps est que le potentiel V ne tend pas vers 0 à l' infini sur X, sauf si $N = 2$. En effet V ne tend pas vers 0 le long des sous espaces $\{x_i = x_j\}$. Pour décrire de façon précise la géométrie de ces espaces ainsi que les décompositions possibles en paquets de particules on introduit les notions suivantes: on note $\mathcal{A}$ l'ensemble des partitions de $\{1,\ldots,N\}$, ou l'ensemble des décompositions possibles en paquets de particules. Sur $\mathcal{A}$, on a une relation d'ordre naturelle en disant que $a \subset b$ si a est une partition plus fine que b. La partition la plus fine est bien sûr $\{\{1\},\ldots,\{N\}\}$, notée a_{min}, qui correspond à l'éclatement total du système. La partition la plus grossière $\{1,\ldots,N\}$, qui correspond au cas où le système reste stable, est notée a_{max}. On note d'autre part (ij) la partition formée de la paire $\{i,j\}$ et des singletons $\{k\}$ pour $k \neq i,j$. Pour $a \in \mathcal{A}, a = \{A_1,\ldots,A_k\}$, on pose:

$$X_a = \{x \in X \mid x_i = x_j \, si \, (ij) \subset a\} \tag{6}$$

On vérifie facilement que si $a \subset b$ on a $X_b \subset X_a$. C'est en fait cet ordre sur les X_a qui est le plus important (cf Remarque 2.1). Si on pose $X^a = X_a^{\perp}$, on a:

$$X^a = \{x \in X \mid R_i^a(x) \stackrel{\text{def}}{=} \sum_{j \in A_i} m_j x_j = 0\}. \tag{7}$$

On définit *l'interaction entre amas* par:

$$I_a(x) = \sum_{(ij) \not\subset a} V_{ij}(x). \tag{8}$$

On pose alors $H_a = H - I_a$. Comme les termes d' interaction dans H_a ne dépendent que des variables sur X^a, on peut décomposer H_a comme :

$$H_a = \mathbf{1}_{|X^a} \otimes -\Delta_{|X_a} + (-\Delta_{|X^a} + V^a(x^a)) \otimes \mathbf{1}_{|X_a}. \tag{9}$$

Ici $V^a = V - I_a$ est une fonction sur X^a. Le premier terme représente l'énergie cinétique des centres de masse des amas de a, et le deuxième représente l'énergie interne des amas de a. On note H^a le Hamiltonien :

$$-\Delta_{|X^a} + V^a(x^a)$$

agissant sur $L^2(X^a)$. On note finalement par T_a le Hamiltonien $-\Delta_{|X_a}$.

Remarque 2.1.— *On peut définir une classe de Hamiltoniens à N corps* généralisés*(cf. Agmon [Ag]) en oubliant la structure de particules, et en introduisant a priori une famille de sous espaces vectoriels X_a pour $a \in \mathcal{A}$ dans un espace vectoriel de dimension finie X avec la relation d'ordre sur $\mathcal{A}$ $a \subset b$ si $X_b \subset X_a$. Dans cette classe de Hamiltoniens rentrent par exemple les Hamiltoniens atomiques ainsi que des systèmes à N corps où on ajoute des interactions entre des* groupes *de particules: par exemple on peut admettre des interactions qui ont lieu uniquement quand trois particules sont proches les unes des autres. Tous les résultats décrits dans la suite s'étendent directement aux Hamiltoniens d'Agmon.*

H^a décrit un nouveau système à N corps formé de la collection des amas de a, avec uniquement leurs interactions internes. Les H^a pour $a \neq a_{max}$

sont appellés les *sous systèmes* de H. Les valeurs propres de H^a pour $a \neq a_{max}$ sont appelés les *seuils* de H. On notera Σ l'ensemble des seuils. Sous les hypothèses (H) Σ est un ensemble fermé dénombrable ([M,PSS,FH]). Les seuils correspondent à des niveaux d'énergie où de nouvelles possibilités de désintégration apparaissent. Citons par exemple le célèbre théorème HVZ (Hunziker, Van Winter, Zhislin):

THÉORÈME 2.2.— *Le spectre essentiel de H est égal à* $[inf\Sigma, +\infty[$.

Ainsi $inf\Sigma$ est le niveau d'énergie minimal pour pouvoir désintégrer le système. De même, 0 est le niveau d'énergie minimal où le système peut se ' casser ' en N morceaux indépendants. D'autre part les seuils sont de façon générale des niveaux d'énergie où le système a un comportement plus pathologique. Par exemple sous les hypothèses (H), les seuils sont les seuls points d'accumulation possibles pour les valeurs propres (éventuellement plongées) de H. Ce sont aussi les points où la multiplicité du spectre continu change. Enfin ce sont des niveaux où les estimations de propagation (voir Sect. 6) ne sont plus valables. Ceci vient du fait qu'un système à un niveau d'énergie de seuil peut se trouver dans une configuration formée de paquets stables ayant des impulsions relatives nulles. Dans le cas des potentiels à courte portée (voir plus bas), ces états peuvent être éliminés par un argument de densité qui provient du lemme évident suivant:

Lemme 2.3.— it Pour $u \in \mathcal{H}_c(H)$, $E_\Delta(H)u$ tend vers 0 quand l'intervalle Δ tend vers un point $\{\lambda_0\}$.

Dans le cas à longue portée, il semble qu'il soit nécessaire d'invoquer un autre mécanisme pour obtenir la désintégration de ces états. L'un de ces mécanismes pourrait être la *diffusion*, par analogie avec le problème à deux corps.

Un comportement asymptotique élémentaire pour $e^{-itH}u$ pour $t \to \pm\infty$ est décrit par trois types de données :

- une décomposition en paquets, i. e un élément a de $\mathcal{A}$.
- une fonction u_a dans $L^2(X_a)$ qui décrit le mouvement relatif des centres de masse des paquets.

- une fonction propre ψ^a de H^a dans $L^2(X^a)$ qui décrit l'état stable de chaque paquet de particules.

La donnée d'une décomposition $a \in \mathcal{A}$ et d'une fonction propre ψ^a (modulo multiplication par une constante) s'appelle un *canal de réaction.* On le note par la lettre grecque $\alpha = (a, m)$, où m est le numéro de la valeur propre ϵ_α deH^a (avec multiplicité). On note alors ψ^α la fonction propre de H^a associée au canal α.

Le mouvement relatif des centres de masse des paquets dépend fortement de la décroissance à l'infini des potentiels V_{ij}. Si les potentiels $V_{ij}(x)$ décroissent à l'infini comme $\langle x\rangle^{-\rho}$ pour $\rho > 1$ (potentiels à courte portée), on peut approximer l'évolution relative des paquets par une évolution libre donnée par le Laplacien T_a. Si les potentiels V_{ij} décroissent comme $\langle x\rangle^{-1}$ ou plus lentement, il faut corriger l'évolution libre pour tenir compte de la décroissance plus lente des interactions à l'infini. Nous reviendrons sur les problèmes posés par les potentiels à longue portée dans la Section 7. Dans toute la suite, on ne considèrera que des potentiels à courte portée.

Donnons d'abord les hypothèses sur les potentiels: on a vu qu'on pouvait considérer $V_{ij}(x_i - x_j)$ comme une fonction V_a sur X^a pour $a = (ij)$. On suppose que V_a vérifie les conditions suivantes :

(H.i) $V_a(x^a)(-\Delta^a + 1)^{-1}$ est compact sur $L^2(X^a)$.

(H.ii) $\langle x\rangle^\mu V_a(x^a)(-\Delta^a + 1)^{-1}$ est borné.

(H.iii) $\langle x\rangle^{1+\mu}\nabla V_a(x^a)(-\Delta^a + 1)^{-1}$ est borné.

(H.iv) $(x^a \cdot \nabla)^2 V_a(x^a)(-\Delta^a + 1)^{-1}$ est borné.

On dira que les potentiels sont à courte portée si $\mu > 1$. Notons que l'hypothèse (H.iv) n'est pas strictement nécessaire pour obtenir les résultats que nous allons décrire : la complétude asymptotique est vraie sans elle (voir le récent travail de Graf [G]) et l'absence de spectre singulier continu aussi sous des hypothèses plus faibles (voir [BGM]).

Pour des potentiels à *courte portée* les *opérateurs d'onde* sont définis de la manière suivante :

DÉFINITION 2.4.— *Pour un canal α, on définit les opérateurs d'onde*

$\Omega_\alpha^\pm$ *par : pour* $u_a \in L^2(X_a)$

$$\Omega_\alpha^\pm u_a = \lim_{t\to\pm\infty} e^{itH} e^{-it(T_a+\epsilon_\alpha)} u_a \otimes \psi^\alpha$$

Le résultat qui suit est standard:

THÉORÈME 2.5.— (i) *Sous les hypothèses (H), pour* $\mu > 1$, *les opérateurs d'onde* $\Omega_\alpha^\pm$ *existent.*

(ii) *pour* $\alpha \neq \beta$, $Im\Omega_\alpha^\pm \perp Im\Omega_\beta^\pm$.

Le point (i) du Théorème ci-dessus signifie que pour toute évolution asymptotique $e^{-it(T_a+\epsilon_\alpha)}u^a \otimes \psi^\alpha$ donnée, il existe un état u tel que $e^{-itH}u$ soit asymptotique à cette évolution. Le point (ii) signifie simplement qu'un état u ne peut avoir deux évolutions asymptotiques différentes quand $t \to \pm\infty$, ou en d'autres termes que la classification asymptotique adoptée est suffisament fine.

La *complétude asymptotique* correspond au fait que toutes les évolutions possibles sont décrites par la classification asymptotique :

DÉFINITION 2.6.— *Le système à N corps H est asymptotiquement complet si :*

$$\bigoplus_\alpha Im\Omega_\alpha^\pm = \mathcal{H}_c(H).$$

Comme on l'a dit dans l'introduction, la complétude asymptotique entraine (et est en fait beaucoup plus forte) l'absence de spectre singulier continu. Cette propriété est en fait une conséquence de l'estimation de Mourre (cf [M,PSS,FH] Section 6) valide sous les hypothèses (H).

3. LA DÉSINTÉGRATION ASYMPTOTIQUE

Pour démontrer la complétude asymptotique, Sigal et Soffer (cf. [SS1]) ont introduit une description intermédiaire du comportement asymptotique, la *désintégration asymptotique* (asymptotic clustering). Donnons d'abord une caractérisation équivalente de la complétude asymptotique:

PROPOSITION 3.1.— *Le système à N corps H est asymptotiquement complet si et seulement si :* $\forall u \in \mathcal{H}_c(H)$ *et* $\forall \epsilon > 0$, *il existe un ensemble fini* Σ_ϵ *de canaux et pour* $\alpha \in \Sigma_\epsilon$ *des vecteurs* $u_{\alpha,\epsilon} \in L^2(X_a)$ *tels que :*

$$\lim_{t\to\pm\infty} \| e^{-itH}u - \sum_{\alpha\in\Sigma_\epsilon} e^{-it(T_a+\epsilon_\alpha)}u_{\alpha,\epsilon} \otimes \psi^\alpha \| \leq \epsilon. \tag{10}$$

Pour définir la propriété de désintégration asymptotique, on compare l'évolution totale à des évolutions plus grossières que celles utilisées dans la complétude asymptotique.

DÉFINITION 3.2.— *Le système à N corps H se* désintègre asymptotiquement *à l'énergie E si il existe un intervalle* Δ *autour de E tel que* $\forall u \in Im E_\Delta(H) \cap \mathcal{H}_c(H)$, *il existe des vecteurs* $\psi^\pm_{a,E} \in L^2(X)$ *tels que :*

$$\lim_{t\to\pm\infty} \| e^{-itH}u - \sum_a e^{-itH_a}\psi^\pm_{a,E} \| = 0.$$

Cette propriété exprime le fait que le système va se désintégrer en un certain nombre de paquets pour lesquels on a une évolution plus simple donnée par le Hamiltonien H_a. Par contre elle ne dit rien sur la stabilité des paquets. L'idée est que si les paquets sont instables, ils vont à leur tour se désintégrer en sous-paquets, jusqu'à ce qu'il ne reste plus que des paquets stables. Cette intuition est traduite dans le Théorème suivant :

THÉORÈME 3.3.— *Si le système à N corps H se désintègre asymptotiquement à toutes les énergies en dehors des seuils ainsi que tous les sous systèmes* H^a, *le système est asymptotiquement complet.*

Démonstration : soit $\psi \in \mathcal{H}_c(H)$. Grâce au Lemme 2, et au fait que l'ensemble Σ est fermé et dénombrable, on peut trouver un compact Δ évitant les seuils tel que :

$$\| \psi - E_\Delta(H)\psi \| \leq \epsilon. \tag{11}$$

En notant $\phi = E_\Delta(H)\psi$, on peut trouver un nombre fini d'intervalles Δ_i tels que H se désintègre asymptotiquement sur Δ_i. On peut écrire : $\phi = \sum \phi_i$,

avec $\phi_i \in Im E_{\Delta_i}(H) \cap \mathcal{H}_c(H)$. Comme H se désintègre asymptotiquement, il existe des $\phi^{\pm}_{a,i}$ tels que :

$$\lim_{t \to \pm\infty} \| e^{-itH} \phi_i - \sum_a e^{-itH_a} \phi^{\pm}_{a,i} \| = 0. \tag{12}$$

En posant $\phi^{\pm}_a = \sum_i \phi^{\pm}_{a,i}$, on a :

$$\lim_{t \to \pm\infty} \| e^{-itH} \phi - \sum_a e^{-itH_a} \phi^{\pm}_a \| = 0. \tag{13}$$

Notons par P_a la projection sur le spectre ponctuel de $H^a \otimes \mathbf{1}_{|X_a}$. On a :

$$P_a = \sum_{canaux\ de\ a} P_\alpha \otimes \mathbf{1}_{|X_a}. \tag{14}$$

Ici P_α désigne le projecteur spectral de H^a sur la valeur propre ϵ_α. En écrivant $u^{\pm}_\alpha = \langle \psi^\alpha, \phi^{\pm}_a \rangle_{X^a}$, et $\psi^{\pm}_a = (\mathbf{1} - P_a)\phi^{\pm}_a$, on a :

$$\lim_{t \to \pm\infty} \| e^{-itH} \phi - \sum_\alpha e^{-it(T_a + \epsilon_\alpha)} u^{\pm}_\alpha - \sum_a e^{-itH_a} \psi^{\pm}_a \| = 0. \tag{15}$$

Le point important est que $\psi^{\pm}_a$ est orthogonal aux fonctions propres de H^a, ce qui permet d'appliquer la propriété de désintégration asymptotique à chaque terme

$$e^{-itH_a} \psi^{\pm}_a = e^{-itT_a} e^{-itH^a} \psi^{\pm}_a.$$

En regroupant les termes, on arrive après un nombre fini d'étapes à l'équation (10). Par exemple en collectant les termes ne contenant que des e^{-itT_a} on obtient un terme $e^{-itH_{a_{min}}}$,qui correspond à une composante où le système est complètement séparé.

4. L'ENSEMBLE DE PROPAGATION

Pour démontrer la propriété de désintégration asymptotique, Sigal et Soffer utilisent la voie la plus directe, qui est de démontrer l'existence

d'opérateurs d'onde semblables à ceux de la définition 2.3, mais avec la dynamique perturbée figurant à *droite* (cf (19)). L'existence de ces opérateurs d'onde (appelés opérateurs d'onde de *Deift-Simon*) est beaucoup plus difficile à démontrer que celle des opérateurs d'onde standard: dans le cas de deux corps elle est par exemple équivalente à la complétude asymptotique. Un outil essentiel pour démontrer l'existence de ces opérateurs d'onde est une majoration géométrique d'un ensemble de l'espace des phases $T^\star(X)$ appellé *ensemble de propagation.* Cet ensemble dépend d'un paramètre E qui est le niveau d'énergie considéré et sera noté PS_E.

Commencons par donner la définition de PS_E: on utilise des localisations dans l'espace des phases sous forme d'operateurs pseudodifférentiels de symbole:

$$j(x,\xi) = j(x,\xi,\gamma)\,,\ \gamma = \hat{x}\cdot\xi.$$

Ici $\hat{x}$ est égal à $\frac{x}{\langle x\rangle}$. On suppose que j est à support compact en ξ et γ et vérifie des estimations en x du type:

$$|\ \partial_x^\alpha j(x,\xi)\ | \leq C_\alpha \langle x\rangle^{-|\alpha|}, \forall \alpha \in N^n. \tag{16}$$

La quantification de $j(x,\xi)$ a peu d'importance, on peut par exemple adopter la quantification de Weyl. On notera $J(x,D_x)$ le quantifié de $j(x,\xi)$ et $suppJ$ le support de j, que l'on peut supposer conique en x.

DÉFINITION 4.1.— *Soit E un niveau d'énergie donné. On dit que un ouvert $\mathcal{F}$ conique en x de $T^\star(X)$ n'est pas dans PS_E si il existe un opérateur pseudodifférentiel satisfaisant les estimations (16) tel que $\mathcal{F} \subset suppJ$ et un intervalle Δ autour de E tels que :*

$$\int_{-\infty}^{+\infty} \|\langle x\rangle^{-1/2} J(x,D_x) e^{-itH} u\|^2 dt \leq C\|u\|^2 \tag{17}$$

pour tout u dans $ImE_\Delta(H) \cap \mathcal{H}_c(H)$.

La condition (17) signifie que la probabilité de présence totale dans $\mathcal{F}$ (pondérée par le poids $\langle x\rangle^{-1}$) est finie. Le facteur $\langle x\rangle^{-1/2}$ dans (17) est essentiel: par exemple une conséquence de l'estimation de Mourre pour H

(cf. Mourre [M], Perry-Sigal-Simon [PSS], Froese-Herbst [FH]) est que pour tout niveau E en dehors des seuils, il existe un intervalle $\Delta \ni E$ tel que:

$$\forall s > 0 \int_{-\infty}^{+\infty} \|\langle x\rangle^{-1/2-s} e^{-itH} u\|^2 dt \leq C\|u\|^2 \tag{18}$$

pour tout u dans $Im E_\Delta(H) \cap \mathcal{H}_c(H)$. (18) traduit approximativement le fait que $e^{-itH}u$ s'éloigne de l'origine dans X (c'est à dire d'une configuration où toutes les particules sont proches), à vitesse constante si u est localisé en énergie en dehors des seuils. On peut raffiner la définition de PS_E en $PS_E^{\pm}$ définis en intégrant dans (17) entre 0 et $\pm\infty$.

La majoration géométrique de PS_E démontrée par Sigal et Soffer est la suivante: la première remarque (connue depuis longtemps) est que pour un niveau d'énergie E donné seuls les seuils correspondant à des canaux *ouverts* sont importants: un canal α est dit *ouvert* si on a $E \geq \epsilon_\alpha$, où ϵ_α est le seuil associé au canal α. La raison en est que le système sur le niveau d'énergie E ne peut pas se désintégrer sur un canal fermé β associé à une décomposition en amas b: en effet la conservation de l'énergie entraîne que :

$$E = \epsilon_\beta + D_{x_b}^2.$$

On peut en effet négliger le terme d'interaction $I_b(x)$ qui est petit si les amas de b sont bien séparés.

Le Théorème clé de Sigal et Soffer est alors le suivant:

THÉORÈME 4.2.— *PS_E est inclus dans :* $\bigcup_{\alpha\ ouvert}\{(x,\xi) \mid x \in X_a,\ x_a \| \xi_a\ ,\ \xi_a^2 = E - \epsilon_\alpha\}$.

On a ici identifié X avec $X^\star$ à l'aide de la forme quadratique q et on note ξ_a la projection orthogonale de ξ sur $X_a^\star$ pour la forme quadratique $\hat{q}$ duale de q. La signification de cette majoration est la suivante: l'impulsion relative ξ_a des amas de a n'est restreinte que par la condition énergétique $\xi_a^2 = E - \epsilon_\alpha$, et pour t grand, la position relative des amas devient parallèle à l'impulsion relative, comme dans le mouvement d'une particule libre. Les impulsions et positions internes des amas ne sont pas décrites car elles sont gouvernées par le mouvement purement quantique e^{-itH^a}. Le Théorème

(4.2) est valable aussi pour des potentiels à *longue portée.* Nous donnerons dans la section 6 les idées essentielles de la preuve du Théorème 4.2).

5. LES OPÉRATEURS D'ONDE DE DEIFT-SIMON ET LA COMPÉTUDE ASYMPTOTIQUE

Dans cette section nous allons démontrer le Théorème suivant:

THÉORÈME 5.1.— *Le système H se désintègre asymptotiquement à toutes les énergies en dehors des seuils.*

Ce résultat entraine la complétude asymptotique grâce au Théorème 3.3 et au fait qu'on peut appliquer le Théorème 5.1 aux sous systèmes H^a.

Pour définir les opérateurs d'onde de *Deift-Simon* Sigal et Soffer ont introduit une partition de l'unité approchée de l'espace des phases qui permet de ' découpler ' les canaux de réaction.

PROPOSITION 5.2.— *Pour toute énergie E en dehors des seuils, il existe une famille $j_{a,E}(x,\xi)$ pour $a \in \mathcal{A}$ d'opérateurs pseudodifférentiels d'ordre 0 tels que* :

(i) $\sum_a j_{a,E} = 1 + O(\langle x\rangle^{-1})$

(ii) $j_{a,E}(x,\xi)$ *est une fonction de* (x, ξ_a, γ)

(iii) $j_{a,E}$ *est supporté dans* $\mathcal{J}_a$, *où* :

$$\mathcal{J}_a = \{(x,\xi) \mid \forall b \not\subset a\,,\ \langle x^b\rangle \geq \delta\langle x\rangle\}$$

(iv) $\nabla j_{a,E}(x,\xi) = \langle x\rangle^{-1} k_a(x,\xi) + O(\langle x\rangle^{-2})$

Ici $k_a(x,\xi)$ est un opérateur pseudodifférentiel d'ordre 0 supporté en dehors de PS_E et on pose :

$$\nabla j_{a,E}(x,\xi) = \nabla_{(x,\gamma)} j_{a,E}(x,\xi_a,\gamma)_{|\gamma=\hat{x}\cdot\xi}.$$

La condition (iii) entraine que $j_{a,E}$ est supporté dans une région où les paquets de a s'éloignent les uns des autres.

On définit alors les opérateurs d'onde de Deift-Simon par:

$$W^{\pm}_{a,E} u = \lim_{t\to\pm\infty} e^{itH_a} J_{a,E}(x,D_x) e^{-itH} u. \tag{19}$$

On a le résultat suivant qui est facile à démontrer:

PROPOSITION 5.3.— *Si les opérateurs de Deift-Simon (19) existent pour tout* $u \in Im E_\Delta(H) \cap \mathcal{H}_c(H)$ *pour un intervalle* $\Delta \ni E$, *le système* H *se désintègre asymptotiquement à l'énergie* E.

Il ne reste plus qu'à démontrer l'existence des opérateurs d'onde de Deift-Simon :

PROPOSITION 5.4.— *Pour tout* E *en dehors des seuils, les opérateurs de Deift-Simon existent sur un intervalle* $\Delta \ni E$ *ne rencontrant pas les seuils de* H.

Démonstration : par un argument de densité standard, et utilisant le fait (cf. [PSS]) que les valeurs propres de H ne peuvent s'accumuler qu'aux seuils, on peut supposer que E n'est pas une valeur propre de H et prendre un intervalle $\Delta \ni E$ ne rencontrant pas les seuils et valeurs propres de H. On va utiliser la méthode de Cook (cf. [RS]). Posons:

$$W_{a,E}(t) = e^{itH_a} J_{a,E}(x, D_x) e^{-itH}.$$

En calculant la dérivée de $W_{a,E}(t)$, on obtient:

$$W_{a,E}(t) = J_{a,E} + i \int_0^t e^{isH_a}(H_a J_{a,E} - J_{a,E} H) e^{-isH} ds. \tag{20}$$

On a:

$$H_a J_{a,E} - J_{a,E} H = [H_a, J_{a,E}] - J_{a,E} I_a. \tag{21}$$

À cause du support de $J_{a,E}$, on voit que $J_{a,E} I_a (H+i)^{-1}$ est de la forme $B\langle x\rangle^{-\mu}$, où B est un opérateur borné. Le facteur $(H+i)^{-1}$ se traite par des arguments standard de troncature en énergie, et nous supposerons pour simplifier que $J_{a,E} I_a \langle x\rangle^{\mu}$ est borné. Regardons maintenant le terme $[H_a, J_{a,E}]$: pour simplifier l'argument, nous allons supposer que les potentiels sont réguliers et que l'on peut utiliser le calcul symbolique des

opérateurs pseudodifférentiels. Posons $j_{a,E}(x,\xi) = k_a(x,\xi_a,\gamma)$. Le terme principal dans le symbole de $[H_a, J_{a,E}]$ est $m_a =:$

$$2\xi \cdot (\partial_x k_a + \partial_\gamma k_a(\frac{\xi}{\langle x\rangle} + x \cdot \xi \frac{x}{\langle x\rangle^3})) - \partial_{x^a} V^a(x^a) \cdot \frac{x^a}{\langle x\rangle} \partial_\gamma k_a. \tag{22}$$

Comme $\partial_{x^a} V^a(x^a) \cdot x^a$ est *borné* (et non $O(\langle x\rangle)$ comme on pourrait le croire *a priori*), on voit que m_a est de la forme :

$$m_a(x,\xi) = \langle x\rangle^{-1} \tilde{j}_a \tag{23}$$

où $\tilde{j}_a$ est un opérateur pseudodifférentiel d'ordre 0 supporté hors de PS_E, par la Proposition 5.2 (ii). Prenons maintenant $u \in Im E_\Delta(H)$ et $v \in Im E_{\Delta'}(H)$, pour un intervalle $\Delta' \supset \Delta$. Utilisant que $J_{a,E} I_a \langle x\rangle^\mu$ est borné et l'inégalité de Cauchy-Schwartz, on a :

$$\begin{aligned}
&| \int_{t'}^{t} \langle (H_a J_{a,E} - J_{a,E} H) e^{-isH} u, e^{-isH_a} v\rangle ds \,| \leq \\
&\left[\int_{t'}^{t} \| q_{1,a} \langle x\rangle^{-1/2} e^{-isH} u\|^2 ds\right]^{1/2} \\
&\times \left[\int_{t'}^{t} \| q_{2,a} \langle x\rangle^{-1/2} e^{-isH_a} v\|^2 ds\right]^{1/2} \\
&+ C \left[\int_{t'}^{t} \| \langle x\rangle^{-\epsilon} e^{-isH} u\|^2 ds\right]^{1/2} \\
&\times \left[\int_{t'}^{t} \| \langle x\rangle^{-\epsilon} e^{-isH_a} v\|^2 ds\right]^{1/2}
\end{aligned} \tag{24}$$

Ici $\epsilon = min(1, \mu/2)$ et $q_{i,a}$ sont des opérateurs pseudodifférentiels supportés hors de PS_E . Grâce à (17) et (18), toutes ces intégrales sont convergentes. Appliquant le critère de Cauchy pour les intégrales, on montre alors immédiatement que la limite (19) existe.

6. LES ESTIMATIONS DE PROPAGATION

Dans cette section, nous allons donner quelques ingrédients de la preuve (longue et technique) du Théorème 4.2. Le but est de trouver un ensemble assez riche d'opérateurs pseudodifférentiels $a(x, D_x)$ vérifiant (17). Pour celà, un Théorème abstrait de Kato ([Ka2]) permet de se ramener à la construction d'opérateurs ayant des commutateurs localement positifs avec H. On dit qu'un opérateur J est *localement H-régulier* à l'énergie E, si on a l'estimation suivante :

$$\int_{-\infty}^{+\infty} \|J(x, D_x)e^{-itH}E_\Delta(H)u\|^2 dt \leq C\|u\|^2 \tag{25}$$

pour un voisinage Δ de E et pour tout $u \in \mathcal{H}_c(H)$.

THÉORÈME 6.1.— *Soit C un opérateur autoadjoint non borné tel que :*

i) *$E_\Delta(H)CE_\Delta(H)$ est borné*

ii) *il existe des opérateurs localement H-réguliers à l'énergie E, B_i et B_i'pour $1 \leq i \leq k$ et un opérateur B tels que :*

$$E_\Delta(H)[H, iC]E_\Delta(H) \geq E_\Delta(H)(B^*B - \sum_i B_i'B_i)E_\Delta(H). \tag{26}$$

Alors B est H-régulier à l'énergie E.

Ce Théorème permet de ramener la H-régularité d'un opérateur à l'existence de commutateurs localement positifs.

La notion d'ensemble de propagation a en fait beaucoup de liens avec la notion de *front d'onde* utilisée dans l'étude des équations aux dérivées partielles linéaires. Ceci se voit aussi au niveau des méthodes: la construction d'opérateurs pseudodifférentiels ayant un commutateur positif avec un opérateur donné H est le moyen le plus souple pour démontrer des Théorèmes de propagation du front d'onde (cf. Hörmander [Ho]). Une différence importante avec les Théorèmes de propagation des singularités est que le Théorème (4.2) fait intervenir les *seuils* qui sont des quantités quantiques: on ne peut pas accéder à ce type de quantités en remplaçant brutalement les commutateurs par des crochets de Poisson.

Nous allons donner quelques outils de la preuve de (4.2) d'après Derezinski [De] qui a simplifié la preuve originale de Sigal-Soffer en introduisant plus de calcul pseudodifférentiel. Les opérateurs qui vont jouer le rôle de C dans le Théorème (6.1) sont du type suivant:

$$C = g(D_x)f(\gamma)Q(x) \tag{27}$$

où $\gamma = \hat{x} \cdot \xi$, $\hat{x} = \frac{x}{\langle x \rangle}$, Q est une troncature conique d'ordre 0. L'idée clé de la démonstration est d'utiliser des commutateurs entre H et des fonctions de γ. les facteurs $g(D_x)$ et $Q(x)$ servent uniquement à localiser dans des régions convenables. Cette idée pourrait d'ailleurs être aussi appliquée au problème classique: on peut par exemple de cette façon montrer de manière elémentaire que pour le problème à deux corps, le long d'une trajectoire qui s'échappe à l'infini le rayon vecteur devient parallèle à la vitesse, ce qui est le contenu du Théorème (4.2) dans ce cas.

Un point important est que le commutateur de H et d'une fonction de γ a une forme simple (cf. [De] Lemme 6.1).

Lemme 6.2.— *Soit $F \in C^\infty(\mathbf{R})$ telle que $F' = f^2$ avec $f \in S(\mathbf{R})$. On a:*

$$\begin{aligned} &(H-\lambda)^{-1} i[H, F(\gamma)](H-\lambda)^{-1} = \\ &\langle x \rangle^{-1/2} f(\gamma)(H-\lambda)^{-1} i[H, A](H-\lambda)^{-1} f(\gamma)\langle x \rangle^{-1/2} \\ &- 2\langle x \rangle^{-1/2}(H-\lambda)^{-1} f^2(\gamma)\gamma^2 (H-\lambda)^{-1}\langle x \rangle^{-1/2} + O(\langle x \rangle^{-2}) \end{aligned} \tag{28}$$

Ici A désigne le générateur des dilatations $(x \cdot D_x + D_x \cdot x)/2$.

On reconnaît ici le commutateur entre H et A qui est la quantité importante dans l'estimation de *Mourre* ci dessous. Notons Σ_a le sous ensemble de Σ formé des valeurs propres des H^b pour $b \subset a$, $b \neq a$. On pose pour ϵ assez petit:

$$\theta_a(E) = 2(inf_{\beta \in \Sigma_a,\, \beta \, seuil \, ouvert}(E - \beta)). \tag{29}$$

$$\theta_a^\epsilon(E, \xi_a) = 2\xi_a^2 + inf\{\theta_a(E') \mid E - E' \mid \leq \epsilon\}. \tag{30}$$

THÉORÈME 6.3.— $\forall \delta > 0$, $\forall \epsilon > 0$, *il existe un intervalle* $\Delta \ni E$ *tel que* :

$$E_\Delta(H)[H, iA]E_\Delta(H) \geq (\theta(E) - \delta)E_\Delta(H). \tag{31}$$

$$E_\Delta(H_a)[H_a, iA]E_\Delta(H_a) \geq (\theta_a^\epsilon(E, D_a) - \delta)E_\Delta(H_a). \tag{32}$$

(32) est un raffinement de (31). Par exemple dans la région

$$Y_a^\epsilon \stackrel{\text{def}}{=} \{x \in X \mid \langle x^b \rangle \geq \epsilon_0 \langle x \rangle \,, \forall b \not\subset a\} \tag{33}$$

on a:

$$H = H_a + O(\langle x \rangle^{-\mu}). \tag{34}$$

où $O(\langle x \rangle^{-\mu})$ signifie un terme d'erreur borné si on le compose par $(H + i)^{-1}\langle x \rangle^\mu$. Dans la région Y_a^ϵ, l'estimation (31) peut donc être remplacée par l'estimation plus forte (32), qui tire partie du terme d'énergie cinétique relative entre paquets T_a dans H_a. Il faut noter que pour ϵ_0 assez petit, les Y_a^ϵ pour $a \neq a_{max}$ forment une partition de l'unité en dehors d'un voisinage de l'origine dans X.

En utilisant le Théorème 6.3 et le Lemme 6.2, on peut obtenir une estimation fine sur les commutateurs. On pose:

$$Z_a = X_a \setminus \bigcup_{b \not\subset a} X_b. \tag{35}$$

En clair Z_a est la région de X où les particules sont regroupées suivant les paquets de a mais pas suivant d'autres paquets. On définit alors la fonction $\theta^\epsilon(E, x, \xi)$ de la façon suivante : si $x \in Z_b$ on a :

$$\theta(E, x, \xi) = \theta_b^\epsilon(E, \xi_b).$$

On a alors la Proposition:

PROPOSITION 6.4.— *Soit* $a \in \mathcal{A}$, $\nu > 0$, $\delta > 0$, $\epsilon > 0$, $F \in C^\infty(\mathbf{R})$ *telle que* $F' = f^2$ *avec* $f \in S(\mathbf{R})$. *Soit* g *une fonction de troncature dans*

$C_0^\infty(X_a^\star)$, et $Q(x)$ une fonction homogène de degré 0 supportée dans Y_a^ϵ. Notons Ψ l'opérateur $g(D_a)\langle x\rangle^{-1/2}Q(x)^{1/2}f(\gamma)$. Posons

$$\theta = inf\{\theta^\epsilon(E,x,\xi) \mid x \in suppQ\,,\ \xi_a \in suppg\,,\ dist(\hat{x}\cdot\xi,\ suppf) \leq \nu\}.$$

Alors il existe un intervalle $\Delta \ni E$ et une constante c_1 tels que :

(36)

$$\frac{1}{2}E_\Delta(H)(H-\lambda)i[F(\gamma),(H-\lambda)^{-1}]Q(x)g^2(D_a)E_\Delta(H)(H-\lambda) + adjoint$$
$$\geq(\theta - 2sup\{t^2 \mid t \in suppf\} - \delta)E_\Delta(H)\Psi^\star\Psi E_\Delta(H)$$
$$- c_1E_\Delta(H)\langle x\rangle^{-1-\mu}E_\Delta(H)$$

Cette Proposition permet alors sans trop de peine d'obtenir le Théorème 4.2, en choisissant convenablement la fonction f.

7. POTENTIELS À LONGUE PORTÉE ET SYSTÈMES DISPERSIFS

Le résultat de Sigal et Soffer laisse encore un certain nombre de questions ouvertes. Notons tout d'abord qu' une nouvelle démonstration très élégante de la complétude asymptotique dans le cas à courte portée a été donnée par Graf [G], qui utilise une seule observable de propagation (les opérateurs C de (25)) qui dépend du temps. La plus importante est celle des potentiels à *longue portée*. Ce problème est extrèmement important du point de vue physique, car le potentiel de Coulomb est précisément à longue portée. Les seuls résultats complets sont ceux obtenus par V.Enss (cf. [E1] et [E2] pour une démonstration nouvelle) pour $N = 3$ et pour des potentiels décroissant à l'infini comme $\langle x\rangle^{-\mu}$ pour $\mu > \sqrt{3} - 1$. Enss définit des opérateurs d'onde *modifiés* pour tenir compte de l'influence des potentiels à l'infini (on peut facilement montrer que les opérateurs d'onde du Théorème (2.4) n'existent plus si $\mu \leq 1$). Ces opérateurs d'onde modifiés ou opérateurs d'onde de *Dollard* (cf [Do]) qui existent tant que $\mu > 1/2$, sont définis de la manière suivante. Nous supposerons pour simplifier que les potentiels d'interaction sont des fonctions *bornées*. On pose:

(37) $$H_a(t) = H_a + I_a(D_at)$$

et on note $U_{a,D}(t)$ la solution de:

$$i\frac{dU_{a,D}}{dt}(t) = H_a(t)U_{a,D}(t)\,,\; U_{a,D}(0) = \mathbf{1}. \tag{38}$$

On définit alors les opérateurs d'onde de Dollard par:

$$\Omega^{\pm}_{D,\alpha}u_a = \lim_{t\to\pm\infty} e^{itH}U_a(t)u_a \otimes \psi_\alpha. \tag{39}$$

Il faut remarquer que pour des potentiels à longue portée, même l'existence des opérateurs d'onde de Dollard n'est pas évidente. L'évolution décrite par $U_{a,D}(t)u_a \otimes \psi_\alpha$ correspond à des paquets stables évoluant suivant e^{-itH^a} et dont les centres de masse évoluent suivant une dynamique perturbée décrite par le Hamiltonien dépendant du temps $T_a + I_a(D_a t)$. Enss obtient (sans hypothèses de nature implicite sur la décroissance des états liés des sous systèmes) l'existence des opérateurs d'onde de Dollard pour $\mu > 1/2$ et la complétude pour $\mu > \sqrt{3} - 1$.

Un autre résultat sur les potentiels à longue portée a été démontré par Sigal et Soffer (cf [SS2]). Il s'agit de la propriété de désintégration asymptotique. Sigal et Soffer ont montré que pour des potentiels de type Coulombien (i.e. vérifiant (H) avec $\mu = 1$) on a la propriété de désintégration asymptotique, si on remplace l'évolution approchée e^{-itH_a} par une évolution modifiée $U_a(t)$ définie par :

$$i\frac{dU_a}{dt}(t) = \tilde{H}_a(t)U_a(t)\,,\; U_a(0) = \mathbf{1} \tag{40}$$

où $\tilde{H}_a(t)$ est défini par :

$$\tilde{H}_a(t) \;=\; H_a + \chi_a(x/\alpha t)I_a(x^a, D_a t) \tag{41}$$

où $\chi_a(x)$ est une troncature conique supportée dans une région semblable à Y^ϵ_a. A la différence de $U_{a,D}(t)$, $U_a(t)$ ne commute pas avec e^{-itH^a}, ce qui veut dire que dans l'évolution $U_a(t)u$, le mouvement interne des paquets est perturbé par l'influence de I_a à l'infini. Enfin Sigal et Soffer ont annoncé la complétude asymptotique pour $N = 4$ pour des potentiels Coulombiens.

Une autre classe de problèmes ouverts concerne les systèmes à N corps *dispersifs*. Un système à N corps dispersif est obtenu de façon générale en remplaçant dans un Hamiltonien à N corps d'Agmon (voir la remarque (2.1)) l'énergie cinétique $\sum_{i=1}^{N} -\Delta_{\frac{x_i}{2m_i}}$ par un opérateur $\omega(D_x)$ pour une fonction $\omega(\xi)$ réelle. Ce type de Hamiltoniens intervient dans un grand nombre de problèmes. Par exemple pour incorporer des corrections relativistes dans (1), on peut remplacer

$$\sum_{i=1}^{N} -\frac{\Delta_{x_i}}{2m_i} \tag{42}$$

par :

$$\omega(D_x) = \sum_{i=1}^{N}(-\Delta_{x_i} + m_i^2)^{1/2} \tag{43}$$

On rencontre aussi des systèmes dispersifs dans la *physique des solides*, par exemple dans le scattering d'ondes de spin pour le Hamiltonien de Heisenberg et dans certains modèles à plusieurs électrons dans un cristal.

On voit immédiatement une différence importante avec les Hamiltoniens à N corps standard, qui est qu'il n'existe plus de forme quadratique naturelle pour définir des espaces X^a supplémentaires aux X_a. Or les espaces X^a sont nécessaires pour définir les sous systèmes et les opérateurs d'onde. On peut cependant définir une classe raisonnable de systèmes dispersifs (qui contient par exemple le Hamiltonien de trois particules relativistes de même masse) pour lesquels on a une bonne définition de sous systèmes (cf. [Ge]). Comme conséquence, on peut démontrer une estimation de Mourre semblable à (31) et en déduire l'absence de spectre singulier continu, l'existence des opérateurs d'onde correctement définis et leur complétude dans une région du spectre appelée *région à deux corps*.

BIBLIOGRAPHIE

[Ag] S. AGMON - *Lectures on exponential decay of solutions of second order elliptic equations*, Math. Notes Princeton Univ. Press 1982.

[BGM] A. BOUTET de MONVEL-BERTHIER, V. GEORGESCU, M. MANTOIU - *Mourre's theory in a Besov space setting*, C.R.A.S. t310 (1990).

[Com] J.- M. COMBES - *Relatively compact interactions in many particles systems*, Comm. Math. Phys. **12**(1969).

[Do] J.D. DOLLARD - *Quantum mechanical scattering for short-range and Coulomb interactions*, Rocky Mountain J. Math. **1**(1971).

[De] J. DEREZINSKI - *A new proof of propagation theorem for N-body Quantum systems*, Com. Math. Phys. **122**(1989).

[DL] F. DYSON-A. LENARD - *Stability of matter* I,II, J. Math. Phys. **8** (1967), **9**(1969).

[E1] V. ENSS - *Quantum scattering theory for two and three-body systems with potentials of short and long range*, in : *Schrödinger Operators*, S.Graffi ed. Springer LN Math. 1159 (1985).

[E2] V. ENSS - *Long range scattering for two and three body quantum systems*, Actes du Congrès de Saint Jean de Monts (1989).

[FH] R. FROESE, I. HERBST - *A new proof of the Mourre estimate*, Duke Math. J **49** (1982).

[Ge] C. GÉRARD - *The Mourre estimate for regular dispersive N-body systems*, Preprint de l'Ecole Polytechnique (1990).

[G] G.M. GRAF - *Asymptotic completeness for N-body short- range quantum systems : a new proof*, Preprint ETH (1989).

[Hö] L. HÖRMANDER - *On the existence and regularity of solutions of linear pseudodifferential equations*, L'Enseign. Math. **17** (1971).

[Ka1 T. KATO - *On the existence of solutions of the Helium wave equation*, Trans. Amer. Math. Soc. **70** (1951).

[Ka2] T. KATO - *Smooth operators and commutators*, Studia Math. **31** (1968).

[LL] L. LANDAU, E. LIFSCHITZ - *Mécanique Quantique* Editions Mir Moscou 1967.

[L] E.H. LIEB - *The stability of matter : from atoms to stars*, Bull. de l'A.M.S. Vol 22(1) (1990).

[LT] E. LIEB, W. THIRRING - *Bound for the kinetic energy of fermions which proves the stability of matter*, Phys. Rev. Lett. **35** (1975).

[M] E. MOURRE - *Absence of singular continuous spectrum for certain selfadjoint operators*, Comm. Math. Phys. **78** (1981).

[Pe] D.B. PEARSON - *Singular continuous measures in scattering theory*, Comm. in Math. Phys. **60** (1978).

[PSS] P. PERRY, I. M. SIGAL, B. SIMON - *Spectral analysis of N-body Schrödinger operators*, Ann. of Math. **114** (1981).

[RS] M. REED, B. SIMON - *Methods of Modern Mathematical Physics* II, III, Academic Press (1975) (1979).

[SS1] I.M. SIGAL, A. SOFFER - *N-particle scattering problem: asymptotic completeness for short range systems*, Ann. Math. **126** (1987).

[SS2] I.M. SIGAL, A.SOFFER - *Long range many-body scattering: asymptotic clustering for Coulomb type systems*, Invent. Math. **99** (1990).

Christian GÉRARD
ÉCOLE POLYTECHNIQUE
Centre de Mathématiques
URA 169 du CNRS
F-91128 PALAISEAU CEDEX

Astérisque

ÉTIENNE GHYS

Les groupes hyperboliques

Astérisque, tome 189-190 (1990), Séminaire Bourbaki,
exp. n° 722, p. 203-238

<http://www.numdam.org/item?id=SB_1989-1990__32__203_0>

© Société mathématique de France, 1990, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Séminaire BOURBAKI mars 1990
42ème année, 1989-90, n° 722

LES GROUPES HYPERBOLIQUES

par **Étienne GHYS**

La théorie combinatoire des groupes étudie les groupes infinis de *type fini*, c'est-à-dire possédant une partie génératrice finie. Jusqu'à une période assez récente, l'essentiel des méthodes utilisées par cette théorie provenait de la topologie. Le groupe est donné par une présentation et on étudie la topologie d'un polyèdre dont le groupe fondamental est le groupe donné (voir, par exemple [36]). Il y a cependant quelques exceptions dont la plus notable est l'étude par M. Dehn du groupe fondamental des surfaces pour laquelle il utilise une méthode très géométrique : il s'agit d'exploiter l'existence de métriques à courbure négative sur les surfaces compactes de genre supérieur ou égal à deux (voir [13]). Aujourd'hui, grâce aux idées de nombreux mathématiciens, ce sont les méthodes géométriques qui sont les plus fructueuses. Dans cet exposé, nous décrirons l'approche de M. Gromov ([21], [24], [25]) pour laquelle la notion de présentation passe au second plan.

L'article [25] pose les fondements de la théorie des groupes hyperboliques. Il s'agit d'une classe de groupes dont la définition sera donnée plus loin et qui généralise largement la classe des groupes fondamentaux des variétés compactes à courbure négative. Faute de place, il est impossible de rendre compte ici de l'intégralité de ces travaux. *On trouvera peu de démonstrations dans cet exposé.* Bien des aspects importants ne sont pas abordés comme les inégalités isopérimétriques ou la construction de flots géodésiques. Pour plus d'informations et de détails, le lecteur pourra consulter un certain nombre de prépublications ([3], [11], [12], [18], [38]) ainsi, bien sûr, que les articles originaux. Nous nous contenterons d'une description générale de la théorie en essayant de la placer dans son con-

texte. Nous insisterons par ailleurs sur un certain nombre de problèmes ouverts qui semblent importants pour le développement futur.

Ma compréhension de ce sujet est due en grande partie à un séminaire organisé à Berne par le troisième cycle romand. Je tiens à en remercier tous les participants et tout particulièrement Norbert A'Campo, André Haefliger et Pierre de la Harpe. Je remercie également Jean Barge et Christophe Bavard pour leurs conseils.

1. LA MÉTRIQUE DES MOTS ET SA GÉOMÉTRIE

1.1. Soit Γ un groupe de type fini et $S \subset \Gamma$ une partie génératrice finie. Si γ est un élément de Γ , sa *longueur par rapport à* S, notée $\|\gamma\|_S$, est la longueur minimale d'un mot en les éléments de S ou leurs inverses représentant γ. On définit la distance $d_S(\gamma_1, \gamma_2)$ entre deux éléments γ_1 et γ_2 de Γ comme étant égale à $\|\gamma_1^{-1}\gamma_2\|_S$. Le groupe Γ, muni de d_S, devient ainsi un espace métrique homogène car les translations à gauche de Γ sont évidemment des isométries.

L'inconvénient principal de cette métrique des mots est bien sûr qu'elle dépend du choix de S . Pour tenir compte de cette dépendance, on introduit la définition suivante, qui remonte à G.A. Margulis .

DÉFINITION.— *Soient* (X_1, d_1) *et* (X_2, d_2) *deux espaces métriques. Une quasi-isométrie entre ces espaces est la donnée de deux applications* $f : X_1 \to X_2$ *et* $g : X_2 \to X_1$ *et de constantes* $C \geq 0$ *et* $\lambda > 0$ *vérifiant, pour tous* x_1, x_1' *de* X_1 *et* x_2, x_2' *de* X_2 *:*

$$d_2(f(x_1), f(x_1')) \leq \lambda\, d_1(x_1, x_1') + C \qquad d_1(g(x_2), g(x_2')) \leq \lambda\, d_2(x_2, x_2') + C$$
$$d_2(f \circ g(x_2), x_2) \leq C \qquad d_1(g \circ f(x_1), x_1) \leq C\ .$$

On dit alors que (X_1, d_1) *et* (X_2, d_2) *sont quasi-isométriques.*

Par exemple, les espaces (Γ, d_S) et $(\Gamma, d_{S'})$ sont toujours quasi-isométriques si S et S' sont deux parties génératrices finies. Il suffit de prendre pour λ la longueur maximale d'un élément d'une partie génératrice par rapport à l'autre et $C = 0$.

L'avantage de permettre une valeur non nulle pour C est le suivant. Une quasi-isométrie n'est pas nécessairement constituée d'applications continues : on n'impose aucune condition à petite distance. Par contre, il s'agit d'"homéomorphismes bi-Lipschitz à grande distance". Voici quelques exemples.

Deux espaces métriques bornés sont quasi-isométriques. On voit donc que la théorie que nous allons décrire néglige délibérément les groupes finis.

Les ensembles $\mathbf{Z}$ et $\mathbf{R}$, munis de leurs métriques usuelles, sont quasi-isométriques: l'application $f : \mathbf{Z} \to \mathbf{R}$ peut être le plongement naturel et $g : \mathbf{R} \to \mathbf{Z}$ l'application "partie entière".

Plus généralement, on associe à un groupe Γ et à une partie génératrice finie S un *graphe de Cayley* $\mathcal{G}(\Gamma, S)$. Il s'agit du graphe dont les sommets sont les éléments de Γ et où une arête joint γ_1 à γ_2 si $d_S(\gamma_1, \gamma_2) = 1$. Ce graphe peut être muni d'une métrique naturelle, invariante par Γ, pour laquelle chaque arête est isométrique à un intervalle de longueur 1 de $\mathbf{R}$ et telle que la distance entre deux points est la plus petite longueur d'un chemin qui les joint. De même que dans le cas de $\mathbf{Z}$ et $\mathbf{R}$, les espaces (Γ, d_S) et $\mathcal{G}(\Gamma, S)$ sont quasi-isométriques. L'avantage de $\mathcal{G}(\Gamma, S)$ est qu'il est connexe par arcs et même géodésique. Rappelons qu'un espace métrique (X, d) est *géodésique* si deux points quelconques x, y peuvent être joints par un *segment*, c'est-à-dire s'il existe un plongement isométrique $\sigma : [0, L] \to X$ avec $\sigma(0) = x$ et $\sigma(L) = y$. On note souvent $[x, y]$ l'image de σ même si, en général, cette image n'est pas déterminée par ses extrémités.

Une grande famille d'exemples de quasi-isométries est fournie par la proposition élémentaire suivante qui est implicitement connue depuis longtemps.

PROPOSITION.— *Soit Γ un groupe opérant par isométries, librement et proprement, sur l'espace métrique (X, d) supposé géodésique et propre (i.e. les boules fermées sont compactes). On suppose que le quotient X/Γ est compact. Alors, Γ est de type fini et (X, d) est quasi-isométrique à Γ muni de la distance d_S associée à n'importe quelle partie génératrice finie S.*

Exemples.— i) Le groupe fondamental d'une variété compacte V est quasi-isométrique au revêtement universel de V muni du relevé d'une métrique riemannienne quelconque de V. Par exemple, pour chaque entier n, tous les groupes fondamentaux des variétés compactes de dimension n à courbure -1 sont quasi-isométriques entre eux.

ii) un groupe de type fini Γ est quasi-isométrique à n'importe quel sous-groupe Γ_1 d'indice fini. Il suffit en effet de choisir une partie génératrice finie quelconque S pour Γ et de faire agir Γ_1 sur $\mathcal{G}(\Gamma, S)$. En particulier, deux groupes *commensurables*, c'est-à-dire possédant des sous-groupes d'indices finis isomorphes, sont quasi-isométriques.

iii) Si Γ est un sous-groupe discret d'un groupe de Lie G et si le quotient G/Γ est compact, alors Γ est quasi-isométrique au groupe G muni d'une métrique riemannienne invariante à droite quelconque. Il n'est pas difficile de trouver des exemples de sous-groupes discrets co-compacts non commensurables. Pour les groupes de type fini, la quasi-isométrie est donc une notion plus faible que la commensurabilité.

Ainsi, nous avons associé à chaque groupe de type fini Γ un espace métrique bien défini à quasi-isométrie près. L'étude de Γ se fera à travers celle de la géométrie de cet espace métrique.

1.2. Convenons de dire qu'une propriété d'un groupe de type fini est *géométrique* si elle est préservée par quasi-isométrie. Pour terminer ce paragraphe, nous allons donner deux sortes d'exemples. Tout d'abord, nous allons montrer qu'un grand nombre de propriétés bien connues, de nature algébrique, sont en fait géométriques. Ensuite, nous montrerons comment ce concept de propriété géométrique propose une nouvelle méthode pour étudier et classer les groupes : quels sont les groupes qui possèdent une géométrie donnée ?

PROPOSITION.— *La propriété d'être de présentation finie est géométrique.*

Ceci résulte du fait suivant que nous retrouverons plus loin. Soit S une partie génératrice finie du groupe Γ et n un entier naturel. On considère le

polyèdre P_n de dimension 2 dont les sommets sont les éléments de Γ, dont les arêtes sont les couples (γ_0, γ_1) avec $d_S(\gamma_0, \gamma_1) \leq n$ et dont les 2-simplexes sont les triplets $(\gamma_0, \gamma_1, \gamma_2)$ avec $d_S(\gamma_i, \gamma_j) \leq n$ (pour $i, j = 0, 1, 2$). Alors, Γ est de présentation finie si et seulement si P_n est simplement connexe pour n assez grand. Il n'est pas difficile de vérifier la nature géométrique de cette caractérisation.

THÉORÈME.— *La propriété d'être virtuellement nilpotent est géométrique.*

Rappelons qu'une propriété est satisfaite virtuellement si elle est satisfaite par un sous-groupe d'indice fini. Ce théorème est un corollaire immédiat du résultat de M. Gromov ([23], [41]) selon lequel un groupe Γ est virtuellement nilpotent si et seulement si la fonction $e(n) = Card\{\gamma \in \Gamma\,,\, \|\gamma\|_S \leq n\}$ est à croissance polynomiale.

Soit Γ un groupe nilpotent de type fini. On sait que, à indice fini près, on peut toujours supposer Γ sans torsion [34]. Dans ce cas, il existe un groupe de Lie nilpotent simplement connexe $\Gamma \otimes \mathbf{R}$, canoniquement associé à Γ, qui contient Γ comme sous-groupe discret co-compact [34]. Ce groupe de Lie nilpotent $\Gamma \otimes \mathbf{R}$ n'est pas en général gradué mais on peut considérer le gradué associé $(\Gamma \otimes \mathbf{R})_{\text{grad}}$ qui est un groupe de Lie nilpotent de même dimension. P. Pansu démontre le résultat suivant [33] :

THÉORÈME.— *Soit Γ_1 et Γ_2 deux groupes nilpotents de type fini, sans torsion. Si Γ_1 et Γ_2 sont quasi-isométriques, les groupes de Lie gradués associés $(\Gamma_1 \otimes \mathbf{R})_{\text{grad}}$ et $(\Gamma_2 \otimes \mathbf{R})_{\text{grad}}$ sont isomorphes.*

La démonstration, qu'il n'est pas possible de reproduire ici, est fondée sur les faits suivants. On se fixe une partie génératrice finie S_1 pour Γ_1 et on considère la suite d'espaces métriques $(\Gamma_1, \frac{1}{n} d_{S_1})$. Il s'avère que cette suite d'espaces converge, dans la topologie de Hausdorff-Gromov pointée [22] vers $(\Gamma_1 \otimes \mathbf{R})_{\text{grad}}$ muni d'une "métrique de Carnot-Carathéodory" explicite [32]. Si l'on suppose que Γ_1 et Γ_2 sont quasi-isométriques, l'influence de la constante C intervenant dans la quasi-isométrie disparaît à la limite et $(\Gamma_1 \otimes \mathbf{R})_{\text{grad}}$ et $(\Gamma_2 \otimes \mathbf{R})_{\text{grad}}$ sont homéomorphes par un homéomorphisme

bi-Lipschitz. P. Pansu généralise à ce contexte le théorème de Rademacher et montre qu'un tel homéomorphisme ne peut exister que si $(\Gamma_1 \otimes \mathbf{R})_{\mathrm{grad}}$ et $(\Gamma_2 \otimes \mathbf{R})_{\mathrm{grad}}$ sont isomorphes.

Voici un cas particulier (dont la démonstration utilise le théorème de M. Gromov sur la croissance et la première partie de la preuve du théorème précédent).

COROLLAIRE.— *La propriété d'être virtuellement abélien est géométrique.*

Problème.— *Donner une preuve "élémentaire" de ce corollaire.*

Peut-on aller plus loin que le théorème de P. Pansu ?

Problème.— *Soient Γ_1 et Γ_2 deux groupes nilpotents de type fini, sans torsion, quasi-isométriques. Peut-on affirmer que les groupes de Lie $(\Gamma_1 \otimes \mathbf{R})$ et $(\Gamma_2 \otimes \mathbf{R})$ qui les contiennent comme réseaux co-compacts sont isomorphes ?*

La propriété généralisant la nilpotence est bien sûr la résolubilité.

Problème.— *La propriété d'être virtuellement résoluble (resp. virtuellement polycyclique) est-elle géométrique ?*

Le cas de la moyennabilité, généralisant la résolubilité, est beaucoup plus facile à traiter.

PROPOSITION.— *La moyennabilité est une propriété géométrique.*

Ceci résulte du critère de moyennabilité de Følner [20]. Soit Γ un groupe de type fini, S une partie génératrice finie et A une partie finie quelconque de Γ. On appelle frontière de A, et on note $\mathrm{fr}(A)$, l'ensemble des éléments γ de A tels qu'il existe s de $S \cup S^{-1}$ avec $\gamma . s$ hors de A. Le groupe Γ est moyennable si et seulement si il existe une suite de parties finies A_n telle que $\mathrm{card}\,\mathrm{fr}(A_n) / \mathrm{card}\, A_n$ tende vers 0.

Examinons maintenant quelques propriétés "opposées" à la moyennabilité.

PROPOSITION.— *La propriété d'être virtuellement libre est géométrique.*

Nous donnons plus loin une indication sur la preuve : elle utilise la "technique hyperbolique".

Problème.— *Donner une démonstration "élémentaire" de ce dernier résultat.*

THÉORÈME.— *Si un groupe sans torsion* Γ *est quasi-isométrique à un produit libre de deux groupes sans torsion non triviaux, alors* Γ *est lui-même un produit libre non trivial.*

Il suffit d'utiliser le théorème de J. Stallings décrivant les groupes ayant une infinité de bouts et de constater que la notion de bouts d'un groupe est géométrique.

Voici encore un exemple de propriété "anti-moyennable" pour laquelle on aimerait disposer d'une définition géométrique.

Problème.— *La propriété T de Kazdan (voir* [27], [28]) *est-elle géométrique ?*

1.3. Nous venons de voir qu'un certain nombre de propriétés algébriques sont géométriques. Ceci suggère d'inverser la démarche et d'essayer de classer les groupes par leur géométrie. On se fixe un espace métrique (X, d). Quels sont les groupes de type fini quasi-isométriques à (X, d) ? Les premiers exemples à considérer sont bien sûr les espaces riemanniens symétriques. Seul le cas non compact nous intéresse. Commençons par le rang 1. Le premier résultat est une reformulation d'un exemple vu plus haut. Notons qu'il généralise le théorème de Bierberbach décrivant la structure des groupes cristallographiques.

THÉORÈME.— *Si un groupe de type fini est quasi-isométrique à un espace euclidien, il contient un sous-groupe abélien d'indice fini.*

THÉORÈME.— *Soit* Γ *un groupe quasi-isométrique à l'espace hyperbolique* $\mathbf{H}^n$ $(n \geq 3)$. *Alors,* Γ *est une extension finie d'un sous-groupe discret co-compact d'isométries de* $\mathbf{H}^n$.

Nous donnerons plus loin une indication sur la preuve de ce théorème. Dans le cas $n = 3$, il est dû à M. Gromov et D. Sullivan ([21] et [39]) (voir

aussi la prépublication de J.W. Cannon et D. Cooper ([7] et [8]). Le cas $n \geq 4$ est dû à M. Gromov et P. Tukia ([21] et [42]). Le cas $n = 2$ n'est que partiellement résolu : d'après P. Tukia [43], le même énoncé est cependant valable si Γ est sans torsion.

Problème.— *Le problème précédent est-il valable si* $n = 2$?

Selon P. Pansu [33], la démonstration du théorème précédent s'étend aux autres espaces riemanniens symétriques non compacts de rang 1.

THÉORÈME.— *Soit* Γ *un groupe de type fini quasi-isométrique à l'espace hyperbolique complexe ou quaternonien ou au plan hyperbolique sur les octaves de Cayley. Alors,* Γ *est une extension finie d'un groupe discret cocompact d'isométries de cet espace symétrique.*

Problème.— *Quels sont les groupes quasi-isométriques aux espaces riemanniens symétriques de rang supérieur à* 1, *par exemple* $SL(3,\mathbf{R})/SO(3,\mathbf{R})$?

Ce type de question n'est pas seulement intéressant en ce qui concerne les espaces symétriques. Rappelons que huit variétés riemanniennes simplement connexes de dimension trois sont fondamentales pour la description des variétés compactes de dimension 3. Ce sont :

i) les espaces euclidiens, hyperboliques et sphériques : $\mathbf{R}^3$, $\mathbf{H}^3$, $\mathbf{S}^3$;

ii) les produits $\mathbf{H}^2 \times \mathbf{R}$ et $\mathbf{S}^2 \times \mathbf{R}$;

iii) trois groupes de Lie simplement connexes munis de métriques riemanniennes invariantes. Le premier est le groupe de Heisenberg, noté ici **Nil**, et formé des matrices réelles du type $\begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}$. Le second, noté **Sol**, est le groupe résoluble formé des matrices $\begin{pmatrix} \exp(z) & 0 & x \\ 0 & \exp(-z) & y \\ 0 & 0 & 1 \end{pmatrix}$. Le troisième est le revêtement universel de $SL(2,\mathbf{R})$.

Ces variétés sont (presque) caractérisées par le fait que leurs groupes d'isométries opèrent transitivement sur les points (voir [35]). W. Thurston conjecture que toute variété compacte de dimension 3 peut se décomposer en "morceaux" uniformisables par l'une de ces géométries. Pour cette rai-

son, le problème suivant mérite l'attention.

Problème.— *Quels sont les groupes quasi-isométriques à l'une de ces huit géométries ?*

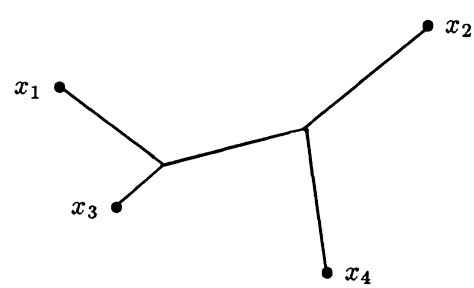
Nous avons déjà répondu à cette question dans le cas de $\mathbf{R}^3$, $\mathbf{H}^3$, **Nil**. Le problème est facile dans le cas de $\mathbf{S}^2 \times \mathbf{R}$. Il est trivial et sans intérêt dans le cas de $\mathbf{S}^3$. Les cas de $\mathbf{H}^2 \times \mathbf{R}$, **Sol** et $\widetilde{SL}(2, \mathbf{R})$ restent ouverts. G. Mess m'a fait remarquer que $\mathbf{H}^2 \times \mathbf{R}$ et $\widetilde{SL}(2, \mathbf{R})$ sont quasi-isométriques.

2. LES ESPACES MÉTRIQUES HYPERBOLIQUES

Conformément à la méthode que nous venons de décrire, nous allons présenter dans ce paragraphe la classe des espaces métriques hyperboliques, proches des variétés à courbure négative. Cette classe est invariante par quasi-isométrie et servira de base à la notion de groupe hyperbolique.

Considérons un arbre T, c'est-à-dire un graphe connexe sans cycle et associons à chaque arête a de T un réel strictement positif $\ell(a)$. On peut alors munir T d'une métrique d qui en fait un espace métrique géodésique et pour laquelle chaque arête a est isométrique à l'intervalle $[0, \ell(a)]$ de $\mathbf{R}$; on parle alors d'*arbre métrique.*

Dans un tel arbre métrique T, deux points quelconques sont joints par un unique segment. Considérons quatre points x_1, x_2, x_3, x_4 de T et les segments qui les joignent deux à deux. On obtient une figure du genre suivant :



On constate donc que, à une renumérotation des indices près, on a :

$$d(x_1, x_2) + d(x_3, x_4) = d(x_1, x_4) + d(x_2, x_3) \ .$$

On dira qu'un espace métrique est hyperbolique s'il vérifie une telle relation à une constante additive près. Plus précisément :

DÉFINITION.— *Un espace métrique (X, d) est hyperbolique s'il existe une constante $\delta \geq 0$ telle que :*

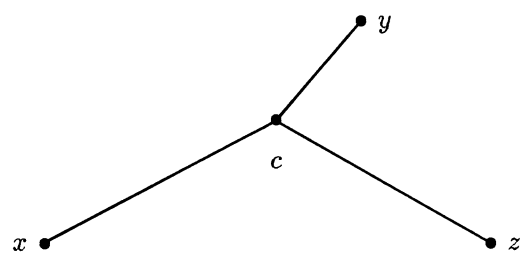
$$d(x_1, x_2) + d(x_3, x_4) \leq \max\{d(x_1, x_4) + d(x_2, x_3)\ ,\ d(x_1, x_3) + d(x_2, x_4)\} + 2\delta$$

pour tout quadruplet (x_1, x_2, x_3, x_4) de points de X. On dira parfois que X est δ-hyperbolique si l'on veut préciser la valeur de δ.

Bien sûr, un arbre métrique est un espace métrique 0-hyperbolique. La réciproque est presque vraie : il n'est pas difficile de s'assurer qu'un espace métrique 0-hyperbolique *fini* est isométrique à une partie d'un arbre métrique. Pour les espaces métriques infinis, il faut faire appel à la notion plus générale d'arbre réel (voir [37]).

M. Gromov donne beaucoup de définitions équivalentes de l'hyperbolicité. Nous nous contenterons de deux d'entre elles qui ont l'avantage d'être très intuitives.

Considérons tout d'abord trois points x, y, z dans un arbre métrique :



On voit que la distance entre x et le "centre" c du triangle $\{x, y, z\}$ est $\frac{1}{2}(d(x, y) + d(x, z) - d(y, z))$. Cette dernière quantité a un sens si x, y, z sont trois points d'un espace métrique quelconque. Elle se note $(y/z)_x$ et

nous l'appellerons le *produit de Gromov de y et z relatif à x*. L'énoncé suivant n'est qu'une reformulation de la définition ; il montre un aspect "quasi-ultramétrique" des espaces métriques hyperboliques.

DÉFINITION.— *Un espace métrique (X, d) est hyperbolique s'il existe une constante $\delta \geq 0$ telle que, pour tous x_1, x_2, x_3, w de X, on ait :*

$$(x_1 \mid x_3)_w \geq \min((x_1 \mid x_2)_w, (x_2 \mid x_3)_w) - \delta.$$

Voici encore une définition (bien sûr équivalente aux précédentes !).

DÉFINITION.— *Un espace géodésique (X, d) est hyperbolique s'il existe une constante $\delta \geq 0$ telle que pour tout triplet (x, y, z) de points de X et tous choix de segments $[x, y]$, $[y, z]$, $[z, x]$, on ait la propriété suivante. Tout point de $[x, y]$ est à distance inférieure à δ d'un point de la réunion $[y, z] \cup [z, x]$. On exprime cette propriété en disant que les triangles de X sont δ-fins.*

Cette définition, la plus intuitive, permet de trouver une grande famille d'exemples.

PROPOSITION.— *Soit V une variété riemannienne simplement connexe complète à courbure sectionnelle inférieure à $-k^2 < 0$. Alors, V est un espace métrique hyperbolique.*

La preuve résulte des théorèmes de comparaison de Alexandrov-Toponogov qui montrent qu'un triangle de V est plus fin qu'un triangle correspondant de l'espace hyperbolique à courbure constante $-k^2$. Il faut encore vérifier que les triangles de ce dernier espace hyperbolique sont uniformément fins, mais ceci est élémentaire.

Bien sûr, les espaces métriques hyperboliques ne se limitent pas aux variétés à courbure négative. Par exemple, considérons la réunion disjointe de deux variétés V_1 et V_2 simplement connexes à courbure -1 et identifions un point x_1 de V_1 avec un point x_2 de V_2. L'espace X ainsi obtenu peut être muni d'une métrique géodésique pour laquelle les plongements de V_1 et V_2 sont isométriques. Il est facile d'analyser les triangles de X et de vérifier que cet espace est hyperbolique.

Plus généralement, on peut dégager une notion de polyèdre à courbure négative qui produit beaucoup d'exemples. Nous n'expliciterons que le cas de dimension 2. Soit P un polyèdre localement fini de dimension 2. On munit chaque face de P d'une métrique qui la rend isométrique à un triangle du plan hyperbolique $\mathbf{H}^2$. On suppose que ces métriques sont compatibles sur les arêtes. Le polyèdre P peut alors être muni d'une structure d'espace métrique géodésique en définissant la distance entre deux points par la borne inférieure des longueurs des chemins qui les joignent. Nous allons énoncer une condition simple qui garantit l'hyperbolicité de cet espace.

Soit p un sommet de P. Le "link" de p est un graphe dont chaque arête correspond à un triangle de P ayant p comme sommet. Ainsi, ce "link" est muni d'une métrique provenant de l'angle de ces triangles en p. Nous dirons que P est à *courbure inférieure à* -1 si, pour tout sommet p de P, toute courbe fermée simple dans le "link" de p est de longueur supérieure ou égale à 2π.

THÉORÈME.— *Soit P un polyèdre localement fini, de dimension 2, simplement connexe, équipé d'une métrique comme ci-dessus à courbure inférieure à -1. Alors, P est un espace métrique hyperbolique.*

2.2. Les espaces métriques hyperboliques ont presque toutes les propriétés des espaces hyperboliques $\mathbf{H}^n$. Un exemple important est donné par l'étude des quasi-géodésiques.

DÉFINITION.— *Soient (X, d) un espace métrique et $\lambda > 0$, $C \geq 0$ deux constantes. Une (λ, C)-quasi-géodésique est une application f (pas nécessairement continue) d'un intervalle I de $\mathbf{R}$ vers X telle que :*

$$\frac{1}{\lambda}\,|t_2 - t_1| - C \leq d(f(t_1), f(t_2)) \leq \lambda\,|t_2 - t_1| + C$$

pour tous t_1, t_2 de I.

Par exemple, l'image d'un segment de X par une (λ, C)-quasi-isométrie est une (λ, C)-quasi-géodésique. Le comportement de ces (λ, C)-quasi-géodésiques est le même qu'en géométrie hyperbolique habituelle.

THÉORÈME.— *Pour tous $\delta \geq 0$, $\lambda > 0$, $C \geq 0$, il existe une constante K ayant la propriété suivante. Soit $f : I \to X$ une (λ, C)-quasi-géodésique d'un espace métrique géodésique δ-hyperbolique. Alors, si $[a, b]$ est un intervalle contenu dans I, la distance de Hausdorff entre $f([a, b])$ et n'importe quel segment $[f(a), f(b)]$ est inférieure à K.*

La démonstration s'inspire de la démonstration classique (voir, par exemple [40]). Notons que ce théorème est évident pour les arbres : une quasi-isométrie d'un arbre ne peut faire "d'allers et retours" trop longs et ne peut donc s'éloigner trop d'un segment.

Voici un corollaire important pour la théorie.

COROLLAIRE.— *Soient (X_1, d_1) et (X_2, d_2) deux espaces métriques géodésiques quasi-isométriques. Si (X_1, d_1) est hyperbolique, il en est de même pour (X_2, d_2).*

Fixons en effet $f : X_1 \to X_2$ et $g : X_2 \to X_1$ les applications dont l'existence est assurée par la quasi-isométrie entre X_1 et X_2. On suppose X_1 δ-hyperbolique. Soient $[x, y]$, $[y, z]$, $[z, x]$ trois segments de X_2 joignant x, y, z. Les images $g([x, y])$, $g([y, z])$ et $g([z, x])$ sont trois (λ, C)-quasi-géodésiques qui sont à distance inférieure à K de segments $[g(x), g(y)]$, $[g(y), g(z)]$ et $[g(z), g(x)]$. La δ-hyperbolicité de X_1 permet de montrer que tout point de $g([x, y])$ est à distance inférieure à $4\delta + 2K$ de $g([y, z]) \cup g([z, x])$. En appliquant f, on obtient la $(\lambda(4\delta+2K)+C)$-finesse du triangle x, y, z.

Ce corollaire montre bien la différence entre l'hyperbolicité et la courbure négative. Par exemple, le produit riemannien du plan hyperbolique $\mathbf{H}^2$ avec la sphère $\mathbf{S}^2$ est hyperbolique car quasi-isométrique à $\mathbf{H}^2$, mais ne peut pas être muni d'une métrique riemannienne à courbure négative. La notion d'hyperbolicité ne tient pas compte de la nature locale de la métrique. C'est pour cette raison que M. Gromov utilise dans [21] le terme "coarse hyperbolicity".

3. LES GROUPES HYPERBOLIQUES

3.1. Le lecteur aura deviné la définition suivante.

DÉFINITION.— *Un groupe de type fini Γ est hyperbolique si l'espace métrique (Γ, d_S) est hyperbolique pour une partie génératrice finie S.*

Il est clair maintenant que cette propriété ne dépend pas du choix de S ; l'hyperbolicité d'un groupe est une propriété géométrique.

Exemples : i) Un groupe libre est hyperbolique car son graphe de Cayley pour un système libre de générateurs est un arbre.

ii) Le groupe fondamental d'une variété compacte V à courbure négative est hyperbolique car il est quasi-isométrique au revêtement universel de V.

iii) Le groupe fondamental d'un polyèdre fini à courbure négative est hyperbolique.

iv) Un produit libre de deux groupe hyperboliques est hyperbolique (c'est un exercice facile).

La classe des groupes hyperboliques généralise l'importante notion de groupes à petite simplification $C'(1/6)$. Nous en rappelons rapidement la définition.

Soit $(S; R)$ une présentation d'un groupe Γ. Autrement dit, les éléments de R sont des mots en $S \cup S^{-1}$ et le groupe Γ est isomorphe au quotient du groupe libre de base S par le sous-groupe normal engendré par R. On suppose S et R finis. On peut toujours supposer que R est stable par passage à l'inverse et par permutations cycliques. Un mot m en $S \cup S^{-1}$ est une *pièce* si m est un préfixe commun à deux éléments distincts de R, c'est-à-dire si R contient deux éléments de la forme $r_1 = m\,m_1$ et $r_2 = m\,m_2$. Enfin, la longueur d'un mot w, c'est-à-dire le nombre de lettres qui le compose, est noté $|w|$.

DÉFINITION.— *Soit λ un réel positif et inférieur à 1. On dit que la présentation $(S; R)$ vérifie la condition $C'(\lambda)$ si pour toute pièce m, préfixe d'une relation r de R, on a : $|m| < \lambda\,|r|$.*

Un groupe est à petite simplification $C'(\lambda)$ s'il possède une présentation

vérifiant cette condition.

Ces groupes sont très bien compris, tout spécialement lorsque $\lambda = 1/6$ (voir [16], [18], [29]). Cependant, cette notion souffre d'un certain nombre d'inconvénients. D'abord, il est difficile de déterminer si un groupe est $C'(\lambda)$ puisque cette condition peut être vérifiée pour une présentation et pas pour une autre. D'autre part, un groupe à petite simplification $C'(1/6)$ sans torsion a une dimension cohomologique inférieure à 2. Ces groupes ne rendent donc pas compte des groupes fondamentaux des variétés compactes à courbure négative de dimension supérieure ou égale à 3. La théorie des groupes hyperboliques remédie en partie à ces inconvénients. Signalons cependant (nous y reviendrons plus loin) que les groupes $C'(1/5)$ sont également intéressants mais n'entrent pas dans le cadre hyperbolique.

THÉORÈME.— *Un groupe à petite simplification $C'(1/6)$ est hyperbolique.*

On trouvera les détails de la démonstration dans [15] ou [18]. Disons simplement que l'idée est la suivante. La présentation $(S; R)$ de Γ permet de construire un 2-complexe fini P dont le groupe fondamental est Γ. La condition $C'(1/6)$ permet alors de montrer que le revêtement universel $\widetilde{P}$ de P est hyperbolique.

Signalons, pour compléter ces quelques exemples de groupes hyperboliques, que M. Gromov énonce un résultat qui montre que les groupes hyperboliques constituent la "majorité". Soit $N(p, q, n_1, \cdots, n_q)$ le nombre de présentations de groupes ayant p générateurs et q relateurs de longueurs $n_1, n_2, \cdots, n_q$. Soit $N_h(p, q, n_1, \cdots, n_q)$ le nombre de celles qui définissent un groupe hyperbolique. L'affirmation de "généricité" s'exprime par le fait que, p et q étant fixés, la proportion N_h/N tend vers 1 lorsque $n_1, n_2, \cdots, n_q$ tendent vers l'infini.

3.2. La première étape dans la compréhension des groupes hyperboliques est une construction due à I. Rips. Fixons toujours un groupe Γ et une partie génératrice finie S. Fixons par ailleurs un entier positif n. Le polyèdre de Rips $P_n(\Gamma)$ est le polyèdre dont les sommets sont les éléments de Γ et

pour lequel $(k+1)$ éléments $\gamma_0, \gamma_1, \cdots, \gamma_k$ de Γ forment un k-simplexe s'ils sont distincts deux à deux et à distances relatives inférieures à n ; par exemple, le 1-squelette de $P_1(\Gamma)$ est le graphe de Cayley de (Γ, S). Il s'agit d'un polyèdre localement fini de dimension finie : les simplexes sont de dimension k inférieure au cardinal d'une boule de Γ de rayon n. L'action de Γ sur lui-même par translations à gauche se prolonge en une action de Γ sur $P_n(\Gamma)$. Cette action est propre, libre sur les sommets. Le stabilisateur de chaque point est fini et l'action est donc libre si Γ est sans torsion. Notons enfin que le quotient de $P_n(\Gamma)$ par cette action de Γ est compact.

Le théorème suivant est dû à I. Rips.

THÉORÈME.— *Si Γ est hyperbolique, $P_n(\Gamma)$ est contractile pour n assez grand.*

Avant d'esquisser la démonstration de ce théorème, donnons-en quelques corollaires.

Si Γ est sans torsion, l'espace quotient $P_n(\Gamma)/\Gamma$ est un espace d'Eilenberg-McLane qui est un polyèdre fini (après subdivision barycentrique). L'existence d'un tel espace est une propriété de finitude très intéressante (voir par exemple [4]). En particulier, Γ est de présentation finie et de dimension cohomologique finie.

Lorsque l'on ne fait pas d'hypothèse sur la torsion de Γ, on obtient les mêmes résultats "rationalisés".

COROLLAIRE.— *Soit Γ un groupe hyperbolique. Alors* : i) *Γ est de présentation finie.*

ii) *Γ ne possède qu'un nombre fini de classes de conjugaison d'éléments de torsion.*

ii) *La cohomologie rationnelle de Γ est de dimension finie.*

Esquissons la démonstration du théorème. Soit $Q \subset P_n(\Gamma)$ un sous-polyèdre fini. Nous nous proposons de construire une rétraction par déformation de Q sur un point. Parmi tous les sommets de Q, choisissons-en un, noté x, qui est plus éloigné de l'élément neutre e de Γ que tous les autres sommets *i.e.* pour tout sommet y de Q, on a :

$$d_S(e, y) \leq d_S(e, x) \ .$$

Supposons que (Γ, d_S) soit δ-hyperbolique et choisissons l'entier n supérieur à $4\delta + 2$. On suppose que $d_S(e,x) \geq n/2$ car, dans le cas contraire, Q serait un simplexe de $P_n(\Gamma)$ et il serait très facile de construire la rétraction cherchée. Soit x' un point de Γ situé sur un segment $[e,x]$ à distance $n/2$ de x (on suppose n pair pour simplifier). On a donc :

$$d_S(e,x') = d_S(e,x) - \frac{n}{2}.$$

La définition même de l'hyperbolicité, appliquée aux quatre points e, x, x', y montre le fait suivant. Si un sommet y de Q est à distance inférieure à n de x, ce même sommet est aussi à distance inférieure à n de x'.

On comprend alors comment procéder. Déplaçons le sommet x de Q vers le point x' et ne déplaçons pas les autres sommets de Q. Ceci produit une homotopie entre le plongement $Q \hookrightarrow P_n(\Gamma)$ et une application $j : Q \to P_n(\Gamma)$. On peut alors répéter l'opération sur le polyèdre $j(Q)$. Après un nombre fini d'étapes de ce genre, on aura construit une homotopie entre le plongement $Q \hookrightarrow P_n(\Gamma)$ et une application $j' : Q \to P_n(\Gamma)$ dont l'image est contenue dans la boule de centre e et de rayon $n/2$. L'application j' est alors homotope à une constante.

Signalons, pour terminer ce paragraphe, quelques questions soulevées par ce théorème.

Problème : *Un groupe hyperbolique contient-il un sous-groupe d'indice fini sans torsion ? Un groupe hyperbolique est-il résiduellement fini (rappelons qu'un groupe Γ est résiduellement fini si, pour tout γ non trivial dans Γ, il existe un sous-groupe d'indice fini qui ne contient pas γ) ?*

Problème : *La dimension cohomologique rationnelle d'un groupe* (resp. *la dimension cohomologique virtuelle*) *est-elle un invariant géométrique ? Voir* [2] *pour le cas hyperbolique.*

Le polyèdre $P_n(\Gamma)$ est certes contractile pour n assez grand mais il n'est pas muni d'une métrique naturelle. Il serait agréable de remplacer $P_n(\Gamma)$ par un espace convexe. Rappelons qu'un espace métrique (X,d) géodésique est *convexe* si pour toute paire de segments $\sigma : [a,b] \to X$ et $\sigma' : [a',b'] \to X$ la fonction distance $(t,s) \in [a,b] \times [a',b'] \mapsto d(\sigma(t), \sigma'(s))$ est convexe. Ceci

entraîne bien sûr l'unicité du segment joignant deux points et démontre en particulier la contractibilité de X. Un exemple classique est fourni par les variétés simplement connexes complètes à courbure négative ou nulle.

Problème : *Soit Γ un groupe hyperbolique. Existe-t-il un espace métrique convexe (X, d), de dimension finie, tel que Γ opère proprement, par isométries de X, avec quotient compact ?*

4. LE BORD

4.1. Soit V une variété riemannienne complète, simplement connexe, à courbure sectionnelle inférieure à $-k^2 < 0$. On sait qu'il est possible de compactifier V en lui adjoignant un *bord* ∂V. Les points de ∂V correspondent aux points à l'infini des rayons géodésiques $[0, +\infty[\to V$ et deux tels rayons définissent le même point du bord s'ils sont à distance bornée. Le bord ainsi obtenu peut être naturellement muni d'une topologie ; il est homéomorphe à une sphère. Presque toute l'étude des variétés à courbure négative passe par l'étude de la géométrie de cette sphère sur laquelle agit le groupe d'isométries de V.

Cette construction ainsi que ses principales propriétés peuvent être généralisées au contexte des espaces et groupes hyperboliques.

Soit (X, d) un espace métrique δ-hyperbolique, géodésique et propre, muni d'un point base w. On dit qu'une suite (x_n) de points de X *tend vers un point à l'infini* si les produits de Gromov $(x_n \mid x_p)_w$ tendent vers l'infini lorsque n et p tendent vers l'infini. Deux telles suites (x_n) et (y_p) définissent le même point à l'infini si $(x_n \mid y_p)_w$ tend vers l'infini. L'ensemble des points à l'infini ainsi obtenu se note ∂X et s'appelle le *bord* de X. Il est facile de s'assurer que cette définition ne dépend pas du choix du point base w.

Cette définition ne diffère pas de celle que nous avons évoquée dans le cas des variétés à courbure négative. En effet, considérons un rayon géodésique issu de w, c'est-à-dire une application $g : [0, +\infty[\to X$ telle que $d(w, g(t)) = t$. La suite x_n définie par $x_n = g(n)$ vérifie évidemment la condition que $(x_n \mid x_p)_w$ tend vers l'infini. Réciproquement, si une suite

de points x_n tend vers un point à l'infini, il n'est pas difficile de montrer qu'une suite de segments $[x_0, x_n]$ "tend" vers un rayon géodésique.

En d'autres termes, on peut aussi définir le bord de X comme l'ensemble des rayons où l'on identifie deux rayons s'ils sont à distance bornée.

Revenons à la première définition et montrons comment il est possible de définir une topologie sur ∂X. Si a et b sont deux points de ∂X, on pose :

$$(a \mid b)_w = \inf \varinjlim_{n,p \to \infty} (x_n \mid y_p)_w \in \mathbf{R} \cup \{\infty\}$$

où la borne inférieure est prise sur toutes les suites (x_n) et (y_n) tendant respectivement vers a et b.

PROPOSITION.— *Les ensembles* $\mathcal{U}_k = \{(a,b) \in (\partial X)^2 , (a|b)_w \geq k\}$ *engendrent une structure uniforme sur* ∂X. *Pour la topologie correspondante,* ∂X *est compact.*

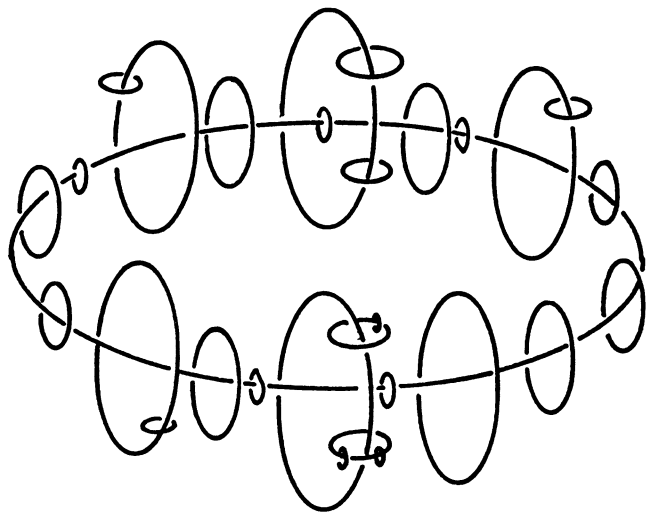
Exemples : i) Le bord d'une variété riemannienne complète simplement connexe à courbure sectionnelle inférieure à $-k^2 < 0$ coïncide avec le bord usuel ; c'est donc une sphère.

ii) Le bord d'un arbre métrique localement fini coïncide avec l'ensemble de ses bouts (au sens de Freudenthal). En effet, dans ce cas, deux rayons de même origine ne sont à distance bornée que s'ils coïncident. Dans le cas général, l'ensemble $bt(X)$ des bouts de X et ∂X sont reliés de la façon suivante. Si (x_n) tend vers un point de ∂X, cette suite quitte tout compact et définit un bout. On obtient ainsi une application $\partial X \to bt(X)$ qui est surjective. Les fibres de cette surjection sont précisément les composantes connexes de ∂X (ce fait m'a été signalé par F. Paulin).

iii) Soit X l'espace obtenu en recollant deux disques de Poincaré sur un point. Le bord de X est la réunion disjointe de deux cercles.

iv) Il ne faut pas se laisser abuser par la simplicité des exemples précédents. Soit X l'espace obtenu en recollant deux surfaces compactes Σ_1 et Σ_2 à courbure -1 sur un point w et $\widetilde{X}$ le revêtement universel de X muni de la métrique géodésique naturelle. Il est clair que $\widetilde{X}$ est hyperbolique et que son bord s'identifie à l'ensemble des rayons géodésiques de $\widetilde{X}$ issus d'un point $\widetilde{w}$ situé au-dessus de w ou encore à l'ensemble des

applications $g : [0, \infty[\to X$ localement isométriques et issues de w. Parmi ces applications, certaines ont leur image entièrement contenue dans Σ_1, produisant ainsi un cercle dans $\partial\widetilde{X}$. D'autres ont leur image contenue dans Σ_2. D'autres encore peuvent "osciller" entre Σ_1 et Σ_2 un certain nombre de fois avant de se stabiliser dans Σ_1 ou Σ_2. D'autres enfin peuvent osciller une infinité de fois entre Σ_1 et Σ_2. La figure suivante essaie de suggérer la structure de $\partial\widetilde{X}$.



Ainsi, la nouveauté par rapport aux variétés à courbure négative est le fait que le bord de X hérite d'une topologie plus complexe.

L'une des propriétés principales de ∂X est qu'il ne dépend que de la classe de quasi-isométrie de X. C'est l'idée importante de (la première partie de) la démonstration du théorème de rigidité de Mostow [31].

PROPOSITION.— *Une quasi-isométrie entre deux espaces métriques hyperboliques géodésiques et propres se prolonge en un homéomorphisme de leurs bords.*

La démonstration résulte du fait que l'image d'un rayon géodésique par une quasi-isométrie reste à distance bornée d'un rayon.

En particulier, si Γ est un groupe hyperbolique, on peut définir son *bord*

$\partial\Gamma$ comme étant le bord de l'espace métrique (Γ, d_S) (ou plus précisément du graphe de Cayley puisque nous supposons nos espaces géodésiques). Ce bord ne dépend pas du choix de la partie génératrice S.

On a ainsi associé à chaque groupe hyperbolique un espace compact $\partial\Gamma$. L'action de Γ sur lui-même par translations produit alors à l'infini une action de Γ sur $\partial\Gamma$ par homéomorphismes. C'est cette action qui permet de mieux comprendre la structure du groupe Γ.

Avant de montrer sur un exemple comment fonctionne ce programme, énonçons une proposition élémentaire.

PROPOSITION.— *Soit Γ un groupe hyperbolique*

i) *si $\partial\Gamma$ est vide, Γ est fini.*

ii) *$\partial\Gamma$ contient deux points si et seulement si Γ contient un sous-groupe cyclique infini d'indice fini.*

iii) *dans les autres cas, $\partial\Gamma$ est infini.*

Il s'agit d'abord de montrer que $\partial\Gamma$ contient au moins deux points dès que Γ est infini. Ceci résulte du fait suivant. Soit γ_n une suite infinie d'éléments distincts de Γ. Supposons, pour simplifier, que $d_S(e, \gamma_n)$ soit pair et soit α_n le milieu d'un segment $[e, \gamma_n]$. Il est clair que, par passage à une sous-suite, α_n^{-1} et $\alpha_n^{-1}\gamma_n$ définissent deux points différents de $\partial\Gamma$.

Si $\partial\Gamma$ contient exactement deux éléments, Γ a deux bouts et il est bien connu que Γ contient un sous-groupe cyclique d'indice fini.

Si $\partial\Gamma$ est fini, $\partial\Gamma$ coïncide avec l'ensemble des bouts de Γ et on sait qu'un groupe ne peut avoir que $0, 1, 2$ ou une infinité de bouts.

Voici, en application, une idée de démonstration d'un théorème déjà énoncé au premier paragraphe.

THÉORÈME.— *Un groupe Γ quasi-isométrique à un groupe libre est virtuellement libre.*

Pour simplifier, supposons Γ sans torsion. Ainsi, Γ est un groupe hyperbolique et son bord est homéomorphe à celui d'un groupe libre, c'est-à-dire un ensemble de Cantor. Il en résulte que Γ a une infinité de bouts. Les théorèmes de Stallings (sur les bouts) et de Grushko montrent alors que Γ est isomorphe à un produit libre $\Gamma_1 * \cdots \Gamma_k$ de groupes ayant au plus

deux bouts. En choisissant convenablement la partie génératrice finie de Γ, on constate que le graphe de Cayley de chaque Γ_i se plonge géodésiquement dans celui de Γ. Chaque Γ_i est donc hyperbolique et son bord est contenu dans celui de Γ. Puisque Γ_i a au plus 2 bouts et que $\partial\Gamma_i$ est totalement discontinu, $\partial\Gamma_i$ contient au plus 2 points. Ceci montre que chaque Γ_i, étant sans torsion, est isomorphe à $\mathbf{Z}$. Ainsi, Γ est un groupe libre. Lorsque l'on ne fait plus d'hypothèse sur la torsion de Γ, la démonstration est un peu plus complexe mais utilise les mêmes idées.

Problème.— *Décrire la topologie de $\partial\Gamma$, tant du point de vue global que local (connexité locale si $\partial\Gamma$ est connexe, par exemple ?). Voir* [2].

4.2. Une fois la définition du bord mise au point, il n'est pas très difficile d'étendre les résultats bien classiques concernant la structure des isométries d'une variété à courbure négative. Nous ne ferons que citer le résultat obtenu dans le cas des groupes hyperboliques.

THÉORÈME.— *Soit γ un élément d'un groupe hyperbolique Γ. Deux cas sont possibles :*

i) *γ est d'ordre fini.*

ii) *L'action de γ sur $\partial\Gamma$ a précisément deux points fixes x_+ et x_-, l'un attractif et l'autre répulsif. Plus précisément, pour tout voisinage $\mathcal{U}$ de x_+ (resp. x_-) et tout compact K de $\partial\Gamma - \{x_-\}$ (resp. $\partial\Gamma - \{x_+\}$, il existe un entier n_0 tel que $\gamma^n(K) \subset \mathcal{U}$ pour $n \geq n_0$ (resp. $n \leq n_0$).*

De plus, si a est un point de $\partial\Gamma$ et Γ_a le sous-groupe de Γ stabilisant a, alors Γ_a est fini ou contient un sous-groupe infini cyclique d'indice fini.

La méthode de F. Klein pour construire des groupes libres (le "lemme du ping-pong", voir [26]) entraîne le corollaire suivant qui décrit la structure des sous-groupes d'un groupe hyperbolique.

COROLLAIRE.— *Soit Γ_1 un sous-groupe d'un groupe hyperbolique. Alors, trois cas sont possibles :*

i) *Γ_1 est fini.*

ii) *Γ_1 contient un sous-groupe infini cyclique d'indice fini.*

iii) *Γ_1 contient un sous-groupe libre à deux générateurs.*

Jusqu'à présent, nous nous sommes contentés d'une topologie sur le bord ∂X. Ce bord est muni en fait d'une structure beaucoup plus riche : une structure quasi-conforme. Fixons un réel $\varepsilon > 0$. Si a et b sont deux points du bord ∂X d'un espace métrique géodésique hyperbolique propre, on pose

$$\rho_\varepsilon(a, b) = \exp(-\varepsilon(a \mid b)_w).$$

Malheureusement, ρ_ε ne définit pas une distance sur ∂X : il ne vérifie qu'une inégalité quasi-ultramétrique :

$$\rho_\varepsilon(a, c) \leq (1 + \varepsilon') \max(\rho_\varepsilon(a, b), \rho_\varepsilon(b, c))$$

avec $\varepsilon' = \exp(\varepsilon\delta) - 1$.

Cependant, ρ_ε fait "presque" l'affaire. On pose :

$$d_\varepsilon(a, b) = \inf \sum \rho_\varepsilon(x_i, x_{i+i})$$

où la borne inférieure est prise sur toutes les chaînes finies connectant a à b. On s'assure alors que, si ε est asez petit, ρ_ε et d_ε diffèrent peu :

$$(1 - 2\varepsilon')\, \rho_\varepsilon(a, b) \leq d_\varepsilon(a, b) \leq \rho_\varepsilon(a, b).$$

Pour ε assez petit, d_ε est donc une distance sur ∂X qui définit la topologie de ∂X.

Convenons de dire qu'un homéomorphisme f d'un espace métrique (X_1, d_1) vers (X_2, d_2) est K-quasi-conforme si, pour tout x de X_1, on a

$$\limsup_{r \to 0} \frac{\operatorname{Sup}\{d_2(f(x), f(y)) \mid d_1(x, y) = r\}}{\operatorname{Inf}\{d_2(f(x), f(y)) \mid d_1(x, y) = r\}} \leq K.$$

Nous savons qu'une isométrie d'un espace δ-hyperbolique X induit un homéomorphisme de ∂X. Il se trouve que cet homéomorphisme est $K(\varepsilon, \delta)$-quasi-conforme pour la métrique d_ε où $K(\varepsilon, \delta)$ est une constante tendant vers 1 lorsque ε tend vers 0. D'une certaine façon, on peut donc dire que l'action d'une isométrie à l'infini est "conforme". De la même façon, on s'assure que l'homéomorphisme de ∂X induit par une quasi-isométrie de X est un homéomorphisme K-quasi-conforme pour une certaine constante K.

C'est dans ce sens que nous dirons que le bord d'un groupe hyperbolique est muni d'une structure quasi-conforme naturelle.

La nature locale de cette structure quasi-conforme pour un groupe hyperbolique général est encore mystérieuse et mérite sans conteste une étude approfondie. On trouvera dans [33] une description précise dans le cas des espaces riemanniens symétriques.

Nous avons énoncé plus haut le résultat selon lequel un groupe quasi-isométrique à $\mathbf{H}^n$ ($n \geq 3$) est une extension finie d'un groupe discret cocompact d'isométries de $\mathbf{H}^n$. La méthode d'approche est la suivante. Un tel groupe est bien sûr hyperbolique et son bord est quasi-conformément celui de $\mathbf{H}^n$, c'est-à-dire une sphère $\mathbf{S}^{n-1}$. L'action de Γ sur $\partial\Gamma$ mène à une action de Γ sur $\mathbf{S}^{n-1}$ qui est uniformément quasi-conforme. Lorsque $n = 3$, on montre que cette action est en fait conforme pour une certaine structure conforme mesurable. Le théorème d'Ahlfors-Behrs permet alors de conjuguer cette action à une action conforme de Γ sur $\mathbf{S}^2$, c'est-à-dire à un groupe Kleinien. Lorsque $n \geq 4$, la preuve de Gromov-Tukia est plus compliquée.

5. ASPECTS ALGORITHMIQUES

5.1. Nous allons décrire dans ce paragraphe un certain nombre de résultats dont l'origine est due à J. Cannon [5] et qui ont été développés par M. Gromov ([21], [25]) et par J. Cannon, D. Epstein, D. Holt, M. Paterson et W. Thurston [9]. Il s'agit d'adapter au contexte des groupes de type fini les idées et méthodes de la dynamique symbolique (M. Morse, R. Bowen, M. Manning).

Pour motiver ce qui va suivre, rappelons d'abord comment résoudre le problème des mots dans un groupe libre Γ de base $a_1, \cdots, a_n$. Tout élément de Γ s'écrit de manière *unique* comme un mot *réduit*, c'est-à-dire ne contenant pas de sous-mot du type $a_i \cdot a_i^{-1}$ ou $a_i^{-1} \cdot a_i$. Il est important de constater que, pour décider si un mot est réduit, il n'est pas nécessaire de le connaître dans son intégralité mais il suffit de vérifier si tous ses sous-mots de longueur 2 sont réduits.

M. Dehn montre qu'un phénomène analogue se produit pour le groupe fondamental d'une surface compacte orientable de genre $g \geq 2$, présenté de manière usuelle :

$$\Gamma = (a_1, b_1, \cdots, a_g, b_g \,;\, a_1\, b_1\, a_1^{-1}\, b_1^{-1} \cdots a_g\, b_g\, a_g^{-1}\, b_g^{-1} = 1)\,.$$

Désignons par R l'unique relateur de cette présentation et soient $R_1 = R, R_2, \cdots, R_{2g}$ les $2g$ permutations cycliques du mot R. Supposons qu'un mot m en les $a_i^{\pm 1}$ soit de la forme $m_1\, w\, m_2$ où w est un préfixe de l'un des $R_i^{\pm 1}$, i.e. tel que $R_i^{\pm 1} = w \cdot w'$. Dans le groupe Γ, l'élément correspondant à m est égal à celui correspondant à $m_1\, w'^{-1}\, m_2$. Si la longueur de w est strictement supérieure à la moitié de celle de R, le mot $m_1\, w'^{-1}\, m_2$ est strictement plus court que m. On montre ainsi, par récurrence, que tout élément de Γ peut être représenté par un mot m en les $a_i^{\pm 1}$ *réduit au sens de Dehn*, c'est-à-dire vérifiant :

i) m est un mot réduit (*i.e.* ne contenant ni $a_i\, a_i^{-1}$ ni $a_i^{-1}\, a_i$) ;

ii) si w est un préfixe de $R_i^{\pm 1}$ avec $|w| > \frac{1}{2}\,|R|$, alors w n'est pas un sous-mot de m.

Le résultat important de M. Dehn est le suivant : un mot non trivial réduit au sens de Dehn représente un élément non trivial de Γ.

Ici encore, on observe que pour décider si un mot est réduit au sens de Dehn, il suffit de vérifier si tous ses sous-mots de longueur $2g$ le sont. Une mémoire de taille $2g$ suffit ...

Nous allons généraliser cette idée en deux étapes. Nous introduirons d'abord la notion que M. Gromov appelle *groupe Markovien* (voir aussi [19]). Puis nous dirons quelques mots sur la notion plus efficace de *groupe automatique.*

Soit $\mathcal{G}$ un graphe fini orienté muni d'un sommet privilégié $*$ et dont les arêtes sont étiquetées par les éléments d'un ensemble fini S. Deux arêtes différentes peuvent porter la même étiquette. Considérons un chemin fini de $\mathcal{G}$ d'origine $*$, c'est-à-dire une suite finie de sommets $x_0, x_1, \cdots, x_n$ telle qu'une arête orientée joigne x_i à x_{i+1} $(i = 0, 1, \cdots, n)$. On peut alors lire sur l'arête (x_i, x_{i+1}) un élément de S et on produit ainsi un mot m de n lettres en les éléments de S. L'ensemble $\mathcal{L}$ des mots ainsi obtenus sera appelé le *langage* de $\mathcal{G}$. C'est une partie de l'ensemble S^* de toutes les

suites finies d'éléments de S. Une partie de S^* est un *langage de Markov* si elle est le langage d'un certain graphe de ce type.

Supposons maintenant que l'on considère un groupe Γ et que l'ensemble S soit une partie finie de Γ. Un élément de S^*, c'est-à-dire un mot en les éléments de S, définit par produit un élément de Γ. On a donc une application naturelle $\pi : S^* \to \Gamma$. Cette application est surjective si S engendre Γ comme monoïde.

DÉFINITION.— *On dit qu'un groupe Γ est Markovien s'il existe une partie finie S de Γ et un graphe fini $\mathcal{G}$, orienté, muni d'un point base et étiqueté par S dont le langage $\mathcal{L} \subset S^*$ soit tel que la restriction de π à $\mathcal{L}$ soit bijective. En d'autres termes, tout élément de Γ s'écrit de manière unique comme un mot en les éléments de S appartenant au langage de $\mathcal{G}$.*

Si, de plus, on peut choisir pour S n'importe quelle partie finie engendrant Γ comme monoïde et si l'application $\pi : \mathcal{L} \to \Gamma$ préserve les longueurs naturelles de part et d'autre (i.e. $|w| = \|\pi(w)\|_S$), on dira que Γ est fortement Markovien.

Par exemple, le lecteur n'aura aucun mal à construire un graphe $\mathcal{G}$, étiqueté par $S = \{a, a^{-1}, b, b^{-1}\}$ et dont le langage est constitué des mots réduits de S^*. Ainsi, un groupe libre est Markovien.

A la terminologie près, le résultat suivant est dû à J. Cannon [5].

THÉORÈME.— *Tout groupe hyperbolique est fortement Markovien.*

Avant de donner quelques indications sur la preuve de ce théorème, explicitons un corollaire important.

COROLLAIRE.— *Soit Γ un groupe hyperbolique et S une partie génératrice finie quelconque. Soit $a_S(n)$ le nombre d'éléments de Γ de la longueur n par rapport à S. Alors, la série formelle $f(t) = \sum_{n\geq 0} a_S(n)\, t^n$ est une fraction rationnelle de la variable t.*

Ceci résulte du théorème précédent et de l'énoncé analogue pour le nombre $a(n)$ de chemins de longueur n dans un graphe fini, qui se calcule facilement en termes des puissances de la matrice d'incidence du graphe.

Nous commençons maintenant l'esquisse de la preuve du théorème de J. Cannon. Soit Γ un groupe engendré comme monoïde par la partie finie

S et m un élément de S^*, c'est-à-dire un mot en les éléments de S. On dit que m est minimal si m est un mot de longueur minimale représentant $\pi(m)$ de Γ , i.e. si $|m| = \|\pi(m)\|_S$. Les mots minimaux forment une partie $\mathcal{M}$ de S^*. Nous allons montrer que $\mathcal{M}$ est un langage de Markov.

Soit m un élément de $\mathcal{M}$. On lui associe l'ensemble $C(m)$ des mots w de S^* tels que mw soit un mot de $\mathcal{M}$. Nous disons que m et m' sont de même type si $C(m) = C(m')$. L'ensemble $\mathcal{G}$ des types forme un graphe orienté étiqueté par S ; on joint le type t_1 au type t_2 par une arête portant l'étiquette s si t_1 est le type d'un mot $s_1, \cdots, s_n$ de $\mathcal{M}$ et si t_2 est le type de $s_1, \cdots, s_n, s$, supposé appartenir aussi à $\mathcal{M}$. Le sommet privilégié $*$ de $\mathcal{G}$ est celui correspondant à la suite vide. Il est évident que les chemins de $\mathcal{G}$ issus de $*$ correspondent bijectivement aux mots de $\mathcal{M}$. Par conséquent, si $\mathcal{G}$ est fini, la partie $\mathcal{M}$ de S^* est un langage de Markov.

Supposons donc que Γ soit hyperbolique et montrons qu'il n'y a qu'un nombre fini de types. Soit R un entier ayant la propriété suivante. Si γ_1 et γ_2 sont deux éléments de Γ à distance 1, alors deux segments quelconques $[e, \gamma_1]$ et $[e, \gamma_2]$ sont à distance de Hausdorff inférieure à R. L'existence d'un tel R résulte immédiatement de l'hyperbolicité de Γ. Si γ est un élément de Γ, nous appellerons $(2R+1)$-*niveau* de γ la partie $N(\gamma)$ de la boule B de Γ de centre e de et rayon $2R+1$ formée des éléments ζ tels que $d_S(\gamma\zeta, e) < d(\gamma, e)$. Comme il n'y a qu'un nombre fini de parties de B, la finitude du nombre de types et donc le fait que $\mathcal{M}$ est un langage de Markov résultent de l'affirmation suivante.

Si $\pi(m)$ et $\pi(m')$ ont même $(2R+1)$-niveau, ils ont même type.

Il s'agit de montrer, par récurrence sur $|w|$ que si mw est dans $\mathcal{M}$, il en est de même pour $m'w$. Si w est vide, c'est évident... Par récurrence, on suppose que mw, $m'w$ et mws sont dans $\mathcal{M}$ pour un certain s de S et il s'agit de montrer que $m'ws$ est dans $\mathcal{M}$. Soit $\alpha\beta$ un élément de $\mathcal{M}$ tel que $\pi(m'ws) = \pi(\alpha\beta)$ et $|\alpha| = |m'| - 1$. On vérifie facilement que la définition de R permet d'affirmer que $d_S(\pi(\alpha), \pi(m')) \leq 2R+1$. Il en résulte que $\pi(m')^{-1}\pi(\alpha)$ est dans le $(2R+1)$-niveau de $\pi(m')$ et donc dans celui de $\pi(m)$. En d'autres termes :

$$d_S(\pi(m'^{-1}\alpha), e) < d_S(\pi(m), e) = |m|.$$

On observe alors que : $\pi(mws) = \pi(m\, m'^{-1}\, \alpha\beta)$. Il en résulte que :

$$|mws| < |m| + |\beta|$$

$$|m| + |w| + 1 < |m| + |\beta|$$

$$|\beta| \geq |w| + 2\,.$$

Finalement : $|m'ws| \leq |\alpha| + 1 + |\beta| - 2 + 1 = |\alpha| + |\beta| = d_S(\pi(m'ws), e)$. Nous avons donc bien montré que $m'ws$ est minimal.

Ainsi, $\mathcal{M}$ est un langage de Markov. Ceci ne montre pas encore le théorème que nous avons en vue car l'application $\pi : \mathcal{M} \to \Gamma$ est bien sûr surjective mais certainement pas injective. Un élément de Γ peut en général s'écrire de plusieurs manières comme mot de longueur minimale. Pour sélectionner un unique mot de $\mathcal{M}$ représentant un élément de Γ, on choisit un ordre total quelconque sur S. Pour chaque élément de Γ, on sélectionne l'élément de $\pi^{-1}(\gamma)$ qui est le premier par ordre lexicographique. Cette méthode détermine une partie $\mathcal{L}$ de $\mathcal{M}$ pour laquelle $\pi : \mathcal{L} \to \Gamma$ est bien sûr bijective. Il n'est pas très difficile de déduire du fait que $\mathcal{M}$ est un langage de Markov qu'il en est de même pour $\mathcal{L}$. Ceci établit le théorème.

5.2. La notion de groupe Markovien a un grave inconvénient : le graphe étiqueté $\mathcal{G}$ ne détermine pas le groupe. Nous savons en effet, par définition, que tout élément du groupe s'écrit comme un mot en les générateurs appartenant au langage de $\mathcal{G}$, mais nous n'avons aucune information sur la manière de multiplier deux éléments du groupe. Voici un exemple. Les deux groupes $\Gamma_1 = (a, b, c \,|\, ab = ba\,,\ ac = ca\,,\ bc = cb)$ et $\Gamma_2 = (a, b, c \,|\, ac = ca\,,\ bc = cb\,,\ ab = bac)$ ne sont pas isomorphes (l'un est $\mathbf{Z}^3$ et l'autre le groupe de Heisenberg) ; cependant, tout élément de Γ_1 ou Γ_2 s'écrit de manière unique comme $a^m\, b^n\, c^p$ $(m, n, p \in \mathbf{Z})$. Il est donc facile de trouver un même langage de Markov pour Γ_1 et Γ_2.

Les groupes automatiques, introduits dans [9], n'ont pas cet inconvénient. Nous allons d'abord élargir la notion de langage de Markov par celle de *langage régulier*. Il s'agit d'un concept classique en informatique.

DÉFINITION.— *Un automate fini M est constitué des données suivantes :*

i) *un ensemble fini E dont les éléments sont appelés les états, dont l'un, noté $*$, est l'état initial. On dispose aussi d'une partition de E en deux parties O et N (pour "oui" et "non")* ;

ii) *un ensemble fini A, appelé alphabet* ;

iii) *une application de transition $(a, \varepsilon) \in A \times E \mapsto a \,.\, \varepsilon \in E$.*

Supposons que l'on se donne un élément de A^*, c'est-à-dire une suite finie $(a_1, a_2, \cdots, a_n)$ d'éléments de A. On peut alors définir une suite d'états par :

$$\varepsilon_1 = a_1 \cdot * \quad , \quad \varepsilon_2 = a_2 \cdot \varepsilon_1, \cdots, \varepsilon_n = a_n \cdot \varepsilon_{n-1} \,.$$

L'ensemble $\mathcal{L}(M)$ des mots de A^* tels que le dernier état ε_n soit dans O est le *langage* de l'automate M. Une partie $\mathcal{L}$ de A^* est un *langage régulier* s'il existe un automate fini dont c'est le langage. L'avantage des langages réguliers par rapport aux langages de Markov est que, dans cette nouvelle situation, un préfixe d'un élément du langage n'est pas nécessairement dans ce langage.

Avant de pouvoir introduire la notion de groupe automatique, il nous faut encore donner une définition technique. Soient A_1 et A_2 deux ensembles finis. Un langage $\mathcal{L}$ sur (A_1, A_2) est une partie de $A_1^* \times A_2^*$. Une difficulté se présente car $A_1^* \times A_2^*$ contient des couples de mots de longueurs différentes et un langage sur (A_1, A_2) n'est pas un langage sur $A_1 \times A_2$. On introduit alors deux nouveaux symboles Fr_1 et Fr_2 et on pose $B = (A_1 \cup \{Fr_1\}) \times (A_2 \cup \{Fr_2\}) - \{(Fr_1, Fr_2)\}$. En complétant la composante la plus courte d'un élément de $A_1^* \times A_2^*$ à l'aide de Fr_1 ou Fr_2, on obtient deux mots de même longueur, c'est-à-dire un élément de B^*. Un langage $\mathcal{L}$ sur (A_1, A_2) se complète donc en un langage $\overline{\mathcal{L}}$ sur B. On dira que $\mathcal{L}$ est un langage régulier sur (A_1, A_2) si $\overline{\mathcal{L}}$ est régulier, c'est-à-dire s'il existe un automate d'alphabet B dont le langage est $\overline{\mathcal{L}}$. On dira aussi que cet automate est sur (A_1, A_2) et que son langage est $\mathcal{L}$.

DÉFINITION.— *Un groupe Γ est automatique s'il existe une partie finie $S = \{s_1, \cdots, s_n\}$ de Γ engendrant Γ comme monoïde et des automates finis $W, M_0, M_1, \cdots, M_n$ tels que* :

i) *l'alphabet de W est S et l'application $\pi : \mathcal{L}(W) \to \Gamma$ est surjective* ;

ii) *pour $0 \leq i \leq n$, M_i est un automate sur (S, S) et son langage est*

constitué des couples (m, m') *de mots de* S^* *tels que* m *et* m' *sont dans* $\mathcal{L}(W)$ *et que* $\pi(m) = \pi(m') \cdot s_i$. *(Pour* $i = 0$, *on pose* $s_o = e$, *élément neutre de* Γ.*)*

En d'autres termes, tout élément de Γ s'écrit comme un mot en S appartenant à un langage régulier, mais on ne suppose pas *a priori* l'unicité de l'écriture (on pourrait en fait le supposer). Cependant, l'automate M_0 permet de décider si deux mots du langage de W définissent le même élément de Γ. Par ailleurs, les automates $M_1, M_2, \cdots, M_n$ permettent de multiplier à droite par $s_1, s_2 \cdots, s_n$ et décrivent donc la structure algébrique du groupe.

Il est bien connu que la présentation d'un groupe par générateurs et relations est particulièrement peu commode. L'idée développée dans [9] est que la donnée d'un groupe automatique par ses automates est remarquablement efficace et permet des calculs très rapides dans le groupe. Une partie de [9] consiste à mettre au point des méthodes de construction explicite d'automates de taille "raisonnable" (voir aussi [14]).

THÉORÈME.— *Un groupe hyperbolique est automatique.*

La démonstration est essentiellement la même que celle que nous avons esquissée plus haut pour montrer qu'un groupe hyperbolique est fortement Markov.

La classe des groupes automatiques dépasse de loin celle des groupes hyperboliques. Elle contient par exemple les groupes virtuellement abéliens de type fini et elle est stable par produits finis. Elle ne contient cependant pas les groupes nilpotents non abéliens. Malheureusement, la structure algébrique et géométrique de ces groupes automatiques est beaucoup moins bien comprise que celle des groupes hyperboliques (voir cependant [15] et [17]). Pour terminer ce paragraphe, nous énonçons deux problèmes qui illustrent notre manque de connaissance géométrique de ces groupes.

Problème.— *Peut-on développer une théorie du bord des groupes automatiques, analogue à celle développée dans ce cas hyperbolique ?*

Problème.— *Le groupe fondamental d'une variété compacte à courbure négative ou nulle est-il automatique ?*

6. VERS LES GROUPES SEMI-HYPERBOLIQUES

On aimerait aller plus loin... Beaucoup de groupes intéressants ne sont pas hyperboliques alors que la méthode géométrique devrait permettre de mieux les comprendre. Voici quelques exemples :

i) le groupe fondamental d'une variété compacte à courbure négative ou nulle ;

ii) les groupes à petite simplification $C'(1/5)$;

iii) les réseaux dans les groupes de Lie semi-simples, en particulier $SL(n, \mathbf{Z})$.

Il s'agirait de trouver une condition de nature métrique sur le graphe de Cayley qui soit invariante par quasi-isométrie et qui permette de rendre compte de ces exemples. La difficulté est claire : contrairement à la négativité stricte, la négativité au sens large de la courbure est une propriété instable et se comporte mal par quasi-isométrie.

Pour terminer cet exposé, nous voudrions décrire deux notions généralisant l'hyperbolicité et qui pourraient peut-être servir de base à ces "groupes semi-hyperboliques" que l'on aimerait définir.

La première est introduite par J. Cannon [6].

DÉFINITION.— *Soit S une partie génératrice finie du groupe Γ . On dit que Γ est presque convexe par rapport à S s'il existe des constantes k et $C > 0$ ayant la propriété suivante. Soient γ_1 et γ_2 deux éléménts de Γ sur la sphère de centre e (élément neutre de Γ) et de rayon n et tels que $d_S(\gamma_1, \gamma_2) \leq k$. Alors, il existe un chemin de longueur inférieure à C dans le graphe de Cayley, joignant γ_1 à γ_2 et entièrement contenu dans la boule de centre e et de rayon n.*

J. Cannon montre que les groupes virtuellement abéliens sont presque convexes pour n'importe quelle partie génératrice finie. Il est par ailleurs très facile de s'assurer que les groupes hyperboliques sont presque convexes (pour tout S). Dans [9], les auteurs annoncent qu'il en est de même pour tous les groupes automatiques.

Problème.— *La presque convexité d'un groupe dépend-elle de la partie*

génératrice finie ? Est-ce une propriété géométrique ?

Problème.— *Le groupe fondamental d'une variété compacte à courbure négative ou nulle est-il presque convexe ?*

Voici enfin une autre notion, dégagée par W. Thurston (voir [1], [9]). Convenons de dire qu'un chemin dans un groupe Γ muni d'une partie génératrice finie S est une application $c : \{0, 1, \cdots, n\} \to \Gamma$ telle que $d_S(c(i), c(i+1)) = 1$ $(i = 0, \cdots, n-1)$. L'origine de c est $c(0)$ et son extrémité est $c(n)$. Il est commode de prolonger c en une application $\overline{c} : \mathbf{N} \to \Gamma$ par $\overline{c}(i) = c(n)$ pour $i > n$.

DÉFINITION.— *Un groupe Γ muni d'une partie génératrice finie est peignable s'il est possible de choisir, pour tout γ de Γ , un chemin c_γ d'origine e et d'extrémité γ de telle sorte que la propriété suivante soit satisfaite. Il existe une constante C telle que, si $d_S(\gamma_1, \gamma_2) = 1$, on ait* $\sup_{i \in \mathbf{N}} d_S(\overline{c}_{\gamma_1}(i), \overline{c}_{\gamma_2}(i) \leq C$.

Bien sûr, un groupe hyperbolique est peignable puisqu'il suffit de choisir pour c_γ un chemin de longueur minimale joignant e à γ. Les groupes automatiques sont peignables mais la réciproque n'est pas connue. Les groupes peignables permettent une généralisation partielle du théorème de I. Rips décrit plus haut [1]. Cependant, d'après W. Thurston, $SL(3, \mathbf{Z})$ n'est pas peignable.

On voit donc que la définition de ce que devrait être un groupe semi-hyperbolique n'est pas claire...

Signalons pour terminer qu'il serait également intéressant de comprendre la géométrie d'un certain nombre de groupes non semi-hyperboliques. On ne connaît presque rien concernant la géométrie des groupes polycycliques par exemple, à part le fait que certains d'entre eux ne sont pas presque convexes [10].

BIBLIOGRAPHIE

[1] J.M. ALONSO - *Combings of groups*, prépublication M.S.R.I. 04623-89.

[2] M. BESTVINA, G. MESS - *The boundary of negatively curved groups*, prépublication, 1990.

[3] B.H. BOWDITCH - *Notes on Gromov's hyperbolicity for path-metric spaces*, prépublication Université de Warwick, août 1989.

[4] K.S. BROWN - *Cohomology of groups*, Springer, 1982.

[5] J.W. CANNON - *The combinatorial structure of co-compact discrete hyperbolic groups*, Geom. Dedicata 16 (1984), 123-148.

[6] J.W. CANNON - *Almost convex groups*, Geom. Dedicata 22 (1987), 197-210.

[7] J.W. CANNON - *Negatively curved spaces and groups, the problem of constant negative curvature*, trois textes distribués au "Topical meeting on hyperbolic geometry and ergodic theory", Trieste, avril 1989.

[8] J.W. CANNON, D. COOPER - *A characterization of co-compact Kleinian groups and Kleinian groups of finite volume*, prépublication.

[9] J.W. CANNON, D.B.A. EPSTEIN, D.F. HOLT, M.S. PATERSON, W.P. THURSTON - *Word processing and group theory*, prépublication Université de Warwick, 1988.

[10] J.W. CANNON, W.J. FLOYD, M.A. GRAYSON, W.P. THURSTON - *Solvgroups are not almost convex*, Geom. Dedicata 31 (1989), 291-300.

[11] M. COORNAERT, T. DELZANT, A. PAPADOPOULOS - *Notes sur les groupes hyperboliques de Gromov*, publication IRMA Strasbourg, 1989.

[12] M.W. DAVIS and T. JANUSZKIEWICZ - *Hyperbolization of polyhedra*, preprint.

[13] M. DEHN - *Papers on group theory and topology*, translated and introduced by J. Stillwell, Springer, 1987.

[14] D.B.A. EPSTEIN - *Computers, groups and geometry*, Astérisque 163-164 (1988), 9-29.

[15] S.M. GERSTEN - *Problems on automatic groups*, prépublication M.S.R.I. 07023-89.

[16] S.M. GERSTEIN, H. SHORT - *Automatic groups and small cancellation theory*, à paraître dans Inventiones.

[17] S.M. GERSTEIN, H. SHORT - *Rational subgroups of biautomatic groups*, à paraître dans Annals of Mathematics.

[18] É. GHYS, P. DE LA HARPE (éditeurs) - *Sur les groupes hyperboliques*, d'après Mikhael Gromov, avec la collaboration de W. Ballman, A. Haefliger, E. Salem, R. Strebel et M. Troyanov, Progress in Mathematics, Volume 83, Birkhaüser, 1990.

[19] R.H. GILMAN - *Groups with a rational cross section*, in Combinatorial group theory and topology, Ann. of Math. Studies 111, Princeton University Press 1987, 175-183.

[20] F. GREENLEAF - *Invariant means on topological groups and their applications*, Van Nostrand, 1969.

[21] M. GROMOV - *Hyperbolic manifolds, groups and actions*, in Riemann surfaces and related topics, Ann. of Math. Studies 97, Princeton University Press 1980, 183-213.

[22] M. GROMOV - *Structures métriques pour les variétés riemanniennes*, rédigé par J. Lafontaine et P. Pansu, Cedic F. Nathan, 1981.

[23] M. GROMOV - *Groups of polynomial growth and expanding maps*, Publ. Math. I.H.E.S. 53 (1981), 53-73.

[24] M. GROMOV - *Infinite groups as geometric objects*, proceed. I.C.M. Warszawa 1 (1984), 385-392.

[25] M. GROMOV - *Hyperbolic groups*, in "Essays in group theory", éd. S.M. Gersten, M.S.R.I. Pub. 8 (Springer, 1987), 75-263.

[26] P. DE LA HARPE - *Free groups in linear groups*, L'Enseignement mathématique 23 (1983), 129-144.

[27] P. DE LA HARPE, A. VALETTE - *La propriété T de Kazdan pour les groupes localement compacts*, à paraître dans Astérisque.

[28] D. KAZDAN - *On a connection between the dual space of a group with the structure of its closed subgroups*, Func. Anal. and its applications, 1:1 (1967), 71-74.

[29] R.C. LYNDON, P.E. SCHUPP - *Combinatorial group theory*, Springer, 1977.

[30] G.A. MARGULIS - *Groupes discrets d'isométries des variétés à courbure négative*, proceed. I.C.M. Vancouver, 1974, Vol. 2, 21-34.

[31] D. MOSTOW - *Rigidity of locally symmetric spaces*, Princeton University Press, 1972.

[32] P. PANSU - *Croissance des boules et des géodésiques fermées dans les nilvariétés*, Ergod. Th. Dynam. Sys. 3 (1983), 415-445.

[33] P. PANSU - *Métriques de Carnot-Carathéodory et quasi-isométries des espaces symétriques de rang* 1, Ann. of Math. 129 (1989), 1-60.

[34] M.S. RAGUNATHAN - *Discrete subgroups of Lie groups*, Springer, 1972.

[35] P. SCOTT - *The geometries of* 3*-manifolds*, Bull. London Math. Soc. 15 (1983), 401-487.

[36] P.SCOTT, T. WALL - *Topological methods in group theory*, in "Homological group theory", Lecture Notes 36, London Math. Soc. 1979, 137-203.

[37] P.B. SHALEN - *Dendrology of groups : an introduction*, in "Essays in group theory", éd. S.M. Gerten, M.S.R.I. Pub. 8 (Springer, 1987), 265-319.

[38] H. SHORT (éditeur) - *Notes on negatively curved groups*, avec la collaboration de J.M. Alonso, T. Brady, D. Cooper, T. Delzant, V. Ferlini, M. Lusztig, M. Mihalik, M. Shapiro, prépublication M.S.R.I. 08023-89.

[39] D. SULLIVAN - *On the ergodic theory at infinity of an arbitrary discrete group of hyperbolic notions*, in "Riemann surfaces and related topics", Ann. of Math. Studies 97, Princeton University Press 1980, 465-496.

[40] W.P. THURSTON - *The geometry and topology of* 3*-manifolds*, Lecture Notes, Princeton, 1978.

[41] J. TITS - *Groupes à croissance polynomiale*, Séminaire N. Bourbaki, février 1981, exposé 572, Lecture Notes in Math. 901 (1981), Springer-Verlag, 176-188.

[42] P. TUKIA - *On quasi-conformal groups*, J. d'Anal. Math. 46 (1986), 318-346.

[43] P. TUKIA - *Homeomorphic conjugates of Fuchsian groups*, J. reine angew. Math. 391 (1988), 1-54.

Étienne GHYS

ÉCOLE NORMALE SUPÉRIEURE DE LYON
U.R.A. DO 746 du CNRS
46 allée d'Italie
69364 LYON CEDEX 07

Astérisque

CHRIS PETERS

Algebraic Fermi curves

Astérisque, tome 189-190 (1990), Séminaire Bourbaki,
exp. n° 723, p. 239-258

<http://www.numdam.org/item?id=SB_1989-1990__32__239_0>

© Société mathématique de France, 1990, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Séminaire BOURBAKI mars 1990
42ème année, 1989-90, n° 723

ALGEBRAIC FERMI CURVES
[after Gieseker, Trubowitz and Knörrer]

by Chris PETERS

0. INTRODUCTION

We give an overview of the work [GKT2] of Gieseker, Trubowitz and Knörrer on the theory of algebraic Fermi curves. A technical summary of the results can be found in [GKT1]. Here we concentrate more on the background from solid state physics (to be recalled in §1) and a more leisurely account of their main results and techniques.

In the discrete approximation one can use techniques from algebraic geometry, while even in the original independent electron approximation one works with highly non algebraic analytic varieties where both the geometry and the analysis are very difficult.

More results in the discrete case can be found in [B1], [B2], [K] and [PS]. Some related results in the continuum case can be found in [BKT], [G] and [KT]. See also §8.

1. BACKGROUND FROM PHYSICS

The following model from solid state physics is called *the independent electron model.* Details can be found e.g. in [AM]. Fix a lattice $\Gamma \subset \mathbb{R}^d$ $(d \leq 3)$ of ions (so we assume that the ions don't move) and a gas of electrons, which move independently under the influence of a potential $q(x)$ which is periodic in Γ (this potential describes the total effect of ions plus electrons). Each individual electron is given by its wave function which is a

superposition of solutions $\Psi : \mathbb{R}^d \to \mathbb{C}$ of the Schrödinger equation

$$(-\Delta + q(x))\Psi = \lambda\Psi, \lambda \in \mathbb{R} \tag{1.1}$$

with boundary conditions

$$\Psi(x+\gamma) = e^{i\langle k,\gamma\rangle}\Psi(x) \ \forall\gamma \in \Gamma,\ k \in \mathbb{R}^d \text{ fixed.} \tag{1.2}$$

Assuming that $q \in L^2(\mathbb{R}^d/\Gamma)$, (1.1) and (1.2) determine a self adjoint boundary value problem yielding a discrete spectrum

$$E_1(k) \leq E_2(k) \leq \ldots,$$

where every $E_j(k)$ (the *energy for crystal momentum* k) depends continuously on k and is called the j-th band function. It is periodic in the dual lattice

$$\Gamma^\sharp = \{b \in (\mathbb{R}^d)^* \mid \langle b, \Gamma\rangle \subset 2\pi\mathbb{Z}\}.$$

To explain what physicists mean by Fermi-surface, let F be a fundamental domain for the lattice Γ and let us approximate solid matter by a box $L \cdot F \subset \mathbb{R}^d$, $L \in \mathbb{Z}_+$ containing $L^d n = N$ electrons (n=*electronic density* is kept fixed) and take the limit when L goes to infinity. In other words restrict solutions of the preceding problem to L^2-functions on the box $L \cdot F$ having the same values on corresponding boundary points. Then the crystal momenta belong to $(1/L) \cdot \Gamma^\sharp$. The Pauli exclusion principle dictates that each electron can be placed in exactly one energy level (two if we take spin into account) so that the lowest energy level for the system consisting of N electrons in the box of solid matter is the sum of the first N eigenvalues for these momenta. The largest energy of an individual electron for this *ground state* of the box has a finite limit when L goes to infinity and is called the Fermi-energy. The surface in crystal momentum k-space with this energy is the Fermi-surface. It separates occupied states from non-occupied states at absolute zero. The shape of the Fermi-surface can be measured experimentally. Its properties in turn predict qualitative behaviour of matter, e.g. whether it acts as a conductor, semi-conductor or insulator.

More generally one can define the Fermi-hypersurface in $\mathbb{R}^d$ for energy λ as the hypersurface in the space of crystal momenta with energy precisely λ. In view of the periodicity with respect to $\Gamma^\sharp$ one can replace this Fermi-hypersurface by its image in $\mathbb{R}^d/\Gamma^\sharp$. For simplicity, let us assume that $\Gamma = \mathbb{Z}^d$. Then $\mathbb{R}^d/\Gamma^\sharp$ is a direct product of d circles which we can view as unit circles in the complex plane. This leads to the description of the Fermi-variety as

$$\{(\xi_1, \ldots, \xi_d) \in (S^1)^d \mid \exists \Psi \neq 0 \text{ solving (1.1) with } \Psi(x_1, \ldots, x_i + 1, \ldots, x_d) = \xi_i \Psi(x) \text{ for } i = 1, \ldots, d\}$$

This Fermi-variety can be considered as the fiber over λ of a hypersurface inside $(S^1)^d \times \mathbb{R}$ under projection onto the last factor.

Going one step further, we can consider solutions (ξ, λ) varying in $(\mathbb{C}^*)^d \times \mathbb{C}$, yielding a complex analytic variety B fibered in $d-1$-dimensional varieties on which the Fermi-hypersurfaces are real cycles of real dimension $d-1$.

For $d = 1$ the variety B is a hyperelliptic curve which generically has infinitely many branch points. It has been studied by McKean and Trubowitz in [MT]. For higher d there are some partial results available, see §8. These are motivated by certain results in a discrete approximation, to which we will turn in a moment. Here the analogue of the Fermi variety is an algebraic variety and so one can make use of the rich arsenal of results and methods from Algebraic Geometry.

2. A DISCRETE MODEL

In order to focus on the geometric aspects of the problem Gieseker, Knörrer and Trubowitz turn to a discrete approximation, which we now describe. Inside $\mathbb{Z}^d$ one takes the lattice

$$\Gamma = \oplus_{j=1}^d \mathbb{Z} \cdot a_j \mathbf{e}_j,$$

where $\mathbf{e}_j$ is the j-th standard basis vector. Introduce a fundamental domain for Γ:

$$F := \{(x_1, \ldots, x_d) \in \mathbb{Z}^d \mid 1 \leq x_j \leq a_j, j = 1, \ldots, d\}.$$

The vector space of complex valued Γ-periodic functions on $\mathbb{Z}^d$ with the usual inner product

$$\langle \varphi, \psi \rangle = 1/(a_1 \cdots a_d) \sum_{x \in F} \varphi(x)\overline{\psi}(x)$$

is denoted by

$$L^2(\mathbb{Z}^d/\Gamma).$$

Potentials $q(x)$ are in this set $L^2(\mathbb{Z}^d/\Gamma)$, in particular they are allowed to be complex valued. Define the shift operators S_j acting on functions $\Psi : \mathbb{Z}^d \to \mathbb{C}$ by

$$S_j \Psi(x_1, \ldots, x_j, \ldots, x_d) = \Psi(x_1, \ldots, x_j + 1, \ldots, x_d)$$

and the discrete Laplacian by

$$\Delta = \sum_{j=1}^{d} S_j + S_j^{-1}.$$

The corresponding discrete problem translates into

$$\text{(2.1)} \qquad \begin{cases} (-\Delta + q - \lambda)\Psi = 0 & (\lambda \in \mathbb{C}) \\ S_j^{a_j} \Psi = \xi_j \Psi & (\xi_j \in \mathbb{C}^*), j = 1, \ldots, d \end{cases}$$

and one introduces

$$B(q) = \{(\xi_1, \ldots, \xi_d, \lambda) \in (\mathbb{C}^*)^d \times \mathbb{C} \mid \exists \Psi \neq 0, \ \Psi \text{ solves (2.1)}\}.$$

In [G-K-T] this variety is called *Bloch variety*. By the projection $\pi : B \to \mathbb{C}$ onto the second factor it is fibered into varieties of dimension $d - 1$,

the *(complex) Fermi-varieties.* The fiber $\pi^{-1}(\lambda)$ is denoted by F_λ. The analogue of the Fermi-surface from physics is the intersection of F_λ with $(S^1)^d \times \{\lambda\}$ for real values of λ.

Since $S_j^{a_j}\Psi = \xi_j\Psi$, the function Ψ is determined by its A values on the fundamental domain F, where

$$A = a_1 \cdots a_d.$$

Now (2.1) translates into the eigenvalue problem for the $A \times A$-matrix $\mathcal{P}$ one gets by writing out $-\Delta + q$ as acting on the A-dimensional space $\{\Psi(x), x \in F\}$. Since this matrix has entries which are linear functions in the variables $\xi_1, \xi_1^{-1}, \ldots, \xi_d, \xi_d^{-1}$, we conclude that $B(q)$ is an *algebraic hypersurface* of degree A in $(\mathbb{C}^*)^d \times \mathbb{C}$ given by the characteristic equation $P(\xi_1, \ldots, \xi_d, \lambda) = 0$ of the matrix $\mathcal{P}$:

$$B(q) = \{(\xi_1, \ldots, \xi_d, \lambda) \in (\mathbb{C}^*)^d \times \mathbb{C} \mid P(\xi_1, \ldots, \xi_d, \lambda) = 0\}. \tag{2.2}$$

3. THE DENSITY OF STATES

In solid state physics another experimentally observable quantity plays an important rôle : the (integrated) density of states. If H_n is the operator $-\Delta + q$ acting on the space of complex valued functions on $\mathbb{Z}^n$ with periodicity $n\Gamma$, we can define the integrated density of states function as $\rho(\lambda) = \lim_{n\to\infty} \rho_n(\lambda)$, with

$$\rho_n(\lambda) = 1/(n^d A) \cdot \text{ number of eigenvalues of } H_n \text{ less than or equal to } \lambda.$$

An easy computation shows that the (non-integrated) density of states function $d\rho/d\lambda$ is equal to

$$\frac{1}{(2\pi)^d A} \sum_{j=1}^{A} \int_{\mathbb{R}^d/2\pi\mathbb{Z}^d} \delta(\lambda - E_j(k))dk,$$

where δ is the delta-function and $E_j(k)$ is the (analogue of the) j-th band function. Since the region over which we integrate is precisely the 'real' Fermi-surface $\phi_\lambda = F_\lambda \cap (S^1)^d \times \{\lambda\}$ we get

$$\frac{d\rho}{d\lambda} = \frac{1}{(2\pi)^d A} \sum_{j=1}^{A} \int_{E_j(k)=\lambda} \frac{dS}{|\nabla_k E_j|} = \frac{1}{(2\pi)^d A} \int_{\phi_\lambda} \omega_\lambda, \tag{3.1}$$

where

$$\omega_\lambda = (-1)^i \frac{\frac{\partial}{\partial\lambda} P d\xi_1 \wedge \ldots \wedge \widehat{d\xi_i} \wedge \ldots d\xi_d}{\xi_1 \cdots \xi_d \frac{\partial}{\partial \xi_i} P}$$

is the restriction to F_λ of the relative $d-1$-form ω on the Bloch variety defined by

$$\pi^*(d\lambda) \wedge \omega = \frac{d\xi_1}{\xi_1} \wedge \ldots \wedge \frac{d\xi_d}{\xi_d}.$$

So the density of states appears as an integral of a holomorphic $d-1$-form over a real $d-1$-cycle on F_λ. Note that one can define this only for q real valued and λ real. If now λ is a regular value for the projection π, the fibration π is differentiably a product near λ so the cycle ϕ_λ extends naturally to fibres near the fibre we started with and $\frac{d\rho}{d\lambda}$ defines a germ of an analytic function near λ.

The preceding observations formed the starting point for [G-K-T] and led to some striking results which we can now formulate.

4. MAIN RESULTS IN DIMENSION $d = 2$

We assume from now on that

$$a := a_1 \text{ and } b := a_2 \text{ are distinct odd primes.}$$

(4.1) **Theorem** *There is a Zariski open dense set $L_1 \subset L^2(\mathbb{Z}^2/\Gamma)$ such that $B(q) = B(q')$, $q \in L_1$, $q' \in L^2$ implies that there exists some $(x_0, y_0) \in \mathbb{Z}^2/\Gamma$ with $q'(x,y) = q(\pm x + x_0, \pm y + y_0)$.*

In other words for generic potentials the Bloch-variety determines the potential up to the obvious symmetries.

To formulate the next results, we need to introduce precise genericity conditions.

(4.2) **Definition**
(1) A potential $q \in L^2(\mathbb{Z}^2/\Gamma)$ is generic for the Bloch-projection $B(q) \to \mathbb{C}$ if π has exactly

$$\nu = 2a^2b^2 + 6ab(a+b) + 12ab - 12(a^2+b^2) - 2(a+b) - 12$$

critical values.
(2) A real valued potential is generic with respect to the density function if the analytic continuation of the germ of the density of states function (3.1) near a real value where it is analytic (that is, near a real non-critical value of the Bloch-projection) has precisely ν ramification points.

The next result states that generic potententials have good properties and that there are many of them.

(4.3) **Proposition** *(1) The potentials generic with respect to the Bloch projection form a Zariski open dense subset $L_2 \subset L^2(\mathbb{Z}^2/\Gamma)$.*
(2) A real potential which is generic for the Bloch projection is generic with respect to the density of states function and conversely.
(3) Moreover for potentials in L_2 we have
- The Bloch variety is smooth.
- The Fermi curves over $4ab$ of the critical values of π have exactly one ordinary double point and exactly two ordinary double points over the remaining critical values.

Finally we have

(4.4) **Theorem** *Let $q, q' \in L^2(\mathbb{Z}^2)$ be real valued potentials and assume that the germs of the density of states functions for q and q' near a real*

point coincide. If $q, q' \in L_2$ *either* $B(q) = B(q')$ *or* $B(q') = jB(q)$, *where* j *is the involution* $j(\xi_1, \xi_2, \lambda) = (\xi_1^{-1}, \xi_2, \lambda)$.

Combining the previous results we see that the density of states function for a generic real potential essentially determines the potential.

Remark

One would also want to see from properties of the germ f at λ of the density of states function alone whether the fibre over λ is smooth. In fact this can be read off from the lattice Γ_λ generated by analytic continuation of f inside the ring of germs of holomorphic functions at λ. If some continuation of f yields a germ which is multivalued at λ, the fibre over this point certainly is singular, so we may assume that this is not the case. The result complementing Proposition 4.3 says that the Fermi curve over λ is smooth when Γ_λ has rank $2ab$. Moreover, if this is the case, one only has to find ν branch points for f since one can show that there cannot be more of them in this case. Concerning the proofs we make a few preliminary remarks. The proof of theorem 4.1 is rather straightforward and uses the geometry of a suitable compactification of the Bloch variety. We give a sketch in section 6 after we discuss an intrinsic compactification in the next section. The proof of Proposition 4.3 is surprizingly subtle and uses several delicate degeneration arguments, which also play a rôle in the proof of Theorem 4.4. We don't say anything about the proof of Proposition 4.3, but we give a sketch of the long and intricate arguments employed in the proof of Theorem 4.4.

5. A COMPACTIFICATION OF THE BLOCH VARIETY

Motivated by an idea of Mumford (see [M]), Bättig in [B1] has constructed the following intrinsic compactification of the Bloch variety .

Consider the algebraic torus $T = (\mathbb{C}^*)^3 \subset (\mathbb{C}^*)^2 \times \mathbb{C}$. We let T_Σ be the toroidal compactification of T corresponding to the fan Σ in $\mathbb{R}^3$ consisting

of the cones (with vertex the origin) over the faces of the prism of Fig. 1.

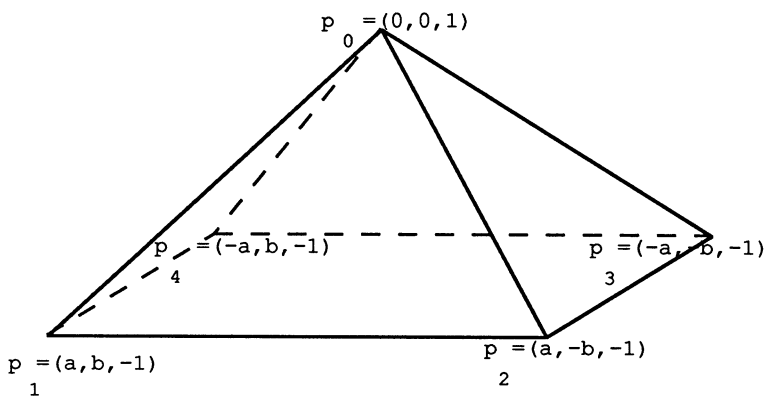


Figure 1. Fan Σ.

The corresponding 'cradle' (Fig. 2) is a singular complete algebraic variety with one-dimensional singular locus. The latter is stratified into nine T-orbits, four of dimension 1 and five of dimension 0. The one-dimensional orbits correspond to the codimension one cones over the four horizontal edges of the prism. These four curves have transversal A_k type, two with $k = 2a - 1$ and two with $k = 2b - 1$. The zero dimensional orbits in the closures of the one dimensional orbits correspond to the zero codimensional faces. Observe that $(\mathbb{C}^*)^2 \times \mathbb{C}$ is embedded in T_Σ as the open chart defined by the torus embedding T_σ, where σ is the cone $\mathbb{R}_{\geq 0}(0,0,1)$. We therefore can take the closure of $B(q)$ in the cradle T_Σ. The resulting variety is always singular in the four points P_{ij} where it meets the singular locus of the cradle (see Fig. 2). Blow up these singular points in the cradle and form the proper transform $\overline{B(q)}'$ of $B(q)$.

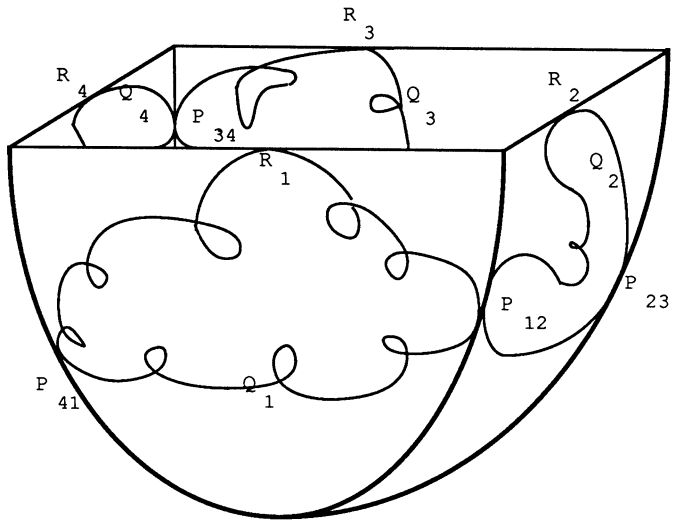


Figure 2. Cradle T_Σ.

Before stating the next proposition, recall the notation

$$\mu_a := \text{ group of } a\text{-th roots of unity}$$
$$\mu_a^\times := \text{ the set of primitive } a\text{-th roots of unity.}$$

(5.1) **Proposition** *(i) The four exceptional surfaces on the blown up cradle intersect the proper transform* $\overline{B(q)}'$ *of* $B(q)$ *in four curves* H_{ij}. *These curves are hyperelliptic. They are isomorphic in pairs. The two (isomorphism classes of) curves are the Bloch varieties for the one dimensional potential obtained by averaging over each of the two coordinates.*
(ii) There are precisely four other curves Q_j *added at infinity* $\overline{B(q)}' \setminus B(q)$. *These curves are singular rational curves with* $(a-1)(b-1)$ *ordinary double points naturally indexed by the elements of* $\mu_a^\times \times \mu_b^\times$. *The curve* Q_j *intersects the* T*-orbit corresponding to the one codimensional cone over the line through* p_0 *and* p_j *(see Fig. 1) in a point* R_j *which is a smooth point*

on $\overline{B(q)}'$.

(iii) The Bloch projection $\pi : B(q) \to \mathbb{C}$ *extends to a rational map* $\overline{\pi}' : \overline{B(q)}' - - \to \mathbb{P}^1$ *which is everywhere defined except at the points* R_j, $j = 1,2,3,4$. *After blowing up* $\overline{B(q)}'$ *at these points we obtain the compactified Bloch variety* $\overline{B(q)}$ *and the map* $\overline{\pi}'$ *extends as a morphism.*

$$\overline{\pi} : \overline{B(q)} \to \mathbb{P}^1.$$

The four exceptional curves are sections for this fibration.

(5.2) **Remark** In [GKT] the compactification is described in a more complicated, but equivalent way.

6. SKETCH OF THE PROOF OF THEOREM 4.1

Recall the definition of the Fourier coefficients of a potential $q \in L^2(\mathbb{Z}^2/\Gamma)$. For each $\rho = (\rho_1, \rho_2) \in \mu_a \times \mu_b$ we set

$$\hat{q}(\rho) = \frac{1}{ab} \sum_{(m,n)\in F} q(m,n)\overline{\rho}_1^m \overline{\rho}_2^n.$$

The Bloch-variety $B(q) = \{(\xi_1, \xi_2, \lambda) \mid P(\xi_1, \xi_2, \lambda) = 0\}$ determines:
(i) The polynomial $P(1,1,\lambda)$, whose roots are the periodic spectrum of the Schrödinger operator,
(ii) The values at q of the function

$$f_\rho(q) = \hat{q}(\rho)\hat{q}(\overline{\rho}), \quad \rho \in \mu_a^\times \times \mu_b^\times.$$

The last assertion can be shown by looking at the equation of the Bloch-variety near one of the points Q_j (see Proposition 5.1). It turns out that there are local coordinates (x,y,z) near Q_j independent of the potential q such that the Bloch-variety has an equation

$$f_\rho\, x^2 = y^2 + z^2 + \text{ higher order terms }.$$

The polynomial $P(1,1,\lambda)$ belongs to the affine ab-dimensional space

$$\mathcal{P} = \text{ polynomials of degree } ab \text{ with } -1 \text{ as leading coefficient.}$$

Define a family of algebraic morphisms

$$\varphi_\epsilon : L^2 \to \mathcal{P},$$

sending q to the determinant of $-\epsilon\Delta + q - \lambda$ acting on the periodic functions L^2. Of course $\varphi_1 = P(1,1,\lambda)$ and $\varphi_0 = \prod_{(m,n)\in F}((q(m,n) - \lambda)$, so a fibre of φ_0 consists of precisely those potentials that are related by the obvious action of the symmetric group $\mathfrak{S}_{ab}$ on L^2:

$$\sigma(q)(m,n) = q(\sigma(m,n)), \quad \sigma \in \mathfrak{S}_{ab}.$$

The subgroup $\mathfrak{D} \subset \mathfrak{S}_{ab}$ generated by $(n,m) \mapsto (n+1,m)$, $(n,m) \mapsto (n,m+1)$, $(n,m) \mapsto (-n,-m)$ has the property that any element σ in it preserves the Bloch-variety: $B(\sigma(q)) = B(q)$. We need to see that for generic q conversely $B(q') = B(q)$ implies that $q' = \sigma(q)$, $\sigma \in \mathfrak{D}$. To this end fix $\rho \in \mu_a^\times \times \mu_b^\times$ and set $f = f_\rho$. This function takes the same values in the points of a fibre of φ_1 which are related by an element of $\mathfrak{D}$. To decide whether $\sigma \in \mathfrak{S}_{ab}$ belongs to $\mathfrak{D}$ we use

(6.1) **Lemma** *If $f(\sigma(q)) = f(q)$ for all potentials q, σ belongs to $\mathfrak{D}$.*

The proof of this lemma is relatively easy if one uses some carefully chosen potentials.

Next, we remark that

$$\varphi_\epsilon(q)(\lambda) = \epsilon^{ab}\varphi_1(\frac{q}{\epsilon})(\frac{\lambda}{\epsilon}).$$

So if $\{q_1,\ldots,q_N\}$ is a fiber of φ_ϵ, the points $q_1/\epsilon,\ldots,q_N/\epsilon$ form a fiber of φ_1 and conversely. So it suffices to show that the function f separates points in a fibre of φ_ϵ, $(\epsilon \neq 0)$ not related by an element of $\mathfrak{D}$. It is easily

seen that for $|\epsilon|$ small, the map φ_ϵ is a finite dominant morphism of degree $N = |\mathfrak{S}_{ab}| = (ab)!$. Note that φ_ϵ factors as $\hat{\varphi}_\epsilon \cdot p$, where $p : L^2 \to L^2/\mathfrak{D}$ is the is the quotient map. Likewise f factors as $\hat{f} \cdot p$. There is a Zariski-open subset U of $\mathbb{C}$ and a Zariski-open subset $\mathcal{P}_1$ of $\mathcal{P}$ such that $P \in \mathcal{P}_1$ if and only if there exists $\epsilon \in U$ with $P = \varphi_\epsilon(q)$ for some $q \in L^2$ with the following two properties:

i. The fibre of $\varphi_\epsilon^{-1}(P)$ consists of N points,

ii. The function $\hat{f}$ separates the points of the fibre of $\hat{\varphi}_\epsilon^{-1}(P)$.

Since by Lemma 6.1 the function $\hat{f}$ separates the fibres of $\hat{\varphi}_0$ it follows that U and $\mathcal{P}_1$ are non-empty. ∎

7. SKETCH OF THE PROOF OF THEOREM 4.4

Step 1 : the monodromy representation

On the Bloch variety we have an involution i given by

$$i(\xi_1, \xi_2, \lambda) = (\xi_1^{-1}, \xi_2^{-1}, \lambda).$$

We first divide out $\overline{B(q)}$ by this involution, obtaining a variety $\overline{Y(q)}$ with fibres $Y(q)_\lambda$. If q is generic with respect to the Bloch projection one can show:

> 1) $Y(q)_\lambda$ is smooth whenever $\lambda \in \mathbb{P}^1 \setminus D$, ($D$ a finite set of points, called the *Van Hove singularities*),
>
> 2) The fibre over a finite Van Hove singularity contains precisely one ordinary double point which either is smooth on $\overline{Y(q)}$ or an ordinary double point. The second type of singularity is called a *spectral Van Hove singularity*, because it lies over a point of the periodic-anti-periodic spectrum.

3) Y_∞ has four components, the non-isomorphic components of F_∞ : two hyperelliptic curves corresponding to the one-dimensional averaged potentials and two rational curves. Each of the four points where a rational curve and a hyperelliptic curve meet is an ordinary double point for Y_∞ and smooth on $\overline{Y(q)}$. They define four vanishing cycles which are easily seen to be homologous and so yield a class $\gamma_\infty \in H_1(Y_\lambda, \mathbb{Z})$ for λ close to ∞.

These facts suggest to study the monodromy representation

$$r : \pi_1(\mathbb{P}^1 \setminus D, \lambda) \to \text{Aut } H_1(Y_\lambda, \mathbb{Z}) \tag{7.1}$$

by means of a Lefschetz-type argument. This turns out to be surprizingly difficult. One lets q degenerate to a generic separable potential (i.e. of the form $q_1(x_1) + q_2(x_2)$) where the monodromy can be computed explicitly and then one has to use connectedness of the set of good potentials. The final result is as follows

(7.2) **Proposition** *i) The monodromy representation (7.1) is absolutely irreducible.*
ii) For λ a negative real number close to ∞ the smallest r-invariant sublattice of $H_1(Y_\lambda, \mathbb{Q})$ generated by $\frac{1}{2}(\gamma_\infty - r(\alpha)\gamma_\infty)$, $\alpha \in \pi_1(\mathbb{P}^1 \setminus D, \lambda)$ is equal to $H_1(Y_\lambda, \mathbb{Z})$.

Step 2: Recovering γ_∞.

Since ω is i-invariant it descends to a relative holomorphic one form for the family $Y(q) \to \mathbb{C}$ denoted by the same symbol. Let α be a non bounding 1-cycle on Y_λ. Displace α to a cycle on Y_s for s in a small open neighbourhood U of λ, where the fibration is provided with some differentiable trivialisation. This cycle is still denoted as α. On U we have a germ $f_\alpha = \int_\alpha \omega_s$ of an analytic function. Let $\mathcal{O}$ denote the ring of germs of holomorphic

functions near λ. Analytic continuation of f_α over paths in $\mathbb{P}^1 \setminus D$ defines an injection

$$I : H_1(Y_\lambda, \mathbb{Z}) \longrightarrow \mathcal{O}.$$

A special loop l_∞ is defined as follows. First, starting from λ, go to left along the negative real axis, make a big circle which clockwise encircles all Van Hove singularities, then go back to λ along the real axis. If $g \in \mathcal{O}$ we let g_∞ be the germ obtained from g by analytically continuation along the loop l_∞.

Let q be a generic real potential and λ not a Van Hove singularity. Then

$$f := \int_{\phi_\lambda + i(\phi_\lambda)} \omega_\lambda$$

is twice the density of states. Let H_λ be the lattice inside $\mathcal{O}$ generated by all analytic continuations of the density of states function $\frac{1}{2}f$. Choose $g \in H_\lambda$ such that

1 g is invariant under complex conjugation,

2 g_∞ differs from g.

Let $h := g - g_\infty$. It can be shown that

$$I(\gamma_\infty) = \frac{2\pi ab}{\lim\limits_{t \to -\infty} h(t)} h,$$

where we take the limit along the negative real axis. So from monodromy alone we have recovered γ_∞. From Proposition 7.2 we see that we can recover $H_1(Y_\lambda, \mathbb{Z})$.

Step 3: Invoking Torelli's theorem

If now q' is another real potential with the same density of states function near λ we can define for s near λ an r-equivariant isomorphism

$$\alpha : H_1(Y(q)_s, \mathbb{Z}) \to H_1(Y(q')_s, \mathbb{Z}) \tag{7.3}$$

upon setting

$$\int_\gamma \omega_s(q) = \int_{\alpha(\gamma)} \omega_s(q'), \ \ \forall \gamma \in H_1(Y(q)_s, \mathbb{Z}).$$

If one collects the periods for a basis of the regular one forms for Y_s with respect to a homology basis in a $2g$ by g matrix, one gets the period matrix Ω_s for Y_s. Different bases correspond to equivalent period matrices. Recall

(7.4) **Torelli's theorem** *Two Riemann surfaces are isomorphic if and only if their period matrices are equivalent.*

This suggest that we should find the periods of all one forms rather than only those for the density of states form ω_s. To do this we have to use irreducibility of the monodromy representation (7.1) again together with a deep result: the *Theorem of the fixed part* due to Deligne. To explain the consequence of this theorem needed in the proof we have to recall the notion of *Hodge structure of weight* w on a finitely generated $\mathbb{Z}$-module H. It is nothing but a direct sum decomposition of the $\mathbb{C}$-vector space $H \otimes_{\mathbb{Z}} \mathbb{C}$ into subspaces $H^{k,w-k}$ *of Hodge type* $(k, w-k)$ with the property that $H^{w-k,k} = \overline{H^{k,w-k}}$ (conjugation with respect to the natural complex structure on $H \otimes_{\mathbb{Z}} \mathbb{C}$).
The $\mathbb{Z}$-module $H^1(F(q)_s.\mathbb{Z})$ carries a weight one Hodge structure: $H^{1,0}F(q)_s$ consists of the g rows of Ω_s, each considered as an element of $H^1(F(q)_s, \mathbb{C})$ $= \mathrm{Hom}_{\mathbb{C}}(H_1(F(q), \mathbb{Z}), \mathbb{C})$ written out in the basis dual to the given homology basis.
The usual linear algebra constructions applied to Hodge structures yield new Hodge structures. E.g. if H and H' carry Hodge structures of weight w the $\mathbb{Z}$-module $\mathrm{Hom}_{\mathbb{Z}}(H, H')$ carries a weight zero Hodge structure: a $\mathbb{C}$-linear $\psi : H \to H'$ has type $(-i, i)$ if $\psi(H^{k,w-k}) \subset (H')^{k-i,w-k+i}$.
The consequence of Deligne's Theorem of the Fixed Part [D, Cor. 4.1.2] reads as follows:

(7.5) **Theorem** *The weight zero Hodge structure on the $\mathbb{Z}$-module* $\mathrm{Hom}(H^1(Y(q')_\lambda, \mathbb{Z}), H^1(Y(q)_\lambda, \mathbb{Z})$ *induces one on the sublattice of homomorphisms which are equivariant with respect to the monodromy representation (7.1).*

Since monodromy acts irreducibly on cohomology with complex coefficients, Schur's lemma implies that these equivariant homomorphisms form a rank one lattice and Deligne's theorem implies that they all have type (0,0), i.e they preserve the Hodge types. But then the homomorpism α (see (7.3)) also preserves the Hodge types, i.e the Riemann surfaces $Y(q)_\lambda$ and $Y(q')_\lambda$ have the same period matrices and Torelli's theorem implies that they must be isomorphic. From this point on it is not difficult to get a global isomorphism between the Bloch varieties $B(q)$ and $B(q')$ respecting the Bloch-projections.

8. RELATED RECENT RESULTS

8.1 Kappeler in [K] generalizes Theorem 4.1 to any dimension. His proof is similar to the one from [GKT2] and which is presented in §6, but the use of the compactification is eliminated since another function is used to separate the fibres of $\hat{\varphi}_\epsilon$ (see §6 for notation).

8.2 The density of states function can be used to distinguish the spectral Van Hove singularities (see the beginning of §7) from the other Van Hove singularities. So for a real potential which is generic in the sense of definition 4.2. the density of states function determines the periodic-antiperiodic spectrum.

In the continuum case, if the lattice Γ is generic in the sense that there are at most two lattice points on any sphere centered at the origin, the periodic-antiperiodic spectrum is known to determine the Bloch variety (Theorem 6.2 in [ERT]). So in the continuum case one would like to show that the periodic-antiperiodic spectrum can be recovered from the density of states

function alone.

8.3 Observe that in the discrete case, the Bloch variety B is the locus of points in $(\mathbb{C}^*)^d \times \mathbb{C}$ where the $d+1$ commuting operators

$$S_\lambda := \Delta + q - \lambda, T_{\xi_j} := S_j^{a_j} - \xi_j, j = 1, \ldots, d,$$

have a common kernel in the space

$$V^d = \{\Psi : \mathbb{Z}^d \to \mathbb{C}\}.$$

In other words B is the support of the subsheaf $\mathcal{L}$ of the trivial bundle $B \times V^d$ given by

$$\mathcal{L} := \{((\xi_1, \ldots, \xi_d), \lambda, \Psi) \in (\mathbb{C}^*)^d \times \mathbb{C} \times V^d \mid S_\lambda \Psi = 0 = T_{\xi_j} \Psi, j = 1, \ldots, d\}.$$

Bättig shows in [B1] how for $d = 2$ one can extend $\mathcal{L}$ to a sheaf over his compactification $\overline{B}$ (see §5). Moreover he rewrites the spectral problem on certain coordinate patches in such a way that one immediately sees that the curves M_{ij} (loc. cit.) are the supports of a sheaf defining the one-dimensional problem for the potential obtained by averaging q over one of the two coordinates.
For $d = 3$ Bättig describes in [B2] a toroidal compactification of the complex Fermi surface F_λ. Here one gets four curves at infinity independent of q and twelve hyperelliptic curves independent of λ, but depending on q. The twelve curves come in three quadruples of mutually isomorphic curves and each of these curves is isomorphic to the Bloch variety for the potential obtained from q by averaging over two of the three coordinates.
It turns out that in the continuum case for $d = 3$ a certain directional compactification exists with similar properties. See [BKT] for details (see also [KT] for the two dimensional continuum case).

8.4 A more or less standard argument shows that the data $(B, \mathcal{L}|B)$ ($\mathcal{L}$ is the sheaf considered in §8.3; it is a line bundle on B) gives back the potential q. See [Mu, §2] and [VKN] for a related situation.

If one could characterize $\mathcal{L}|B$ intrinsically from the geometry of B it would follow that B gives back the potential. In this respect it is useful to note that one can show that the compactified Bloch variety for $d = 2$ has first Betti number zero so that a line bundle is completely characterized by its Chern class in $H^2(\overline{B})$. The problem however is to find a good description of this cohomology group which would single out Chern classes coming from potentials in this way.

8.5 Gerard in [G] studies the singularities of the resolvent $r(\lambda)$ of $-\Delta + q$ on $\mathbb{R}^d$ and shows that one can analytically locally extend $r(\lambda)$ around a spectral value λ and the singularities one gets are Van Hove singularities. Here one has to redefine the Van Hove singularities as being critical values for the Bloch projection π restricted to a stratum of a Thom stratification for π. Also the global problem is considered. A similar statement holds, but one possibly must add some extra singularities. It would be interesting to see whether the compactification from [BKT] can be used to see whether these singularities actually are present, at least for generic potentials.

BIBLIOGRAPHY

[AM] Ashcroft,N. and N. Mermin : *Solid State Physics. Holt,Rinehard and Winston* 1976.

[B1] Bättig, D.: *A toroidal compactification of the two dimensional Bloch variety. Thesis, ETH Zürich* 1988.

[B2] Bättig, D.: A toroidal compactification of the complex Fermi surface, preprint 1989.

[BKT] Bättig, D., H. Knörrer, E. Trubowitz: A directional compactification of the complex Fermi surface, preprint 1989.

[D] Deligne, P.: Théorie de Hodge 2, *Publ. Math IHÉS* **40**, 5-57 (1972).

[ERT] Eskin, G., J. Ralston, E. Trubowitz : On isospectral periodic potentials in $\mathbf{R}^n$.*Comm. Pure Appl. Math.***37** (1984) 647-676.

[G] Gerard, G. : Resonance theory for periodic Schrödinger operators, preprint 1989.

[GH] Griffiths,P. and J.Harris: *Principles of Algebraic Geometry, John Wiley & Sons* 1978.

[GKT1] Gieseker,D., H. Knörrer and E. Trubowitz: An overview of the geometry of Algebraic Fermi curves, *Preprint UCLA* 1989.

[GKT2] Gieseker,D., H. Knörrer and E. Trubowitz: *The geometry of algebraic Fermi curves, manuscript* 1989.

[K] Kappeler, T. : On isospectral potentials on a discrete lattice II, to apear in *Adv. in Appl. Math.*

[KT] Knörrer, H. and E. Trubowitz: A directional compactification of the complex Bloch variety, to appear in *Comm. Math. Helv.* 1990.

[M] Moerbeke, P. van: About isospectral deformations of discrete laplacians. In *Global Analysis*, Proc. Calgary 1978,*Springer Lecture Notes in Math.* **755** (1978), 313-370.

[Mu] Mumford, D.: An algebro-geometric construction of commuting operators and of solutions of the Toda lattice equation, Korteweg de Vries equation and related non-linear equations.*Proc. Int. Symp. Alg. Geometry, Kyoto 1977*, 115-153.

[MT] McKean,H., E. Trubowitz: Hills operator and hyperelliptic function theory in the presence of infinitely many branch points. *Comm. Pure Appl. Math* **29**, 143-226 (1976).

[PS] Peters,C. and J. Stienstra: A pencil of K3- surfaces related to Apéry's recurrence for $\zeta(3)$ and Fermi surfaces for potential zero. In : *Arithmetic of Complex Manifolds*, Proc. Erlangen 1988, *Springer Lecture Notes in Mathematics* **1399** pp 110-127, 1989.

[VKN] Veselov, A., I. Krichever, S. Novikov: Two-dimensional periodic Schrödinger operators and Prym's Θ-functions, In *Geometry of Today, Roma 1984*, Birkh. Verlag 1985, 283-301.

Chris Peters
Mathematisch Instituut
Rijks Universiteit Leiden
Niels Bohrweg 1
2333AL Leiden
Netherlands

Astérisque

JOHANNES SJÔSTRAND

Asymptotique des résonances pour des obstacles

Astérisque, tome 189-190 (1990), Séminaire Bourbaki,
exp. n° 724, p. 259-283

<http://www.numdam.org/item?id=SB_1989-1990__32__259_0>

© Société mathématique de France, 1990, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Séminaire BOURBAKI

42ème année, 1989-90, $n°$ 724 Mars 1990

Asymptotique des résonances pour des obstacles

Johannes Sjöstrand

0. Introduction

Cet exposé est principalement consacré aux travaux de G. LEBEAU sur la diffraction des singularités Gevrey (justifiant de vieilles idées de J. Keller et D. Ludwig) et de l'application de ces résultats à la distribution des pôles de "scattering" (résonances) dans le plan complexe, due à C. BARDOS-G. LEBEAU-J. RAUCH. On donnera quelques indications sur les démonstrations qui sont à la fois techniques et subtiles. Afin d'expliquer vraiment ces démonstrations il aurait fallu, d'abord, un exposé sur la théorie de la transformation FBI, il m'a donc semblé plus raisonnable de ne pas consacrer tout l'exposé à ces démonstrations mais plutôt de placer les résultats dans leur contexte naturel.

Dans la section 1 on rappelle quelques notions de base de la théorie de "scattering" de Lax-Phillips qui s'applique pour des perturbations à support compact en dimension impaire. On décrit aussi quelques développements plus récents : une formule de trace de Bardos-Guillot-Ralston améliorée par Melrose, et une borne globale sur le nombre de résonances dû à ce dernier.

Dans la section 2 on présente les théorèmes de base sur la propagation des singularités près d'un obstacle dans les cas C^∞, analytique et Gevrey 3. On tente aussi une vague explication de la démonstration de Lebeau du fait que les singularités mod Gevrey 3 ne sont pas diffractées par un obstacle strictement convexe.

Dans la section 3, on discute quelques résultats sur la distribution des résonances dans le cas des obstacles C^∞, d'abord un résultat sur l'absence des résonances dans un voisinage logarithmique de l'axe réel pour des obstacles non captants et ensuite des résultats d'Ikawa et de C. Gérard sur le comportement des résonances pour certains obstacles captants.

Dans la section 4, on décrit les résultats de Bardos-Lebeau-Rauch sur la distribution des résonances des obstacles analytiques non-captants et en particulier pour ceux qui sont strictement convexes. Les résonances se placent alors plus loin dans le plan complexe et l'étude devient plus délicate.

Au départ, je voulais aussi décrire brièvement des résultats analogues pour l'équation de Schrödinger (où la théorie de Lax-Phillips ne s'applique pas en général) et me plonger dans les travaux de Babich et ses collaborateurs pour les décrire. Le temps m'a malheureusement manqué.

1. Théorie de Lax-Phillips

On donne ici quelques ingrédients de base de la théorie de scattering de Lax et Phillips [**LP1**], ainsi que quelques développements plus récents.

Soit Ω un ouvert connexe de la forme $\mathbf{R}^n \setminus \mathcal{O}$ ou $\mathcal{O}$ est un compact de bord C^∞ et n un nombre impair. On s'intéresse au comportement quand $|t| \to \infty$ des solutions de

$$\Box v = 0 \text{ dans } \mathbf{R} \times \Omega \ , \quad v\,|_{\mathbf{R}\times\partial\Omega} = 0 \ , \tag{1.1}$$

où v appartient à un espace convenable de distributions prolongeables à $\mathbf{R}_t \times \mathbf{R}^n_x$ et $\Box = \partial_t^2 - \Delta_x$ désigne le d'Alembertien. On veut notamment comparer le comportement asymptotique de ces solutions avec celui des

solutions de l'équation des ondes libre dans $\mathbf{R}\times\mathbf{R}^n$. Posant $u_0 = v$, $u_1 = \partial_t v$, $u = (u_0, u_1)$ on obtient

$$\partial_t u = Au\ ,\quad u\,|_{\mathbf{R}\times\partial\Omega} = 0\ , \tag{1.2}$$

où $A = \begin{pmatrix} 0 & 1 \\ \Delta & 0 \end{pmatrix}$. Posons $\mathcal{H}(\Omega) = H_D(\Omega)\times L^2(\Omega)$, où $H_D(\Omega)$ est l'adhérence de $C_0^\infty(\Omega)$ pour la norme de Dirichlet :

$$\|u\|^2_{H_D} = \int_\Omega \sum_1^n \left|\partial_{x_j} u(x)\right|^2 dx\ .$$

Alors $\mathcal{H}(\Omega)$ est un espace de Hilbert et on peut considérer $\frac{1}{i}A$ comme un opérateur auto-adjoint non-borné dans $\mathcal{H}(\Omega)$ de domaine : $\left\{(u_0,u_1)\in \mathcal{H}(\Omega)\,;u_1\in H_D(\Omega), \Delta u_0 \in L^2(\Omega)\right\}$. Si $U(t) = \exp tA = \exp\left(it\frac{1}{i}A\right)$ est le groupe unitaire associé et si $u(0)\in\mathcal{H}(\Omega)$ alors $u(t) = U(t)(u(0))$ nous donne une solution de (1.2) au sens des distributions. Remarquons qu'on a une inclusion naturelle : $\mathcal{H}(\Omega)\subset\mathcal{H}(\mathbf{R}^n)$, définie en prolongeant les éléments de $\mathcal{H}(\Omega)$ par 0 dans $\mathcal{O}$.

Lax et Phillips introduisent une variante (explicite) de la transformée de Radon, $\mathcal{R}_0 : \mathcal{H}(\mathbf{R}^n)\to L^2(\mathbf{R}\times S^{n-1})$ avec les propriétés suivantes :

(1.3)
- *a)* $\mathcal{R}_0$ est unitaire,
- *b)* si $\mathcal{R}_0 u(s,\omega)$ s'annule pour $|s|<T$, alors u s'annule pour $|s|<T$,
- *c)* $\mathcal{R}_0 U_0(t) = \tau_t\circ\mathcal{R}_0$, où $(\tau_t f)(s,\omega) = f(s-t,\omega)$,
- *d)* il y a des formules explicites pour $\mathcal{R}_0$ et $\mathcal{R}_0^{-1}$.

Ici $U_0(t) = \exp tA_0$ est défini comme auparavant avec Ω remplacé par $\mathbf{R}^n$. On appelle $\mathcal{R}_0$ une représentation de translation pour le groupe d'évolution libre. Pour $\rho\geq 0$ on pose

$$D_\rho^+ = \left\{u\in\mathcal{H}(\mathbf{R}^n)\,;\,U_0(t)u = 0 \text{ si } t\geq 0 \text{ et } |x|\leq\rho+t\right\}$$

$$D_\rho^- = \left\{u\in\mathcal{H}(\mathbf{R}^n)\,;\,U_0(t)u = 0 \text{ si } t\leq 0 \text{ et } |x|\leq\rho+|t|\right\},$$

et on peut montrer que

$$\mathcal{R}_0 D_\rho^\pm = \left\{f\in L^2(\mathbf{R}\times S^{n-1})\,;\,f(s,\omega) = 0 \text{ si } \pm s\leq\rho\right\}.$$

En particulier D_ρ^+ et D_ρ^- sont orthogonaux.

Si on choisit $\rho > 0$ assez grand pour que $\mathcal{O} \subset B(0,\rho) = \{x \in \mathbf{R}^n ; |x| < \rho\}$, alors $D_\rho^\pm$ peuvent aussi être considérés comme des sous-espaces de $\mathcal{H}(\Omega)$, et pour $u \in D_\rho^\pm$, on a $U(t)u = U_0(t)u$ si $\pm t \geq 0$. En utilisant que A n'a pas de valeurs propres on peut montrer que

$$\bigcup_{t\in\mathbf{R}} U(t)D_\rho^\pm \text{ sont denses dans } \mathcal{H}(\Omega)\ . \tag{1.4}$$

Grâce à cette propriété on peut définir des représentations de translation sortantes $(+)$ et entrantes $(-)$ par :

$$\text{Si } u \in D_\rho^\pm \text{ on pose } \mathcal{R}_\pm U(t)u = \mathcal{R}_0 U_0(t)u = \tau_t \mathcal{R}_0 u\ . \tag{1.5}$$

On obtient alors :

$$\begin{aligned} &a)\quad \mathcal{R}_\pm : \mathcal{H}(\Omega) \to L^2(\mathbf{R}\times S^{n-1}) \text{ est unitaire,} \\ &b)\quad \mathcal{R}_\pm u = R_0 u \text{ si } u \in \mathcal{D}_\rho^\pm \\ &c)\quad \mathcal{R}_\pm U(t) = \tau_t \mathcal{R}_\pm\ . \end{aligned} \tag{1.6}$$

La relation avec les opérateurs d'onde $W_\pm = s - \lim_{t\to\pm\infty} U(-t)U_0(t)$ (isométries : $\mathcal{H}(\mathbf{R}^n) \to \mathcal{H}(\Omega)$) est :

$$R_+ W_+ = R_- W_- = R_0\ . \tag{1.7}$$

En particulier l'image de $W_\pm$ est $\mathcal{H}(\Omega)$ ($\Rightarrow$ complétude asymptotique) et on peut définir l'opérateur de scattering $S = W_+^{-1} W_- : \mathcal{H}(\mathbf{R}^n) \to \mathcal{H}(\mathbf{R}^n)$ qui est unitaire et qui commute avec $U_0(t)$. (1.7) donne

$$S = R_0^{-1} R_+ R_-^{-1} R_0\ . \tag{1.8}$$

Via R_0 on peut donc identifier S avec l'opérateur unitaire dans $L^2(\mathbf{R}\times S^{n-1})$, $\widetilde{S}\cdot : R_- u \mapsto R_+ u$, qui commute avec les translations. C'est donc un opérateur de convolution, $\widetilde{S}u = k * u$. En utilisant indirectement que les supports se propagent avec une vitesse ≤ 1, on voit que S envoie D_ρ^- dans $(D_\rho^+)^\perp$ ce qui entraîne que le support de la distribution k est contenu dans $]-\infty, 2\rho]$. La matrice de scattering $\mathcal{S}(\lambda) \underset{\text{def}}{=} \int e^{it\lambda} k(t)\,dt$ admet donc un prolongement holomorphe dans le demi-plan inférieur.

Un autre objet important est le semi-groupe de Lax-Phillips. On fixe $\rho > 0$ avec $\mathcal{O} \subset B(0,\rho)$ et on introduit les projecteurs orthogonaux

$P_+, P_- : \mathcal{H}(\Omega) \to \mathcal{H}(\Omega)$ sur $D_+^{\rho\perp}$ et $D_-^{\rho\perp}$ respectivement. Pour $t \geq 0$ on pose :

$$Z(t) = P_+ U(t) P_- \,, \tag{1.9}$$

et on vérifie que $Z(t)$ est un semi-groupe de contractions, fortement continu sur $K \underset{\text{def}}{=} \mathcal{H}(\Omega) \cap (D_+^\rho \oplus D_-^\rho)^\perp$. (Si u est à support dans $B(0,\rho)$, alors $Z(t)u = U(t)u$ dans $B(0,\rho)$). Soit B le générateur du semi-groupe $\{Z(t)\}$. Dans la représentation de translation sortante, K devient :

$$R_+ K = \Big(L^2([\rho,+\infty[\times S^{n-1}) \oplus \widetilde{S}\Big(L^2(]-\infty,-\rho] \times S^{n-1}\Big)\Big)^\perp =$$

$$= L^2\Big(]-\infty,\rho] \times S^{n-1}\Big) \cap \Big(\widetilde{S}\Big(L^2(]-\infty,-\rho] \times S^{n-1}\Big)\Big)^\perp$$

et l'action de $R_+ Z(t) R_-$ sur cet espace est $1_{]-\infty,\rho]}\tau_t$. Exploitant ce lien entre S et $Z(t)$ et un résultat de compacité pour $Z(t)(1+B)^{-1}$ quand $t > 2\rho$, Lax et Phillips [**LP1**] démontrent :

THÉORÈME 1.1.

a) *$\mathcal{S}(z)$ se prolonge en une fonction méromorphe dans $\mathbb{C}$ à valeurs dans $\mathcal{L}\big(L^2(S^{n-1}), L^2(S^{n-1})\big)$ et avec les pôles contenus dans $\{z \in \mathbb{C}\,;\, \operatorname{Im} z > 0\}$.*

b) *Le spectre de B est discret et contenu dans $\{z \in \mathbb{C}\,;\, \operatorname{Re} z < 0\}$.*

c) *λ est un pôle de $\mathcal{S}$ ssi $i\lambda \in \sigma(B)$.*

Les pôles de $\mathcal{S}$ sont appelés pôles de "scattering", ou résonances. Une autre caractérisation utile des résonances est donnée par :

THÉORÈME 1.2 ([**LP1**]). *Pour $f, g \in C_0^\infty(\Omega)$ la fonction $\lambda \mapsto ((\lambda - A)^{-1} f \mid g)_{\mathcal{H}(\Omega)}$, définie pour $\operatorname{Re}\lambda > 0$, admet une extension méromorphe à $\mathbb{C}$ dont les pôles sont contenus dans $\sigma(B)$. Si $\mu \in \sigma(B)$, on peut trouver $f \in C_0^\infty(\Omega)$ tel que $((\lambda - A)^{-1} f \mid f)$ a un pôle en μ.*

Surtout après l'apparition des résultats suffisamment précis sur la propagation des singularités il est devenu intéressant d'avoir des formules de

trace reliant la groupe $U(t)$ avec la matrice de scattering et les résonances. Dans cet exposé on ne discutera que la formule qui s'applique aux résonances. Bardos-Guillot-Ralston [**BGR**] ont montré que si $f \in H^{n+1}(\mathbf{R})$ est à support compact contenu dans $]2\rho, +\infty[$, alors $\int f(t)\,Z(t)\,dt$ est nucléaire et

$$\text{tr} \int f(t)U(t)\,dt = \text{tr} \int f(t)\,Z(t)\,dt = \sum_j \hat{f}(\lambda_j)\ , \tag{1.10}$$

où la somme à droite converge absolument et les λ_j parcourent $\frac{1}{i}\sigma(B)$, (répétés selon la multiplicité algébrique de chaque valeur propre). L'opérateur $\int f(t)U(t)\,dt$ n'est pas nucléaire, mais son noyau s'annule pour $|x-y| \leq 1$, $|x|$ assez grand et on arrive à définir sa trace. En considérant $\int f(t)\,Z(t)\,dt$ dans un espace convenablement modifié, Melrose [**M1**] a étendu la validité de (1.10) au cas où $\text{supp}\, f \subset\subset]0, +\infty[$. Dans le même travail il a aussi obtenu une majoration du type de Weyl :

$$\#\ \{\lambda_j\ ;\ |\lambda_j| \leq R\} \leq C(1+R)^n\ ,\quad R \geq 0\ . \tag{1.11}$$

Grâce à ces améliorations (1.10) prend la forme

$$\text{tr}\, U(t) = \text{tr}\, Z(t) = \sum_j e^{it\lambda_j}\ ,\quad t > 0 \tag{1.12}$$

au sens des distributions, et où la série converge au sens des distributions. Pour d'autres résultats concernant le membre de gauche de (1.11) voir Zworski [**Z**], Intissar [**In**].

2. Propagation des singularités pour le problème de Dirichlet

Il est commode d'utiliser le formalisme des transformations de Fourier-Bros-Iagolnitzer pour décrire de façon uniforme les résultats. (Voir [**S1**] pour plus de détails). Soit $Y \subset \mathbf{R}^n$ un ouvert, $(y_0, \eta_0) \in T^*Y \setminus 0 = Y \times (\mathbf{R}^n \setminus \{0\})$.

Soit $\varphi(x,y)$ une fonction holomorphe définie dans un voisinage de $(x_0, y_0) \in \mathbb{C}^n \times \mathbb{C}^n$ avec les propriétés :

$$\frac{\partial \varphi}{\partial y}(x_0,y_0) = -\eta_0\,,\ \text{Im}\,\frac{\partial^2 \varphi}{\partial y^2}(x_0,y_0) > 0\,,\ \det \frac{\partial^2 \varphi}{\partial x\,\partial y}(x_0,y_0) \neq 0\,. \tag{2.1}$$

Pour $x \in \text{Vois}(x_0)$, la fonction $\mathbf{R}^n \cap \text{Vois}(y_0) \ni y \mapsto \text{Im}\,\varphi(x,y)$ a un minimum non-dégénéré en un point $y(x)$. Si on pose $\eta(x) = -\dfrac{\partial\varphi}{\partial y}(x, y(x))$, l'application $x \mapsto (y(x), \eta(x))$ est un difféomorphisme analytique d'un voisinage (complexe) de x_0 sur un voisinage réel de (y_0, η_0). La fonction $\Phi(x) = -\,\text{Im}\,\varphi(x, y(x))$ est bien définie et strictement plurisousharmonique dans un voisnage de x_0. Le difféomorphisme symplectique $\mathcal{H}_T : \left(y, -\dfrac{\partial\varphi}{\partial y}(x,y)\right) \mapsto \left(x, \dfrac{\partial\varphi}{\partial x}(x,y)\right)$ d'un voisinage complexe de (y_0, η_0) sur un voisinage complexe de (x_0, ξ_0) envoie les points réels sur un voisinage de (x_0, ξ_0) dans

$$\Lambda_\Phi = \left\{ \left(x, \frac{2}{i}\frac{\partial\Phi}{\partial x}\right) : x \in \text{Vois}(x_0) \right\}.$$

Si $\chi \in C_0^\infty(\mathbf{R}^n)$ est à support dans un petit voisinage de y_0 et vaut 1 près de ce point, alors pour tout $u \in \mathcal{D}'(Y)$, la fonction (= transformée FBI de u)

$$T_\chi u(x,\lambda) = \int e^{i\lambda\varphi(x,y)}\chi(y)u(y)\,dy \tag{2.2}$$

est bien définie pour $x \in \text{Vois}(x_0)$, $\lambda \geq 1$ et vérifie

$$|T_\chi u(x,\lambda)| \leq C_0\,\lambda^{N_0}\,e^{\lambda\Phi(x)}\,, \tag{2.3}$$

(où C_0, N_0 dépendent de u).

DÉFINITION 2.1. On dit respectivement que $(y_0,\eta_0) \notin WF_{C^\infty}(u)$, $(y_0,\eta_0) \notin WF_a(u)$, $(y_0,\eta_0) \notin WF_{G_3}(u)$, s'il existe un voisinage complexe V de x_0 tel que respectivement :

- $\forall N \geq 0$, $\exists C > 0$, t.q. $|T_\chi u(x,\lambda)| \leq C\lambda^{-N}e^{\lambda\Phi(x)}$, $x \in W$, $\lambda \geq 1$,
- $\exists C > 0$, t.q. $|T_\chi u(x,\lambda)| \leq Ce^{\lambda(\Phi(x)-1/C)}$, $x \in V$, $\lambda \geq 1$,
- $\exists C > 0$, t.q. $|T_\chi u(x,\lambda)| \leq Ce^{\lambda\Phi(x)-\lambda^{1/3}/C}$, $x \in V$, $\lambda \geq 1$.

(Pour l'équivalence entre ces définitions et les définitions plus classiques d'Hörmander et de Sato, voir **[S1]** (et aussi **[Bo]**) dans le cas analytique, **[LasS]** dans le cas C^∞, **[Le2]** dans le cas Gevrey 5). Les ensembles $WF_{C^\infty}(u) \subset WF_{G^3}(u) \subset WF_a(u)$ sont fermés et coniques dans $T^*Y \setminus 0$ et leurs projections dans Y sont les supports singuliers de u modulo $C^\infty(Y)$,

$G^3(Y)$, $\mathcal{A}(Y)$ respectivement. (Le support singulier modulo $\mathcal{K}$ est le plus petit fermé de Y en dehors duquel u est de classe $\mathcal{K}$, $\mathcal{K} = C^\infty$, G^3, $\mathcal{A}$). Ici

$$G^3(Y) = \Big\{ u \in C^\infty(Y) ; \forall K \subset\subset Y, \exists C > 0 \text{ t.q. } \forall \alpha \in \mathbf{N}^n, y \in K : \\ |\partial_y^\alpha u(y)| \leq (\alpha!)^3 C^{|\alpha|+1} \Big\} ,$$

avec les notations :

$\alpha = (\alpha_1, \ldots, \alpha_n)$, $\alpha! = \alpha_1! \ldots \alpha_n!$, $\partial_y^\alpha = \partial_{y_1}^{\alpha_1} \ldots \partial_{y_n}^{\alpha_n}$, $|\alpha| = \alpha_1 + \ldots + \alpha_n$.

$\mathcal{A}(Y) = G^1$ est l'espace des fonctions analytiques réelles sur Y.

Soit Ω comme dans la section 1, et écrivons x_0 à la place de t. Si $x^0 \in \partial\Omega$, on peut introduire de nouvelles coordonnées $y_1, \ldots, y_n$ centrées en x^0, telles que Ω soit donné par $y_n > 0$ et telles qu'aux facteurs négligeables > 0 près, $\Box = D_{y_n}^2 + R(y, D_{y'})$, où $y_0 = x_0$, $y = (y_0, y_1, \ldots, y_n)$, $y' = (y_0, \ldots, y_{n-1})$. (Si $\partial\Omega$ est analytique on peut choisir les nouvelles coordonnées analytiques). R est un opérateur différentiel d'ordre 2 dont le symbole principal $r(y, \eta')$ vérifie : $r(y, \eta') = 0, \eta' \neq 0 \Rightarrow \partial_{\eta'} r(y, \eta') \neq 0$. Soit p le symbole principal de $\Box$ ($= \xi_1^2 + \ldots + \xi_n^2 - \xi_0^2$ dans les coordonnées initiales et $= \eta_n^2 + r(y, \eta')$ dans les nouvelles coordonnées définies sur $T^*\Omega \setminus 0$). Dans $T^*\partial\Omega \setminus 0$ on introduit les trois zones : $\mathcal{E}$ = région elliptique : $r(0, y', \eta') > 0$, $\mathcal{H}$ = région hyperbolique : $r(0, y', \eta') < 0$, $\mathcal{G}$ = région de "glancing" : $r(0, y', \eta') = 0$. Soit $\Sigma_b = p^{-1}(0) \big|_{\mathbf{R} \times \Omega} \cup \mathcal{H} \cup \mathcal{G}$ avec sa topologie naturelle avec la propriété que $(y_\nu, \eta_\nu) \in p^{-1}(0) \big|_{\mathbf{R} \times \Omega}$ tend vers $(y', \eta') \in \mathcal{H} \cup \mathcal{G}$, $\nu \to \infty$, si $(y_\nu)_n \searrow 0$, $(y'_\nu, \eta'_\nu) \to (y', \eta')$.

Soit W un ouvert de $\mathbf{R} \times \mathbf{R}^n$ et $u \in \mathcal{D}'(W \cap (\mathbf{R} \times \Omega))$ une distribution prolongeable telle que $\Box u \in C^\infty(W \cap (\mathbf{R} \times \bar{\Omega}))$. On définit alors $WF_{C^\infty}^b(u) \subset ((T^*(\mathbf{R} \times \partial\Omega) \setminus 0) \cup (T^*(\mathbf{R} \times \Omega) \setminus 0)) \big|_W$ par :

$$-WF_{C^\infty}^b(u) \big|_{W \cap (\mathbf{R} \times \Omega)} = WF_{C^\infty}(u) .$$

– Un point $(y'_0, \eta'_0) \in T^*(\mathbf{R} \times \partial\Omega) \big|_W$ n'appartient pas à $WF_{C^\infty}^b(u)$ s'il existe $\varepsilon > 0$ tel que (y'_0, η'_0) n'appartient pas à $WF_{C^\infty}(u(\cdot, y_n))$ de façon uniforme au sens de la Définition 2.1 ($\exists$ choix de V et $C = C_N$ indépendant de y_n), quand $0 \leq y_n \leq \varepsilon$.

De même, si $\partial\Omega$ est analytique et $\Box u$ est analytique sur $W \times (\mathbf{R} \times \bar{\Omega})$, on définit $WF_a^b(u)$ et $WF_{G^3}^b(u)$. On sait dans les trois cas que $WF^b_\cdot(u)$ est un ensemble fermé conique dont la projection sur l'espace des x est respectivement le support singulier de u modulo $C^\infty(W \cap (\mathbf{R} \times \bar{\Omega}))$, $\mathcal{A}(W \cap (\mathbf{R} \times \bar{\Omega}))$, $G^3(W \cap (\mathbf{R} \times \bar{\Omega}))$. Si on suppose en plus que $u\,|_{(\mathbf{R}\times\partial\Omega)\cap W} \in C^\infty$ et $\in \mathcal{A}$ respectivement, alors la régularité microlocale pour des problèmes aux limites elliptiques entraîne que $WF^b_\cdot(u) \subset \Sigma_b\,|_W$. Le problème de propagation des singularités est alors d'analyser $WF^b_\cdot(u)$ de plus près. Pour cela on introduit les notions de rayon C^∞ ([**MS**,II]) et de rayon analytique [**S2**].

DÉFINITION 2.2. Un rayon analytique est une courbe (continue) $\gamma : I \to \Sigma_b$ (où I est un intervalle) tel que :

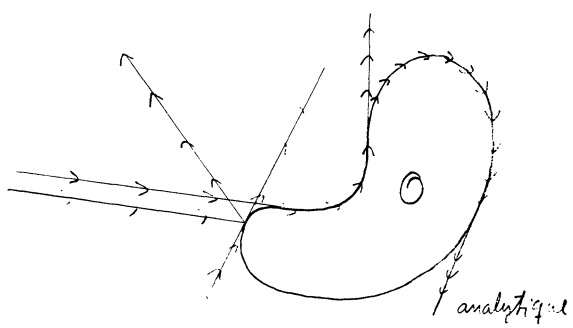
1. si $\gamma(t) \in p^{-1}(0)\,|_{\mathbf{R}\times\Omega}$ alors $\dfrac{d\gamma}{dt}(t)$ existe et vaut $\left(\dfrac{\partial p}{\partial \xi}(\gamma(t)), -\dfrac{\partial p}{\partial x}(\gamma(t))\right)$,

2. si $\gamma(t) \in \mathcal{H}$ alors $\exists \varepsilon > 0$, t.q. $\gamma(s) \in p^{-1}(0)\,|_{\mathbf{R}\times\Omega}$ pour $0 < |s-t| < \varepsilon$,

3. si $\gamma(t) \in \mathcal{G}$, et si en utilisant les coordonnées y on écrit $\gamma(s) = (y(s), \eta(s))$ pour $\gamma(s) \in p^{-1}(0)\,|_{\mathbf{R}\times\Omega}$, $\gamma(s) = (y'(s), \eta'(s))$ pour $\gamma(s) \in \mathcal{H} \cup \mathcal{G}$, alors $(y'(s), \eta'(s))$ est dérivable en $s = t$ et la dérivée vaut $\left(\dfrac{\partial r}{\partial \eta'}, -\dfrac{\partial r}{\partial y'}\right)(y'(t), 0; \eta'(t))$.

La définition d'un rayon C^∞ est la même à ceci près qu'on remplace $\mathcal{H}$ par $\mathcal{H} \cup \mathcal{G}_+$ dans 2., où $\mathcal{G}_+ \subset \mathcal{G}$ est la région diffractive définie par $\dfrac{\partial r}{\partial y_n}(y', 0, \eta') < 0$. Tout rayon C^∞ est analytique!

Voici le tracé de la projection dans $\bar{\Omega}$ de quelques rayons :



Tout rayon C^∞ ou analytique peut se prolonger en un rayon avec $\mathbf{R}$ comme intervalle de définition. En ce qui concerne les rayons C^∞, le prolongement est unique sauf dans des cas pathologiques, qui ne se produisent pas quand $\partial\Omega$ est analytique.

Soit $u \in \mathcal{D}'((\mathbf{R}\times\Omega)\cap W)$ une distribution prolongeable vérifiant

$$(2.4)_{C^\infty} \qquad \Box u \in C^\infty((\mathbf{R}\times\bar{\Omega})\cap W),\ u\,|_{(\mathbf{R}\times\partial\Omega)\cap W} \in C^\infty$$

ou bien dans le cas où $\partial\Omega$ est analytique :

$$(2.4)_{\mathcal{A}} \qquad \Box u \in \mathcal{A}((\mathbf{R}\times\bar{\Omega})\cap W),\ u\,|_{(\mathbf{R}\times\partial\Omega)\cap W} \in \mathcal{A}\ .$$

THÉORÈME 2.3 (Melrose-Sjöstrand [**MS**]). *Si u vérifie $(2.4)_{C^\infty}$ et $\rho_0 \in WF^b_{C^\infty}(u)$ alors il existe un rayon C^∞ maximal γ dans $\Sigma_b\,|_W$ (c.à.d. non prolongeable en tant que rayon C^∞ dans $\Sigma_b\,|_W$) contenu dans $WF^b_{C^\infty}(u)$.*

Ivrĭi [**Iv**] a obtenu presque le même résultat. Son analyse près de $\mathcal{G}_+$ est basée sur des inégalités d'énergie, évitant ainsi (contrairement à [**MS**]) tout appel aux constructions de paramétrixes assez lourdes dans cette région (obtenues antérieurement par M. Taylor et Melrose). Voir aussi [**Hö**].

Dans la suite de cette section on suppose que $\partial\Omega$ est analytique. Nous avons le :

THÉORÈME 2.4 (Sjöstrand [**S2**]). *Si u vérifie $(2.4)_{\mathcal{A}}$ et $\rho_0 \in WF^b_a(u)$, alors il existe un rayon analytique maximal γ dans $\Sigma_b\,|_W$ qui est contenu dans $WF^b_a(u)$.*

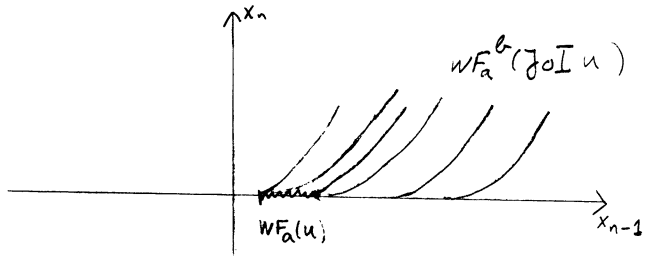
Comme l'ont remarqué Friedlander-Melrose [**FM**] dans le cas d'un opérateur modèle explicitement traitable, on peut avoir une propagation des singularités analytiques (et même Gevrey d'indice < 3) le long des rayons analytiques non C^∞. Un tableau assez vaste de ces phénomènes de diffraction se trouve dans Sjöstrand [**S2-4**], Kataoka [**K**], Lebeau [**Le3**], Laubin [**La1,2**].

Lebeau a montré qu'on a le même type de propagation pour les singularités $\mathrm{mod}\, G^3$ que pour les singularités $\mathrm{mod}\, C^\infty$, c.à.d. qu'on n'a pas de diffraction :

THÉORÈME 2.5 (Lebeau [**Le1,2**]). *Si u vérifie $(2.4)_{\mathcal{A}}$, et $\rho_0 \in WF^b_{G^3}(u)$ alors le rayon C^∞ maximal γ dans $\Sigma_b\,|_W$ passant par ρ_0 est contenu dans $WF^b_{G^3}(u)$.*

Comme $\partial\Omega$ est analytique il y a un rayon C^∞ maximal unique passant par ρ_0. B. et R. Lascar [**Las**] ont récemment amélioré ce résultat en traitant aussi les cas ou le bord est seulement Gevrey (on perd alors dans les indices Gevrey de la conclusion). Leur méthode, partiellement inspirée de celle d'Ivrĭi mentionnée auparavant, est entièrement basée sur des inégalités. La démonstration de Lebeau utilise un mélange subtil de constructions directes et d'inégalités dont nous ne pouvons ici donner qu'une très vague idée :

ESQUISSE DE LA DÉMONSTRATION DU THÉORÈME 2.5 : En dehors de G_+ l'étude de la propagation Gevrey se fait essentiellement comme dans la démonstration du Théorème 2.4. On se restreint donc à un voisinage d'un point de G_+, et on choisit de nouvelles coordonnées $x = (x_0, \ldots, x_n) = (x', x_n)$ telles que $\Box = R(x, D_{x'}) + D^2_{x_n}$. La première étape est de construire certaines solutions oscillantes de l'équation homogène et une idée essentielle est alors de faire une transformation de Fourier formelle en x_n et de considérer $R(x', -D_{\xi_n}, D_{x'}) + \xi_n^2$ pour lequel on peut facilement donner des solutions oscillantes, et il s'agit ensuite de donner un sens à la transformation de Fourier inverse de ces solutions en choisissant convenablement un contour d'intégration. (Voir aussi [**S4**], [**La2**]). A cette étape la fonction d'Airy apparaît naturellement. Lebeau construit ainsi un opérateur microlocal $\mathcal{J} \circ I : \left\{\text{distributions sur } x_n = 0\right\} \to \left\{\text{distributions prolongeables}\right\}$ avec la propriété que $\Box(\mathcal{J} \circ Iu)$ est analytique jusqu'au bord pour tout u et tel que $WF^b_a(\mathcal{J} \circ Iu) \subset WF_a(u) \cup \left\{\gamma(t); t \geq 0 \text{ et } \gamma \text{ est un rayon analytique avec } \gamma(0) \in WF_a(u)\right\}$. (En réalité toutes ces constructions sont faites après une transformation de FBI). On a donc déjà ici un phénomène de diffraction :



Pour aller plus loin, il faut étudier les opérateurs trace :

$$K^{(0)}u(x') = (\mathcal{J} \circ Iu)\,|_{x_n=0}\ ,\ K^{(1)}u(x') = (\partial_{x_n}\mathcal{J} \circ Iu)\,|_{x_n=0}\ ,$$

et pour résoudre le problème de Dirichlet avec inhomogénéité sur le bord, il faut inverser $K^{(0)}$. On montre que (dans une représentation FBI convenable) $K^{(0)}$ est une sorte d'opérateur pseudodifférentiel de symbole dans la classe $\mathcal{E}^+_\gamma$: $p = \sum_{k\geq 0} p_k(x,\xi,\lambda)(iT)^{-k}$ (où $\lambda \geq 1$ est le grand paramètre FBI et T est un paramètre formel qui moralement vaut λ) avec p_k holomorphe dans $\Omega_{\lambda,r,\delta,\gamma}$: $|x' - x'_0| < r$, $|\xi'' - \xi''_0| < r$, $|\xi_{n-1}| < r$, $\operatorname{Im}\xi_{n-1} < \gamma\lambda^{-2/3} + \delta\,|\operatorname{Re}\xi_{n-1}|$ et :

$$\sup_{\Omega_{\lambda,r,\delta,\gamma}} \left|\left(\xi_{n-1} - i\gamma\lambda^{-2/3}\right)^k p_k\right| \leq AB^k k!\ .$$

Ici $\delta > 0$, et on a choisit la transformation de FBI de telle façon que G_+ corresponde à $\xi_{n-1} = 0$. $(x'_0, \xi''_0, 0)$ est fixé ainsi que $r > 0$.

Pour l'opérateur $K^{(0)}$, on peut choisir $\gamma > 0$ arbitrairement grand et on trouve aussi que p_0 a un zéro simple en

$$\xi_{n-1} = \lambda^{-2/3} e^{2\pi i/3}\left(\omega\rho^{-1} + \mathcal{O}(\lambda^{-1/3})\right)\ ,$$

où $-\omega$ est le premier zéro de la fonction d'Airy (sur l'axe $]-\infty, 0[$ compté à partir de 0) et ρ est essentiellement la courbure de la géodésique du bord. De plus p_0 est elliptique en dehors de ce point dans une bande $\operatorname{Im}\xi_{n-1} < \lambda^{-2/3}\left(\operatorname{Im}(e^{2\Pi i/3}) + \varepsilon_0\right)$ pour un $\varepsilon_0 > 0$ convenable.

Pour ces symboles, Lebeau donne une recette de quantification pour définir des opérateurs "unilatéraux" qui opèrent dans l'espace des fonctions à croissance tempérée (par rapport au poids FBI, ce qui correspond aux distributions) qui décroissent exponentiellement pour $\operatorname{Re} x_{n-1} < \widetilde{a}$. Ici on

travaille dans un domaine complexe avec $\operatorname{Re} x_{n-1} \in]a, b[$ et on suppose $a < \widetilde{a} < b$. Il montre ensuite, en faisant appel à la théorie de la deuxième microlocalisation (voir [**S1**], [**Le3**] et les travaux de Kashiwara-Kawaï et Laurent qui y sont cités) que l'on a bien un calcul symbolique qui marche modulo $\mathcal{O}(e^{-\lambda/C})$. Ceci n'est pas évident car les symboles peuvent être singuliers à distance $\sim \lambda^{-2/3}$ de l'axe réel ce qui laisse penser que les erreurs vont plutôt être $\mathcal{O}\left(e^{-\lambda^{1/3}C}\right)$, c.à.d. qu'on ait seulement un calcul modulo Gevrey 3. Ces opérateurs propagent en général les singularités analytiques dans la direction $\operatorname{Re} x_{n-1}$ croissante et ce ne sont donc pas du tout des opérateurs pseudodifférentiels analytiques classiques. Utilisant le fait qu'on peut déformer des contours d'intégration jusqu'à $\operatorname{Im} \xi_{n-1} \sim \lambda^{2/3}$, on voit que si u est à décroissance exponentielle aussi pour $\operatorname{Re} x_{n-1} > \widetilde{b}$ (avec $a < \widetilde{a} < \widetilde{b} < b$) alors l'image de u par un opérateur unilatéral est $\mathcal{O}\left(e^{-\lambda^{1/3}\cdot \text{const.}}\right)$ sur tout compact dans $\operatorname{Re} x_{n-1} > \widetilde{b}$.

L'opérateur $K^{(0)}$ est elliptique près du réel et peut donc être inversé modulo $\mathcal{O}\left(e^{-\lambda/C}\right)$ en tant qu'opérateur sur les fonctions exponentiellement petites à gauche. En utilisant aussi que $K^{(0)}$ est de type principal un peu plus loin dans le complexe (racine simple $\approx \lambda^{-2/3} e^{2\Pi i/3} \omega \rho^{-1}$) on arrive à préciser les propriétés de propagation de ${K^{(0)}}^{-1}$ et de $K^{(1)} {K^{(0)}}^{-1}$. Au lieu de montrer simplement que ces opérateurs produisent des fonctions $\mathcal{O}\left(e^{-\lambda^{1/3}\cdot \text{const.}}\right)$ à droite (par rapport à $\operatorname{Re} x_n$) de la région où la donnée n'est pas exponentiellement petite, Lebeau arrive à préciser le taux de décroissance et même à donner un développement asymptotique. Cette précision qui n'est pas indispensable pour prouver le Théorème 2.5, devient fondamentale dans la démonstration du Théorème 4.2.

La fonction $v = \mathcal{J} \circ I \circ {K^{(0)}}^{-1} u$ est une solution sortante du problème de Dirichlet inhomogène : $\Box v \in$ analytique, $v \big|_{\mathbb{R} \times \partial\Omega} = u$ et on a $(\partial_{x_n} v) \big|_{x_n = 0} = K^{(1)} {K^{(0)}}^{-1} u$. L'opérateur $K^{(1)} {K^{(0)}}^{-1}$ est donc "l'opérateur de Neumann sortant". Il est classique que si on contrôle bien cet opérateur, alors on obtient des théorèmes de propagation par un argument de dualité. Ainsi on obtient bien le Théorème 2.5 près de G_+.

3. Distribution des pôles pour des obstacles C^∞

Comme déjà observé dans le livre [**LP1**], la distribution des pôles de scattering proche de l'axe réel dépend de la géométrie de l'obstable $\mathcal{O}$.

DÉFINITION 3.1. $\mathcal{O}$ est captant ("trapping") s'il existe un rayon C^∞ maximal dans Σ_b dont la projection dans $\overline{\Omega}$ est contenue dans l'enveloppe convexe de $\mathcal{O}$.

Si $\mathcal{O}$ est non captant et $\mathcal{O} \subset B(0,R)$, alors il existe $T_R > 0$ tel que pour tout rayon C^∞ maximal $\gamma : \mathbf{R} \to \Sigma_b \cap \{|\xi| = \frac{1}{2}\}$, l'ensemble des t tel que $\Pi_x \gamma(t) \in B(0,R)$ est vide ou bien un intervalle de longueur $\leq T_R$. On a les implications : $\mathcal{O}$ est convexe $\Rightarrow$ $\mathcal{O}$ est étoilé $\Rightarrow$ $\mathcal{O}$ est captant. Dans le cas d'un obstacle convexe, Lax et Phillips [**LP2**] ont montré qu'il existe $a > 0$ t.q. la région $\{\lambda \in \mathbb{C}\,;\, \operatorname{Im}\lambda \leq a \log|\lambda|\}$ ne contienne qu'un nombre fini de pôles de scattering. D'après leur Théorème 2.2, c), il s'agit de montrer qu'il existe $T > 0$ tel que l'image de $Z(T)$ soit contenu dans le domaine de B. Pour les obstacles non captants, il résulte de (4.4) dans la section suivante et du Théorème 2.3 qu'on a bien cette propriété (et que $Z(t)$ est compact pour $T > 0$ assez grand), donc en dessous d'une courbe logarithmique on n'a qu'un nombre fini de pôles de scattering.

Le cas d'un obstacle captif le plus simple est sans doute celui où $\mathcal{O}$ est une réunion de deux obstacles $\mathcal{O}_1, \mathcal{O}_2$ disjoints et strictement convexes. Soient $x_j \in \partial\mathcal{O}_j$, $j = 1,2$ les deux points qui réalisent la distance entre le obstacles et posons $d = |x_1 - x_2| = \operatorname{dist}(\mathcal{O}_1, \mathcal{O}_2)$. A quelques identifications triviales près, le seul rayon C^∞ maximal qui reste au-dessus de l'enveloppe convexe de $\mathcal{O}$ pour toujours est celui qui fait un aller retour éternel entre x_1 et x_2. En suivant un rayon optique partant d'un point de $\partial\mathcal{O}_1$ proche de x_1 dans une direction proche de la normale jusqu'à son retour à $\partial\mathcal{O}_1$ après une reflexion dans $\partial\mathcal{O}_2$, on obtient une application de Poincaré : $T^*(\partial\mathcal{O}_1) \cap \operatorname{Vois}((x_1,0)) \to T^*(\partial\mathcal{O}_1) \cap \operatorname{Vois}((x_1,0))$, et comme l'ont remarqué Bardos-Guillot-Ralston [**BGR**], le point fixe $(x_1,0)$ est du type hyperbolique

et plus précisément les valeurs propres de la différentielle de l'application de Poincaré sont de la forme

$$\frac{1}{\nu_{n-1}} \leq \frac{1}{\nu_{n-2}} \leq \ldots \leq \frac{1}{\nu_1} < 1 < \nu_1 \leq \nu_2 \leq \ldots \leq \nu_{n-1} \ .$$

Guidés par des considérations heuristiques, Bardos-Guillot-Ralston ont introduit des pseudo-pôles de la forme :

$$\lambda_{j,\alpha} = \frac{1}{d}\pi j + \frac{i}{2}\left(\frac{\mu_1 + \ldots + \mu_{n-1}}{2} + \sum_1^{n-1} \alpha_j \mu_j\right) \ ,$$

avec $j \in \mathbb{Z}$, $\alpha = (\alpha_1, \ldots, \alpha_{n-1}) \in \mathbb{N}^{n-1}$, $\mu_j = \log \nu_j$. Pour chaque α on obtient une rangée parallèle à l'axe réel. On définit la multiplicité d'un pseudo-pôle $\lambda_{j,\alpha}$ comme le nombre $m(\alpha)$ de différents $\beta \in \mathbb{N}^{n-1}$ avec $\lambda_{j,\beta} = \lambda_{j,\alpha}$. La première rangée des $\lambda_{j,0}$ est la plus proche de l'axe réel et $m(0) = 1$.

Ikawa [**I1**] a démontré que dans une bande $\operatorname{Im}\lambda \leq \dfrac{\mu_1 + \ldots + \mu_{n-1}}{4} + c$ pour un $c > 0$, les pôles avec $|\lambda|$ assez grand sont contenu dans la réunion des disques $D\left(\lambda_{j,0}, C\,|\lambda_{j,0}|^{-1/2}\right)$ si $C > 0$ est assez grand, et que chaque disque contient un tel pôle si $|j|$ est assez grand. Ensuite dans [**I2**] il a précisé le résultat montrant qu'il y a exactement un pôle dans chaque disque pour $|j|$ grand, qui admet un développement asymptotique. Suite à [**I1**] mais indépendamment de [**I2**], C. Gérard a obtenu une justification complète de toutes les rangées. Son résultat coïncide avec celui d'Ikawa [**I2**] pour la première rangée :

THÉORÈME 3.1 ([**Ge**]). *On fixe un* $C > 0$ *avec* $C \neq \operatorname{Im}\lambda_{0,\alpha}$, $\alpha \in \mathbb{N}^{n-1}$. *Alors les pôles dans la bande* $0 < \operatorname{Im}\lambda < C$ *avec* $|\lambda|$ *grand peuvent être décrits de la manière suivante : pour chaque* $\lambda_{j,\alpha}$ *dans la bande il y a* $m(\alpha)$ *pôles* $z^1_{j,\alpha}$, $z^2_{j,\alpha}, \ldots, z^{m(\alpha)}_{j,\alpha}$ *comptés avec leur multiplicité, avec les développements asymptotiques :*

$$z^p_{j,\alpha} \sim \lambda_{j,\alpha} + \sum_{\nu=1}^{\infty} a^{p,\nu}_{j,\alpha}\left(\lambda^{1/N(p,\alpha)}_{j,\alpha}\right)^{-\nu} \ , \quad j \to \infty \ .$$

Ici $N(p,\alpha)$ *est un entier qui vaut* 1 *pour la première rangée.*

La démonstration d'Ikawa est basée sur une étude asymptotique des solutions du problème mixte quand $t \to \infty$. Celle de C. Gérard utilise le point de vue plus direct exprimé dans le Théorème 1.2 et qui est lié à d'autres théories, voir par exemple Aguilar-Combes [**AC**], Balslev-Combes [**BaC**], Vainberg [**V1,2**], Helffer-Martinez [**HeMa**].

Dans le cas de deux obstacles convexes, convenablement applatis près de x_1 et x_2, Ikawa [**I3**] a montré à l'aide de la formule de trace de Bardos-Guillot-Ralston-Melrose qu'il y a une suite de pôles λ_j avec $\operatorname{Im}\lambda_j \to 0$. Il a aussi abordé l'étude du cas où $\mathcal{O}$ est une réunion finie d'obstacles strictement convexes disjoints $\mathcal{O}_1, \ldots, \mathcal{O}_N$. Sous l'hypothèse : (l'enveloppe convexe de $\mathcal{O}_j \cup \mathcal{O}_k) \cap \mathcal{O}_\ell = \phi$ pour tous j,k,ℓ avec $\ell \neq j,k$, les rayons C^∞ forment un système dynamique hyperbolique et dans ce cas Ikawa a trouvé (en imposant parfois d'autres hypothèses) une bande parallèle à l'axe réel qui ne contient qu'un nombre fini de pôles et une bande plus large qui en contient une infinité. Voir [**I4,5**] et sans doute des travaux à venir.

Pour finir cette section, mentionnons le travail de T. Beale [**Be**] concernant les pôles engendrés par un obstacle connexe avec une cavité reliée à l'extérieur par un mince tunnel. Quand le tunnel se rétrécit (en fonction d'un paramètre) des pôles convergent vers les valeurs propres du problème de Dirichlet associé à la cavité limite (disconnectée de l'extérieur). Ces résultats ont récemment été améliorés par P. Hislop et A. Martinez [**HMa**].

4. Distribution des pôles pour des obstacles analytiques captants

Dans cette section on se propose de résumer les résultats de Bardos-Lebeau-Rauch [**BLeRa**]. On supposera désormais que $\partial\Omega$ soit analytique.

THÉORÈME 4.1 ([**BLeRa**]). *Si $\mathcal{O} = \mathbf{R}^n \setminus \Omega$ est non captant, alors il existe une constante $C > 0$ telle qu'il n'y a qu'un nombre fini de pôles dans* $\left\{\lambda \in \mathbb{C}\,;\, \operatorname{Im}\lambda \leq \frac{1}{C}\,|\lambda|^{1/3}\right\}$.

Ce résultat est une conséquence assez directe du Théorème 2.5, et il a aussi été démontré par Popov [**Po**]. Avec des hypothèses en plus, on peut montrer que pour $C > 0$ assez grand il y a une infinité de pôles avec $\operatorname{Im}\lambda \leq C\,|\lambda|^{1/3}$: Supposons que $\mathcal{O}$ soit strictement convexe et qu'il existe dans $\partial\mathcal{O}$ une géodésique fermée γ, de longueur $T > 0$ vérifiant :

(4.1) Il existe un voisinage V de T tel que si $\widetilde{\gamma}$ est une géodésique fermée de longueur $\widetilde{T} \in V$, alors $\widetilde{\gamma} = \gamma$.

(4.2) γ est non-dégénérée au sens que l'application de Poincaré linéarisée associée à γ (agisant dans un espace de dimension $2(n-2)$) n'a pas de valeur propre égale à 1 .

Remarquons que les géodésiques de $\partial\mathcal{O}$ correspondent aux rayons analytiques qui glissent le long du bord. Il est montré dans [**BLeRa**] que les hypothèses (4.1), (4.2) sont génériquement satisfaites.

Comme souvent dans les problèmes de diffraction, la fonction d'Airy $Ai(x)$, définie comme la transformation de Fourier inverse de $e^{i\xi^3/3}$, joue un rôle important. Les zéros de $Ai(x)$ se trouvent dans $]-\infty, 0[$, et on note $-\omega$ celui qui se trouve le plus près de 0. Soit $\rho(s) > 0$ la courbure de γ au point $\gamma(s)$ et posons :

$$C_\gamma = \omega \cos\left(\frac{\Pi}{6}\right)\left(2^{1/3}T\right)^{-1}\int_0^T \rho(s)^{2/3}\,ds\ .$$

Alors on a :

THÉORÈME 4.2 ([**BLeRa**]). *Sous les hypothèses* (4.1), (4.2), *pour tout* $\varepsilon > 0$, *il y a une infinité de pôles dans* $\left\{\lambda \in \mathbb{C}\,;\ \operatorname{Im}\lambda \leq (C_\gamma + \varepsilon)\,|\lambda|^{1/3}\right\}$.

L'ingrédient principal dans la démonstration de ce résultat est l'étude de la distribution $\operatorname{tr} Z(t) = \sum e^{i\lambda_j t}$, $t > 0$. Nous avons le :

THÉORÈME 4.3 ([**BLeRa**]). *On suppose* $\mathcal{O}$ *strictement convexe. Alors*

(i) $\operatorname{tr} Z(t)$ *appartient à* $G^3(]0,+\infty[)$

(ii) *Si* L *est l'ensemble des longueurs des géodésiques fermées dans* $\partial\Omega$, *alors* $\operatorname{tr} Z(t)$ *est analytique dans* $]0,+\infty[\setminus L$.

(iii) *Sous les hypothèses du Théorème* 4.2, *on a pour tout* $\varepsilon > 0$:

$$\limsup_{\ell\to\infty} \left| \sup_{|t-T|<\varepsilon} \partial_t^\ell \operatorname{tr} Z(t) \Big/ ((3\ell)!) \right|^{1/3\ell} \geq (C_\gamma T)^{-1} .$$

Ici (i), (ii) sont des conséquences assez directes des Théorèmes 2.4, 2.5. C'est le point (iii) qui est le plus important pour la démonstration du Théorème 4.2.

Décrivons maintenant assez brièvement les démonstrations. Le Théorème 4.1 est une conséquence assez directe du Théorème 2.5 : On commence par remarquer que si $R > \rho$ (où $\mathcal{O} \subset B(0,\rho)$) et $u \in \mathcal{H}(\Omega)$ est à support dans $B(0,R)$, alors si $t_1 > 0$ est assez grand pour que tout rayon C^∞ partant d'au dessus d'un point de $\bar{\Omega} \cap \overline{B(0,R)}$ avec vitesse 1 dans l'espace des x, ait quitté $\bar{\Omega} \cap \overline{B(0,R)}$ au temps $t \geq t_1$, alors $u(t,x)$ est de classe Gevrey 3 sur $[t_1,+\infty[\times (\bar{\Omega} \cap \overline{B(0,R)})$. Par un argument d'analyse fonctionnelle, on arrive à l'inégalité

$$|\partial_t^\ell u| + |\partial_t^\ell \nabla u| \leq A C^\ell (3\ell)! \, \|u(0)\|_{\mathcal{H}(\Omega)} , \tag{4.3}$$

pour $t \in [t_1,t_2]$, $(t_2 > t_1)$, $x \in \Omega \cap \overline{B(0,R)}$, $\ell = 0,1,2\ldots$, où les constantes A, C sont indépendantes de u.

On utilise ensuite une formule de [**LP1**], valable pour $t \geq 4\rho$:

$$Z(t) = P_+ \Big(U(2\rho) - U_0(2\rho) \Big) Q_{5\rho} U(t-4\rho) Q_{3\rho} \left(U(2\rho) - U_0(2\rho) \right) P_- , \tag{4.4}$$

où $Q_r f(x) = \chi\left(\dfrac{|x|}{r}\right) f(x)$, $\chi \in C^\infty(\mathbf{R})$, $\chi = 1$ sur $]-\infty,1]$, $\chi = 0$ sur $[2,+\infty[$. On en déduit :

$$B^\ell Z(t) = P_+ \left(U(2\rho) - U_0(2\rho) \right) Q_{5\rho} \partial_t^\ell U(t-4\rho) Q_{3\rho} \left(U(2\rho) - U_0(2\rho) \right) P_- .$$

Appliquant (4.3) avec $R = 10\rho$ et avec $t = t_0$ assez grand, on obtient avec des nouvelles constantes A, C :

$$\left\| B^\ell Z(t_0) \right\| \leq A C^\ell (3\ell)! \ .$$

Si $\mu \in \sigma(B)$, alors

$$\mu^\ell e^{\mu t_0} \in \sigma\left(B^\ell Z(t_0)\right) \ ,$$

et donc

$$|\mu|^\ell \, e^{t_0 \operatorname{Re} \mu} \leq A C^\ell (3\ell)! \ . \tag{4.5}$$

Choisissant ℓ convenablement, en fonction de μ (pour $|\mu|$ grand), on obtient $\operatorname{Re} \mu \leq -\dfrac{1}{\text{Const.}} |\mu|^{1/3}$, ce qui donne le Théorème 4.1. La démonstration de Popov est différente mais son ingrédient essentiel est toujours le Théorème 2.5 de Lebeau.

Voyons ensuite comment déduire le Théorème 4.2 du Théorème 4.3. Soit $C > 0$ et supposons que $\sigma(B) \cap \left\{ \mu \in \operatorname{Re} \mu \geq -C |\mu|^{1/3} \right\}$ soit fini. En utilisant (1.12), on trouve

$$\operatorname{tr} Z(t) = \sum_{\operatorname{Re} \mu_j < -C|\mu_j|^{1/3}} e^{-t\mu_j} + f(t) \ , \quad t > 0 \ , \tag{4.6}$$

où f est une fonction entière. Utilisant ensuite (1.11), on trouve

$$\partial_t^\ell (\operatorname{tr} Z(t) - f(t)) \leq \text{Const.} \, e^{ct} (Ct)^{-3\ell - 2n - 3} (3\ell + 3n + 2)! \tag{4.7}$$

et en comparant avec (iii) du Théorème 4.3 pour t dans un voisinage de T, on obtient bien $C \leq C_\gamma$.

Il reste à discuter la démonstration du Théorème 4.3, qui est considérablement plus difficile. Si $E(t) = \int E(t, x, y) v(y) dy$ désigne la solution du problème mixte : $\Box u = 0$ dans $\mathbf{R} \times \Omega$, $u \,|_{\mathbf{R} \times \partial\Omega} = 0$, $u(0) = 0$, $\partial_t u(0) = v$, alors on voit que $U(t) = \begin{pmatrix} \partial_t E & E \\ E\Delta & \partial_t E \end{pmatrix}$ et donc d'après (1.12) :

$$\operatorname{tr} Z(t) = 2 \operatorname{tr} \partial_t E = 2 \partial_t \int_\Omega E(t, x, x) dx$$

(au sens des distributions).

On peut ensuite réduire cette relation au bord :

$$\text{tr}\, Z(t) = -2\partial_t \int_{\partial\Omega} B(t,x,x)\,dx \ , \tag{4.8}$$

avec

$$B(t,x,y) = \int_{\mathbf{R}} \int_{\partial\Omega} h_0^+(t-s, z-x) k^+(s,z,y)\,dz\,ds \ , \tag{4.9}$$

où $k^+(t,x,y) = \partial_{n_x} K^+(t,x,y)$, $K^+(t,x,y) \in \mathcal{D}'(\mathbf{R}\times\partial\Omega\times\partial\Omega)$ étant le noyau de l'opérateur K^+ qui donne la solution $u = K^+ v$ de $\Box u = 0$ dans $\mathbf{R}\times\Omega$, $u\,|_{\mathbf{R}\times\partial\Omega} = v$, $u = 0$ pour $t << 0$, $v \in C_0^\infty(\mathbf{R}\times\partial\Omega)$. De plus h_0 est la solution élémentaire de $\Box^2$ dans $\mathbf{R}\times\mathbf{R}^n$ à support dans $t \geq 0$. Notons que $k^+(t,x,y)$ est le noyau de l'opérateur de Neumann qui intervient dans la preuve du Théorème 2.5.

Il s'agit alors d'analyser les noyaux $h_0^+(t,x,y)$ et $k^+(t,x,y)$ sur $\mathbf{R}\times\partial\Omega\times\partial\Omega$. Le premier noyau à une représentation intégrale explicite qu'on arrive avec un peu de travail à réécrire comme une intégrale oscillante sur le bord. La difficulté principale se cache dans l'étude de k^+. On peut d'abord localiser les fronts d'ondes Gevrey 3 (et analytiques) en utilisant le Théorème 2.5 (et 2.4). Pour mieux connaître ensuite k_+ près du front d'onde analytique on utilise des solutions oscillantes entrantes construites par Lebeau dans [**Le1**]. On peut ensuite faire des intégrations par parties et obtenir le comportement asymptotique de certaines intégrales FBI de k_+. Ainsi on arrive finalement à montrer que dans la région $t > 0$, $|x-y| < t$: $WF_a(B) \subset \Lambda$, $B \in I^3_{\Lambda,\psi}$ où

$$\Lambda = \Lambda_+ \cup \Lambda_-, \ \Lambda_\pm = \Big\{(t,\tau\,;x,\xi\,;y,-\eta)\,;\pm\tau = |\xi|\,,(x,\xi) = \exp t H_p(y,\eta)\Big\},$$

$p = |\xi|$ (considérée comme symbole sur $T^*\partial\Omega \setminus 0$). On définit ψ comme l'intégrale de $e^{\pm i\pi/6}(|\tau|\,\rho^2/2)^{1/3}\omega$ le long du flot de H_p avec la condition initiale : $\psi = 0$ sur la diagonale.

Il faut aussi expliquer ce qu'est la classe $I^3_{\Lambda,\psi}$. De manière générale, soit Λ une variété Lagrangienne analytique, réelle, conique et soit ψ une fonction sur Λ qui est positivement homogène de degré $\frac{1}{3}$ avec $\text{Re}\,\psi \geq 0$. On dit alors que la distribution f appartient à $I_{\Lambda,\psi}$ au point (y_0,η_0) si avec T_χ comme au début de la Section 2 on ait dans un voisinage de x_0 :

$$T_\chi f(x,\lambda) = e^{i\lambda g(x) - \lambda^{1/3}\widehat{\psi}(x)} b(x,\lambda) + r(x,\lambda) \ ,$$

où : g est donné par : $\mathcal{H}_T(\Omega) = \left\{\left(x, \frac{\partial g}{\partial x}(x)\right)\right\}$, $g(x_0) = \varphi(x_0, y_0)$, $\widehat{\psi}(x) = (\psi \circ \mathcal{H}_T^{-1})\left(x, \frac{\partial g}{\partial x}(x)\right)$ + constante imaginaire convenable, b a un développement asymptotique de la forme :

$$\left| b(x,\lambda) - \sum_{k=0}^{N} b_k(x)\,\lambda^{m-\frac{n}{2}-\frac{k}{3}} \right| \leq A B^k (k!)\,\lambda^{m-\frac{n}{2}-\frac{N+1}{3}},$$

b_k holomorphe, et r vérifie $|r(x,\lambda)| \leq e^{\lambda\Phi(x)-C_0\lambda^{1/3}}$ avec $C_0 > \operatorname{Re}\widehat{\psi}(x_0)$.

Utilisant enfin les hypothèses (4.1), (4.2), on arrive à analyser l'intégrale dans (4.8) et montrer (iii) du Théorème 4.3.

Bibliographie

[**AC**] J. AGUILAR, J.M. COMBES, *A class of analytic perturbations for one-body Schrödinger Hamiltonians,* Comm. Math. Phys. 22 **(1971)**, 269-279.

[**BaC**] E. BALSLEV, J.M. COMBES, *Spectral properties of many-body Schrödinger operators with dilation analytic interactions,* Comm. Math. Phys. 22 **(1971)**, 280-294.

[**BGR**] C. BARDOS, J.C. GUILLOT, J. RALSTON, *La relation de Poisson pour l'équation des ondes dans un ouvert non borné. Application à la théorie de la diffusion,* Comm. P.D.E., 7 **(1982)**, 905-958.

[**Be**] J.T. BEALE, *Scattering frequencies of resonators,* C.P.A.M. 26 **(1973)**, 549-563.

[**Bo**] J-M. BONY, *Equivalence des diverses notions de spectre singulier analytique,* Sém. Goulaouic-Schwartz, **(1976-77)**, Exposé $n°$ 3.

[**BLeRa**] C. BARDOS, G. LEBEAU, J. RAUCH, *Scattering frequences and Gevrey 3 singularities,* Inv. Math. 90(1) **(1987)**, 77-114.

[**FM**] F.G. FRIEDLANDER, R.B. MELROSE, *The wave front set of the solution of a simple initial boundary value problem with glancing rays II,* Math. Proc. Camb. Phil. Soc. 81 **(1977)**, 97-120.

[**Ge**] C. GÉRARD, *Asymptotique des pôles de la matrice de scattering pour deux obstacles strictement convexes,* Bull. de la S.M.F., 116(1) **(1988)**, Mémoire $n°$ 31.

[**HeMa**] B. HELFFER, A. MARTINEZ, *Comparaison entre les diverses notions de résonances,* Helv. Phys. Acta 60 **(1987)**, 992-1003.

[**HMa**] P. HISLOP, A. MARTINEZ, *Scattering resonances of a Helmholz resonator,* Prépublication d'orsay 89-40, **(1989)**.

[**Hö**] L. HÖRMANDER, *The analysis of linear partial differential operators 1-4,* Grundlehren, Vol. 256, 257, 274, 275, **(1983-85)**.

[**I1**] M. IKAWA, *On the poles of the scattering matrix for two strictly convex obstacles,* J. Math. Kyoto Univ., 23(1) **(1983)**, 127-194, et 23(4) **(1983)**, 795-802, *On the distribution of the poles of the scattering matrix for two strictly convex obstacles,* Hokkaido Math. J., 12 **(1983)**, 343-359.

[**I2**] M. IKAWA, *On the poles of the scattering matrix for two convex obstacles,* Journées E.D.P., St Jean de Monts **(1985)**, Exposé $n°$ 5, Distribué par OFFILIB.

[**I3**] M. IKAWA, *Trapping obstacles with a sequence of poles of the scattering matrix converging to the real axis,* Osaka J. Math. 22(4) **(1985)**, 657-689.

[**I4**] M. IKAWA, *Decay of solutions of the wave equations in the exterior of several convex bodies,* Ann. Inst. Fourier 38(2) **(1988)**, 113-146.

[**I5**] M. IKAWA, *On the existence of the poles of the scattering matrix for several convex bodies,* Proc. Japan Acad., 44 A(4) **(1988)**, 91-93.

[**Iv**] V. IVRĬI, *Wave fronts for solutions of boundary value problems for a class of symmetric hyperbolic systems,* Sibirsk Mat. Z. 21(4) **(1980)**, 62-71 et

Sib. J. Math. 21 **(1980)**, 527-534.

[**In**] A. INTISSAR, *A polynomial bound on the number of the scattering poles for a potential in even dimensions,* Comm. P.D.E. 11 **(1986)**, 367-396.

[**K**] K. KATAOKA, *Microlocal theory of boundary value problems I, II,* J. Fac. Sci. Univ. Tokyo 27 **(1980)**, 355-399, 28 **(1981)**, 31-56.

[**Las**] B. LASCAR, R. LASCAR, *Propagation des singularités Gevrey pour la diffraction,* Prépublication **(1989)**.

[**LasS**] B. LASCAR, J. SJÖSTRAND, *Equation de Schrödinger et propagation des singularités ...,* Astérisque $n°$ 95, **(1982)**, 167-207.

[**La1**] P. LAUBIN, *Etude 2-microlocale de la diffraction, Dissertation,* Université de Liège, Fac. des Sciences **(1987)**, p. 165-202 dans Advances in microlocal analysis, Ed. H.G. Garnir, Nato ASI Series C, Vol. 168, Reidel **(1986)**.

[**La2**] P. LAUBIN, *Asymptotic solutions of hyperbolic boundary value problems with diffraction,* p. 165-202 dans Advances in microlocal analysis, Ed. H.G. Garnir, Nato ASI Series C, Vol. 168, Reidel **(1986)**.

[**LP1**] P. LAX, R. PHILLIPS, *Scattering theory,* Pure and Appl. Math., Academic Press **(1967)**.

[**LP2**] P. LAX, R. PHILLIPS, *A logarithmic bound on the location of the poles of the scattering matrix*, Arch. Rat. Mech. and Anal., 40 **(1971)**, 268-280.

[**Le1**] G. LEBEAU, *Régularité Gevrey 3 pour la diffraction,* Comm. P.D.E., 9(15) **(1984)**, 1437-1494.

[**Le2**] G. LEBEAU, *Propagation des singularités pour le problème de Dirichlet,* p. 203-224 dans Advances in microlocal analysis, Ed. H.G. Garnir, Nato ASI Series C, Vol. 168, Reidel **(1986)**.

[**Le3**] G. LEBEAU, *Deuxième microlocalisation sur des sous-variétés isotropes,* Ann. Inst. Fourier, 35(2) **(1985)**, 145-216.

[M1] R. MELROSE, *Polynomial bound on the number of scattering poles,* J. Funct. Anal. 53 **(1983)**, 287-303, amélioration dans : Journées E.D.P., St Jean de Monts **(1984)**, exposé $n°$ 3, (Ecole Polytechnique).

[MS] R. MELROSE, J. SJÖSTRAND, *Singularities of boundary value problems, I,II,* C.P.A.M. 31 **(1978)**, 595-617, C.P.A.M. 35 **(1982)**, 129-168.

[MoRSt] C. MORAWETZ, J. RALSTON, W. STRAUSS, *Decay of solutions of the wave equation outside nontrapping obstacles,* C.P.A.M., 30 **(1977)**, 447-508.

[Po] G. POPOV, *Some estimates of Green's functions in the shadow,* Osaka J. Math. 24(1) **(1987)**, 1-12.

[RaS] J. RAUCH, J. SJÖSTRAND, *Propagation of analytic singularities along diffracted rays,* Indiana Univ. Math. J. 30(3) **(1981)**, 389-401.

[S1] J. SJÖSTRAND, *Singularités analytiques microlocales,* Astérisque 95, **(1982)**.

[S2] J. SJÖSTRAND, *Propagation of analytic singularities for second order Dirichlet problems,* Comm. P.D.E. 5(1), **(1980)**, 41-94.

[S3] J. SJÖSTRAND, *Propagation of analytic singularities for second order Dirichlet problems, II, III,* Comm. P.D.E., 5(2), **(1980)**, 187-207, 6(5), **(1981)**, 499-567.

[S4] J. SJÖSTRAND, *Analytic singularities of solutions of boundary value problems,* p. 235-269 dans Singularities in boundary value problems, Ed. H.G. Garnir, Nato ASI Series C, Vol. 65, Reidel **(1981)**.

[V1] B.R. VAINBERG, *On the analytic properties of the resolvent for a certain class of operator-pencils,* Mat. Sb 77(119), **(1968)**, $n°$ 2, Math. USSR. Sb. 6 **(1968)**, $n°$ 2.

[V2] B.R. VAINBERG, *On exterior elliptic problems ...,* Mat. Sb. 92(134), **(1973)**, $n°$ 2, Math. USSR. Sb. 21 **(1973)**, $n°$ 2.

[Z] M. ZWORSKI, *Sharp polynomial bounds on the number of scattering poles,* Duke Math. J. 59(2), **(1981)**, 311-325.

Johannes Sjöstrand

Université de Paris-Sud

Département de Mathématiques

91405 Orsay Cedex, France

Astérisque

DANIEL BENNEQUIN

Topologie symplectique, convexité holomorphe et structures de contact

Astérisque, tome 189-190 (1990), Séminaire Bourbaki,
exp. n° 725, p. 285-323

<http://www.numdam.org/item?id=SB_1989-1990__32__285_0>

© Société mathématique de France, 1990, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Séminaire BOURBAKI juin 1990
42ème année, 1989-90, n° 725

TOPOLOGIE SYMPLECTIQUE, CONVEXITÉ HOLOMORPHE ET STRUCTURES DE CONTACT
[d'après Y. Eliashberg, D. Mc Duff et al.]

par **Daniel BENNEQUIN**

1. VARIÉTÉS DE STEIN ET STRUCTURES DE CONTACT

1.1. Un champ différentiable F d'hyperplans tangents sur une variété lisse M est une *structure de contact* s'il est défini près de chaque point x de M par une équation de Pfaff $\alpha = 0$, telle que la dérivée extérieure $d\alpha$ de la 1-forme α soit une forme inversible sur l'hyperplan F_x (*cf.* [A, 1 & 2], [E.1], [A.D.], [L,M.]) ; le couple (M, F) est une *variété de contact.* Les composantes connexes d'une variété de contact sont toutes de dimension impaire ; chaque structure de contact est naturellement munie d'une structure de fibré conformément symplectique.

Dans l'exposé qui suit, toutes les structures de contact considérées vont être de classe C^∞ et transversalement orientables : elles seront donc définies par des *formes de contact* de classe C^∞ α sur la variété toute entière. Soit α une forme de contact définissant F sur M^{2n-1} ; la forme volume $\alpha \wedge (d\alpha)^{n-1}$ oriente M. Lorsque M est ainsi orientée et que F est orientée (transversalement) par α, on dit que F est *directe.* Quand n est pair les deux orientations de F donnent la même orientation de M alors qu'elles donnent des orientations différentes de M quand n est impair.

L'espace des éléments de contact d'une variété, l'espace des jets d'ordre 1 de fonctions numériques sur une variété, les variétés pré-quantiques possèdent des structures de contact canoniques. L'analyse complexe est également une source de problèmes de Géométrie de Contact.

1.2. Soient W une variété analytique complexe et G une sous-variété à bord de codimension zéro de la variété réelle sous-jacente à W ; soient Ω l'intérieur de G et M le bord de G ; nous désignerons par J la structure presque complexe du fibré tangent $T(W)$ et par F le sous-fibré (de codimension un) $T(M) \cap J(T(M))$ de $T(M)$. La variété M sera orientée comme bord de Ω (une normale sortante suivie d'une base orientée de $T_x M$ forment un repère orienté de $T_x W$) et F sera orienté par J ; soit α une forme différentielle C^∞ sans singularité sur M, nulle sur F, donnant la bonne orientation transverse de F ; l'équation

$$L(v, w) = d\alpha(v, Jw) + i\, d\alpha(v, w)$$

définit une forme hermitienne sur (F, J) qui s'appelle une *forme de Levi* de M. Sa classe conforme est intrinsèquement définie.

Si $\rho = 0$ est une équation transverse de M avec $\rho < 0$ dans Ω, une forme α convenable sur M est

$$\alpha = \frac{1}{i}\, d'\rho = \frac{1}{2i}\,(d'\rho - d''\rho) = d^J\rho.$$

Le domaine Ω est *strictement pseudo-convexe* (en abrégé s.p.c.) si les formes de Levi sur M sont définies positives. On dit aussi que M et G sont s.p.c..

Pour un domaine de $\mathbf{C}^2$, en coordonnées $z_1 = x_1 + iy_1$ et $z_2 = x_2 + iy_2$, Ω est s.p.c. si l'expression suivante est strictement positive :

$$\begin{aligned} L(\rho) = {} & \Big(\frac{\partial^2\rho}{\partial x_1^2} + \frac{\partial^2\rho}{\partial y_1^2}\Big)\Big(\Big(\frac{\partial\rho}{\partial x_2}\Big)^2 + \Big(\frac{\partial\rho}{\partial y_2}\Big)^2\Big) \\ & + \Big(\frac{\partial^2\rho}{\partial x_2^2} + \frac{\partial^2\rho}{\partial y_2^2}\Big)\Big(\Big(\frac{\partial\rho}{\partial x_1}\Big)^2 + \Big(\frac{\partial\rho}{\partial y_1}\Big)^2\Big) \\ & - 2\Big(\frac{\partial^2\rho}{\partial x_1\partial x_2} + \frac{\partial^2\rho}{\partial y_1\partial y_2}\Big)\Big(\frac{\partial\rho}{\partial x_1}\,\frac{\partial\rho}{\partial x_2} + \frac{\partial\rho}{\partial y_1}\,\frac{\partial\rho}{\partial y_2}\Big) \\ & - 2\Big(\frac{\partial^2\rho}{\partial x_1\partial y_2} - \frac{\partial^2\rho}{\partial x_2\partial y_1}\Big)\Big(\frac{\partial\rho}{\partial x_1}\,\frac{\partial\rho}{\partial y_2} - \frac{\partial\rho}{\partial x_2}\,\frac{\partial\rho}{\partial y_1}\Big). \end{aligned}$$

Cette notion de convexité provient des recherches de Hartogs et Levi au début du siècle sur les domaines d'holomorphie dans $\mathbf{C}^2$. (Références d'ensemble [B.,F.,G.], [HÖ], [G.,R.]).

Une *structure de Cauchy-Riemann* (en abrégé C.R.) sur une variété M est une structure presque complexe J sur un champ différentiable F d'hyperplans tangents à M. Si (M, F, J) est une structure C.R., le fibré $F \otimes \mathbf{C}$ se décompose en $F' \oplus F''$, vecteurs de type (1,0) et vecteurs de type (0,1) ; on dit que J est *intégrable* si le crochet de deux sections de F' est encore une section de F'. Une hypersurface d'une variété analytique complexe est une variété C.R. intégrable. Les notions de forme de Levi et de pseudo-convexité appartiennent aux structures C.R. intégrables : en effet, si α définit F et si v et w sont deux sections de F, on a $v + iJv \in F'$, $w + iJw \in F'$ et

$$\begin{aligned} d\alpha(v, Jw) - d\alpha(w, Jv) &= \alpha([w, Jv]) - \alpha([v, Jw]) \\ &= -Im(\alpha[v + iJv, w + iJw]), \end{aligned}$$

donc la restriction de $d\alpha$ à F est compatible avec J dès que J est intégrable.

Pourtant, nous dirons qu'une structure C.R., même non intégrable, est s.p.c. si il existe une forme α définissant F telle que $d\alpha(v, Jv) > 0$ pour tout vecteur $v \neq 0$ dans un des hyperplans F.

Le champ d'hyperplans complexes d'une variété C.R. s.p.c. est une structure de contact. Le champ F du bord M d'un domaine strictement pseudo-convexe Ω dans une variété analytique W est une structure de contact directe si M est orientée comme bord de Ω dans W et si F est orienté par J.

1.3. D'après K. Oka [O. VI & IX], les domaines s.p.c. Ω de $\mathbf{C}^n$ (et ceux qui sont étalés sur $\mathbf{C}^n$) sont des domaines d'holomorphie (il existe des fonctions holomorphes sur Ω qui ne s'étendent pas au-delà de Ω). H. Cartan et P. Thullen ont caractérisé les domaines d'holomorphie par la convexité holomorphe :

Soit E un sous-ensemble de W, l'*enveloppe holomorphe de E par rapport à W*, notée $\hat{E}_W$ est l'ensemble des points de W où la valeur absolue de n'importe quelle fonction holomorphe sur W reste majorée par sa borne supérieure sur E ; et la variété W est dite *holomorphiquement convexe* si $\hat{E}_W$ est compact dès que E l'est.

Si W est holomorphiquement convexe et si l'on peut trouver assez de fonctions holomorphes globalement définies sur W pour séparer deux points

arbitraires et pour former des coordonnées locales holomorphes au voisinage de tout point, on dit que W est une *variété de Stein.*

H. Grauert ([H.G]) a démontré que tout Ω s.p.c. relativement compact dans une W analytique est holomorphiquement convexe, et aussi que W est de Stein si et seulement si elle est holomorphiquement convexe et ne contient aucun sous-ensemble analytique compact à part les points.

Nous appellerons *domaine de Grauert* ouvert (resp. fermé) un ouvert s.p.c. relativement compact d'une variété analytique (resp. sa fermeture).

Donc un domaine de Grauert ne contenant aucun sous-ensemble analytique compact de dimension > 0 est une variété de Stein. En fait, il résulte du travail de H. Grauert, H. Rossi, R. Narasimhan qu'un domaine de Grauert s'obtient toujours par éclatements d'un nombre fini de points (éventuellement singuliers) dans un espace de Stein (*cf.* [G.,R.] et [C.]).

D'après Remmert et Stein, toute variété de Stein de dimension n se plonge dans un $\mathbf{C}^N$; Bishop avait montré que $N = 2n + 1$ suffit, puis Gromov et Eliashberg ont déterminé la meilleure borne possible : $N = \left[\frac{3n}{2}\right] + 2$ ([M.G.,E.]).

1.4. Une fonction de W dans $\mathbf{R}$ est *(strictement) pluri-sous-harmonique* (en abrégé (s) p.s.h.) si sa restriction à tout germe de courbe holomorphe est (strictement) sous-harmonique (*cf.* [HÖ]). En d'autres termes, la 2-forme de type $(1,1)$ $\omega = dd^J\rho = 2id'd''\rho$ est une forme symplectique adaptée à J, strictement positive par rapport à J (la formule $\omega(v, Jw) + i\omega(v, w)$ définit une structure hermitienne définie positive). Avec ρ s.p.s.h., W est kählerienne.

Les niveaux réguliers d'une fonction s.p.s.h. sont s.p.c.. Et W est de Stein si et seulement si elle admet une fonction s.p.s.h. φ telle que tous les sous-ensembles $\varphi \leq C$ soient compacts (H. Grauert (*cf.* [HÖ])).

D'après Lefschetz, Serre, Andreotti, Frankel, Milnor, ..., sur une variété analytique de Stein W , de dimension n, il existe une fonction φ s.p.s.h. qui est une fonction de Morse propre avec tous ses points critiques d'indices $\leq n$. En particulier, W a le type d'homotopie d'un CW complexe de dimension $\leq n$.

De plus, si Ω est un domaine de Grauert dans W, il existe une φ

possédant toutes ces propriétés dont $M = \partial\Omega$ est un niveau régulier. (En particulier, M est connexe dès que Ω est connexe.)

Yakov Eliashberg s'est attaché récemment à la caractérisation topologique des variétés de Stein :

THÉORÈME 1 (Eliashberg) ([E.2,3]).— *Soit W une variété C^∞ réelle de dimension $2n$ munie d'une structure* presque complexe *J' et soit φ une fonction de Morse propre minorée sur W dont tous les points critiques sont d'indice $\leq n$. Si $n > 2$, J' est homotope à une structure complexe intégrable J sur W qui rend la fonction φ strictement pluri-sous-harmonique ; la variété analytique complexe (W, J) est une variété de Stein.*

Soit Ω un ouvert relativement compact dans W dont la frontière M est un niveau régulier de φ ; vis-à-vis de J, Ω est un domaine strictement pseudo-convexe et une variété de Stein.

Eliashberg utilise ce résultat (et quelques autres) pour répondre à une question de M. Wodzicki :

COROLLAIRE.— *Toute variété de Stein X de dimension > 2 possède une filtration $X = X_n \supset X_{n-1} \supset \cdots \supset X_0$ par des sous-variétés de Stein de dimension n telle que chaque X_k, $k = 0, \cdots, n$ a le type d'homotopie d'un CW-complexe de dimension k et que $\pi_i(X_{k+1}, X_k) = 0$ pour $k = 0, \cdots, n-1$, et $i \leq k$.*

Il faut aussi signaler le travail connexe de A. Weinstein ([W]).

1.5. La dimension (complexe) 2 montre effectivement moins de souplesse mais elle cache aussi beaucoup plus de richesses ; c'est à elle que la plus grande partie de l'exposé est consacrée. Par exemple, je vais tenter de donner une idée de la démonstration du résultat suivant dans les paragraphes 4, 5, 6 :

THÉORÈME 2 (Eliashberg, Bedford & Klingenberg) (*cf.* [E.4], [B.,K.]).— *Soient Ω un domaine de Grauert de dimension 2 et M son bord ;*

toute sphère Σ, de dimension 2 plongée dans M est le bord d'une boule B de dimension 3 plongée dans Ω.

En fait B est C^2-proche d'une boule B' (avec $\partial B' = \Sigma' \subset M$, C^2

proche de Σ) dont l'intérieur est feuilleté par des disques holomorphes plongés dans Ω.

Si Ω est de Stein, $B' \cup \Sigma'$ est l'enveloppe holomorphe de Σ' par rapport à $\Omega \cup M$.

COROLLAIRE.— *La variété $D^2 \times S^2$ n'admet aucune structure analytique complexe qui la rende strictement pseudo-convexe.*

Remarque.— Bedford et Klingenberg ont écrit la démonstration dans le cadre de Stein, Eliashberg a donné tous les éléments d'une démonstration dans un cadre plus général : celui des domaines *presque complexes positifs* (par rapport à une structure symplectique sur $G = \Omega \cup M$) de [M.G.] (*cf.* [D.B.2] p. 115, et voir §3.4, §§4, 5, 6). L'énoncé que je viens de donner est à cheval entre les deux cadres à cause du lemme suivant :

Lemme.— *En dimension 2, un domaine de Grauert fermé G est positif (c'est-à-dire qu'il existe ω symplectique sur G strictement positive par rapport à la structure complexe : $\omega(v, Jv) > 0$ si $v \neq 0$).*

En effet, il existe un sous-ensemble analytique compact X de dimension complexe ≤ 1 dans G, un morphisme propre π de G sur un espace de Stein K qui est un isomorphisme hors de X et qui envoie X sur des points, et une fonction φ s.p.s.h., sur K (voir par exemple [C.]). Soit ρ une fonction C^∞ sur G, s.p.s.h. dans un voisinage U des singularités de X ; soit ω_X une 2-forme fermée sur G qui donne une aire sur $X \backslash (X \cap U)$ (elle existe car aucune des composantes connexes de X n'est homologue à zéro dans G, exercice) ; pour des constantes a et b convenables, la forme fermée

$$\omega = dd^J(\pi^*(\varphi)) + add^J\rho + b\omega_X$$

est strictement positive sur J.

(L'auteur pense qu'en fait G peut être muni d'une structure kählerienne.)

La preuve du théorème 2 est une analyse des disques holomorphes appuyés sur Σ (problème de Riemann-Hilbert non linéaire), commencée par Bishop, Kenig, Webster, Hunt, Moser, Bedford, Gaveau, Gromov... (*cf.* §§4, 5, 6). Une analyse des familles à un paramètre de sphères dans M et de leurs enveloppes permet encore d'établir le résultat suivant :

THÉORÈME 3 (Eliashberg) ([E.4]).— *Toute variété de Stein Ω de bord $M = S^3$ (la sphère de dimension 3 réelle) est difféomorphe à la boule B^4. De plus, il existe sur Ω une fonction s.p.s.h. constante sur M ne présentant qu'un seul point critique, et le champ de plans F sur M est isomorphe à la structure de contact standard directe de S^3 (celle de la sphère ronde dans $\mathbf{C}^2$).*

Si l'on ajoute à ces théorèmes ceux de D. Mc Duff sur les variétés symplectiques de dimension 4 ([M.D.1,2,3] *cf.* §2), il vient :

COROLLAIRE (Y. Eliashberg, D. Mc Duff).— *Tout domaine de Grauert dont le bord est difféomorphe à S^3 est difféomorphe à la somme connexe (intérieure) de la boule B^4 avec un nombre fini de plans projectifs (retournés) $\overline{\mathbf{P}^2(\mathbf{C})}$ (c'est-à-dire la boule de $\mathbf{C}^2$ éclatée en certains points), et la structure de contact au bord est standard.*

On ignore encore comment cela s'étend à d'autres bords que S^3 mais les résultats sur le remplissage symplectique (*cf.* §2) font penser que la marge de manœuvre de Ω ainsi que celle de F seront très limitées par la topologie de M^3.

Les variétés de dimension 3 fermées orientées possèdent une excellente théorie de la divisibilité par somme connexe : J. Milnor ([M.1]) a démontré que toute M^3 (fermée orientée) se décompose de manière unique (aux unités S^3 et $-S^3$ près) en facteurs premiers (indécomposables)

$$M^3 = M_1^3 \# M_2^3 \cdots \# M_N^3.$$

THÉORÈME 4 (Eliashberg) ([E.4]).— *Soit M^3 le bord d'un Ω relativement compact de Stein ; M est décomposable si et seulement si il existe Ω_1 et Ω_2 relativement compacts de Stein non difféomorphes à B^4 dont Ω est la somme connexe au bord.*

De plus, si Ω est somme connexe au bord de Ω_1 et Ω_2 de façon topologique, il est automatiquement somme connexe de deux variétés de Stein Ω_1', Ω_2' (difféomorphes à Ω_1, Ω_2) le long d'une boule B^3 Levi plate standard, c'est-à-dire une boule feuilletée par des disques holomorphes dont les bords

forment un système de parallèles sur la sphère S^2 au bord de B^3 (somme connexe rigide).

Ce théorème peut être rapproché du Théorème de Donaldson [D.1] d'indécomposabilité des surfaces projectives.

2. REMPLISSAGES SYMPLECTIQUES

2.1. Soit ω une structure symplectique sur une variété réelle lisse W de dimension $2n$; une hypersurface orientée M de W est du *type de contact* (Weinstein, *cf.* [W.]) s'il existe une forme de contact α sur M, telle que $\alpha \wedge (d\alpha)^{n-1}$ définisse l'orientation de M (*i.e.* α directe) et telle que $d\alpha$ coïncide avec ω en restriction à $T(M)$ (la forme α est dite *adaptée* à M et à ω). La forme ω est donc exacte au voisinage d'une hypersurface du type de contact.

Soient M du type de contact dans (W,ω) et α adaptée ; soient ξ le champ de Reeb de α ($i(\xi)\alpha = 1$, $i(\xi)d\alpha = 0$) et ν la normale orientée à M dans W (M est le bord du côté où pointe $-\nu$), nous dirons que M est *convexe vis-à-vis* de ω (ou symplectiquement convexe) si $\omega(\nu,\xi) > 0$ (W sera toujours orientée par ω^n).

Notons que la classe d'isomorphisme de la structure de contact (directe) F associée à une forme adaptée est bien définie par M, lorsque M est compacte sans bord (car $t\alpha + (1-t)\alpha'$, $0 \leq t \leq 1$, est adaptée si α et α' le sont). Supposons que M soit le bord orienté d'un domaine relativement compact Ω de W ; si M est du type de contact et convexe du côté de Ω, nous dirons que la structure de contact F sur M adaptée à M et à ω est un *bord* de la variété symplectique (Ω,ω), ou bien que (Ω,ω) est un *remplissage symplectique* de (M,F).

Toute variété symplectique (W,ω) possède une structure *presque complexe* J (bien définie à homotopie près) qui est *positive* ($\omega(v,Jv) > 0$ si $v \neq 0$) ; elle en possède même qui sont adaptées ($\omega(v,Jv)$ définit un produit scalaire). Pour une telle structure J, le bord (M,F) de (Ω,ω) est C.R. et strictement pseudo-convexe.

Inversement, si M est le bord d'un domaine de Grauert Ω d'une variété de Stein, sa structure C.R. est le bord symplectique de Ω pour $\omega = dd^J\rho$ avec ρ s.p.s.h. sur W constante et régulière sur M.

Remarque.— Une notion un peu différente est introduite par Eliashberg [E.5] : dans une variété symplectique (W,ω), supposons que l'hypersurface M soit le bord d'un domaine Ω et orientons M comme bord de Ω, la structure symplectique ω sur Ω *domine* une structure de contact *directe* F sur M si elle induit la structure conforme symplectique canonique sur F (avec la bonne orientation). (Si ξ est une normale directe à F dans M et ν une normale sortante à M, $\omega(\nu,\xi) > 0$ résulte des choix d'orientations.) Lorsque $n > 2$, si ω domine F, il existe une forme adaptée α qui définit F. En effet, soit α une forme de contact nulle sur F et satisfaisant $\omega_{|F} = d\alpha_{|F}$, il existe alors une 1-forme β sur M telle que $d\alpha = \omega + \alpha \wedge \beta$. Soit ξ le champ de Reeb de α ; quitte à changer β en $\beta - \beta(\xi)\alpha$, on peut supposer $\beta(\xi) = 0$. De l'égalité $d\alpha \wedge \beta = \alpha \wedge d\beta$ résulte alors $d\beta = \alpha \wedge i(\xi)d\beta$, donc $d\alpha \wedge \beta = 0$ et $\omega \wedge \beta = 0$, d'où $\beta = 0$ si dim $F \geq 4$. Lorsque $n = 2$, il se peut que ω domine F sans que F soit isomorphe à une structure adaptée à M et à ω

Notons que toute structure de contact directe est dominée par sa *symplectisation* (*cf.* [A.1]). (La symplectisation de F sur M est le cône symplectique Σ_F de $T^*M\backslash M$ constitué par les formes linéaires sur les espaces tangents aux points de M qui définissent les hyperplans F avec leur orientation transverse.)

2.2. Une variété symplectique (W,ω) est *asphérique symplectiquement* s'il n'existe pas de classe sphérique dans $H_2(W;\mathbf{Z})$ strictement positive sur ω ; elle est dite *standard à l'infini* (ou *asymptotiquement plate*) si le complémentaire d'un compact dans W est isomorphe symplectiquement au complémentaire d'un compact dans un espace vectoriel symplectique. Gromov [M.G.] avait démontré que $\mathbf{R}^4$ muni de sa structure standard est la seule variété symplectiquement asphérique et asymptotiquement plate de dimension 4 ; il s'ensuit que tout remplissage symplectique asphérique de la sphère de contact standard S^3 est symplectomorphe à une boule plongée

dans le $\mathbf{R}^4$ standard.

Disons que (W,ω) est *minimale* si elle ne contient pas de sphère de dimension 2 plongée symplectique et *exceptionnelle* (*i.e.* d'auto-intersection -1 en homologie).

THÉORÈME 5 (D. Mc Duff) (*cf.* [M.D.3]).— *Les espaces lenticulaires L_p, $p \geq 1$ (en particulier $S^3 = L_1$, $SO_3 = L_2$, $\mathbf{P}^3_2(\mathbf{R}) = L_4$ (c'est le fibré en cercles tangents à $\mathbf{P}^2(\mathbf{R})$)), munis de leurs structures de contact standard directes (quotients de celle de S^3) possèdent des remplissages minimaux. Si $p \neq 4$, le remplissage minimal est unique à difféomorphisme près et L_4 a exactement deux remplissages minimaux à difféomorphisme près.*

En fait, D. Mc Duff démontre que tous ces remplissages s'obtiennent en prenant le complémentaire d'une sphère holomorphe C (d'auto-intersection p) dans une surface complexe projective : pour L_p ($p > 1$) une bonne surface est $\mathbf{P}(\mathcal{O}(p) \oplus \mathbf{1})$ (topologiquement, c'est $S^2 \times S^2$ ou $\mathbf{CP}^2 \# \overline{\mathbf{CP}}^2$). Lorsque $p = 1$ ou 4, $\mathcal{O}(p)$ se plonge aussi dans $\mathbf{P}^2(\mathbf{C})$ et C est une droite ou une conique.

Le théorème vient d'un résultat sur les variétés symplectiques fermées :

THÉORÈME 6 ([M.D.3]).— *Soit C une sphère de dimension 2 symplectique plongée dans une variété symplectique minimale (W,ω) compacte sans bord ; si l'auto-intersection homologique $p = C.C$ est ≥ 0, alors (W,ω) est isomorphe à $\mathbf{P}^2(\mathbf{C})$ (avec un multiple de la structure standard) ou bien à un fibré symplectique en sphère S^2 sur une surface de Riemann compacte X, et C vient, soit d'une droite ou d'une conique dans le cas de $\mathbf{P}^2(\mathbf{C})$, soit d'une fibre ou de l'image d'une section dans le cas du fibré symplectique. Le type de (W,C) est déterminé à isotopie près sauf si $p = 0$ ou 4.*

Ce théorème permet aussi d'obtenir une sorte d'unicité symplectique des remplissages minimaux Ω_p des lenticulaires L_p : la forme ω sur Ω_p est déterminée dès qu'on se donne sa classe de cohomologie dans $H^2(\Omega_p, \mathbf{R})$ et une forme adaptée $d\alpha$ sur L_p.

Tous les autres remplissages symplectiques des L_p se déduisent des Ω_p minimaux par *éclatements symplectiques* : on remplace une boule isomorphe à la boule de rayon λ dans le $\mathbf{R}^4$ symplectique standard par la courbe

exceptionnelle de $\overline{\mathbf{P}^2(\mathbf{C})}$ (avec la structure $\lambda^2\omega_0$) (*cf.* [M.D.2]).

Remarque.— Dans [MA] Michèle Audin explique pourquoi il n'existe pas de somme connexe symplectique pour les variétés fermées (D. Mc Duff, M. Gromov). (Soulignons que sur $\mathbf{P}^2(\mathbf{C})$ il n'y a pas de structure presque complexe qui induise l'orientation opposée, donc les éclatements ne sont pas des sommes connexes symplectiques.)

Observons que l'on ignore encore s'il existe une structure symplectique sur $\mathbf{P}^2(\mathbf{C})$ non isomorphe à un multiple de la structure standard. Afin de prouver qu'une telle structure est impossible, il suffirait de démontrer l'existence de sphères symplectiques plongées pour toute structure symplectique sur $\mathbf{P}^2(\mathbf{C})$. La récente généralisation par Donaldson des théorèmes d'annulation de Kodaira aux structures presque complexes va dans ce sens.

2.3. En ce qui concerne les variétés symplectiques de dimension > 4, on dispose du résultat suivant :

THÉORÈME 7 (M. Gromov, D. Mc Duff, A. Floer, Y. Eliashberg).— *Les remplissages asphériques de la structure standard sur la sphère S^{2n-1} sont tous* difféomorphes *à la boule B^{2n}. Toute variété symplectique asphérique et standard à l'infini est difféomorphe à $\mathbf{R}^{2n}$.*

Comme les théorèmes 5 et 6, ce théorème se démontre grâce à la technique des courbes pseudo-holomorphes de M. Gromov.

Du théorème 7 et des constructions qui donnent le théorème 1, Eliashberg [E.5] déduit des exemples nouveaux de structures de contact exotiques sur les sphères en dimension ≥ 5.

THÉORÈME 8 (Eliashberg).— *Pour tout $n > 2$, il existe sur S^{2n-1} des structures de contact qui bordent des variétés symplectiques et qui ne sont pas isomorphes à la structure standard. Si n est impair, il existe de telles structures dans la classe d'homotopie de la structure standard.*

La proposition à laquelle Eliashberg fait appel pour la construction du théorème 8 a son intérêt propre pour l'Analyse complexe, puisqu'elle généralise la proposition bien connue (*cf.* Harvey, Wells, Nirenberg, [N.,W.]) :

dans une variété analytique complexe W, toute variété *totalement réelle* V (*i.e.* $T(V) \cap J(T(V)) = 0$) admet un système fondamental de voisinages de Stein s.p.c.. Eliashberg étend cela aux sous-variétés immergées :

soit V une sous-variété immergée totalement réelle à points doubles transverses telle que J laisse stable la réunion des espaces tangents de V aux points doubles ; alors V admet un système fondamental de voisinages de Stein strictement pseudo-convexes.

Les remplissages des structures exotiques du théorème 8 s'obtiennent par sommes connexes au bord de plombages de Milnor des voisinages de S^n dans son cotangent.

Pour des exemples nouveaux de structures exotiques sur $\mathbf{R}^{2n-1}$, $n > 2$, voir le travail de Marie-Paule Muller ([M.P.M.]).

Un problème encore largement ouvert ici est de caractériser les structures de contact qui se remplissent symplectiquement. Il faudrait aussi comprendre quand est-ce qu'un bord symplectique peut être transformé en bord holomorphe C.R..

D'après Milnor, toute variété de contact fermée de dimension $2n-1$ est le bord d'une variété compacte de dimension (réelle) $2n$ qui possède une structure presque complexe ([M.2]). On ne sait pas si une variété fermée de dimension $2n-1$, bord d'une variété compacte presque complexe de dimension $2n$ peut être munie d'une structure de contact.

3. SURFACES RÉELLES DANS LES SURFACES COMPLEXES, ENVELOPPES D'HOLOMORPHIE ET NŒUDS LEGENDRIENS

3.1. L'une des principales conjectures non résolues sur la topologie des surfaces algébriques complexes s'énonce ainsi :

Conjecture 1.— *Soient X une surface complexe projective lisse et A une courbe algébrique lisse connexe et très ample dans X ; soit S une surface réelle orientée connexe plongée dans X, homologue à A, le genre de S est supérieur à celui de A.*

Cette conjecture appartient maintenant au folklore des topologues et des géomètres. Dans le cas où X est le plan projectif, elle est attribuée à René Thom :

Est-ce qu'une surface fermée orientée connexe plongée dans $\mathbf{P}^2(\mathbf{C})$ *de degré* d *peut avoir un genre inférieur à* $\frac{(d-1)(d-2)}{2}$?

Une question analogue est formulée pour les courbes rationnelles :

Est-ce qu'une sphère de dimension 2 immergée dans $\mathbf{P}^2(\mathbf{C})$ *de degré* d *peut voir un nombre de points doubles inférieur à* $\frac{(d-1)(d-2)}{2}$?

L'origine de la question est la conjecture de J. Milnor ([M.3]) sur les entrelacs algébriques ; c'est la version "locale" du problème.

Conjecture 2.— *Soit* δ *le nombre de points doubles ordinaires concentrés en une singularité isolée* 0 *d'une courbe algébrique plane sans composante multiple* ($2\delta = \mu + r - 1$ *où* r *est le nombre de branches passant par* 0 *et* μ *la multiplicité), soit* Γ *l'entrelacs de* S^3 *qu'on obtient par intersection de la courbe singulière avec le bord d'une petite boule* B^4 *autour de* 0 *; il n'existe pas de réunion de disques immergés dans* B^4 *s'appuyant sur* Γ *qui ait moins de* δ *points doubles.*

En particulier : *le nombre gordien du nœud associé à une singularité isolée irréductible est égal à* δ.

Le plus probable est que la minoration δ vienne d'une minoration du genre des surfaces connexes plongées S dans B^4 de bord Γ :

Soit $\chi(S)$ *la caractéristique d'Euler de* S *; a-t-on* $\chi(S) \leq 1 - \mu$?

Les principaux résultats sont ceux de Rokhlin [V.R.], et de Donaldson [D.2] :

Rokhlin trouve une borne inférieure du genre de S dans la surface X qui est à peu près la moitié du genre de la courbe A.

À partir du théorème d'indécomposabilité de [D.1], Donaldson démontre qu'il est impossible de chirurgiser directement A, c'est-à-dire qu'il n'existe pas de disque plongé dans $X \setminus A$, dont le bord est dans A et d'auto-intersection nulle relativement à un déplacement du bord suivant sa normale dans A.

Sur les problèmes de Thom et de Milnor, on pourra consulter l'article de M. Boileau et C. Weber [B.,W.], les travaux de L. Rudolph, O. Viro,

T. Fiedler entre autres. (Dans [L.R.], Rudolph montre qu'aucune des conjectures ne tient si l'on remplace surface lisse par surface topologiquement plate.)

3.2. Y. Eliashberg et V. Harlamov [E.,H.] furent les premiers à relier les questions de 3.1 aux configurations des points complexes sur les surfaces réelles d'une surface complexe et aux enveloppes d'holomorphie.

Considérons une surface fermée orientée immergée S dans une variété presque complexe (W, J) de dimension 4 réelle ; lorsque S se trouve en position générale par rapport à J, il n'y a qu'un nombre fini de points de S où $T(S) = J(T(S))$; on les appelle *points complexes* de S dans W ; ils se répartissent en quatre groupes : les elliptiques positifs (en nombre e_+), les elliptiques négatifs (en nombre e_-), les hyperboliques positifs (en nombre h_+) et les hyperboliques négatifs (en nombre h_-). Positif ou négatif, selon que l'orientation de S est compatible avec J ou $-J$, elliptique ou hyperbolique selon que l'application de Gauss de S dans le fibré en grassmanniennes des deux-plans orientés tangents à W rencontre positivement ou négativement la variété des droites J-complexes (*cf.* [E.1,4] ou [D.B.1,2], par exemple) (voir aussi le §4).

Notons χ la caractéristique d'Euler de S, ν le nombre d'Euler de son fibré normal et c le nombre de Chern de S vis-à-vis de J ; les nombres $d_+ = e_+ - h_+$ et $d_- = e_- - h_-$ se calculent par les formules de Lai [H.L.] :

$$d_+ = \frac{1}{2}(\chi + \nu + c)$$

$$d_- = \frac{1}{2}(\chi + \nu - c)$$

La conjecture 1 de 3.1 revient à

$$d_- \leq 0$$

pour une surface *plongée* S homologue à A. Car $\chi(A) + A \,.\, A = c(A)$ puisque A est loin des points complexes négatifs, et $\nu(S) = S \,.\, S = A \,.\, A$ et $c(S) = c(A)$ (puisque ces nombres sont des invariants homologiques), donc $\chi(S) \leq \chi(A)$ se traduit par $d_-(S) \leq 0$.

3.3. En 1965, E. Bishop [E.BI.] donnait le jour à un phénomène nouveau : lorsque J est intégrable sur W, si P est un point elliptique sur une surface lisse S plongée dans W, il existe un voisinage U de P dans W tel que l'enveloppe d'holomorphie de $S \cap U$ par rapport à U contienne une famille à un paramètre de disques holomorphes. Les bords des *disques de Bishop* sont des courbes simples sur S, deux à deux disjointes, elles entourent P et forment un feuilletage de $S \cap U \backslash \{P\}$.

La réunion des disques de Bishop dans U est une variété C^∞ à bord de dimension 3 et c'est toute l'enveloppe d'holomorphie de $S \cap U$ dans U (voir §4).

Pour comprendre la configuration des points complexes d'une surface S (C^∞ plongée) dans W analytique complexe, il est naturel de chercher à étendre la famille des disques qui naissent aux points elliptiques le plus loin possible. Malheureusement, la proximité des points hyperboliques est en général assez sauvage (exemples de Bedford et de Moser-Webster *cf.* [E.BE.], [M.,W.], et §4.3), et même quand il n'y a pas de points hyperboliques (et que W est le plan complexe), il semble que les disques échappent à un contrôle global (exemple de Eliashberg et Harlamov *cf.* [E.3]). Cependant, il devient possible de décrire ce que deviennent les disques de Bishop lorsque S est au bord d'un domaine strictement pseudo-convexe. C'est ce qui a permis à Bedford, Klingenberg et Eliashberg de prouver le théorème 2 énoncé page 5.

Le premier succès dans le problème global est dû à Bedford et Gaveau [B.,G.] : il s'agissait d'une sphère S^2 plongée dans une hypersurface fermée s.p.c. de $\mathbf{C}^2$, avec seulement deux points complexes génériques (donc $e_+ = 1$ et $e_- = 1$) et qui était le graphe d'une fonction sur une sphère de $\mathbf{R}^3$ à valeurs dans $\mathbf{R}$. Alors Bedford et Gaveau démontraient que les disques de Bishop se propagent comme il faut d'un point elliptique à l'autre : mis tous ensemble ils remplissent une boule de dimension 3 qui est l'enveloppe d'holomorphie de S dans $\mathbf{C}^2$.

L'étape suivante revient à Gromov, qui établit dans [M.G.] le résultat analogue pour toute sphère S^2 plongée dans le bord d'un domaine de Grauert dans une variété de Stein, mais toujours avec deux points complexes génériques.

Auparavant, Bedford [E.BE.] avait réussi à décrire l'enveloppe de certaines perturbations de surfaces possédant des points hyperboliques. En s'appuyant sur cette analyse et/ou en suivant l'approche de Gromov, Bedford-Klingenberg [B.,K.] et Eliashberg [E.4] ont enfin pu aborder la situation générale d'une surface lisse fermée plongée dans le bord s.p.c. d'une variété de Stein. Le théorème 2, page 5, donne un exemple de leurs résultats, les §§5 et 6 donneront plus de détails ; énonçons seulement quelques corollaires "numériques" en rapport avec les conjectures de 3.1.

THÉORÈME 9 (Eliashberg, Bedford-Klingenberg).— *Soit Σ^2 une sous-variété fermée connexe du bord d'un domaine de Grauert de dimension 2 ; si Σ n'est pas une sphère, les deux nombres d_+ et d_- de Σ sont négatifs (≤ 0).*

Comme l'auto-intersection de Σ est nulle sous les hypothèses du théorème, cela signifie : si Σ n'est pas une sphère, on a $\chi(\Sigma) \leq -|c(\Sigma)|$.

3.4. Les énoncés qui étendent le théorème 9 au cas des surfaces compactes à bord se rapprochent encore plus des conjectures 1 et 2.

Plaçons-nous dans une hypersurface s.p.c. M^3, bord d'un domaine relativement compact Ω et notons F le champ des droites complexes tangentes à M (comme au §1). Considérons une courbe fermée simple (réelle) Γ contenue dans M et transverse à F, et orientons-la dans le sens montant (la tangente orientée à Γ suivie d'un repère direct de F forme un repère orienté de M). Soit Σ une surface orientée plongée dans M, bordée par Γ (avec son orientation), et sans composante connexe fermée (*i.e.* connexe relativement à Γ) ; près de son bord, Σ ne présente aucun point complexe.

THÉORÈME 10 (Eliashberg).— $d_-(\Sigma) \leq 0$.

Un analogue de ce théorème, permettant à Σ de pénétrer à l'intérieur du domaine Ω , démontrerait la conjecture 2.

Dans le cas où $M = S^3$ et où Ω est la boule ronde de $\mathbf{C}^2$, le résultat était démontré dans [D.B.1] (*cf.* [A.D.]) par un mélange de géométrie de contact et de topologie ; lorsque Γ est non nouée dans S^3, il résulte aussi de l'existence du polynôme de Jones comme l'ont montré H. Morton, J.

Franks et R.F. Williams (*cf.* [H.M.] et [F.,W.], ou bien [J] page 325).

Notons $\vec{t}$ (resp. $\vec{n}$) la tangente à Γ (resp. la normale à Γ dans Σ) ; soient c le nombre de Chern de $(T(\Omega)|\Sigma, J)$ relatif à la trivialisation $(\vec{t}, \vec{n})$ le long de Γ, et ν le nombre d'Euler du fibré normal à Σ dans Ω relatif à la section $J\vec{t}$ le long de Γ. Les formules de Lai (p. 14) gardent la même forme et le théorème 10 se réénonce :

$$\chi \leq c.$$

Les résultats sur les courbes transverses à F se reformulent avec des *courbes de Legendre* (les courbes horizontales dans F) :

Soit γ un entrelacs orienté de M dont la tangente appartient constamment aux plans de F et soit Σ une surface orientée plongée dans M, de bord γ (connexe relativement à γ) ; le nombre $\tau(\gamma, \Sigma)$ est le nombre algébrique d'intersections de Σ avec la courbe γ' obtenue par un petit déplacement de γ normal à F, et le nombre $\mu(\gamma, \Sigma)$ est le nombre de tours de la tangente à γ dans un repère trivialisant la restriction de F à Σ. Ces deux nombres ne dépendent que de γ et de la classe de Σ dans $H_2(M, \gamma; \mathbf{Z})$; lorsque $H_1(M; \mathbf{Z}) = 0$, ils sont introduits dans [D.B.1], [A.D.], [T.E.], et dans ce cas, ils ne dépendent que de $\gamma \subset M$.

(Attention : les conventions adoptées ici pour les signes d'enlacement sont différentes de celles de [D.B.1], [A.D.], [T.E.], si bien que les nombres notés ℓ et τ dans [D.B.1] et [A.D.] sont notés ici respectivement $-c$ et $-\tau$.)

La surface Σ peut toujours être perturbée (en gardant γ fixe) pour que les points complexes le long de son bord soient alternativement elliptiques positifs et elliptiques négatifs ; il y aura $|\tau|$ points de chaque type sur γ. Les formules de Lai se réécrivent alors :

$$d_+ = \frac{1}{2}(\chi + \tau + \mu)$$

$$d_- = \frac{1}{2}(\chi + \tau - \mu).$$

Et le théorème 10 entraîne :

THÉORÈME 11 (Eliashberg).— $\chi \leq \tau - |\mu|$.

L'analyse des disques de Bishop (*cf.* §6) permet à Eliashberg d'obtenir encore bien d'autres résultats remarquables sur les structures de contact standard, par exemple :

THÉORÈME 12 (Eliashberg).— *Toutes les courbes de Legendre de la structure standard (directe) de S^3 qui sont non nouées dans S^3 et qui satisfont $\tau = +1$ et $\mu = 0$, sont isotopes entre elles à travers les courbes de Legendre.*

3.5. La plupart des résultats qui précèdent, en particulier le théorème 2 et son corollaire, le théorème 3 et son corollaire, le théorème 4, les théorèmes 9, 10, 11 et 12, s'étendent aux structures complexes non intégrables de la manière suivante : on remplace la variété analytique W par une variété de dimension 4, W munie d'une structure symplectique ω et d'une structure presque complexe J positive par rapport à ω (*cf.* [M.G.], ou [D.B.2]) (*i.e.* $\forall x \in W$, $\forall v \in T_x(W)$, $v \neq 0 \Longrightarrow \omega(v, Jv) > 0$), Ω demeure un domaine relativement compact à bord lisse M, et la condition sur le bord est qu'il soit strictement pseudo-convexe au sens des structures C.R. (§1, p. 3). Notons que pour toute structure de contact F sur une variété fermée M qui borde au sens symplectique (§2, p. 7) une variété symplectique (Ω, ω), il existe une structure presque complexe J qui satisfait ces exigences.

La présence de ω permet le contrôle d'aire des disques (pseudo) holomorphes comme dans [M.G.]. La compacité des familles de disques résulte du contrôle d'aire et d'arguments topologiques (*cf.* §6).

Lorsqu'on étudie les familles de disques (pseudo) holomorphes qui s'appuient sur une surface Σ de M, la non-intégrabilité de J fait apparaître deux difficultés nouvelles : la description des points singuliers intérieurs aux disques et le comportement des disques près des points complexes de Σ.

La première difficulté est heureusement levée par le travail de D. Mc Duff [M.D.3]. On peut lever la seconde artificiellement en changeant J près des points complexes de Σ en une structure intégrable C^0-proche de J (ce qui ne change pas la positivité vis-à-vis de J).

Ceci permet à Eliashberg [E.5,6] d'énoncer des résultats purement sym-

plectiques. Donnons quelques exemples.

THÉORÈME 13 (Eliashberg).— *Soit Ω un remplissage symplectique d'une variété de contact de dimension 3 (M, F) ;*

i) *toute sphère S^2 plongée dans M borde une boule B^3 plongée dans Ω ;*

ii) *si M est difféomorphe à S^3, Ω est difféomorphe à $B^4 \# \overline{\mathbf{CP}}^2 \# \cdots \# \overline{\mathbf{CP}}^2$ et F est standard ;*

iii) *soit Σ une surface connexe fermée plongée dans M ; si $\chi(\Sigma) > -|c(\Sigma)|$, Σ est une sphère (notons que le nombre c a une existence symplectique) ;*

iv) *soit Σ une surface orientée à bord Γ transverse montant dans F, sans composante connexe isomorphe à S^2 ; on a*

$$\chi(\Sigma) \leq c(\Sigma);$$

v) *soit Σ une surface orientée à bord γ horizontal dans F, sans composante connexe isomorphe à S^2 ; on a*

$$\chi(\Sigma) \leq \tau - |\mu|.$$

3.6. À plusieurs reprises, nous avons mentionné le travail [M.D.3] de Dusa Mc Duff sur les singularités des courbes intégrales d'une structure presque complexe J (c'est-à-dire les courbes J-holomorphes, ou pseudo-holomorphes) ; il s'agit de résultats techniques de grande importance dans la théorie qui précisent quelques points de [M.G.] (en passant, ils corrigent aussi des affirmations de [D.B.2], par exemple 2.3.2). Ces résultats sont la base de [M.D.1 et 2]. Citons-en deux :

PROPOSITION 1 (D. Mc Duff).— *Toute application J-holomorphe $f : \Sigma \to W$ d'une surface de Riemann dans une variété presque complexe (W, J) peut s'approcher C^1 par une courbe J'-holomorphe d'une structure presque complexe C^0-voisine de J, qui est* immergée.

PROPOSITION 2 (D. Mc Duff).— *Soient C et C' deux germes en 0 de courbes J-holomorphes d'une variété presque complexe de dimension 4*

ayant un point d'intersection isolé en 0, *le nombre d'intersection local de* C *et* C' *est* ≥ 1 *et il vaut* 1 *si et seulement si* C *et* C' *sont transverses.*

3.7. Pour distinguer deux structures de contact en dimension 3 qui appartiennent à la même classe d'homotopie de champs de plans, on doit s'intéresser aux feuillages qu'elles tracent sur des surfaces plongées (une idée qui remonte à Sophus Lie [L]).

Par exemple, sur S^3 d'équation $x_1^2 + y_1^2 + x_2^2 + y_2^2 = 1$ dans $\mathbf{R}^4$, considérons les deux structures suivantes :
F_0 (standard directe) d'équation

$$x_1\,dy_1 - y_1\,dx_1 + x_2\,dy_2 - y_2\,dx_2 = 0,$$

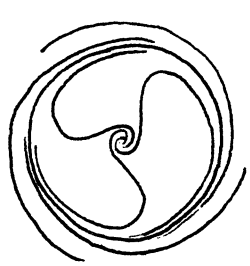
et F_1 (une des structures de Gonzalo-Varela)

$$\cos\Big(\frac{\pi}{4}+2\pi(x_2^2+y_2^2)\Big)(x_1dy_1-y_1dx_1)+\sin\Big(\frac{\pi}{4}+2\pi(x_1^2+y_1^2)\Big)(x_2dy_2-y_2dx_2) = 0;$$

elles sont homotopes à travers les champs de plans tangents sur S^3, mais elle ne sont pas isomorphes, car dans F_1 on peut voir sur un *disque plongé* un cycle limite (*cf.* figure 1), alors que dans F_1 une telle figure ne peut exister. C'est le théorème 11 qui l'interdit (on aurait $\chi = 1$, $\tau = 0$, $\mu = \pm 1$) (c'est l'argument de [D.B.1], (*cf.* [A.D.])).

DÉFINITION.— *Une structure de contact en dimension* 3 *est* supertordue *si l'on peut trouver dans la variété un disque plongé avec un seul point critique et un cycle limite.*

Ce qui peut donner l'une des figures suivantes :



Eliashberg a donc démontré qu'aucune structure de contact qui *borde*

au sens symplectique n'est super-tordue. En particulier, les bords de Grauert dans les surfaces analytiques ne sont pas super-tordus.

Soulignons que la figure 1 est la seule exoticité connue en dimension 3 et l'on peut se demander (Eliashberg) par exemple :

Est-ce qu'une structure de contact sur S^3 non super-tordue est isomorphe à la structure standard ?

Il s'avère que les structures super-tordues sont plus maniables que les structures standard.

THÉORÈME 14 (Eliashberg [E.7]).— *Sur une variété de dimension* 3 *compacte, si deux structures super-tordues sont homotopes en tant que champs de plans, elles sont isomorphes.*

En fait, Eliashberg établit que l'inclusion de l'espace des structures de contact super-tordues dans l'espace des champs de plans est une équivalence d'homotopie faible.

4. POINTS COMPLEXES ET DISQUES HOLOMORPHES

4.1. Soit J une structure presque complexe de classe C^∞ sur une variété W de dimension 4 ; notons G le fibré sur W dont la fibre en $x \in W$ est la grassmannienne Q_x des sous-espaces vectoriels orientés de dimension 2 de l'espace tangent T_xW. L'espace total de G contient les fibrés G_+ et G_- dont les fibres $x \in W$ sont respectivement la droite projective complexe Q_+ des droites J-complexes de T_xW et celle Q_- des droites $-J$-complexes de T_xW. Soit Σ une sous-variété orientée de dimension 2 dans W ; elle se relève par ses plans tangents en une sous-variété $\widetilde{\Sigma}$ de G ; les points complexes de Σ sont les points de rencontre de $\widetilde{\Sigma}$ avec G_+ et G_-.

Si l'on choisit une structure riemannienne sur W adaptée à J, en chaque point x de W la fibre Q_x s'identifie à $S_+ \times S_-$, où S_+ est la sphère de rayon 1 dans l'espace des bivecteurs autoduaux et S_- celle des bivecteurs anti-autoduaux ; Q_+ et Q_- sont respectivement $\{$pôle nord de $S_+\} \times S_-$ et $\{$pôle sud de $S_+\} \times S_-$. C'est donc la projection g_+ sur S_+ parallèlement à S_- qui détermine le type d'un point complexe ; il est > 0 ou < 0 selon qu'on

tape au pôle nord ou au pôle sud, elliptique ou hyperbolique selon que g_+ préserve ou renverse l'orientation. (Remarque corrective : dans [D.B.2], p. 118 en haut, il faut échanger S_+ et S_- de la ligne 5 à la ligne 11.)

Si Σ se tient dans une sous-variété M de dimension 3 dans W et si l'on induit la métrique sur M, g_+ est l'application de Gauss ordinaire ; les points elliptiques apparaissent à courbure positive et les points hyperboliques à courbure négative.

Soit $P \in W$ un point complexe positif de Σ où $\widetilde{\Sigma}$ est transverse à G_+ ; choisissons des coordonnées locales x_1, y_1, x_2, y_2 centrées en P, de manière à ce qu'au point P on ait $J(\partial_{x_1}) = \partial_{y_1}$, $J(\partial_{x_2}) = \partial_{y_2}$. Les fonctions $z_1 = x_1 + iy_1$, $z_2 = x_2 + iy_2$ sont des coordonnées analytiques complexes pour une structure J_0 telle que $J_0(P) = J(P)$.

Les arguments de Bishop (voir aussi [M.,W.]) montrent qu'on peut changer (de façon bianalytique pour J_0) les coordonnées (z_1, z_2) pour que l'équation Σ près de P soit :

$$z_2 = z_1\bar{z}_1 + \gamma(z_1^2 + \bar{z}_1^2) + S(z_1, \bar{z}_1)$$

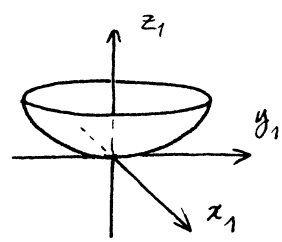
où S est un $O(|z_1|^3)$ et γ un nombre réel > 0 et $\neq \frac{1}{2}$.

L'axe des z_1 est alors la tangente complexe de Σ à l'origine.

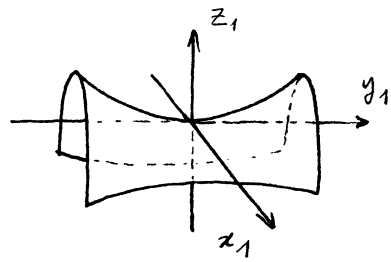
Le nombre γ est un invariant complexe de Σ (c'est-à-dire qu'il est inchangé par toute transformation respectant J en P). Il est compris entre 0 et $\frac{1}{2}$ lorsque P est elliptique et il est supérieur à $\frac{1}{2}$ si P est hyperbolique.

Au troisième ordre en z, la surface Σ est dans l'hyperplan $\mathbf{R}^3$ d'équation $y_2 = 0$, et elle se présente comme suit :

dans le cas elliptique :



dans le cas hyperbolique :



4.2. À présent, supposons J intégrable auprès de P dans W et Σ analytique réelle. Choisissons les coordonnée z_1 et z_2 holomorphes.

Pour faire l'analyse d'un point complexe, Moser et Webster font appel à une complexification locale de Σ.

Soit U un ouvert de W stable par l'involution anti-holomorphe $z = (z_1, z_2) \mapsto (\bar{z}_1, \bar{z}_2) = \bar{z}$ autour de 0, tel que la fonction $R(z, \bar{z}) = z_1\bar{z}_1 + \gamma(z_1^2 + \bar{z}_1^2) + S(z_1, \bar{z}_1) - z_2$ soit analytique réelle de V dans $\mathbf{C}$. L'équation de $\Sigma \cap U$ est $R(z, \bar{z}) = 0$.

Dans $U \times U$, on considère la surface analytique complexe Z définie par les équations :

$$R(z, w) = 0 \qquad \text{et} \qquad \bar{R}(w, z) = 0;$$

$z = (z_1, z_2)$ et $w = (w_1, w_2)$ sont des coordonnées sur $U \times U$ et (z_1, w_1) forment des coordonnées locales sur Z.

Désignons par π' (resp. π'') la restriction à Z de la projection de $U \times U$, sur le facteur des z (resp. des w) ; toutes les deux sont des revêtements ramifiés à deux feuillets, π' se ramifie le long de $C' \subset Z$ tangente à la droite $z_1 + 2\gamma w_1 = 0$ et π'' le long de $C'' \subset Z$ tangente à la droite $2\gamma z_1 + w_1 = 0$ Notons τ' et τ'' les involutions de Z qui échangent les feuillets ; on a $\pi'\tau' = \pi'$, $\pi''\tau'' = \pi''$, τ' fixe C' et τ'' fixe C''.

Introduisons aussi l'involution anti-holomorphe de $U \times U$ et de Z :

$$\rho(z, w) = (\bar{w}, \bar{z}).$$

On a

$$\tau''\rho = \rho\tau'.$$

Soit $\varphi = \tau'\tau'' = \tau'\varphi^{-1}\tau'$ de Z dans Z ; l'application φ est un difféomorphisme analytique complexe de Z qui possède un point fixe en 0.

C'est la dynamique de φ près de 0 qui dicte le comportement des courbes holomorphes appuyées sur Σ (Moser-Webster).

En effet, soit f une fonction analytique réelle de Σ dans $\mathbf{R}$; elle a un prolongement analytique complexe sur un voisinage de Σ dans Z et la réalité de f sur Σ se traduit par $\bar{f}(\rho) = f$ sur Z. Si $f\tau'' = f$ (ou $f\tau' = f$ qui lui est équivalent), la fonction g de U dans $\mathbf{C}$ définie par $g\pi' = f$ est holomorphe (extension de Riemann) et prolonge f. Réciproquement, une fonction f réelle sur Σ qui est la trace d'une g holomorphe sur U s'étend en f sur Z qui vérifie $f\tau'' = f\tau' = f$, donc $f\varphi = f$ (*i.e.* f est une intégrale première holomorphe de φ).

Soient λ et λ^{-1} les solutions de $\gamma = \frac{1}{\lambda+\lambda^{-1}}$ (*i.e.* $\gamma\lambda^2 - \lambda + \gamma = 0$) ; les valeurs propres de $D\varphi$ en 0 sont $\mu = \lambda^2$ et $\mu^{-1} = \lambda^{-2}$. Lorsque $0 < \gamma < \frac{1}{2}$, λ est réelle > 0 et différente de 1 ; lorsque $\gamma > \frac{1}{2}$, λ est complexe de module 1 différente de 1.

Donc un point elliptique donne un φ hyperbolique et une méthode de série majorante permet à Moser et Webster de ramener φ, τ' et τ'' à une forme normale ; il existe des coordonnées (z_1, z_2) où Σ s'écrit :

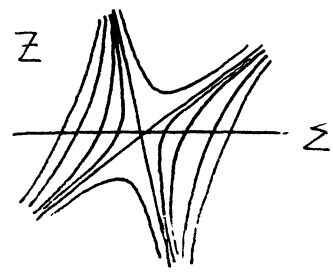
$$\begin{cases} y_2 = 0 \\ x_2 = z_1\bar{z}_1 + (\gamma + \varepsilon x_2^s)(z_1^2 + \bar{z}_1^2), \end{cases}$$

ε valant 0, 1 ou -1, et s étant un entier non nul lorsque $\varepsilon = \pm 1$.

Les nombres (γ, ε, s) sont les invariants holomorphes du germe de Σ ; il existe une variété H^3 Levi-plate qui contient Σ, et l'enveloppe d'holomorphie locale de Σ est la partie de H à l'intérieur de Σ.

L'application φ possède une intégrale première holomorphe et les bords des disques de Bishop sont les traces sur $\Sigma \subset Z$ des niveaux de l'intégrale ;

ce sont les trajectoires d'un flot où φ se plonge pour les valeurs imaginaires pures du paramètre.



Notons que la classification des paires d'involutions conjuguées (comme τ' et τ'') apparaissait dans les recherches de Birkhoff sur le problème restreint des trois corps.

4.3. Pour un point complexe hyperbolique, le point fixe de φ est elliptique et l'on doit faire face à un problème de petits diviseurs. Il existera bien une forme normale, mais les séries qui doivent conjuguer φ à sa forme normale sont en général divergentes ; et Moser-Webster montrent un exemple de surface Σ qui *ne peut pas* être plongée dans une hypersurface Levi-plate (analytique réelle) ; c'est

$$z_2 = z_1\bar{z}_1 + \gamma\bar{z}_1^2 + \gamma z_1^3\bar{z}_1 \qquad \left(\text{avec } \gamma > \frac{1}{2}\right).$$

Ceci n'a pas découragé nos auteurs Bedford, Klingenberg, Eliashberg : pour étudier le passage des disques de Bishop par les points hyperboliques, il suffira de se restreindre à des cas très spéciaux où Σ est déjà aplatie *et* φ complètement intégrable. Nous allons voir que cela peut se faire avec une surface Σ' C^2-proche d'une surface Σ donnée.

Reprenons les notations de 4.2 ; la contre-image de Σ par π' dans Z est constituée par deux surfaces totalement réelles L_1 et L_2 transverses entre elles et transverses à C' et C'' : L_1 est le plan $w_1 = \bar{z}_1$ et $L_2 = \tau'(L_1)$ est tangente en 0 au plan $w_1 = \bar{z}_1 - z_1/\gamma$.

L'idée de D. Burns, E. Bedford et W. Klingenberg est de relever les surfaces holomorphes dans U à bord sur Σ qui arrivent près du point hyperbolique en surfaces holomorphes de Z qui s'appuient sur L_1 *et* L_2.

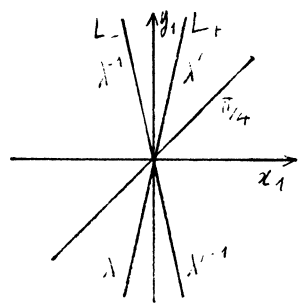
Comme réflexion dans L_1, on choisit $\rho_1 = \rho$, et comme réflexion dans L_2, on choisit $\rho_2 = \tau'\rho\tau' = \varphi\rho$.

Le groupe engendré par ρ_1 et ρ_2 est également engendré par φ et ρ, avec les relations $\rho\varphi\rho^{-1} = \varphi^{-1}$ et $\rho^2 = 1$. C'est un groupe dihédral si $\varphi^n = 1$ ($n \in \mathbf{N}$).

Lorsqu'il existe $n \in \mathbf{N}$ avec $\varphi^n = 1$, nous dirons que le point P de Σ est *rationnel* (vis-à-vis de J). Alors la valeur propre μ est de la forme $\exp(2\pi i \frac{m}{n})$.

On obtient des points rationnels sur la quadrique Σ_γ d'équation $z_2 = z_1\bar{z}_1 + \gamma(z_1^2 + \bar{z}_1^2)$ lorsque les racines λ de $\gamma\lambda^2 - \lambda + \gamma = 0$ sont de la forme $\exp(2\pi i \frac{p}{q})$.

Dans le plan des z_1, les droites d'intersection de Σ_γ avec $z_2 = 0$ ont pour pentes $y_1/x_1 = \pm tg\theta'$, où $\lambda' = \exp(i\theta')$ est donnée par $\lambda'^2 + \gamma(\lambda'^4 + 1) = 0$ donc $\lambda'^2 = -\lambda$ et $(\lambda')^{-2} = -\lambda^{-1}$. Comme $Re(\lambda) < 0$, on a le dessin suivant, où tous les angles sont rationnels (en radians) :



Nous noterons Δ_+^+ (resp. Δ_+^-) le secteur qui contient le $\frac{1}{2}$ axe $x_1 = 0$, $y_1 > 0$ (resp. $y_1 < 0$), Δ_-^+ (resp. Δ_-^-) celui qui contient le $\frac{1}{2}$ axe $y_1 = 0$, $x_1 > 0$ (resp. $x_1 < 0$) ; $\Delta_+ = \Delta_+^+ \cup \Delta_+^-$ et $\Delta_- = \Delta_-^+ \cup \Delta_-^-$ Nous appellerons Δ_+^+ et Δ_+^- les *secteurs aigus* et Δ_-^+, Δ_-^- les *secteurs obtus.*

En examinant le lieu de ramification de π', on voit que les parties des droites complexes $z_2 =$ constante délimitées par Σ_γ et rencontrant les secteurs aigus se relèvent par π' en des bandes holomorphes dans Z qui vont de L_1 à L_2. (De même, dans le cas des points elliptiques, les disques de Bishop se relèvent en des anneaux holomorphes dont un bord est sur L_1 et l'autre sur L_2.)

Soient D le disque de rayon 1 dans $\mathbf{C}$, Δ un voisinage de $1 \in D$ dans D et $f : \Delta \to V$ une application holomorphe qui envoie 1 sur P et $S^1 \cap \bar{\Delta}$ dans Σ ; supposons que $f(\Delta)$ soit un graphe au-dessus de l'axe du z_1 dans l'un des secteurs aigus. Relevons f par π' et prolongeons-la par *réflexion de Schwarz* dans L_1 et L_2. Si P est *rationnel*, on aboutit ainsi au prolongement de f, sur un revêtement ramifié ℓ fois de $\mathbf{C}$ en 1, en une application holomorphe qui est un revêtement ramifié k fois de l'axe des z_1.

Au-dessus de Δ_+, on a un développement limité de l'image :

$$z_2 = g(z_1) = a\, z_1^2 + o(|z_1|^2)$$

car le bord est dans Σ où $z_2 = o(|z_1|^2)$. En regardant de plus près, on voit que $a = 0$ (comparer le long du bord de Δ_+ les expressions $x_1^2(1+2\gamma) + y_1^2(1-2\gamma)$ et $(\alpha + i\beta)(x_1^2 - y_1^2 + 2ix_1y_1)$).

Donc *le bord de $f(\Delta)$ est asymptote aux deux côtés L_- et L_+ de Δ_+.* Et cela, c'est l'essentiel du contrôle qu'il faudra pour faire passer les disques par les points hyperboliques.

5. ENVELOPPE HOLOMORPHE DE SURFACES RÉELLES

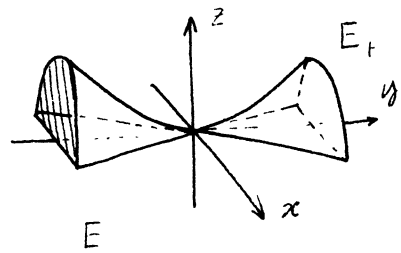
5.1. La partie de l'enveloppe d'holomorphie d'une surface réelle plongée au bord d'un domaine strictement pseudo-convexe de dimension 2, que Eliashberg, Bedford et Klingenberg sont capables de décrire est une *variété à angles* H^3 d'un genre spécial ; commençons par la présenter abstraitement.

Les points de H auront tous un modèle local C^∞ isomorphe à celui d'un des points du fermé E de $\mathbf{R}^3$ défini par :

$$z \geq 0 \quad , \quad z \leq y^2 - x^2$$

ou bien du fermé E_+ de $\mathbf{R}^3$ inclus dans E défini par

$$z \geq 0 \quad , \quad y \geq 0 \quad , \quad z \leq y^2 - x^2$$



Les points de H qui ont pour modèle les points intérieurs de E sont les points *réguliers*, ceux qui ont pour modèle un point de E avec $z = 0$ ou bien $z = y^2 - x^2$ sont les points du *bord* de H, ceux qui ont pour modèle des points de $z = 0$, $y^2 = x^2$ appartiennent aux *arêtes* de H, ceux qui sont comme 0 dans E_+ sont des *pointes* du type I et ceux qui sont comme 0 dans E sont des pointes du type II. Le bord de H est une surface à coins, sauf aux pointes de type II.

Lorsque H n'a pas d'arête, c'est une variété à bord C^∞. Quand il n'y a pas de pointes, H est une variété à coins ordinaire.

Les modèles locaux de H sont ceux de la *théorie de Morse à bord.*

Pour les variétés à angles qui vont nous intéresser, le bord de H pourra toujours s'écrire comme une réunion de deux surfaces (à angles) A et B séparées par les arêtes, et tout sera naturellement orienté.

Il est maintenant possible d'énoncer le théorème principal de [E.5,6] et [B.,K.] :

THÉORÈME 15 (Eliashberg, Bedford-Klingenberg).— *Soit Σ une surface réelle C^∞ orientée fermée plongée dans le bord M d'un domaine de Grauert Ω d'une variété analytique complexe W ; il existe une surface Σ', C^2-proche de Σ dans M et une variété à angle H plongée dans $\Omega \cup M$ dont le bord est réunion le long des arêtes de $A \subset \Sigma'$ et de B, telle que l'intérieur de $B \subset \Omega$. Les pointes de H sont des points complexes hyperboliques de Σ', toutes les arêtes de H sont dans Σ' ; de plus, en un point du type II, la composante adhérente de B est non simplement connexe.*

A contient tous les points complexes elliptiques de Σ', et B est réunion

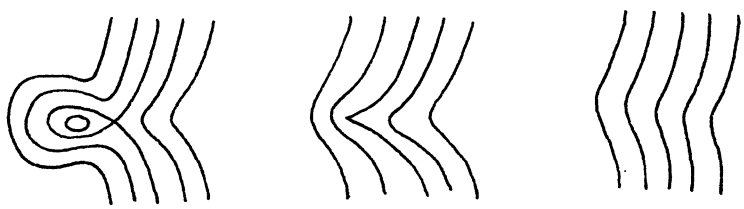
de disques holomorphes.

L'intérieur de H est feuilleté en disques holomorphes, et les bords de ces disques sont des courbes simples C^∞ plongées dans A, sauf aux points hyperboliques de Σ' (où les bords des disques font des angles).

De plus, il existe un unique H maximal possédant toutes ces propriétés.

Remarque 1.— Eliashberg sait démontrer que ce théorème reste vrai sans supposer l'intégrabilité de J sur W, mais en supposant J positive strictement par rapport à une structure symplectique. À proprement parler, Bedford et Klingenberg demandent à W d'être de Stein, mais un argument d'indice (d'opérateurs elliptiques) assez simple permet d'éliminer cette hypothèse (voir §6).

Remarque 2.— Eliashberg énonce aussi la version à un paramètre du théorème 15. Les modèles locaux sont ceux des familles à un paramètre génériques de fonctions sur les variétés à bord de dimension 3, et il faut décrire le passage des points complexes *paraboliques* :



Remarque 3.— Les conclusions du théorème 15 entraînent l'existence d'une variété à bord C^∞ K de bord Σ' contenant H et d'une fonction de Morse $\varphi : K \to \mathbf{R}$ dont les niveaux sont des feuilles holomorphes de H.

Remarque 4.— En un point hyperbolique P de Σ', il n'y a que 4 possibilités :

1) le point est hors de H ;

2) c'est une pointe du type I de H ; une des composantes de B arrive dans un secteur seulement ;

3) le point est régulier dans A ; les disques passent

4) c'est une pointe du type II de H ; les disques s'arrêtent à cause d'un croissant.

Remarque 5.— Comme Σ est dans un bord strictement pseudo-convexe, on peut décider *a priori* dans quel secteur les disques atteignent un point hyperbolique : c'est dans le secteur *aigu* (calculer $L(\rho)$, p. 2 pour $\rho = x_2 - (x_1^2(1+2\gamma) + y_1^2(1-2\gamma))$).

5.2. Montrons, d'après Eliashberg, comment le théorème 15 entraîne le théorème 2 et le théorème 9. Pour cela, il suffit de voir que sous les hypothèses du théorème 15, avec Σ *connexe*, on a $\chi \leq -|c|$ sauf si Σ' est entièrement remplie par H (*i.e.* $B = \emptyset$).

Mais, si $B \neq \emptyset$, on peut "arrondir" H en une variété à bord C^∞ H' plongée dans $\Omega \cup M$. Notons X le bord de H' ; chaque pointe (de type I ou II) qui est hyperbolique positive (resp. négative) sur Σ' donne lieu à un point elliptique négatif (resp. positif) de X ; soient k_+ (resp. k_-) le nombre de ces points.

Si b_0 est le nombre de composantes connexes de X, on a $k_+ + k_- \geq b_0$. Notons $e'_\pm$ et $h'_\pm$ les nombres de points complexes sur X. Comme X borde

dans W, on a $\nu(X) = c(X) = 0$, donc

$$\frac{1}{2}\chi(X) = e'_+ - h'_+ = e'_- - h'_-,$$

mais $2b_0 \geq \chi(X)$, donc $b_0 \geq e_+ + k_- - h'_+$, d'où $k_+ \geq e_+ - h'_+$ et $e_+ - h_+ \leq e_+ - h'_+ - k_+ \leq 0$. De même, $b_0 \geq e_- + k_+ - h'_-$, d'où $k_- \geq e_- - h'_-$ et $e_- - h_- \leq e_- - h'_- - k_- \leq 0$. C.Q.F.D.

Remarque.— Ceci entraîne que sur une sphère plongée dans M, il n'y a jamais de pointe du type II.

Les théorèmes 10 et 11 résultent d'une combinatoire analogue.

6. PROBLÈME DE RIEMANN-HILBERT ET PSEUDO-CONVEXITÉ

6.1. Soit M une sous-variété de dimension 3 d'une variété C^∞ presque complexe (W, J) ; considérons la variété de Fréchet $\mathcal{D}$ des disques C^∞ (non paramétrés) plongés dans W, transverses à M le long de leurs bords. Les propriétés de la transformée de Hilbert usuelle (essentiellement $\|T(u)\|_{C^m} \leq C\|u\|_{C^{m+1}}$ lorsque u est une fonction C^{m+1} du cercle dans $\mathbf{R}$), montrent que le sous-ensemble $\mathcal{H}$ de $\mathcal{D}$ constitué par les disques J-holomorphes est une *bonne sous-variété de Fréchet* de $\mathcal{D}$ (au sens de Hamilton ([R.H.]). Considérons aussi la variété de Fréchet $\mathcal{S}$ des surfaces orientées compactes (éventuellement à bord) Σ, de type topologique donné, plongées dans M et totalement réelles vis-à-vis de J ; c'est aussi une *bonne* variété de Fréchet. Dans le produit $\mathcal{H} \times \mathcal{S}$, on définit l'ensemble $\mathcal{R}$ des couples (D, Σ) tels que le bord de D appartienne à l'intérieur de Σ ; en projetant $\mathcal{R}$ sur $\mathcal{H}$, on voit que $\mathcal{R}$ est une *bonne fibration* au-dessus de $\mathcal{H}$,donc $\mathcal{R}$ est une bonne sous-variété de $\mathcal{H} \times \mathcal{S}$. Soit $\Delta : \mathcal{R} \to \mathcal{S}$ la restriction de la seconde projection.

PROPOSITION.— *L'application Δ est Fredholm et son indice en un point (D_0, Σ_0) de $\mathcal{R}$ est $1 + 2\nu$, où ν est le nombre d'intersection de D_0 avec un indice égal à D_1 C^1-voisin de D_0 dont le bord est dans Σ_0 et ne rencontre pas le bord de D_0.*

Remarque.— En remplaçant le disque par une surface de Riemann à bord X, on aurait la même chose avec indice $\chi(X) + 2\nu$; et en considérant le problème paramétré, on verrait à la place de ν apparaître un nombre de Chern relatif (indice de Maslov).

De la proposition, et des théorèmes de Sard banachiques (applications C^k, $k < \infty$), on déduit en particulier que, étant donné un ouvert C^k-borné $\mathcal{B}$ de $\mathcal{H}$, il est C^k-générique en $\mathcal{S}$ que $\Delta^{-1}(\Sigma) \cap \mathcal{B}$ soit une variété C^∞ de dimension $1 + 2\nu$.

Dans le cas des disques de Bishop, et de tous ceux que considèrent Eliashberg, Bedford et Klingenberg, on a $\nu = 0$: les disques rentrent dans des familles à un paramètre de disques disjoints.

6.2. Plaçons-nous à présent dans les hypothèses du théorème 15.

Le premier endroit où la pseudo-convexité de M intervient est l'utilisation du lemme de E. Hopf (sur la dérivée au bord des fonctions strictement sous-harmoniques) pour démontrer que le bord d'un disque holomorphe de Ω dans la partie totalement réelle Σ^* de Σ est une courbe immergée.

Le second endroit est le contrôle sur la tangente du bord Γ d'un disque holomorphe D de Ω : elle est astreinte à rester dans une distribution de cônes sur Σ^* ; ces cônes sont les complémentaires des traces des plans complexes des hypersurfaces s.p.c. voisines de M contenant Σ.

6.3. Si D est un disque plongé dans Ω, à bord plongé dans Σ^*, avec $\nu(D) = 0$, il entre dans une famille à un paramètre de disques D_t qui ne peuvent pas attraper de singularités au bord. Les bords restent plongés à cause des cônes. Les singularités à l'intérieur contrediraient $\nu = 0$. (Ici dans le cas non-intégrable, il faut utiliser [M.D.3].)

6.4. Supposons que Γ borde une surface compacte dans Σ, et choisissons une métrique riemannienne dans W.

Pour la compacité de la famille de disques, il suffit de faire intervenir une structure symplectique contrôlant J comme dans [M.G.] (*cf.* [D.B.2]).

En effet, l'aire des disques D_t est bornée par une constante fois l'aire de

Σ, et la majoration de l'aire entraîne une majoration de toutes les dérivées *sauf si* des bulles apparaissent. Si l'on n'a pas supposé Ω de Stein, il se pourrait *a priori* que D_t dégénère en réunion d'un disque et d'une sphère (ou de plusieurs sphères) ; c'est là que la généricité est utile :

Si D_t tend vers $D_1 \cup S$, on a $D_1 \,.\, S \geq 1$, et $S \,.\, S \geq 1$ (sinon une petite perturbation de J fait sauter la sphère), donc $D_1 \,.\, D_1 \leq -1$, ce qui n'arrive pas pour Σ générique (l'indice de D_1 serait -1).

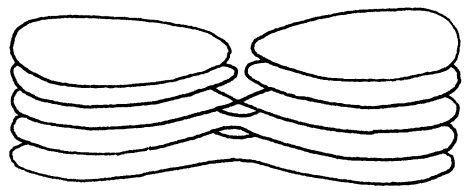
(Notons qu'apparaissent ici des structures complexes non nécessairement intégrables.)

6.5. Démarrons donc avec une famille de disques de Bishop près d'un point elliptique P de Σ ; les arguments précédents "démontrent" que la famille se poursuit gentiment jusqu'au voisinage d'un autre point complexe Q. Ce point ne peut être elliptique que si les disques viennent en coïncidence avec les disques de Bishop de Q (encore la stricte pseudo-convexité et l'argument d'intersection). Supposons donc Q hyperbolique. Si l'on a pris soin de perturber Σ en topologie C^2 pour que tous ses points hyperboliques soient *rationnels*, les disques convergent vers un disque passant par Q. Alors, on applique la remarque 5, page 23, et la discussion de 4.3. Les théorèmes d'approximation pour les fonctions d'une variable complexe (*cf.* [E.BE.]) montrent que quatre possibilités seulement se présentent pour Σ générique :

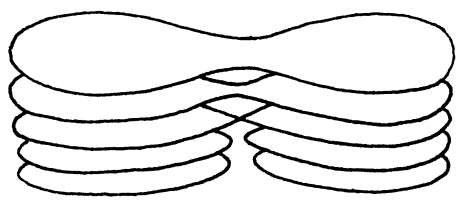
1) le disque arrive par un seul des secteurs Δ_+ et aucun autre disque venant d'une autre famille n'arrive dans le secteur aigu opposé : on a une pointe de type I ;

2) le disque arrive par l'intérieur des deux secteurs aigus et sa limite est un croissant : on a une pointe de type II ;

3) le disque arrive dans Δ_+^+ (resp. Δ_+^-) et un autre disque arrive dans Δ_+^- (resp. Δ_+^+) ; mis ensemble, les deux disques s'approchent par un disque un peu plus grand (Mergelyan), et en perturbant Σ, on continue la famille ;



4) le disque arrive en couvrant tout Δ_+, on l'approche par un disque un peu plus grand (Mergelyan), et on perturbe Σ pour continuer la famille.



7. ANALYSE COMPLEXE ET TOPOLOGIE SYMPLECTIQUE

7.1. Plusieurs autres travaux récents manifestent la fécondité des rapprochements entre la géométrie symplectique (et de contact) et la théorie des fonctions de plusieurs variables complexes (ou la géométrie C.R. et presque complexe).

Les notions de domaine d'holomorphie, de stricte pseudo-convexité, de variétés de Stein proviennent des recherches pour étendre la solution du *problème de Cousin* en plusieurs variables, mais lorsqu'Oka présentait dans [O.], article 1, les principaux problèmes à résoudre, il parlait aussi de la généralisation du *théorème de Runge*. Une belle extension de ce théorème à $\mathbf{C}^2$ est due à Julien Duval ; elle fait encore appel à une notion symplectique.

THÉORÈME 16 (J. Duval [J.D.1]).— *Une sous-variété compacte de* $\mathbf{C}^2$, *lagrangienne pour la structure symplectique standard de* $\mathbf{C}^2$, *est rationnellement convexe.*

COROLLAIRE.— *Les fractions rationnelles sur* $\mathbf{C}^2$ *sont denses dans les fonctions continues sur une sous-variété lagrangienne compacte.*

Inversement, si une sous-variété V fermée de dimension n totalement réelle de $\mathbf{C}^2$ est rationnellement convexe, J. Duval [J.D.2] démontre l'existence d'une structure symplectique adaptée à la structure complexe (et standard à l'infini) pour laquelle V est lagrangienne.

7.2. Les variétés lagrangiennes et les variétés legendriennes interviennent dans pas mal d'endroits en analyse complexe ; par exemple, les *ensembles pics* d'un bord M d'un domaine s.p.c. Ω d'une variété de Stein W sont les sous-ensembles E de M pour lesquels il existe une fonction holomorphe sur Ω C^∞ sur M dont la valeur absolue atteint 1 sur E et reste < 1 sur $\Omega \cup M \backslash E$. Ce sont aussi les sous-ensembles E sur lesquels n'importe quelle fonction C^∞ s'étend en une fonction holomorphe sur Ω, C^∞ sur M. Les sous-variétés de M qui sont des ensembles pics sont horizontales dans la structure C.R. de M (*cf.* [C.,C.], par exemple).

7.3. Polterovitch [L.P.] vient de montrer, en utilisant les disques holomorphes de Gromov que la classe de Maslov d'un tore lagrangien plongé de $\mathbf{C}^2$ ne peut être nulle. Ce résultat est généralisé en toute dimension (dans $\mathbf{C}^n$) par Claude Viterbo ([C.V]) en utilisant le calcul des variations.

7.4. Soient Ω et Ω' deux domaines de Grauert à bords C^∞ M et M' dans des variétés de Stein W et W' ; d'après C. Fefferman (voir [C.F.] et [B.,F.,G.]), tout biholomorphisme $f : \Omega \to \Omega'$ s'étend en un difféomorphisme de M sur M' (et si M et M' sont analytiques réelles, f s'étend analytiquement à un voisinage de M dans W). L'une des principales questions posées par Eliashberg est l'analogue symplectique de ce théorème. Si Ω et Ω' sont des remplissages symplectiques de deux variétés de contact M et M', et s'il existe un difféomorphisme symplectique de Ω sur Ω', quel genre d'équivalence a-t-on entre $\Omega \cup M$ et $\Omega' \cup M'$?

En terminant, je veux remercier tout particulièrement Julien Duval et Yakov Eliashberg pour les discussions passionnantes et instructives que j'ai eues avec eux.

BIBLIOGRAPHIE

[A.1] V.I. ARNOLD - *Méthodes mathématiques de la mécanique classique*, Éditions MIR, Moscou, 1974.

[A.2] V.I. ARNOLD - *Contact geometry and wave propagation*, L'enseignement mathématique, Genève, 1989.

[MA] M. AUDIN - *Sommes connexes de variétés symplectiques ou presque complexes*, preprint IRMA Strasbourg, 1990.

[B.,F.,G.] M. BEALS, C. FEFFERMAN and R. GROSSMAN - *Strictly pseudo-convex domains in* $\mathbf{C}^n$, B.A.M.S., vol. 8 (1983), 125-322.

[E.BE.] E. BEDFORD - *Levi flat hypersurfaces on* $\mathbf{C}^2$ *with prescribed boundary : stability*, Annali Scuola Norm. Sup. Pisa IX (1982), 529-570.

[B.,G.] E. BEDFORD and B. GAVEAU - *Envelopes of holomorphy of certain 2-spheres in* $\mathbf{C}^2$, Amer. J. of Math., 105 (1983), 975-1009.

[B.,K.] E. BEDFORD and W. KLINGENBERG - *On the envelope of holomorphy of a 2-sphere in* $\mathbf{C}^2$, preprint Indiana, 1989.

[D.B.1] D. BENNEQUIN - *Entrelacements et équations de Pfaff*, 3ème rencontre de Géométrie du Schnepfenried, Astérisque 107-108 (1983), 87-161.

[D.B.2] D. BENNEQUIN - *Problèmes elliptiques, surfaces de Riemann et structures symplectiques (d'après M. Gromov)*, Séminaire Bourbaki, exposé n° 657, Astérisque 145-146 (1987), 111-136.

[E.BI.] E. BISHOP - *Differentiable manifolds in complex Euclidian space*, Duke Math. J. 32 (1965), 1-22.

[B.,W.] M. BOILEAU et C. WEBER - *Le problème de J. Milnor sur le nombre gordien des nœuds algébriques*, Séminaire des plans sur Bex., 1982.

[C.] H. CARTAN - *Problèmes d'approximation dans la théorie des fonctions analytiques*, Atti della 2a Riunione del Groupement des Mathématiciens d'expression latine, Florence, 1961.

[C.,C.] J. CHAUMAT et A.M. CHOLLET - *Ensembles pics pour* $A^\infty(D)$, Ann. Inst. Fourier, Grenoble XXIX (1979), 171-200.

[D.1] S. DONALDSON - *Polynomial invariants for smooth 4-manifolds*, to appear in Topology.

[D.2] S. DONALDSON - *Complex curves and surgery*, volume dédié à R.

Thom, Publ. IHES 1988, 91-97.

[A.D.] A. DOUADY - *Nœuds et structures de contact en dimension* 3 *(d'après Bennequin)*, Séminaire Bourbaki, exposé n° 604, Astérisque 105-106 (1983), 129-148.

[J.D.1] J. DUVAL - *Convexité rationnelle des surfaces lagrangiennes de* $\mathbf{C}^2$, preprint 1990 & *Convexité rationnelle de tores lagrangiens de* $\mathbf{C}^2$, Note aux C.R.A.S. 307, série 1, 1988, 943-948.

[J.D.2] J. DUVAL - *Une contrainte géométrique pour certaines sous-variétés rationnellement convexes*, preprint Strasbourg, 1990.

[E.1] Y.ELIASHBERG - *Three lectures on Symplectic Topology* in Cala Gonone. Basic notions, problems and some methods (Septembre 1988).

[E.2] Y.ELIASHBERG - *Existence and non-existence of a Stein complex structure on differentiable manifolds*, preprint MSRI, Berkeley, 1989.

[E.3] Y.ELIASHBERG - *Topological characterization of Stein manifolds of dimension* > 2, Intern. J. of Math. I (1990).

[E.4] Y.ELIASHBERG - *Filling by holomorphic discs and its applications*, preprint Stanford, 1990.

[E.5] Y.ELIASHBERG - *On symplectic manifolds which are bounded by standard contact spheres and exotic contact structures on spheres of dimension* > 3, preprint Berkeley, 1988.

[E.6] Y.ELIASHBERG - *Killing of elliptic complex points and the Legendrian isotopy*, in preparation.

[E.7] Y.ELIASHBERG - *Classification of overtwisted contact structures on* 3*-manifolds*, Invent. Math. 98 (1989) 623-637.

[E.,H.] Y.ELIASHBERG and V. HARLAMOV - *Some remarks on the number of complex points of a real surface in the complex one*, preprint, 1982.

[T.E.] T. ERLANDSSON - *Geometry of contact transformations in dimension* 3, Doctoral dissertation, Uppsala, 1981.

[C.F.] C. FEFFERMAN - *The Bergman kernel and biholomorphic mappings of pseudo-convex domains*, Invent. Math. 26 (1974), 1-65.

[F.,W.] J. FRANKS and R.F. WILLIAMS - *Braids & the Jones polynomials*, T.A.M.S. 303, n° 1, 1987, 97-108.

[H.G.] H. GRAUERT - *On Levi's problem and the embedding of real-analytic manifolds*, Annals of Math., vol. 68 (1958), 460-472.

[M.G.] M. GROMOV - *Pseudo-holomorphic curves on almost complex manifolds*, Invent. Math. 82 (1985), 307-347.

[G.,E.] M. GROMOV and Y. ELIASHBERG - *Non-degenerate mappings of Stein manifolds*, Funkt. Ana. i. Pril. 5 (1971), 82-83.

[G.,R.] R.C. GUNNING and H. ROSSI - *Analytic functions of several complex variables*, Prentice Hall, 1962.

[R.H.] R.S. HAMILTON - *The inverse function theorem of Nash and Moser*, B.A.M.S. (New Series), vol. 7, n° 1 (1982), 65-222.

[HÖ] L. HÖRMANDER - *An introduction to complex analysis in several variables*, North Holland, 1973.

[L.H.] L.R. HUNT - *The local envelope of holomorphy of an n-manifold in* $\mathbf{C}^n$, Bol. Un. Mat. Ital. 4 (1971), 12-35.

[J.] V.F.R. JONES - *Hecke algebra representations of braid groups & link polynomial*, Annals of Math. 126 (1987), 335-388.

[K.,W.] C.E. KENIG et S.M. WEBSTER - *The local hull of holomorphy of a surface in the space of two complex variables*, Invent. Math. 1982, 1-19.

[H.L.] H.F. LAI - *Characteristic classes of real manifolds immersed in complex manifolds*, T.A.M.S. 172 (1972), 1-33.

[L.,M.] P. LIBERMANN et C.M. MARLE - *Géométrie symplectique. Bases de la Mécanique*, vol. 3, publications mathématiques de Paris 7, 1986.

[L.] S. LIE - *Geometrie der Berührungstransformationen*, erster Bandm Teubner, Leipzig, 1896.

[M.D.1] D. Mc DUFF - *Blow-ups and symplectic embeddings in dimension* 4, preprint Stony Brook, 1989, à paraître dans Topology.

[M.D.2] D. Mc DUFF - *The structure of rational and ruled symplectic* 4*-manifolds*, preprint Stony Brook, 1989.

[M.D.3] D. Mc DUFF - *The local behaviour of holomorphic curves in almost-complex* 4*-manifolds*, preprint Stony Brook, 1989.

[M.1] J. MILNOR - *A unique decomposition theorem for* 3*-manifolds*, Am. J. of Math. (1961), 1-7.

[M.2] J. MILNOR - *On the cobordian ring* Ω^* *and a complex analogue* I, Am. J. of Math. 82 (1960), 505-521.

[M.3] J. MILNOR - *Singular points of complex hypersurfaces*, Ann. Study n° 61, Princeton, 1968.

[H.M.] H. MORTON - *Closed braids representations for a link & its 2 variable polynomials*, preprint Liverpool, 1985.

[M.,W.] J. MOSER and S. WEBSTER - *Normal forms for real surfaces in* $\mathbf{C}^2$ *near complex tangents and hyperbolic surface transformations*, Acta Math. 150 (1983), 255-296.

[M.P.M.] M.-P. MULLER - *Une structure symplectique complète sur* $\mathbf{R}^6$ *avec une sphère lagrangienne plongée*, Thèse, IRMA Strasbourg, 1989.

[N.,W.] R. NIRENBERG et R.O. WELLS Jr. - *Approximation theorems on differentiable submanifolds of a complex manifold*, T.A.M.S. 142 (1969), 15-35.

[O.] K. OKA - *Sur les fonctions analytiques de plusieurs variables*, Iwanami Shoten, Tokyo, Japon (1961), 1983.

[L.P.] L.V. POLTEROVITCH - *The Maslov class of the Lagrange surfaces and Gromov's pseudo-holomorphic curves*, preprint Moscou, 1989.

[V.R.] V.A. ROKHLIN - *Two-dimensional submanifolds of* 4 *dim-manifolds*, Funct. Analysis Appl. 6 (1972), 136-138.

[L.R.] L. RUDOLPH - *Some topologically locally flat surfaces in the complex projective plane*, Comment. Math. Helv. 59 (1984), 592-599.

[C.V.] C. VITERBO - *A new obstruction to embedding Lagrangian tori*, Invent. Math. 100, 1989, 301-320.

[W.] A. WEINSTEIN - *Contact surgery and symplectic handlebodies*, preprint University of California, Berkeley, 1989.

Daniel BENNEQUIN

Université de Strasbourg
I.R.M.A.
CNRS LA 1
7, rue René Descartes
F-67084 STRASBOURG CEDEX

Astérisque

LUC ILLUSIE

Cohomologie de De Rham et cohomologie étale p-adique

Astérisque, tome 189-190 (1990), Séminaire Bourbaki,
exp. n° 726, p. 325-374

<http://www.numdam.org/item?id=SB_1989-1990__32__325_0>

© Société mathématique de France, 1990, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Séminaire BOURBAKI juin 1990
42ème année, 1989-90, n° 726

COHOMOLOGIE DE DE RHAM ET COHOMOLOGIE ÉTALE p-ADIQUE

[d'après **G. Faltings, J.-M. Fontaine et al.**]

par **Luc ILLUSIE**

Si X est un schéma propre et lisse sur $\mathbf{C}$, la théorie de l'intégration fournit un *isomorphisme de périodes*

$$H^*_{DR}(X/\mathbf{C}) \xrightarrow{\sim} H^*(X(\mathbf{C}), \mathbf{Q}) \otimes \mathbf{C},$$

où $H^*_{DR}(X/\mathbf{C}) = H^*(X, \Omega^{\cdot}_{X/\mathbf{C}})$ est la cohomologie de de Rham de $X/\mathbf{C}$ et $X(\mathbf{C})$ désigne l'espace analytique associé à X. La théorie des *périodes p-adiques*, à laquelle cet exposé est consacré, permet, si K est une extension finie de $\mathbf{Q}_p$ (plus généralement, un corps de caractéristique nulle, complet pour une valuation discrète, et de corps résiduel parfait de caractéristique $p > 0$), et si X est un schéma propre et lisse sur K, de construire des isomorphismes analogues reliant la cohomologie de de Rham de X/K, $H^*_{DR}(X/K) = H^*(X, \Omega^{\cdot}_{X/K})$, avec les diverses structures naturelles dont elle peut être munie, et la cohomologie étale p-adique $H^*(X_{\bar{K}}, \mathbf{Q}_p)$ (où $\bar{K}$ est une clôture algébrique de K), munie de l'opération du groupe de Galois $G = Gal(\bar{K}/K)$.

Ce sujet a une assez longue histoire. Le point de départ est l'article de Tate [70]. Tate considère le cas où X est une variété abélienne ayant bonne réduction (*i.e.* égale à la fibre générique d'un schéma abélien $\mathcal{X}$ sur l'anneau V des entiers de K). L'action de G sur $\bar{K}$ se prolonge par continuité au complété $\bar{K}^\wedge$. Tate calcule la cohomologie galoisienne continue de G à valeurs dans $\bar{K}^\wedge$ (et ses twists $\bar{K}^\wedge(i)$ par des puissances du

caractère cyclotomique), et par une étude du groupe p-divisible Γ associé à $\mathcal{X}$, construit un isomorphisme canonique, G-équivariant,

$$\left(H^1(X,\mathcal{O}_X)\otimes_K \bar{K}^\wedge\right)\oplus\left(H^0(X,\Omega^1_{X/K})\otimes_K \bar{K}^\wedge(-1)\right)$$
$$\xrightarrow{\sim} H^1(X_{\bar{K}},\mathbf{Q}_p)\otimes_{\mathbf{Q}_p}\bar{K}^\wedge$$

(où G agit diagonalement sur le membre de droite). Il conjecture de plus l'existence de décompositions analogues en tout degré, pour X un schéma propre et lisse arbitraire sur K (voir 2.1.3 pour un énoncé précis, et un historique de cette conjecture, dite *conjecture de Hodge-Tate*, qui a été finalement démontrée, en toute généralité, par Faltings [19]). Dans le cas qu'il considère, Tate montre en outre que le groupe p-divisible Γ est déterminé, à isogénie près, par la représentation de G sur $H^1(X_{\bar{K}},\mathbf{Q}_p)$. Dans la même situation, le groupe $H^1_{DR}(X/K)$ se trouve muni d'une structure plus riche qu'il n'y paraît de prime abord. En effet, en plus de la filtration par $H^0(X,\Omega^1_{X/K})$ (*filtration de Hodge*), $H^1_{DR}(X/K)$ est muni d'une K_0-structure naturelle (où K_0 est le corps des fractions de l'anneau des vecteurs de Witt $W(k)$ du corps résiduel k), à savoir $M\otimes_{W(k)}K_0$, où M est le module de Dieudonné de la fibre spéciale de Γ : cela résulte de l'interprétation "cristalline" de M donnée par Grothendieck (comme H^1 cristallin de $\mathcal{X}\otimes k$) ; cette K_0-structure $M\otimes_{W(k)}K_0$ est munie d'un automorphisme φ, semi-linéaire par rapport à l'automorphisme de Frobenius de K_0, déduit de l'opérateur F sur M. Grothendieck montre de plus ([36], [37]) que Γ est déterminé à isogénie près par $H^1_{DR}(X/K)$, muni de sa filtration de Hodge et de la K_0-structure précédente, avec son opérateur φ. Compte tenu du résultat de Tate mentionné plus haut, cela l'amène à poser la question (*loc. cit.*) (*problème du "foncteur mystérieux"*) de décrire un procédé algébrique permettant de passer directement de $H^1_{DR}(X/K)$ à $H^1(X_{\bar{K}},\mathbf{Q}_p)$ sans l'intermédiaire du groupe p-divisible Γ, et de généraliser ceci en dimension supérieure. Ce problème vient d'être, lui aussi, complètement résolu. Fontaine a réalisé le premier pas, décisif, en construisant une K_0-algèbre B_{cris}, munie de certaines structures additionnelles (action de G, opérateur semi-linéaire φ, filtration après extension des scalaires à K), permettant de définir un foncteur D_{cris} (D comme Dieudonné) de la catégorie des

représentations p-adiques de G vers la catégorie des "φ-modules filtrées sur K" (K-espaces vectoriels filtrés, munis d'une d'une K_0-structure, avec un endomorphisme semi-linéaire φ (voir 1.3.5) : Fontaine montre que ce foncteur résout le problème de Grothendieck pour le H^1, et propose une conjecture précise en dimension supérieure (la *conjecture* C_{cris}), pour les schémas X propres et lisses sur K ayant bonne réduction (voir 2.2.2). Grosso modo, cette conjecture exprime que la représentation de Galois $H^m(X_{\bar{K}}, \mathbf{Q}_p)$ et la cohomologie de de Rham $H^m_{DR}(X/K)$, munie de toutes ses structures (notamment la K_0-structure fournie par la cohomologie cristalline, en vertu d'un résultat de Berthelot-Ogus [6]), se déterminent mutuellement. Démontrée d'abord par Fontaine-Messing pour dim $X < p$ et $K = K_0$, elle a été prouvée en général par Faltings [20]. Pour les schémas X sur K propres et lisses, mais n'ayant pas nécessairement bonne réduction, Fontaine a formulé une variante de la conjecture C_{cris} , la *conjecture* C_{DR}, permettant de reconstituer $H^m_{DR}(X/K)$ à partir de $H^m(X_{\bar{K}}, \mathbf{Q}_p)$ (mais pas l'inverse), et impliquant la conjecture de Hodge-Tate : la conjecture C_{DR} a été également démontrée par Faltings [20]. Dans le cas où X/K a *réduction semi-stable* (voir 4.1.1), des discussions avec Jannsen (*cf.* [45]) ont conduit Fontaine à conjecturer l'existence d'un *opérateur de monodromie* N sur $H^m_{DR}(X/K)$, analogue au "résidu de la connexion de Gauss-Manin" pour les variétés complexes, et à formuler une conjecture plus fine que C_{DR}, la *conjecture* C_{st}, qui affirme que dans ce cas, comme dans le cas de bonne réduction, $H^m_{DR}(X/K)$ et $H^m(X_{\bar{K}}, \mathbf{Q}_p)$ se déterminent mutuellement. L'opérateur N a été construit par Hyodo-Kato [40], et la conjecture C_{st} a été prouvée par Kato pour 2 dim $X < p - 1$ [48] ; le séminaire de Fontaine [Bures] a été consacré à ce sujet.

La théorie présentée ici a déjà de nombreuses applications. Nous en signalons — très brièvement — quelques-unes en 2.2, 2.3 et 2.4.

Ce rapport recoupe [29]. Le lecteur trouvera dans [29] de plus amples développements sur les représentations p-adiques et sur les motivations de la théorie de Hyodo-Kato, ainsi qu'un aperçu de quelques applications arithmétiques globales, dues à Fontaine-Mazur [32], et dont nous ne parlerons pas.

Jean-Pierre Wintenberger m'a beaucoup aidé dans la préparation de

cet exposé, je l'en remercie vivement. Je remercie également Spencer Bloch, Gerd Faltings, Jean-Marc Fontaine et Jean-Pierre Serre pour d'utiles commentaires et suggestions.

SOMMAIRE

0. Notations

1. Les anneaux de Fontaine et les divers types de représentations p-adiques
   1.1. Représentations ℓ-adiques
   1.2. Les anneaux de Fontaine
   1.3. Les divers types de représentations p-adiques

2. Les conjectures C_{cris}, C_{DR}, C_{HT}
   2.1. Les conjectures C_{DR} et C_{HT}
   2.2. La conjecture C_{cris}
   2.3. Cycles de Hodge absolus
   2.4. Nombres de Tamagawa de motifs

3. La méthode de Faltings ([19], [20])
   3.1. Plan
   3.2. Revêtements presque étales et extensions absorbant la ramification
   3.3. Cohomologie galoisienne et différentielles : calculs locaux
   3.4. Globalisation : cycles évanescents cohérents
   3.5. Cycles évanescents discrets et cycles évanescents cohérents
   3.6. Variantes et compléments
      3.6.1. La conjecture C_{cris}
      3.6.2. La conjecture C_{DR}

4. La conjecture C_{st}
   4.1. L'opérateur de monodromie de Hyodo-Kato
   4.2. La méthode de Fontaine-Messing-Kato

0. NOTATIONS

V : anneau de valuation discrète complet
K : corps des fractions de V, supposé de caractéristique 0
k : corps résiduel de V, supposé parfait de caractéristique $p > 0$
S : $\operatorname{Spec} V$, $s = \operatorname{Spec} k$, $\eta = \operatorname{Spec} K$
$\bar{K}$: une clôture algébrique de K ; $\bar{\eta} = \operatorname{Spec} \bar{K}$; $G = \operatorname{Gal}(\bar{K}/K)$
$\bar{V}$: normalisé de V dans $\bar{K}$; $\bar{S} = \operatorname{Spec} \bar{V}$
$\mathfrak{m}$: idéal maximal de $\bar{V}$; $\bar{k} = \bar{V}/\mathfrak{m}$; $\bar{s} = \operatorname{Spec} \bar{k}$
$\bar{V}^\wedge$: $\varprojlim \bar{V}/p^n\bar{V}$
$\bar{K}^\wedge$: $\bar{V}^\wedge[1/p]$: complété p-adique de $\bar{K}$
$\mathfrak{m}^\wedge$: idéal maximal de $\bar{V}^\wedge$
W : $W(k)$; $K_0 = W[1/p]$; σ : l'automorphisme de Frobenius de K_0
W_n : W/p^nW
A/p^n : A/p^nA

1. LES ANNEAUX DE FONTAINE ET LES DIVERS TYPES DE REPRÉSENTATIONS p-ADIQUES

Nous ne donnerons qu'un résumé succinct de la théorie. Pour plus de détails, nous renvoyons le lecteur à [29] et [Bures].

1.1. Représentations ℓ-adiques

Soit ℓ un nombre premier $\neq p$. Par une *représentation ℓ-adique* de G, on entend un $\mathbf{Q}_\ell$-espace vectoriel H de dimension finie munie d'une action linéaire continue de G. On dit que la représentation H est *non ramifiée* si l'inertie I agit trivialement. C'est le cas par exemple si $H = H^n(X_{\bar{\eta}}, \mathbf{Q}_\ell)$, où X est un schéma propre et lisse sur V. Si le corps résiduel k n'est pas trop gros, par exemple si k est fini ou plus généralement si aucune extension finie de k ne contient toutes les racines de l'unité d'ordre une puissance de ℓ, on dispose d'un théorème de structure général, le *théorème de monodromie locale* de Grothendieck [68, Appendice] : si $\rho : G \to GL(H)$ est une représentation ℓ-adique, ρ est *quasi-unipotente*, ce qui signifie qu'il existe un sous-groupe ouvert I_1 de I tel que $\rho(s)$ soit unipotent pour tout

$s \in I_1$. Il en résulte que la restriction de ρ à I_1 se factorise à travers le quotient ℓ-adique modéré $t_\ell : I \to \mathbf{Z}_\ell(1)(\bar{k})$, et qu'il existe un unique homomorphisme nilpotent (le "*logarithme de la monodromie*")

$$N : H(1) \to H$$

tel que $\rho(s)x = \exp(Nt_\ell(s))x$ pour tout $s \in I_1$. L'homomorphisme N est G-équivariant : en particulier, si $k = \mathbf{F}_q$ et $F \in G$ relève un Frobenius géométrique de $\mathrm{Gal}(\bar{k}/k)$, on a

$$NF = qFN. \tag{1.1.1}$$

Sans hypothèse sur k, les représentations ℓ-adiques qu'on rencontre en pratique sont quasi-unipotentes : il en est ainsi de $H^n(X_{\bar{\eta}}, \mathbf{Q}_\ell)$ et $H^n_c(X_{\bar{\eta}}, \mathbf{Q}_\ell)$ pour X_η de type fini sur η ((SGA 7 1) et (SGA $4\frac{1}{2}$ Th. finitude)).

On définit de même la notion de représentation p-adique de G. Elles forment une catégorie beaucoup plus vaste et mystérieuse que celle des représentations ℓ-adiques. Si X est propre et lisse sur S, les représentations $H^n(X_{\bar{\eta}}, \mathbf{Q}_p)$ peuvent être très ramifiées. D'autre part, les représentations p-adiques ne sont pas en général quasi-unipotentes : dans [54], Mazur, Tate et Teitelbaum construisent des formes modulaires sous $\Gamma_0(p)$, de poids $k \geq 3$, pour lesquelles la représentation p-adique associée, $G \to GL_2(\mathbf{Q}_p)$ est irréductible alors que la représentation ℓ-adique admet un N non trivial. La théorie de Fontaine, qu'on va exposer maintenant, permet néanmoins de dégager des classes importantes de représentations p-adiques, et aussi de formuler un analogue, pour l'instant conjectural, du théorème de monodromie locale ℓ-adique (4.2.4).

1.2. Les anneaux de Fontaine

Fontaine construit des anneaux ("B" pour "Barsotti" ou "bivecteurs"$\cdots$)

$$B_{cris}(V) \subset B_{st}(V) \subset B_{DR}(V) \quad , \quad B_{HT}(V),$$

qui sont des K_0-algèbres munies de structures additionnelles. Quand il n'y aura pas de risque de confusion, nous omettrons V de la notation.

1.2.1. *B_{DR} et B_{HT}*

Commençons par le plus gros, B_{DR}, qui est aussi le plus aisé à décrire. Soit A la limite projective de N copies de $\bar{V}/p\bar{V}$ suivant le Frobenius $x \mapsto x^p$. C'est une k-algèbre parfaite. Soit

$$\theta : W(A) \to \bar{V}^{\wedge} \tag{1.2.1.1}$$

l'homomorphisme associant à un vecteur de Witt $(a_0, a_1, \cdots)$ la limite, pour $m \to \infty$, de $b_{0m}^{p^m} + pb_{1m}^{p^{m-1}} + \cdots + p^m b_{mm}$, où $a_n \in A$ est écrit comme une suite $(a_{nm}, m \geq 0)$ avec $a_{nm} = a_{n,m+1}^p$ et $b_{nm} \in \bar{V}$ relève a_{nm}. L'homomorphisme θ est surjectif et son noyau est un idéal principal. Il en est de même de l'homomorphisme de K-algèbres qui s'en déduit :

$$\theta_K : W(A) \otimes_{W(k)} K \to \bar{K}^{\wedge}. \tag{1.2.1.2}$$

On pose

$$B_{DR}^{+}(V) = \varprojlim (W(A) \otimes_{W(k)} K)/(\operatorname{Ker} \theta_K)^n \quad , \quad B_{DR}(V) = \operatorname{Frac} B_{DR}^{+}(V).$$

La K-algèbre B_{DR} est un corps de valuation discrète complet, d'anneau d'entiers B_{DR}^{+}, et de corps résiduel $\bar{K}^{\wedge}$. Le groupe de Galois G opère continûment sur B_{DR}. Soit $(z_n \in \mu_{p^n}(\bar{K}), n \geq 0)$ un générateur de $\mathbf{Z}_p(1)$, d'image $\bar{z}$ dans A. La série

$$\log([\bar{z}]) = \sum_{n \geq 1} (-1)^{n-1} ([\bar{z}] - 1)^n / n,$$

où $[\,]$ désigne le représentant de Teichmüller, converge dans B_{DR}^{+} vers un élément t, qui est une *uniformisante*. On obtient ainsi un plongement, G-équivariant :

$$\mathbf{Z}_p(1) \to B_{DR}^{+} \quad , \quad z \mapsto t.$$

Soit Fil la filtration t-adique de B_{DR}, *i.e.* $\operatorname{Fil}^i B_{DR} = t^i B_{DR}^{+}$, $(i \in \mathbf{Z})$. On a un isomorphisme G-équivariant :

$$\operatorname{gr} B_{\mathrm{DR}} = \bigoplus_{i \in \mathbf{Z}} \bar{K}^{\wedge}(i),$$

où gr est le gradué associé. On note parfois B_{HT} cette dernière algèbre.

1.2.2. *L'anneau B_{cris}*

Soit I l'idéal noyau de l'homomorphisme θ (1.2.1.1). Notons

$$B^+(V) = D_I(W(A))^\wedge$$

l'enveloppe à puissances divisées, p-complétée, de I dans $W(A)$ (*cf.* [4] ou [5]). C'est une $W(k)$-algèbre. Avec les notations précédentes, on a $t \in B^+$ et l'on vérifie que $t^{p-1} \in pB^+$. On pose :

$$B^+_{cris}(V) = B^+(V)[1/p] \subset B_{cris}(V) = B^+(V)[1/t].$$

Ce sont des K_0-algèbres sur lesquelles G opère continûment. L'automorphisme de Frobenius φ de $W(A)$ se prolonge en un automorphisme σ-linéaire φ de B_{cris} tel que $\varphi t = pt$. Enfin, l'application naturelle $W(A) \to B^+_{DR}$ se prolonge en une injection, G-équivariante :

$$B_{cris} \otimes_{K_0} K \to B_{DR}.$$

Elle induit un isomorphisme sur les gradués associés pour la filtration Fil de B_{DR} et la filtration induite, notée aussi Fil.

L'anneau B_{cris} — ou plutôt les anneaux B^+/p^n — ont une interprétation cristalline, qui "explique" leur rôle dans les théorèmes de comparaison : on a des isomorphismes

$$B^+/p^n \xrightarrow{\sim} H^*_{cris}(\mathrm{Spec}\,(\bar{V}/p\bar{V})/\mathrm{Spec}\,W_n),$$

compatibles aux actions naturelles de G et φ [25, §3].

Il est clair sur la définition que B_{cris} ne dépend que de W, plus précisément que $B_{cris}(W) \xrightarrow{\sim} B_{cris}(V)$. On peut montrer que, de même, $B_{DR}(W) \xrightarrow{\sim} B_{DR}(V)$. En particulier, $B^+_{DR}(V)$ contient $\bar{K}$. On peut montrer que $\bar{K}$ est dense dans $B^+_{DR}(V)$ (pour la topologie "canonique", moins fine que celle définie par la valuation) [P. Colmez, Le corps des périodes p-adiques, CRAS 310 (1990), 321-324].

1.2.3. *L'anneau B_{st}*

Soit π une uniformisante de V. Soit $x = (x_n, n \geq 0)$ une suite d'éléments de $\bar{V}$ tels que $x_n = x_{n+1}^p$ et $x_0 = \pi$; soit $\bar{x}$ son image dans A. On a $[\bar{x}] \otimes \pi^{-1} \in 1 + \operatorname{Ker} \theta_K$ (1.2.1.2), ce qui permet de définir :

$$u = \log([\bar{x}] \otimes \pi^{-1}) \in B_{DR}^+.$$

On note B_{st}^+ (resp. B_{st}) le sous-anneau de B_{DR} engendré par B_{cris}^+ (resp. B_{cris}) et u. Il dépend de π, mais non du choix de x. Fontaine montre [27] que u est transcendant sur B_{cris}, de sorte que B_{st}^+ (resp. B_{st}) est une algèbre de polynômes à une indéterminée sur B_{cris}^+ (resp. B_{cris}) (pour une meilleure définition de B_{st}, comme solution d'un problème universel, voir [29] et [27]). B_{st} est stable par G dans B_{DR}. On prolonge φ à B_{st} en posant $\varphi(u) = pu$. Enfin, on définit un opérateur de monodromie

$$N \ : \ B_{st} \to B_{st},$$

comme l'unique B_{cris}-dérivation telle que $Nu = 1$. On a, par construction,

$$N\varphi = p\varphi N$$

(à rapprocher de (1.1.1)). L'application naturelle

$$B_{st} \otimes_{K_0} K \to B_{DR}$$

est injective. On note encore Fil la filtration induite. On a $u \in \operatorname{Fil}^1$.

1.2.4. *Propriétés des anneaux B*

a) On a

$$H^0(G, B_{HT}) = H^0(G, B_{DR}) = K \quad , \quad H^0(G, B_{cris}) = H^0(G, B_{st}) = K_0.$$

Cela découle des résultats de Tate [70,§3] sur le calcul de $H^0(G, \bar{K}\hat{}(i))$, *cf.* 3.2.1.

b) On a

$$B_{cris} = \operatorname{Ker} N : B_{st} \to B_{st}$$

$$\mathbf{Q}_p = \left\{ x \in B_{cris} \,|\, \varphi x = x\,,\ x \otimes 1 \in \mathrm{Fil}^0 \right\}.$$

1.3. Les divers types de représentations p-adiques

La construction de base est la suivante. Notons $\mathrm{Rep}_{\mathbf{Q}_p}(G)$ la catégorie des représentations p-adiques de G (ses objets sont les $\mathbf{Q}_p$-espaces vectoriels de dimension finie munis d'une action linéaire continue de G, les flèches les applications linéaires G-équivariantes). Soit i l'un des symboles *cris*, *st*, *DR*, *HT*. Pour $E \in \mathrm{Rep}_{\mathbf{Q}_p}(G)$, Fontaine définit :

$$D_i(E) = \left(B_i \otimes_{\mathbf{Q}_p} E\right)^G \tag{1.3.1}$$

("D" comme "Dieudonné"). C'est un espace vectoriel sur $K_i = B_i^G$ ($K_i = K_0$ si $i = cris$ ou $st, K_i = K$ sinon), de dimension $\leq \dim E$: d'après les résultats de Tate cités ci-dessus, l'application naturelle

$$a_i : B_i \otimes_{K_i} D_i(E) \longrightarrow B_i \otimes_{\mathbf{Q}_p} E \tag{1.3.2}$$

est injective ; on a d'ailleurs $\dim_{K_i} D_i(E) = \dim_{\mathbf{Q}_p}(E)$ si et seulement si a_i est bijective. On dit que la représentation est *cristalline, semi-stable, de de Rham, de Hodge-Tate* si l'application a_i correspondante est bijective. Il est clair que :

$$\text{cristalline} \Longrightarrow \text{semi-stable} \Longrightarrow \text{de de Rham} \Longrightarrow \text{de Hodge-Tate}.$$

1.3.3. La première classe de représentations à avoir été étudiée est celle des représentations de Hodge-Tate, à la suite du travail de Tate [70], *cf.* les rapports de Serre [63], [66]. Une représentation E est de Hodge-Tate si et seulement si la représentation $\bar{K}^\wedge \otimes_{\mathbf{Q}_p} E$ (G agissant diagonalement) est somme (nécessairement directe) de représentations de la forme $\bar{K}^\wedge(i)$, $i \in \mathbf{Z}$. Pour E de dimension 1, donnée par un caractère $\rho : G \to \mathbf{Q}_p^*$, il découle des résultats de Tate (*loc. cit.*) que E est de Hodge-Tate si et seulement si la restriction de ρ à un sous-groupe ouvert du groupe d'inertie I coïncide avec une puissance du caractère cyclotomique $\chi : G \to \mathbf{Z}_p^*$ (donnant l'action de G sur $\mathbf{Z}_p(1)$). Pour toute représentation $\rho : G \to GL(E)$ de Hodge-Tate, le sous-groupe (compact) $\rho(I)$, image de l'inertie, est *ouvert* dans son

adhérence de Zariski $\rho(I)^{\mathrm{alg}}$ (*cf.* [62], [66]). Le type cristallin correspond à des propriétés plus fortes : pour E de dimension 1, E est cristalline si et seulement si la restriction du caractère correspondant à toute l'inertie est une puissance de χ. Pour E de dimension quelconque, si E est cristalline, alors $\rho(I)^{\mathrm{alg}}$ est *connexe*, d'après un résultat de Fontaine [22] (ceci est encore vrai, d'ailleurs, si E est semi-stable [28]).

1.3.4. Soit X un schéma propre et plat sur $S = \operatorname{Spec} V$, de fibre générique X_η lisse. Les résultats essentiels de la théorie (conjecturés par Fontaine, prouvés dans le cas général par Faltings, voir §2 pour des énoncés précis) sont que :

i) $H^*(X_{\bar\eta}, \mathbf{Q}_p)$, comme représentation de G, est de de Rham, et $D_{DR}(H^*(X_{\bar\eta}, \mathbf{Q}_p))$ est la cohomologie de de Rham de $X_{\bar\eta}$ sur η ;

ii) si X est lisse sur S, $H^*(X_{\bar\eta}, \mathbf{Q}_p)$ est cristalline et $D_{cris}(H^*(X_{\bar\eta}, \mathbf{Q}_p))$ est la cohomologie cristalline de X_s sur $W(k)$, tensorisée avec K_0.

Il y a aussi une conjecture pour le cas semi-stable, voir §4.

1.3.5. Pour $i = cris$, st ou DR, les $D_i(E)$ héritent de structures additionnelles importantes, qui méritent une étude indépendante. Observées d'abord sur la cohomologie de de Rham ou la cohomologie cristalline, elles sont d'ailleurs à l'origine de la définition des anneaux B.

Pour $E \in \mathrm{Rep}_{Q_p}(G)$, $D_{DR}(E)$ (resp. $D_{HT}(E)$) est, de façon naturelle, un K-espace vectoriel filtré (resp. gradué) (et $\operatorname{gr} D_{DR}(E) \subset D_{HT}(E)$). Cette structure est trop faible pour qu'on puisse espérer, lorsque E est de de Rham (resp. de Hodge-Tate), récupérer E à partir d'elle à l'aide de l'isomorphisme (1.3.2). Il en va différemment avec les représentations cristallines ou semi-stables.

Fontaine définit un (φ, N)-*module filtré sur* K comme un K_0-espace vectoriel M, muni d'une application σ-linéaire injective $\varphi : M \to M$, d'une application K_0-linéaire $N : M \to M$ telle que $N\varphi = p\varphi N$, et d'une filtration décroissante $\mathrm{Fil}^{\cdot} M_K$ sur $M_K := K \otimes_{K_0} M$, formée de sous-K-espaces vectoriels, telle que $\cup \mathrm{Fil}^i M_K = M_K$ et $\cap \mathrm{Fil}^i M_K = 0$. Les (φ, N)-modules filtrés sur K forment, de manière évidente, une catégorie additive $\mathrm{MF}_K(\varphi, N)$. Quand $N = 0$, on dit simplement φ-*module filtré*, et l'on note MF_K la sous-catégorie pleine correspondante. Pour $E \in \mathrm{Rep}_{\mathbf{Q}_p}(G)$,

$D_{st}(E)$ (resp. $D_{cris}(E)$) est, de façon naturelle, objet de $\mathrm{MF}_K(\varphi, N)$ (resp. MF_K): φ et N proviennent de φ et N sur B_{st}, et la filtration de la filtration Fil sur B_{DR} via l'inclusion $K \otimes_{K_0} D_{st}(E) \subset D_{DR}(E)$ (resp. $K \otimes_{K_0} D_{cris}(E) \subset D_{DR}(E)$). L'énoncé suivant découle facilement des propriétés des anneaux B (1.2.4) :

PROPOSITION 1.3.6.— *Notons* $\mathrm{Rep}_{st}(G)$ *(resp.* $\mathrm{Rep}_{cris}(G)$*) la sous-catégorie pleine de* $\mathrm{Rep}_{\mathbf{Q}_p}(G)$ *formée des représentations semi-stables (resp. cristallines). Alors le foncteur* D_{st} *(resp.* D_{cris}*) induit un foncteur pleinement fidèle* :

$$D_{st} : \mathrm{Rep}_{st}(G) \longrightarrow \mathrm{MF}_K(\varphi, N) \qquad (\text{resp. } D_{cris} : \mathrm{Rep}_{cris}(G) \longrightarrow \mathrm{MF}_K).$$

1.3.7. Nous dirons qu'un (φ, N)-module filtré M sur K et une représentation semi-stable E sont *associés* si l'on a $M \simeq D_{st}(E)$. Il revient au même de dire qu'on a un isomorphisme

$$\alpha : B_{st} \otimes_{K_0} M \xrightarrow{\sim} B_{st} \otimes_{\mathbf{Q}_p} E$$

compatible aux diverses structures des deux membres (sur le membre de gauche, φ opère par $\varphi \otimes \varphi$, N par $N \otimes 1 + 1 \otimes N$, $g \in G$ par $g \otimes 1$, et Fil, après extension des scalaires à K, est donné par la filtration produit tensoriel ; sur le membre de droite, φ opère par $\varphi \otimes 1$, N par $N \otimes 1$, $g \in G$ par $g \otimes g$, et Fil provient de la filtration de $K \otimes_{K_0} B_{st}$). Grâce à α, M et E se déterminent mutuellement :

$$M \simeq D_{st}(E) \left(= \left(B_{st} \otimes_{\mathbf{Q}_p} E\right)^G \right),$$
$$E \simeq \left\{ x \in B_{st} \otimes_{K_0} M \,\middle|\, Nx = 0\,,\ \varphi x = x\,,\ 1 \otimes x \in \mathrm{Fil}^0 \right\}.$$

De même, un φ-module filtré M sur K et une représentation cristalline E sont dits associés si l'on a $M \simeq D_{cris}(E)$, ce qui revient encore à dire qu'on a un isomorphisme

$$\alpha : B_{cris} \otimes_{K_0} M \xrightarrow{\sim} B_{cris} \otimes_{\mathbf{Q}_p} E$$

compatible aux diverses structures, et grâce auquel M et E se déterminent mutuellement :

$$M \simeq D_{cris}(E) \left(= \left(B_{cris} \otimes_{\mathbf{Q}_p} E\right)^G\right),$$

$$E \simeq \left\{x \in B_{cris} \otimes_{K_0} M \,\middle|\, \varphi x = x\,,\ 1 \otimes x \in \mathrm{Fil}^0\right\}.$$

Nous renvoyons à [28] et [29] pour une description conjecturale de l'image essentielle de D_{st} (resp. D_{cris}) (1.3.6) ("(φ, N)-modules filtrés faiblement admissibles").

2. LES CONJECTURES C_{cris}, C_{DR}, C_{HT}

Ces "conjectures" sont en fait, désormais, des théorèmes de Faltings [19], [20].

2.1. Les conjectures C_{DR} et C_{HT}

2.1.1. Soit X un schéma propre et lisse sur K. La cohomologie de de Rham de X, $H^*_{DR}(X/K) := H^*(X, \Omega^{\cdot}_{X/K})$, est l'aboutissement de la suite spectrale de Hodge,

$$E_1^{ij} = H^j(X, \Omega^i_{X/K}) \Longrightarrow H^*_{DR}(X/K),$$

qui, par la théorie de Hodge, dégénère en E_1 (voir [17] pour une démonstration algébrique élémentaire). Elle est munie de la filtration aboutissement, dite *filtration de Hodge*, $\mathrm{Fil}^{\cdot} H^*_{DR}(X/K)$, de gradué associé $\mathrm{gr}^i H^m_{DR}(X/K) = H^{m-i}(X, \Omega^i)$. Elle se relie à la cohomologie étale p-adique de $X_{\bar{\eta}}$ $(= X_{\bar{K}})$, $H^*(X_{\bar{\eta}}, \mathbf{Q}_p)$, munie de l'action naturelle de G, par le résultat suivant de Faltings, conjecturé par Fontaine [23] :

THÉORÈME 2.1.2 [20] (*conjecture C_{DR}*).— *La représentation $H^*(X_{\bar{\eta}}, \mathbf{Q}_p)$ est de de Rham, et il existe un isomorphisme fonctoriel (de K-modules filtrés)*
$H^*_{DR}(X/K) \xrightarrow{\sim} D_{DR}\left(H^*\left(X_{\bar{\eta}}, \mathbf{Q}_p\right)\right)$ (1.3.2). *En d'autres termes, il existe un isomorphisme fonctoriel*

$$\alpha_{DR} : B_{DR} \otimes_K H^*_{DR}(X/K) \xrightarrow{\sim} B_{DR} \otimes_{\mathbf{Q}_p} H^*\left(X_{\bar{\eta}}, \mathbf{Q}_p\right),$$

compatible aux actions de G et aux filtrations naturelles des deux membres.

L'isomorphisme α_{DR} défini par Faltings est, en outre, compatible à la dualité de Poincaré et à la formation des classes de cycles et classes de Chern. Prenant le gradué associé, on en déduit :

COROLLAIRE 2.1.3. (*conjecture C_{HT}* ou *de Hodge-Tate*).— *Posons $H^*_{Hdg}(X/K) = \mathrm{gr}\, H^*_{DR}(X/K)$ $(= \oplus H^{*-i}(X, \Omega^i))$. La représentation $H^*(X_{\bar\eta}, \mathbf{Q}_p)$ est de Hodge-Tate, et il existe un isomorphisme fonctoriel (de K-modules gradués) $H^*_{Hdg}(X/K) \xrightarrow{\sim} D_{HT}(H^*(X_{\bar\eta}, \mathbf{Q}_p))$. En d'autres termes, il existe un isomorphisme fonctoriel*

$$\alpha_{HT} : B_{HT} \otimes_K H^*_{Hdg}(X/K) \xrightarrow{\sim} B_{HT} \otimes_{\mathbf{Q}_p} H^*(X_{\bar\eta}, \mathbf{Q}_p), \tag{2.1.3.1}$$

compatible aux actions de G et aux graduations naturelles des deux membres.

Cet isomorphisme équivaut encore à la donnée, pour tout m, d'un isomorphisme G-équivariant

$$\alpha_{HT} : \bigoplus_{i \in \mathbf{Z}} H^{m-i}(X, \Omega^i) \otimes_K \bar K\hat{}(-i) \xrightarrow{\sim} H^m(X_{\bar\eta}, \mathbf{Q}_p) \otimes \bar K\hat{} \tag{2.1.3.2}$$

("*décomposition de Hodge-Tate*").

L'existence de telles décompositions avait été conjecturée par Tate dans son séminaire au Collège de France [64], et, comme on l'a rappelé dans l'introduction, démontrée par lui, dans le cas des variétés abéliennes ayant bonne réduction [70]. Sa démonstration fut étendue peu après par Raynaud au cas de mauvaise réduction à l'aide du théorème de réduction semi-stable [SGA 7 IX] (voir [9] pour une présentation des arguments de Raynaud). Pendant plus de dix ans, il n'y eut aucun progrès sur ces questions. Puis, dans [24], Fontaine donna une nouvelle démonstration des résultats de Tate et Raynaud, et à peu près au même moment, Bloch et Kato [7] prouvèrent l'existence d'une décomposition de Hodge-Tate en tout degré m, mais dans le cas où X a bonne réduction *ordinaire*, ce qui signifie que X est la fibre générique d'un schéma propre et lisse $\mathcal{X}$ sur S dont la fibre spéciale Y vérifie $H^*(Y, d\Omega^i_Y) = 0$ pour tout i : leur méthode, consistant à analyser la "suite spectrale des cycles évanescents"

$$E_2^{ij} = H^i(\mathcal{X}_{\bar s}, R^j\Psi(\mathbf{Z}/p^n)) \Longrightarrow H^*(X_{\bar\eta}, \mathbf{Z}/p^n), \tag{2.1.3.3}$$

fournit de plus, dans ce cas, une filtration décroissante, G-équivariante, sur $H^m(X_{\bar{\eta}}, \mathbf{Q}_p)$, de gradué $\mathrm{gr}^{m-i}H^m = H^{m-i,i}(-i)$, où $H^{m-i,i}$ est une représentation non ramifiée. La conjecture de Hodge-Tate fut ensuite démontrée dans le cas général par Faltings [19], alors qu'indépendamment, et presque simultanément, Fontaine et Messing en obtenaient une démonstration dans le cas de bonne réduction (avec certaines restrictions supplémentaires) comme conséquence de la conjecture C_{cris}, voir ci-dessous. La méthode de Faltings (voir n° 3) s'inspire des calculs de Tate [70]. Elle lui a permis, récemment, de prouver aussi la conjecture plus forte C_{DR} [20].

2.2. La conjecture C_{cris}

2.2.1. Soit X un schéma propre et lisse sur K, ayant *bonne réduction, i.e.* tel qu'il existe $\mathcal{X}$ propre et lisse sur S, de fibre générique X. La cohomologie de de Rham de X sur K possède alors une K_0-structure naturelle : d'après un théorème de Berthelot-Ogus [6], il existe en effet un isomorphisme canonique

$$H^*(Y/W) \otimes_W K \xrightarrow{\sim} H^*_{DR}(X/K), \tag{2.2.1.1}$$

où $Y = \mathcal{X}_s$ est la fibre spéciale de $\mathcal{X}$ et $H^*(Y/W)$ désigne la cohomologie cristalline de Y par rapport à W ([4] ; pour une introduction à la cohomologie cristalline, voir [41] ou [42]). De plus, l'endomorphisme de Frobenius absolu de Y induit un endomorphisme σ-linéaire bijectif φ de $H^*_{cris}(X) := H^*(Y/W) \otimes_W K_0$. Le K-espace vectoriel $H^m_{DR}(X/K)$, muni d'une part de la filtration de Hodge Fil (2.1.1), d'autre part de la K_0-structure $H^m_{cris}(X)$ et de φ, est donc un φ-module filtré (1.3.5). Le résultat suivant montre que cette dernière structure ne dépend en fait que de X (et non du modèle $\mathcal{X}$), ce qui avait été d'ailleurs vérifié antérieurement par Gillet et Messing [34] :

THÉORÈME 2.2.2 [20] (*conjecture C_{cris}*).— *Sous les hypothèses de* 2.2.1, *la représentation $H^*(X_{\bar{\eta}}, \mathbf{Q}_p)$ est cristalline, et canoniquement associée* (1.3.7) *au φ-module filtré $H^*_{DR}(X/K)$ défini ci-dessus : il existe un isomorphisme fonctoriel*

$$\alpha_{cris} : B_{cris} \otimes_{K_0} H^*_{cris}(X) \xrightarrow{\sim} B_{cris} \otimes_{\mathbf{Q}_p} H^*(X_{\bar{\eta}}, \mathbf{Q}_p)$$

compatible aux structures naturelles des deux membres (action de G, φ, et filtrations après extension des scalaires à K).

Comme l'isomorphisme α_{DR} plus haut , l'isomorphisme α_{cris} construit par Faltings est compatible à la dualité de Poincaré et à la formation des classes de Chern et classes de cycles.

La conjecture C_{cris}, formulée, comme C_{DR}, par Fontaine dans [23], a d'abord été démontrée par Fontaine et Messing [31] dans le cas où $\dim X < p$ et $K = K_0$. La démonstration donnée par Faltings est, là encore, une adaptation de la méthode qu'il avait suivie pour C_{HT} [19] (voir n° 3). La méthode de Fontaine-Messing est toute différente ; nous en dirons quelques mots au n° 4.

Le théorème 2.2.2 a de nombreuses applications, détaillées dans [31]. Parmi les plus frappantes, citons :

a) la preuve de la *conjecture de l'inertie modérée* de Serre [65, 1.13, p. 278], donnant l'action de l'inertie modérée $\prod_{\ell \neq p} \mathbf{Z}_\ell(1)(\bar{k})$ sur la représentation semi-simplifiée de H/pH, où H est un réseau de $H^*(X_{\bar{\eta}}, \mathbf{Q}_p)$ stable sous G ;

b) une généralisation du théorème de non existence de schémas abéliens sur $\operatorname{Spec} \mathbf{Z}$ non triviaux ([1], [26]) : *si X est un schéma propre et lisse sur $\mathbf{Q}$ ayant partout bonne réduction, alors $H^j(X, \Omega^i) = 0$ pour $i \neq j$ et $i + j \leq 3$* (en particulier, si $\dim X \leq 3$, toute la cohomologie de X est algébrique) [J.-M. Fontaine, Lettre à W. Messing du 15.1.86, à paraître dans Indo-French conf. on geometry, Bombay (1989)], [V.-A. Abrashkin, Modificatsia functora Fontaine-Laffaille, Izv. Akad. Nauk., seria mat. 53 (1989), 451-497]) ; la démonstration combine en fait un raffinement de 2.2.2 relatif à l'action de G sur H/p^nH (H comme en a)) et des minorations de discriminants à la Odlyzko-Poitou-Serre.

2.3. Cycles de Hodge absolus

2.3.1. Supposons que K soit le complété d'un corps de nombres $\mathcal{K}$ en une place $\mathfrak{p}$. Soit $\bar{\mathcal{K}}$ une clôture algébrique de $\mathcal{K}$, choisissons des plongements $\bar{\mathcal{K}} \to \bar{K}$ (ce qui identifie $G = \operatorname{Gal}(\bar{K}/K)$ à un groupe de décomposition de $\operatorname{Gal}(\bar{\mathcal{K}}/\mathcal{K})$) et $t : \bar{\mathcal{K}} \to \mathbf{C}$. Si $\mathcal{X}$ est un schéma propre et lisse sur $\mathcal{K}$, notons

X et X_t les schémas sur K et $\mathbf{C}$ respectivement obtenus par extension des scalaires via l'inclusion naturelle et t. La cohomologie de de Rham $H^m_{DR}(\mathcal{X}/\mathcal{K})$ et la "cohomologie de Betti" $H^m_B(X_t) := H^m(X_t(\mathbf{C}), \mathbf{Q})$ sont alors reliées par deux types d'*isomorphismes de périodes.*

a) *Périodes classiques.* La théorie de l'intégration classique fournit un isomorphisme canonique :

$$\alpha_{B,t} : H^m_{DR}(\mathcal{X}/\mathcal{K}) \otimes_{\mathcal{K},t} \mathbf{C} \xrightarrow{\sim} H^m_B(X_t) \otimes_{\mathbf{Q}} \mathbf{C}.$$

(Quand il n'en pourra résulter de confusion, nous écrirons α_B au lieu de $\alpha_{B,t}$.)

b) *Périodes p-adiques.* On a $H^m_{DR}(X/K) \simeq H^m_{DR}(\mathcal{X}/\mathcal{K}) \otimes_{\mathcal{K}} K$. D'autre part, en vertu du théorème de changement de base propre (SGA 4 XII) et du théorème de comparaison entre cohomologie étale et cohomologie classique (SGA 4 XI), on a des isomorphismes canoniques (déduits de $\bar{\mathcal{K}} \to \bar{K}$ et t)

$$H^m(X_{\bar{K}}, \mathbf{Q}_p) \xrightarrow{\sim} H^m(X_t, \mathbf{Q}_p) \xrightarrow{\sim} H^m_B(X_t) \otimes \mathbf{Q}_p.$$

Grâce à ces isomorphismes, l'isomorphisme α_{DR} de 2.1.2 se récrit

$$\alpha_{DR} : H^m_{DR}(\mathcal{X}/\mathcal{K}) \otimes_{\mathcal{K}} B_{DR} \xrightarrow{\sim} H^m_B(X_t) \otimes_{\mathbf{Q}} B_{DR}.$$

Plus généralement, soient $\mathcal{X} = (\mathcal{X}_1, \cdots, \mathcal{X}_N)$ une famille finie de schémas propres et lisses sur $\mathcal{K}$, et $T = T_{DR}(\mathcal{X}/\mathcal{K})$ (resp. $T_B(X_t)$) une "construction tensorielle", donnée par $H^{a_1}_{DR}(\mathcal{X}_1/\mathcal{K}) \otimes \cdots \otimes H^{a_N}_{DR}(\mathcal{X}_N/\mathcal{K}) \otimes H^{b_1}_{DR}(\mathcal{X}_1/\mathcal{K})^\vee \otimes \cdots \otimes H^{b_N}_{DR}(\mathcal{X}_N/\mathcal{K})^\vee$ (resp. l'analogue avec $H^{\cdot}_B(-_t)$). Alors on a un isomorphisme de périodes classiques:

$$T_{DR}(\mathcal{X}/\mathcal{K}) \otimes_{\mathcal{K}} \mathbf{C} \xrightarrow{\sim} T_B(X_t) \otimes \mathbf{C}$$

et un isomorphisme de périodes p-adiques

$$T_{DR}(\mathcal{X}/\mathcal{K}) \otimes_{\mathcal{K}} B_{DR} \xrightarrow{\sim} T_B(X_t) \otimes B_{DR}.$$

2.3.2. Avec les notations précédentes, soit $x \in T_{DR}(\mathcal{X}/\mathcal{K})$ un *cycle de Hodge pour* t : cela signifie, par définition (*cf.* [15], [56]) que $x \in \mathrm{Fil}^0 T_{DR}$

et que $\alpha_B(x) \in T_B(x_t)$. Si les $\mathcal{X}_i$ sont des variétés abéliennes ou des espaces projectifs, on sait, par un théorème de Deligne [15], que, pour tout autre choix t', on a encore $\alpha_{B,t'}(x) \in T_B(x_{t'})$. Sous les mêmes hypothèses, on a de plus

$$\alpha_B(x) = \alpha_{DR}(x). \tag{2.3.2.1}$$

Ce résultat a été prouvé indépendamment par Blasius (sa démonstration — simplifiée — est expliquée par Ogus dans [58]) et par Wintenberger [72].

Soit $W_\mathfrak{p}$ le sous-groupe de $\mathrm{Gal}(\bar{K}/K_0)$ formé des éléments ayant pour image dans $\mathrm{Gal}(\bar{k}/k)$ une puissance entière du Frobenius du corps (fini) k. Il découle du théorème de Berthelot-Ogus (2.2.1.1) que, lorsque tous les $\mathcal{X}_i$ ont bonne réduction, $W_\mathfrak{p}$ opère de façon naturelle sur $T_{DR}(X/K) \otimes \bar{K}$ [6]. Il résulte de (2.3.2.1) (et de la compatibilité (*cf.* 4.3.5) entre α_{cris} et α_{DR}) qu'alors $W_\mathfrak{p}$ *fixe* les images des cycles de Hodge. Comme application, Ogus [58] obtient un analogue p-adique de la formule de Chowla-Selberg [35], décrivant l'action de $W_\mathfrak{p}$ sur $H^1_{DR}(X_{\bar{K}}/\bar{K})$ pour $\mathcal{X}$ une courbe elliptique à multiplication complexe définie sur $\mathcal{K}$ et ayant bonne réduction en $\mathfrak{p}$, en termes de valeurs de fonctions Γ p-adiques. La démonstration d'Ogus, par réduction à une formule analogue pour les courbes de Fermat, s'inspire de celle de Gross [35] pour la formule classique ; elle utilise des calculs de Coleman [R.F. Coleman, On the Frobenius matrices of Fermat curves, preprint (1990)].

Signalons également, comme application de (2.3.2.1), la description que donne Wintenberger [71] du foncteur module de Dieudonné filtré pour les motifs de type CM sur $\bar{\mathbf{Q}}$, généralisant un théorème (non publié) de Kottwitz (*cf.* aussi [A. Reimann and T. Zink, Der Dieudonnémodul einer polarisierten abelschen Mannigfaltigkeit von CM-typ, Ann. of Math 128 (1988), 461-482]).

2.4. Nombres de Tamagawa de motifs

Faute de place, nous ne donnerons que quelques références : le sujet mériterait, à lui seul, un exposé Bourbaki ! La théorie classique des nombres de Tamagawa relie groupes algébriques et valeurs de fonctions L, voir [11] pour un exposé d'ensemble. Dans [8], Bloch et Kato développent, à

l'aide des techniques de Fontaine et Messing [31], une théorie analogue, encore largement conjecturale, pour les motifs sur $\mathbf{Q}$ (disons, au sens de Grothendieck, voir [67] pour une introduction récente et une liste de références) ; typiquement, il s'agit des diverses réalisations — de Rham, Betti, ℓ-adiques, cristallines, etc. — de "$H^m(X, \mathbf{Z}(r))$" pour X propre et lisse sur $\mathbf{Q}$. Pour un tel motif M, ils construisent notamment des groupes locaux $A(\mathbf{Q}_p)$ jouant le rôle des groupes de points dans le cas des groupes algébriques, et proposent une "conjecture de Tamagawa", qui précise les conjectures de Deligne [14] et Beilinson [3] sur $L(M, 0)$ (voir aussi [61]). Ils la vérifient (partiellement) dans certains cas particuliers (fonction zêta de Riemann, courbes elliptiques à multiplication complexe); un ingrédient clé est une ré-interprétation de l'homomorphisme de Coates-Wiles à l'aide de l'anneau B_{cris}. De nouveaux développements, dans le cadre des "motifs mixtes", ont été donnés dernièrement par Fontaine et Perrin-Riou [33].

3. LA MÉTHODE DE FALTINGS ([19], [20])

3.1. Plan

Nous nous bornerons à esquisser les principales étapes de la démonstration de la conjecture de Hodge-Tate pour X_η, avec X propre et lisse sur S et $X_{\bar\eta}$ intègre. Nous ne dirons que quelques mots, en 3.6, du cas de mauvaise réduction et des variantes C_{cris} et C_{DR}.

La méthode consiste en la construction : i) d'une théorie de cohomologie $X \mapsto H^*(\widetilde{X}, \mathcal{O}^\wedge)$, à valeurs dans les $\bar V^\wedge$-modules munis d'une action semi-linéaire continue de G ; ii) de transformations naturelles compatibles à l'action de G

$$H^*(X_{\bar\eta}, \mathbf{Z}_p) \otimes \bar V^\wedge \xrightarrow{(1)} H^*(\widetilde{X}, \mathcal{O}^\wedge) \xleftarrow{(2)} \oplus H^{*-i}(X, \Omega^i) \otimes_V (\rho^i \bar V^\wedge)(-i),$$

où ρ est un certain élément de $\bar V$, voir 3.3.2. Si $U = \operatorname{Spec} R$ est un ouvert affine de X tel que $U_{\bar\eta}$ soit intègre, notons $\bar R$ le normalisé de R dans un revêtement universel de $U_{\bar\eta}$; le groupe de Galois $\Gamma = \operatorname{Gal}(\bar R/R)$ opère sur $\bar R$, et *a fortiori* son sous-groupe géométrique $\Delta = \operatorname{Gal}(\bar R/R_{\bar\eta})$ ($\Gamma/\Delta = G$).

Considérons la cohomologie galoisienne "continue"

$$H^*(\Delta, \bar{R}^\wedge) := \varprojlim H^*(\Delta, \bar{R}/p^n\bar{R}),$$

qui est formée de $\bar{V}^\wedge$-modules avec opération semi-linéaire de G. Utilisant des techniques inspirées de Tate [70], Faltings montre (voir 3.3) que, pour U assez petit, on peut "à $\mathfrak{m}$-torsion près" remplacer, pour le calcul de cette cohomologie, $\bar{R}$ par l'extension de $R \otimes_V \bar{V}$ obtenue en adjoignant toutes les racines p^n-ièmes de certaines unités de R, et Δ par le groupe de Galois géométrique correspondant, qui est un $\mathbf{Z}_p(1)^d$: on trouve un isomorphisme (G-équivariant) :

$$H^i(\Delta, \bar{R}^\wedge) \otimes \mathbf{Q}_p \xrightarrow{\sim} \Omega^i_{R/V} \otimes_V \bar{K}^\wedge(-i). \tag{3.1.1}$$

Grâce à une variante (voir 3.4.4.2) du théorème des bons voisinages d'Artin (SGA 4 XI), Faltings montre en outre qu'il existe suffisamment de tels U pour lesquels la cohomologie galoisienne $H^*(\Delta, \bar{R}/p^n)$ s'identifie à la cohomologie étale $H^*(U_{\bar{\eta}}, \bar{R}/p^n)$. Un procédé de globalisation standard (voir 3.4, 3.5) fournit alors la définition de $H^*(\widetilde{X}, \mathcal{O}^\wedge)$ et de la transformation (1). Une suite exacte de différentielles globale (voir 3.4.3) permet de définir (2), et l'on déduit de (3.1.1) que $(2) \otimes \mathbf{Q}_p$ est un isomorphisme. Il ne reste plus qu'à montrer que $(1) \otimes \mathbf{Q}_p$ est un isomorphisme, ce qui se fait par un argument global (voir 3.5.2), utilisant la compatibilité de $(2)^{-1} \circ (1)$ à la dualité de Poincaré.

3.2. Revêtements presque étales et extensions absorbant la ramification

3.2.1. Le point de départ est le résultat suivant de Tate [70, 3.2]. Soient $K_\infty = K(\mu_{p^\infty}) \subset \bar{K}$ la sous-extension p-cyclotomique maximale, V_∞ le normalisé de V dans K_∞, $\mathfrak{m}_\infty$ l'idéal maximal de V_∞. Tate montre que V_∞ absorbe déjà pratiquement toute la ramification de $\bar{V}$ sur V. Plus précisément, soit L une extension galoisienne finie de K_∞ contenue dans $\bar{K}$, de groupe H, B le normalisé de V_∞ dans L. Tate prouve que :

a) $\mathfrak{m}_\infty . \Omega^1_{B/V_\infty} = 0$;

b) $\mathfrak{m}_\infty . H^i(H, B^\wedge) = 0$ pour tout $i > 0$, où $H^i(H, B^\wedge)$

$:= \varprojlim H^i(H, B/p^nB)$.

Rappelons brièvement son argument. On peut supposer $V = W(k)$. On connaît alors explicitement (c'est élémentaire) la ramification (*i.e.* groupes de ramification et différente) de $K_n = K(\mu_{p^n})$ sur K (*cf.* par exemple [CL, IV §4]). L'extension L de K_∞ est réunion d'extensions L_n de K_n, galoisiennes de groupe H pour n assez grand. À l'aide du théorème de Herbrand, une étude des groupes de ramification de L_n sur K montre que, pour $n \to \infty$, la valuation de la différente $\mathcal{D}_{L_n/K_n}$ de L_n/K_n est majorée par cp^{-n}, où c est une constante. L'assertion a) en résulte. Comme $v_{K_n}\left(Tr_{L_n/K_n}(B_n)\right) = \left[v_{L_n}\left(\mathcal{D}_{L_n/K_n}\right)/e\right]$, où B_n est le normalisé de K_n dans L_n et e l'indice de ramification de L_n/K_n (constant pour $n \gg 0$), on en déduit aussi que $Tr_{B/V_\infty}(B) \supset \mathfrak{m}_\infty$. Pour $a \in \mathfrak{m}_\infty$, soit $b \in B$ tel que $Tr(b) = a$. Si M est un B-module sur lequel H opère semi-linéairement, on a une application $u_b : M \to M^H$, $m \mapsto Tr_H(bm)$, où $Tr_H = \sum_{s \in H} s$. L'application u_b est fonctorielle en M, et induit sur M^H la multiplication par a. Il en résulte que a annule $H^i(H, M)$ pour tout $i > 0$, d'où b).

3.2.2. Faltings généralise ceci à des algèbres lisses (ou formellement lisses) sur V "assez petites", mais de dimension relative quelconque. Il introduit à cet effet la notion suivante, qui joue un rôle essentiel dans toute la théorie.

Rappelons qu'une algèbre B de type fini sur un anneau A est nette (= non ramifiée) sur A si $\Omega^1_{B/A} = 0$, ce qui s'exprime aussi par le fait que l'immersion diagonale $\operatorname{Spec} B \to \operatorname{Spec} B \otimes_A B$ est ouverte, ou encore que B est facteur direct de $B \otimes_A B$ comme $B \otimes_A B$-module via $m : B \otimes_A B \to B$, $m(x \otimes y) = xy$, *i.e.* qu'il existe un idempotent $e_{B/A} \in B \otimes_A B$ définissant une section $(B \otimes_A B)$-linéaire de m, *cf.* par exemple [59, III §4].

Plaçons-nous maintenant dans la catégorie $\mathcal{C}$ des V_∞-algèbres sans p-torsion (on pourrait remplacer V_∞ par $\bar{V}$, voire par un anneau de base normal dans lequel $p = ux^n$, u une unité, pour une infinité de n). Faltings dit qu'un homomorphisme $A \to B$ de $\mathcal{C}$ est un *revêtement presque étale* ("almost étale covering") si :

i) $B[1/p]$ est un revêtement fini étale de $A[1/p]$ (*i.e.* net et projectif de type fini comme $A[1/p]$-module)

ii) $Tr(B) \subset A$, où $Tr : B[1/p] \to A[1/p]$ est l'homomorphisme trace

iii) $\mathfrak{m}_\infty . e_{B/A} \subset Im\, B \otimes_A B \to (B \otimes_A B)[1/p]$, où $e_{B/A} \subset (B \otimes_A B)[1/p]$ est l'idempotent diagonal défini par i).

Par exemple, l'extension B de V_∞ de 3.2.1 est un revêtement presque étale.

On vérifie facilement que, si B est un revêtement presque étale de A, $\mathfrak{m}_\infty$ annule $Tor_q^A(B, M)$ et $Ext_A^q(B, M)$ pour tout A-module M et tout $q > 0$. D'autre part, du point de vue des relèvements infinitésimaux, les revêtements presque étales se comportent, à peu de choses près, comme les morphismes étales :

3.2.2.1. Si B est un revêtement presque étale de A et $B = A + \mathfrak{m}_\infty B$, tout morphisme de A-algèbres $B \to C/I$, où C est une A-algèbre et I un idéal nilpotent, se relève de manière unique en $B \to C$ (en d'autres termes, B est une A-algèbre formellement étale (*EGA* O_{IV} 19.10.2)).

3.2.2.2. Si $I \subset A$ est nilpotent, pour tout revêtement presque étale B_0 de $A_0 = A/I$ tel que $B_0 = A_0 + \mathfrak{m}_\infty B_0$, il existe un revêtement presque étale B de A tel que $B_0 = (B \otimes_A A_0)/(p - \text{torsion})$.

En outre, on a des propriétés analogues à 3.2.1 a) et b). Convenons de dire qu'un morphisme de V_∞-modules est un $\mathfrak{m}_\infty$-*isomorphisme* (ou un *isomorphisme modulo* $\mathfrak{m}_\infty$-*torsion*) si son noyau et son conoyau sont annulés par $\mathfrak{m}_\infty$ (rappelons que $\mathfrak{m}_\infty^2 = \mathfrak{m}_\infty$). Soit B un revêtement presque étale de A. Alors :

3.2.2.3. L'application $\Omega_A^1 \otimes_A B \to \Omega_B^1$ est un $\mathfrak{m}_\infty$-isomorphisme.

3.2.2.4. Si un groupe fini H opère sur B de manière que $B[1/p]$ soit un revêtement galoisien de $A[1/p]$ de groupe H, pour tout B-module M sur lequel H opère semi-linéairement, on a $\mathfrak{m}_\infty . H^i(H, M) = 0$ pour tout $i > 0$.

La démonstration de 3.2.2.4 est analogue à celle de 3.2.1 b). Celle de 3.2.2.1 à 3.2.2.3 repose sur l'annulation par $\mathfrak{m}_\infty$ de la cohomologie de Hochschild $H^*(B/A, L)$ en degré > 0 (L un $(B \otimes_A B)$-module), conséquence de iii).

Le résultat principal de la théorie est le suivant :

THÉORÈME 3.2.3.— *Soit* $U = \mathrm{Spec}(R)$ *étale sur* $\mathrm{Spec}\, V\left[T_1^{\pm 1}, \cdots, T_d^{\pm 1}\right]$, *via* $T_i \mapsto u_i \in R^*$.

Soient

$$R_n = (R \otimes_V V_n)\left[u_1^{p^{-n}}, \cdots, u_d^{p^{-n}}\right], \; R_\infty = \varinjlim R_n, \; U_\infty = \mathrm{Spec}\, R_\infty,$$

où V_n *est l'anneau des entiers de* $K_n = K(\mu_{p^n})$. *Alors, si* $U' \to U$ *est fini, avec* U' *normal,* U'_η *étale sur* U_η, *le normalisé de* $U_\infty \times_U U'$ *est un revêtement presque étale de* U_∞.

COROLLAIRE 3.2.4.— *Supposons* $U_{\bar\eta}$ *intègre. Soit* $\bar U_{\bar\eta}$ *un revêtement universel de* $U_{\bar\eta}$ (*) *et soit* $\bar U$ *le normalisé de* U_∞ *dans* $\bar U_{\bar\eta}$. *Alors* $\bar U \to (U_\infty)_{\bar S}$ *est limite projective de revêtements presque étales :*

$$\begin{array}{ccccccc}
 & & & & \bar U & \longleftarrow & \bar U_{\bar\eta} \\
 & & & & \downarrow & & \downarrow \\
 & & U_\infty & \xleftarrow{(3)} & (U_\infty)_{\bar S} & & \downarrow \\
 & & \downarrow & & \downarrow & & \downarrow \\
U & \longleftarrow & U_{S_\infty} & \xleftarrow{(2)} & U_{\bar S} & \longleftarrow & U_{\bar\eta} \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
S & \longleftarrow & S_\infty & \xleftarrow{(1)} & \bar S & \longleftarrow & \bar\eta.
\end{array}$$

(N.B. Les carrés sont cartésiens ; d'après 3.2.1, (1), donc aussi (2) et (3) sont limites projectives de revêtements presque étales.)

La démonstration de 3.2.3 est ardue. On remplace U par son hensélisé $U_{(x)} = \mathrm{Spec}\, R_{(x)}$ en un point x de la fibre spéciale U_s, et l'on raisonne par récurrence sur $\dim U_{(x)}$ $(= d + 1 - \dim\{\bar x\})$. Pour $\dim U_{(x)} = 1$, $R_{(x)}$ est un anneau de valuation discrète hensélien, dont le corps résiduel est une extension finie séparable de $k(T_1, \cdots, T_d)$. Pour $d = 0$, le résultat à prouver découle de celui de Tate (3.2.1). Dans le cas général, la méthode de Tate, utilisant les groupes de ramification et le théorème de Herbrand,

(*) On prend ici la limite projective du pro-objet défini dans (SGA 1 V).

ne s'applique plus. Toutefois, si $U' = \mathrm{Spec}(R')$, et R'_n est le normalisé de $R_n \otimes R'$, Faltings montre, par un calcul direct sur les différentielles, que les valuations des différentes de R'_n sur R_n tendent vers 0 quand $n \to \infty$. Le cas où $\dim U_{(x)} = 2$ se ramène au précédent par localisation aux points maximaux de la fibre spéciale de $U'_{(x)}$. Quand $\dim U_{(x)} \geq 3$, on applique l'hypothèse de récurrence à une section hyperplane convenable de $U_{(x)}$, et l'on utilise 3.2.2.1. La démonstration s'inspire ici de celle du théorème de pureté de Zariski-Nagata (SGA 1 X 3.1) donnée par Grothendieck dans (SGA 2 X §3).

3.3. Cohomologie galoisienne et différentielles : calculs locaux

3.3.1. On se place dans la situation de 3.2.4. On pose $\bar{R} = \mathcal{O}(\bar{U})$, $R_{\bar{V}} = R \otimes_V \bar{V}$. Soient Γ et Δ les groupes fondamentaux respectifs de U_η et $U_{\bar{\eta}}$ (associés à $\bar{U}_{\bar{\eta}}$), de sorte que $G = \Gamma/\Delta$.

Faltings montre qu'on peut "presque" calculer $H^*(\Delta, \bar{R}/p^n)$ comme représentation de G. En effet, soit $T = \mathbf{Z}_p(1)^d$ le groupe de Galois de $(U_\infty)_{\bar{S}}$ sur $U_{\bar{S}}$ ($(z_1, \cdots, z_d) \in (\mu_{p^n})^d$ agissant par $u_i^{p^{-n}} \mapsto z_i u_i^{p^{-n}}$), H celui de $\bar{U}$ sur $(U_\infty)_{\bar{S}}$. Considérons la suite spectrale de Hochschild-Serre :

$$E_2^{r,s} = H^r(T, H^s(H, \bar{R}/p^n)) \Longrightarrow H^{r+s}(\Delta, \bar{R}/p^n)$$

(qui est G-équivariante). Comme $\bar{U} \to (U_\infty)_{\bar{S}}$ est limite projective de revêtements presque étales (3.2.4), il résulte de 3.2.2.4 que $\mathfrak{m} \,.\, H^s(H, \bar{R}/p^n) = 0$ pour $s > 0$. Comme d'autre part, $H^0(H, \bar{R}) =$
$\mathcal{O}(U_\infty)_{\bar{S}} = R_{\bar{V}}[u_1^{p^{-\infty}}, \cdots, u_d^{p^{-\infty}}]$, on obtient un isomorphisme canonique, G-équivariant,
(3.3.1.1)

$$H^i(\Delta, \bar{R}/p^n) \xrightarrow{\sim} H^i(T, R_{\bar{V}}[u_1^{p^{-\infty}}, \cdots, u_d^{p^{-\infty}}]/p^n) \pmod{\mathfrak{m}\text{ – torsion}}.$$

De la décomposition (stable par T, et équivariante sous G)

$$(R_{\bar{V}}/p^n)\left[u_1^{p^{-\infty}}, \cdots, u_d^{p^{-\infty}}\right] = (R_{\bar{V}}/p^n) \oplus (\oplus (R_{\bar{V}}/p^n) u_1^{a_1} \cdots u_d^{a_d}),$$

où la seconde somme est étendue aux $a = (a_1, \cdots, a_d) \in \mathbf{Z}[1/p]^d$ tels que $a \neq 0$ et $0 \leq a_i < 1$, on déduit (à l'aide, par exemple, de résolutions de

Koszul) un isomorphisme G-équivariant :

$$(3.3.1.2)\quad H^*(\Delta, \bar{R}/p^n) \xrightarrow{\sim} \Lambda((R_{\bar{V}}/p^n)(-1)^d) \oplus \mathbf{r}_n \qquad (\mathrm{mod}\ \mathfrak{m}-\mathrm{torsion}).$$

où $\mathbf{r}_n$ est annulé par $p^{1/(p-1)}$. Passant à la limite projective sur n, on obtient finalement un isomorphisme G-équivariant de $R_{\bar{V}}^{\wedge}$-modules

$$(3.3.1.3)\qquad H^*(\Delta, \bar{R}^{\wedge}) \xrightarrow{\sim} \Lambda(R_{\bar{V}}^{\wedge}(-1)^d) \oplus \mathbf{r} \qquad (\mathrm{mod}\ \mathfrak{m}^{\wedge}-\mathrm{torsion}),$$

où $\mathbf{r}$ est annulé par $p^{1/(p-1)}$ (Faltings montre même qu'on peut se débarrasser du mod $\mathfrak{m}^{\wedge}$-torsion).

3.3.2. Considérons la suite exacte :

$$(3.3.2.1)\qquad \Omega^1_{U_{\bar{S}}/U} \otimes \mathcal{O}_{\bar{U}} \xrightarrow{i} \Omega^1_{\bar{U}/U} \longrightarrow \Omega^1_{\bar{U}/U_{\bar{S}}} \longrightarrow 0$$

définie par les morphismes $\bar{U} \to U_{\bar{S}} \to U$ de 3.2.4. Comme $\bar{U} \to (U_\infty)_{\bar{S}}$ est limite projective de revêtements presque étales, il résulte de 3.2.2.3 (et (3.3.2.3) ci-dessous) que i est injective et que mod $\mathfrak{m}$-torsion, la suite exacte (3.3.2.1) est scindée (comme suite de $\mathcal{O}_U$-modules). Elle s'identifie en effet, mod $\mathfrak{m}$-torsion, à la suite déduite par extension des scalaires de la suite exacte analogue relative aux morphismes $(U_\infty)_{\bar{S}} \to U_{\bar{S}} \to U$. Pour la même raison, l'homomorphisme naturel $\Omega^1_{U/S} \otimes \mathcal{O}_{\bar{U}} \to \Omega^1_{\bar{U}/\bar{S}}$ induit une flèche

(3.3.2.2)

$$\Omega^1_{U/S} \otimes (\mathcal{O}_{\bar{U}}[1/p]/\mathcal{O}_{\bar{U}}) \longrightarrow \Omega^1_{\bar{U}/U_{\bar{S}}} \quad , \quad d\log u_i \otimes p^{-n} \longmapsto \text{image de } d\log u_i^{p^{-n}},$$

qui est un $\mathfrak{m}$-isomorphisme. D'autre part, d'après un résultat de Fontaine [24], l'application $d\log : \mu_{p^\infty} \to \Omega^1_{\bar{S}/S}$ induit un isomorphisme :

$$(3.3.2.3)\qquad (\mathcal{O}_{\bar{S}}[1/p]/\rho^{-1}\mathcal{O}_{\bar{S}})(1) \xrightarrow{\sim} \Omega^1_{\bar{S}/S},$$

où $\rho \in \bar{V}$ est un élément de valuation $(1/(p-1)) + v(\mathcal{D}_{V/W(k)})$ (v normalisée par $v(p) = 1$) (c'est aussi une conséquence du résultat de Tate (3.2.1) : le fait que $\bar{S} \to S_\infty$ soit limite projective de revêtements presque étales permet de se ramener à établir l'analogue de (3.3.2.3) avec S et $\bar{S}$ remplacés

respectivement $W(k)$ et $W(k)(\mu_{p^\infty})$, où l'on conclut par un calcul direct élémentaire). Prenant l'image inverse de (3.3.2.1) par (3.3.2.2) et tenant compte de (3.3.2.3), on obtient, après application du foncteur module de Tate $\mathrm{Hom}(\mathbf{Q}_p/\mathbf{Z}_p, -)$, une suite exacte canonique de $\bar{R}^\wedge$-modules

$$0 \longrightarrow \bar{R}^\wedge \longrightarrow E \longrightarrow \Omega^1_{R/V} \otimes \rho\bar{R}^\wedge(-1) \longrightarrow 0. \tag{3.3.2.4}$$

Le groupe de Galois $\Gamma = \mathrm{Gal}(\bar{U}/U)$ opère de façon naturelle sur cette suite. On en déduit un homomorphisme de $R^\wedge_{\bar{V}}$-modules, équivariant sous $G = \Gamma/\Delta$,

$$\Omega^1_{R/V} \otimes \rho\bar{V}^\wedge(-1) \longrightarrow H^1(\Delta, \bar{R}^\wedge). \tag{3.3.2.5}$$

Le calcul de (3.3.1.3) montre que celui-ci est un isomorphisme modulo p-torsion. Il en est de même des flèches déduites de (3.2.2.5) par application de Λ^i :

$$\Omega^i_{R/V} \otimes \rho^i\bar{V}^\wedge(-i) \longrightarrow H^i(\Delta, \bar{R}^\wedge). \tag{3.3.2.6}$$

La même conclusion vaut pour la flèche de pro-objets donnant naissance à (3.3.2.6), avec $\bar{V}^\wedge$ (resp. $\bar{R}^\wedge$) remplacé par $\bar{V}/p^{\cdot}$ (resp. $\bar{R}/p^{\cdot}$), et "modulo p-torsion" par "modulo p-torsion bornée" (où $\bar{V}/p^{\cdot}$ (resp. $\bar{R}/p^{\cdot}$) désigne le système projectif des $\bar{V}/p^n\bar{V}$ (resp. $\bar{R}/p^n\bar{R}$)).

3.4. Globalisation : cycles évanescents cohérents

3.4.1. On fixe un schéma X lisse sur S, de dimension relative d. On suppose, pour simplifier, $X_{\bar{\eta}}$ intègre, de point générique ξ, et l'on fixe un point géométrique $\bar{\xi}$ localisé en ξ. Si U est un ouvert (de Zariski) de X, on note $\bar{U}_{\bar{\eta}}$ le revêtement universel de $U_{\bar{\eta}}$ correspondant à $\bar{\xi}$ et $\bar{U}$ le normalisé de U dans $\bar{U}_{\bar{\eta}}$. On pose $\Gamma(U) = \pi_1(U_\eta, \bar{\xi})$, $\Delta(U) = \pi_1(U_{\bar{\eta}}, \bar{\xi})$, de sorte que $G = \Gamma(U)/\Delta(U)$. On dit que U est *petit* si U est affine, $U = \mathrm{Spec}\, R$, avec R étale sur $V\left[T_1^{\pm 1}, \cdots, T_d^{\pm 1}\right]$ (via $T_i \mapsto u_i \in R^*$).

3.4.2. Soit $\widetilde{X}$ la catégorie suivante. Un objet $F = ((F_U), (r_{U_1U_2}))$ de $\widetilde{X}$ est la donnée, pour chaque ouvert de Zariski U de X, d'un faisceau *étale* F_U sur

$U_{\bar{\eta}}$, et pour chaque inclusion $U_2 \subset U_1$, d'un morphisme $r_{U_1U_2} : F_{U_1}|(U_2)_{\bar{\eta}} \to F_{U_2}$, de manière que $r_{U_2U_3} \circ r_{U_1U_2} = r_{U_1U_3}$ et $r_{UU} = Id$. On impose que, pour tout hyperrecouvrement (ouvert de Zariski) tronqué $U_1 \rightrightarrows U_0 \to U$, la suite $F_U \to j_{0*}F_{U_0} \rightrightarrows j_{1*}F_{U_1}$ soit exacte, j_i désignant la flèche de $(U_i)_{\bar{\eta}}$ dans $U_{\bar{\eta}}$. Une flèche $f : L \to M$ de X est un système de flèches $f_U : L_U \to M_U$, compatibles aux $r_{U_1U_2}$. La catégorie $\widetilde{X}$ est un topos. Si $\mathcal{B}$ est une base d'ouverts de X, en astreignant les U à appartenir à $\mathcal{B}$, on obtient un topos équivalent, noté encore $\widetilde{X}$ (définir F_U comme limite inductive des $\mathrm{Ker}\left(j_{0*}F_{U_0} \rightrightarrows j_{1*}F_{U_1}\right)$ suivant les hyperrecouvrements $U_\cdot \to U$ avec U_i somme d'ouverts $\in \mathcal{B}$).

Tout faisceau étale E sur X induit un faisceau, noté $\widetilde{j}^*E$ (ou $E|\widetilde{X}$), sur $\widetilde{X}$, défini par $U \mapsto E|U_{\bar{\eta}}$. D'autre part, G opère par transport de structure sur $\widetilde{X}$, et si X_G désigne le topos zariskien des G-faisceaux sur X, on a un foncteur G-équivariant

$$\psi : \widetilde{X} \longrightarrow X_G, \tag{3.4.2.1}$$

associant à F le faisceau $U \mapsto \Gamma(U_{\bar{\eta}}, F_U)$. Comme par définition $\Gamma(\widetilde{X}, F) = \Gamma(X_{\bar{\eta}}, F_X)$, on a un isomorphisme ($G$-équivariant)

$$\Gamma(X, \psi F) = \Gamma(\widetilde{X}, F). \tag{3.4.2.2}$$

Enfin, si E est un faisceau étale sur X, on a

$$\psi(E|\widetilde{X}) = \varepsilon_* j_* j^* E, \tag{3.4.2.3}$$

où $j : X_{\bar{\eta}} \to X$ est la flèche naturelle, et ε la projection du topos étale sur le topos zariskien.

3.4.3. En associant à un petit ouvert U de X (3.4.1) le faisceau localement constant sur $U_{\bar{\eta}}$ de valeur $\bar{R}$, défini par l'action naturelle de $\Delta(U)$ sur $\bar{R}$, où $\bar{R}$ est le normalisé de $R = \mathcal{O}(U)$ dans le revêtement universel $U_{\bar{\eta}}$, on vérifie qu'on définit un faisceau d'anneaux $\mathcal{O}_{\widetilde{X}}$ de $\widetilde{X}$. Si M est un faisceau localement libre sur X, on notera $M \otimes \mathcal{O}_{\widetilde{X}}$ le faisceau $U \mapsto M(U) \otimes_{\mathcal{O}(U)} \mathcal{O}(\widetilde{U})$ sur X.

La suite exacte de pro-objets donnant naissance à (3.3.2.4)

$$0 \longrightarrow \bar{R}/p^{\cdot} \longrightarrow E_{\cdot} \longrightarrow \Omega^1_{R/V} \otimes \rho\bar{R}/p^{\cdot}(-1) \longrightarrow 0$$

est fonctorielle en le petit ouvert U. Elle définit une suite exacte de pro-$\mathcal{O}_{\widetilde{X}}$-modules

$$0 \longrightarrow \mathcal{O}_{\widetilde{X}}/p^{\cdot} \longrightarrow \mathcal{E}_{\cdot} \longrightarrow \Omega^1_{X/S} \otimes \rho\mathcal{O}_{\widetilde{X}}/p^{\cdot}(-1) \longrightarrow 0. \tag{3.4.3.1}$$

Comme

$$\psi(\Omega^1_{X/S} \otimes \rho\mathcal{O}_{\widetilde{X}}/p^{\cdot}) = \Omega^1_{X/S} \otimes \rho\bar{V}/p^{\cdot},$$

le triangle déduit de (3.4.3.1) par application de $R\psi$ fournit une flèche

$$\Omega^1_{X/S} \otimes \rho\bar{V}/p^{\cdot}(-1)[-1] \longrightarrow R\psi(\mathcal{O}_{\widetilde{X}}/p^{\cdot}) \tag{3.4.3.2}$$

dans la catégorie dérivée $D(\mathcal{O}_X \otimes_V \bar{V}_{\cdot})$ des (pro-) $\mathcal{O}_X \otimes_V \bar{V}$-modules sur $\underset{L}{X}$ (munis d'une action semi-linéaire de G). Utilisant le produit $R\psi(\mathcal{O}_{\widetilde{X}}/p^{\cdot}) \otimes R\psi(\mathcal{O}_{\widetilde{X}}/p^{\cdot}) \to R\psi(\mathcal{O}_{\widetilde{X}}/p^{\cdot})$ et la flèche d'anti-symétrisation

$$\Omega^i_{X/S} \longrightarrow (\Omega^1_{X/S})^{\otimes i} \quad , \quad x_1 \wedge \cdots \wedge x_i \mapsto \sum \varepsilon(s) x_{s(1)} \otimes \cdots \otimes x_{s(i)},$$

on déduit de (3.4.3.2) une flèche

$$\oplus\, \Omega^i_{X/S} \otimes \rho^i\bar{V}/p^{\cdot}(-i)[-i] \longrightarrow R\psi(\mathcal{O}_{\widetilde{X}}/p^{\cdot}) \tag{3.4.3.3}$$

(dans $D(\mathcal{O}_X \otimes_V \bar{V}_{\cdot})$). La flèche

$$\Omega^i_{X/S} \otimes \rho^i\bar{V}/p^{\cdot}(-i) \longrightarrow R^i\psi(\mathcal{O}_{\widetilde{X}}/p^{\cdot}) \tag{3.4.3.4}$$

induite par (3.4.3.3) sur $\mathcal{H}^i$ est $i!$-fois la flèche qu'on obtiendrait en appliquant Λ^i à (3.4.3.4) pour $i = 1$. Passant à la limite projective, *i.e.* appliquant $R\varprojlim$ à (3.4.3.3), on obtient une flèche

$$\oplus\, \Omega^i_{X/S} \otimes \rho^i\bar{V}^{\wedge}(-i)[-i] \longrightarrow R\psi(\mathcal{O}^{\wedge}_{\widetilde{X}}) \tag{3.4.3.5}$$

dans la catégorie dérivée des $\mathcal{O}_X \otimes_V \bar{V}^{\wedge}$-modules sur X munis d'une action semi-linéaire de G, avec $R\psi(\mathcal{O}^{\wedge}_{\widetilde{X}}) := R\varprojlim R\psi(\mathcal{O}_{\widetilde{X}}/p^{\cdot})$. L'un des résultats principaux de Faltings est le suivant :

THÉORÈME 3.4.4.— *La flèche* (3.4.3.5) $\otimes \mathbf{Q}_p$ *est un isomorphisme.*

La démonstration repose sur les calculs locaux de 3.3 et une variante du théorème des bons voisinages d'Artin. Si U est un ouvert de X et $\mathcal{L}$ un faisceau localement constant de torsion sur $U_{\bar{\eta}}$ de valeur L, la suite spectrale des foncteurs composés $H^r(\Delta(U), H^s(\bar{U}_{\bar{\eta}}, L)) \Longrightarrow H^*(U_{\bar{\eta}}, \mathcal{L})$ fournit une flèche

$$H^r(\Delta(U), L) \longrightarrow H^r(U_{\bar{\eta}}, \mathcal{L}) \tag{3.4.4.1}$$

de la cohomologie galoisienne vers la cohomologie étale. Convenons de dire que U est *génériquement un* $K(\pi,1)$*-cohomologique* (ou simplement, par abus, un $K(\pi,1)$) si pour tout $\mathcal{L}$ comme ci-dessus, (3.4.4.1) est un isomorphisme. Faltings établit la variante suivante du théorème d'Artin (SGA 4 XI) :

Lemme 3.4.4.2 [19, 2.1].— *Les U qui sont des $K(\pi,1)$ forment une base d'ouverts de X.*

Pour prouver 3.4.4, on peut donc remplacer X par un petit ouvert qui est un $K(\pi,1)$. La conclusion découle alors des calculs de 3.3.2 (une puissance fixe de p annule le cône de (3.4.3.3)).

Appliquant $R\Gamma(X,-)$ et tenant compte de (3.4.2.2), on déduit de (3.4.3.5) une flèche

$$\oplus\, R\Gamma(X, \Omega^i_{X/S}) \otimes \rho^i \bar{V}\hat{}(-i)[-i] \longrightarrow R\Gamma(\widetilde{X}, \mathcal{O}^{\wedge}_{\widetilde{X}}) \tag{3.4.3.6}$$

dans la catégorie dérivée $D(\bar{V}\hat{})$ des $\bar{V}\hat{}$-modules (avec action semi-linéaire de G), où $R\Gamma(\widetilde{X}, \mathcal{O}^{\wedge}_{\widetilde{X}}) := R \varprojlim R\Gamma(\widetilde{X}, \mathcal{O}_{\widetilde{X}}/p^{\cdot})$.

COROLLAIRE 3.4.5.— *La flèche* (3.4.3.6) $\otimes \mathbf{Q}_p$ *est un isomorphisme.*

3.5. Cycles évanescents discrets et cycles évanescents cohérents.

Les hypothèses et notations de 3.4.1 sont en vigueur.

3.5.1. L'étape suivante est de comparer $R\psi(\mathcal{O}_{\widetilde{X}}/p^{\cdot})$ au complexe des cycles évanescents (*) usuel $R\Psi(\mathbf{Z}/p^{\cdot}) = \bar{i}^* R\bar{j}_* \bar{j}^* \mathbf{Z}/p^{\cdot}$, où $\bar{i} : X_{\bar{s}} \to X_{\bar{S}}$ et $\bar{j}$:

(*) On dit plutôt "proches", de nos jours

$X_{\bar{\eta}} \to X_{\bar{S}}$ sont les inclusions. La flèche évidente $(\mathbf{Z}/p^{\cdot})\,|\,\widetilde{X} \to \mathcal{O}_{\widetilde{X}}/p^{\cdot}$ donne par application de $R\psi$ une flèche

$$R\psi(\mathbf{Z}/p^{\cdot}) \otimes \bar{V}/p^{\cdot} \longrightarrow R\psi(\mathcal{O}_{\widetilde{X}}/p^{\cdot}) \tag{3.5.1.1}$$

dans la catégorie dérivée $D(X, \bar{V}.)$ des pro-$\bar{V}$-modules (zariskiens) sur X (munis d'une action semi-linéaire de G), où $R\psi(\mathbf{Z}/p^{\cdot}) = R\varepsilon_* Rj_* j^*(\mathbf{Z}/p^{\cdot})$ (*cf.* (3.4.2.2)) (la restriction de $R\psi(\mathbf{Z}/p^{\cdot})$ à X_s n'est autre que $R\varepsilon_* R\Psi(\mathbf{Z}/p^{\cdot})$, où ε désigne par abus le composé $(X_{\bar{s}})_{et} \to (X_s)_{et} \to (X_s)_{zar}$). Appliquant $R\Gamma(X, -)$, on en déduit une flèche

$$R\Gamma(X_{\bar{\eta}}, \mathbf{Z}/p^{\cdot}) \otimes \bar{V}^{\wedge}/p^{\cdot} \longrightarrow R\Gamma(\widetilde{X}, \mathcal{O}_{\widetilde{X}}/p^{\cdot}) \tag{3.5.1.2}$$

de $D(\bar{V}.)$, catégorie dérivée des pro-$\bar{V}$-modules avec action semi-linéaire de G, G agissant diagonalement sur le premier membre, puis, par application de $R\varprojlim$, une flèche

$$R\Gamma(X_{\bar{\eta}}, \mathbf{Z}_p)) \otimes \bar{V}^{\wedge} \longrightarrow R\Gamma(\widetilde{X}, \mathcal{O}_{\widetilde{X}}^{\wedge}) \tag{3.5.1.3}$$

de $D(\bar{V}^{\wedge})$ (notation de (3.4.3.6)). On ne sait rien dire de (3.5.1.1), mais Faltings établit le théorème de comparaison suivant :

THÉORÈME 3.5.2.— *Si X est* propre *sur S, la flèche* (3.5.1.3) $\otimes \mathbf{Q}_p$ *est un isomorphisme.*

La démonstration est "formelle". Posons

$$H^*_{et}(X) := H^*(X_{\bar{\eta}}, \mathbf{Z}_p) \otimes \bar{V}^{\wedge}[1/p] \quad , \quad H^*_{Fal}(X) := H^*(\widetilde{X}, \mathcal{O}_{\widetilde{X}}^{\wedge})[1/p] \quad ,$$

$$H^*_{Hdg}(X) := \oplus H^{*-i}(X, \Omega^i) \otimes \bar{V}^{\wedge}(-i)[1/p].$$

Ce sont des "théories de cohomologie" dont les restrictions aux X propres (et lisses) sur S sont à valeurs dans les $\bar{K}^{\wedge}$-espaces vectoriels de dimension finie, munis d'une action semi-linéaire continue de G. D'après (3.4.5), on a un isomorphisme fonctoriel

$$H^*_{Hdg}(X) \xrightarrow{\sim} H^*_{Fal}(X), \tag{3.5.2.1}$$

déduit de (3.4.3.6) $\otimes \mathbf{Q}_p$ par division par $i!$ sur le i-ième composant et application de H^* à l'isomorphisme ainsi obtenu. On veut montrer que la flèche

$$H^*_{et}(X) \longrightarrow H^*_{Fal}(X) \tag{3.5.2.2}$$

définie par (3.5.1.3) est un isomorphisme. Il revient au même de montrer que la flèche composée de (3.5.2.2) et de l'inverse de (3.5.2.1),

$$\beta : H^*_{et}(X) \longrightarrow H^*_{Hdg}(X) \tag{3.5.2.3}$$

est un isomorphisme. Il suffit pour cela de vérifier que β est compatible aux cup-produits (ce qui est facile), et aux morphismes "traces" $H^{2d}_{et}(X)(d) \to \bar{K}\hat{}$, $H^{2d}_{Hdg}(X)(d) \to \bar{K}\hat{}$ définissant les dualités de Poincaré sur les deux membres. La compatibilité de β aux morphismes traces découle elle-même de la compatibilité de β aux classes de cycles lisses. Faltings vérifie cette dernière à l'aide d'une extension de la théorie aux couples (X, D), D un diviseur à croisements normaux dans X.

COROLLAIRE 3.5.3.— *Si X est propre (et lisse) sur S, $X_{\bar{\eta}}$ vérifie C_{HT}* (2.1.3).

Remarque 3.5.4.— Faltings montre en fait que (sous la même hypothèse) :

a) la flèche (3.5.1.2) induit sur H^* un $\mathfrak{m}$-isomorphisme ;

b) l'isomorphisme β (3.5.2.3) est compatible aux isomorphismes de Künneth, aux classes de cycles éventuellement singuliers, et aux classes de Chern de fibrés vectoriels.

3.6. Variantes et compléments

3.6.1. *La conjecture C_{cris}*

a) Faltings définit d'abord, pour tout petit ouvert $U = \mathrm{Spec}(R)$ de X (comme en 3.4.1), un anneau B_{cris}, noté $B(R)$. On part de $\bar{R}$, normalisé de R dans le revêtement universel de $U_{\bar{\eta}}$, et l'on pose, par analogie avec 1.2.2,

$$B^+(R) = D_I\Big(W\Big(\varprojlim_F \bar{R}/p\bar{R}\Big)\Big)\hat{},$$

où la limite projective est celle d'une famille de copies de $\bar{R}/p\bar{R}$ indexée par $\mathbf{N}$ suivant les applications $F : x \mapsto x^p$, I est l'idéal défini par la suite exacte

$$0 \longrightarrow I \longrightarrow W\Big(\varprojlim_F \bar{R}/p\bar{R}\Big) \xrightarrow{\theta} \bar{R}^\wedge \longrightarrow 0,$$

avec $\bar{R}^\wedge$ = complété p-adique de $\bar{R}$,

$$\theta(s_0, s_1, \cdots) = \lim_m r_{0m}^{p^m} + p r_{1m}^{p^{m-1}} + \cdots + p^m r_{mm},$$

$s_n = \lim s_{nm}$, r_{nm} relevant s_{nm} dans $\bar{R}$, et enfin $D_I(-)^\wedge$ est l'enveloppe à puissances divisées de I, p-complétée (on peut montrer que F est surjectif, d'où la surjectivité de θ). Le groupe de Galois $\Gamma(U) = \mathrm{Gal}(\bar{R}/R)$ opère continûment sur $B^+(R)$. L'automorphisme de Frobenius de $\varprojlim_F \bar{R}/p\bar{R}$ se prolonge en un automorphisme φ de $B^+(R)$. La construction est fonctorielle en R, en particulier $B^+(R)[p^{-1}]$ est une algèbre sur $B^+_{cris} = B^+(V)[p^{-1}]$, et contient donc, de façon naturelle $\mathbf{Z}_p(1)$. On pose

$$B(R) = B^+(R)\left[p^{-1}, t^{-1}\right],$$

où t est l'image d'un générateur de $\mathbf{Z}_p(1)$. Les actions de $\Gamma(U)$ et de φ s'étendent à $B(R)$. En outre, $B(R) \otimes_{K_0} K$ a une filtration naturelle $F^\cdot$ provenant de la filtration J-adique de $B^+(R) \otimes_{W(k)} K$ définie par le noyau J du composé $B^+(R) \otimes_{W(k)} V \to \bar{R}^\wedge \otimes_{W(k)} V \to \bar{R}^\wedge$, dont le gradué s'identifie à $\oplus_{n \in \mathbf{Z}} \bar{R}^\wedge(n)[1/p]$. On notera $B^+(R^\wedge)$, $B(R^\wedge)$ les anneaux obtenus par les mêmes constructions effectuées à partir du complété p-adique de R.

b) Paraphrasant 3.4.3, on définit des faisceaux $B^+/(I^{[n]} + p^m B^+)$ sur $\widetilde{X}$, en associant à $U = \mathrm{Spec}\, R$ le faisceau localement constant sur $U_{\bar{\eta}}$ défini par $B^+(R^\wedge)/(I^{[n]} + p^m B^+(R^\wedge))$ muni de l'action $\Delta(U)$. On a une flèche naturelle de $D(B^+(V)/p^\cdot)$

$$(3.6.1.1) \qquad R\Gamma(X_{\bar{\eta}}, \mathbf{Z}/p^\cdot) \overset{L}{\otimes} B^+(V)/I^{[n]} \longrightarrow R\Gamma(\widetilde{X}, \mathbf{Z}/p^\cdot \otimes B^+/I^{[n]}).$$

Il résulte de 3.5.4 a) que, pour X *propre*, (3.6.1.1) est un $\mathfrak{m}_B$-isomorphisme, où $\mathfrak{m}_B$ est la préimage de l'idéal maximal $\mathfrak{m}^\wedge$ de $\bar{V}^\wedge$ par $B^+(V) \to \bar{V}^\wedge$. On en déduit un isomorphisme

$$(3.6.1.2) \qquad H^*(X_{\bar{\eta}}, \mathbf{Z}_p) \otimes B(V) \longrightarrow H^*(\widetilde{X}, B^\wedge)$$

(où le second membre désigne $\left(\varprojlim_n \varprojlim_m H^*(\widetilde{X}, \mathbf{Z}/p^m \otimes B^+/I^{[n]})\right)[1/p, 1/t]$), compatible à toutes les structures.

c) Soit $Y = X_s = X \otimes_V k$ la fibre spéciale de X. Faltings construit une transformation naturelle (compatible à toutes les structures)

$$H^*(Y/W) \otimes_W B(V) \longrightarrow H^*(\widetilde{X}, B^\wedge) \tag{3.6.1.3}$$

où $H^*(Y/W) = \varprojlim H^*_{cris}(Y/W_n(k))$ est la cohomologie cristalline.

i) Supposons d'abord $V = W(k)$. Pour R comme ci-dessus, l'anneau $B^+(R)$ est une algèbre sur $B^+(V)$, mais non sur R. Cependant, $B^+(R^\wedge)/I = \bar{R}^\wedge$ contient R, et comme R est lisse sur V, on peut choisir un relèvement, et même un système compatible de relèvements $r : R \to B^+(R^\wedge)/I^{[m]}$ de cette inclusion, qui sont des homomorphismes de V-algèbres. Si E est un cristal localement libre sur X (donné par un module localement libre avec une connexion intégrable topologiquement p-nilpotente ∇), on peut "évaluer" E sur $B^+(R^\wedge)/I^{[m]}$, *i.e.* former $E(B^+(R^\wedge)/I^{[m]}) := E(R) \otimes_{R,r} B^+(R^\wedge)/I^{[m]}$: à un système transitif d'isomorphismes près, donnés par ∇, le résultat ne dépend pas du choix de r. Pour U variable, les $E(B^+(R^\wedge)/I^{[m]})$ forment un faisceau $E \otimes B^+/I^{[m]}$ sur $\widetilde{X}$. De plus, si x est une section globale horizontale de E (*i.e.* telle que $\nabla x = 0$), l'image $x \otimes 1$ de x dans $E(B^+(R^\wedge)/I^{[m]})$ ne dépend pas du choix de r, et est en outre invariante par $\Gamma(U)$ (et *a fortiori* par $\Delta(U)$) : x définit donc une section globale $\widetilde{x}$ de $E \otimes B^+/I^{[m]}$. On obtient ainsi un système d'homomorphismes fonctoriels G-équivariants

$$H^0_{cris}(X/V, E) \longrightarrow H^0(\widetilde{X}, E \otimes B^+/I^{[m]}) \quad , \quad x \longmapsto \widetilde{x}. \tag{3.6.1.4}$$

Rappelons maintenant qu'on dispose de la résolution du cristal $\mathcal{O}_{X/V}$ par le "linéarisé" du complexe de de Rham, $L(\Omega^\cdot_{X/V}) = \varprojlim pr_{1*} pr_2^* \Omega^\cdot_{X/V}$, où pr_i sont les deux projections du n-ième PD-voisinage infinitésimal de X dans $X \times X$ ([4], [5]) : les composantes de $L(\Omega^\cdot_{X/V})$ sont des (pro-) cristaux localement libres sur X, acycliques pour u_* où u est la projection du topos cristallin sur le topos zariskien. Soit $U_\cdot \to X$ un hyperrecouvrement de X formé de petits ouverts. Le complexe simple associé au bicomplexe

$\Gamma_{cris}(U., L(\Omega^{\cdot}_{X/V}))$ calcule $R\Gamma(Y/W)$. Par (3.6.1.4), $\Gamma_{cris}(U., L(\Omega^{\cdot}_{X/V}))$ s'envoie dans $\Gamma(\widetilde{U}., L(\Omega^{\cdot}_{X/V}) \otimes B^+/I^{[m]})$ et ce dernier complexe s'envoie dans $R\Gamma(\widetilde{U}., L(\Omega^{\cdot}_{X/V}) \otimes B^+/I^{[m]})$, qui s'identifie à $R\Gamma(\widetilde{U}., B^+/I^{[m]})$ donc finalement à $R\Gamma(\widetilde{X}, B^+/I^{[m]})$. Le composé de ces flèches

$$R\Gamma(Y/W) \longrightarrow R\Gamma(\widetilde{X}, B^+/I^{[m]}) \tag{3.6.1.5}$$

donne naissance à (3.6.1.3).

ii) Dans le cas général, Faltings définit (3.6.1.3) par une variante des constructions précédentes, utilisant la théorie des cristaux convergents de Berthelot-Ogus [57].

Le résultat essentiel est que, pour X *propre*, (3.6.1.3) *est un isomorphisme.* Contrairement à 3.4.5, dont la vérification est locale, la démonstration que donne ici Faltings est globale, analogue à celle de (3.5.2). Il s'agit de voir que la transformation naturelle

$$H^*(Y/W) \otimes B(V) \longrightarrow H^*(X_{\bar{\eta}}, \mathbf{Z}_p) \otimes B(V), \tag{3.6.1.6}$$

composée de (3.6.1.3) et de l'inverse de (3.6.1.2), est un isomorphisme. Il suffit pour cela de vérifier, comme le fait Faltings, qu'elle est compatible à la dualité de Poincaré, ou encore à la formation des classes de cycles et classes de Chern, ce qui se ramène à un calcul explicite de cocycles pour la première classe de Chern. On pourrait aussi vérifier que, par extension des scalaires à K et passage au gradué pour les filtrations naturelles des deux membres, (3.6.1.6) induit l'isomorphisme de Hodge-Tate α_{HT} (2.1.3.2) inverse de β (3.5.2.3) (à un signe près en chaque degré peut-être) ; cette vérification, toutefois, n'est pas faite dans [20].

d) Faltings établit aussi, dans [20], d'importants raffinements du théorème de comparaison (3.6.1.6) : versions à coefficients (généralisation de la théorie de Fontaine-Laffaille [30]), versions relatives, variantes dans le cas "ouvert" (complément d'un diviseur à croisements normaux relatifs)... Il y a des applications à des théorèmes de dégénérescence de suites spectrales de Hodge vers de Rham généralisant ceux de [17] et [44], et à la classification des groupes commutatifs finis et plats d'ordre une puissance de p sur $X^{\wedge}$,

pour X lisse sur $V = W(k)$ et $p > 2$, en termes de "cristaux de Dieudonné filtrés".

3.6.2. *La conjecture C_{DR}*

Si l'on part d'un schéma X_K propre et lisse sur K, on peut, d'après un théorème de Nagata [55], trouver un schéma X propre et plat sur S tel que $X \otimes K = X_K$. Travaillant avec la topologie "rigide" sur X au lieu de la topologie de Zariski (ou de la topologie étale), Faltings construit dans [20, VIII], un faisceau d'anneaux B_{DR} sur un topos $\widetilde{X}_{rig}$ convenable, et des transformations naturelles de $H^*_{DR}(X_K/K) \otimes B_{DR}(V)$ et $H^*(X_K, \mathbf{Z}_p) \otimes B_{DR}(V)$ vers $H^*(\widetilde{X}_{rig}, B_{DR})$; un argument global analogue aux précédents montre encore que ce sont des isomorphismes. La définition du faisceau B_{DR}, très délicate, utilise la théorie des champs modulaires $\mathcal{M}_{g,t}$ de courbes stables de genre g privées de t points, généralisation de celle de Deligne-Mumford [18]. Le recours à cette théorie apparaît dans la construction de "petits" ouverts $\operatorname{Spec} R$ de X (pour la topologie rigide), munis d'éléments $u_i \in R \cap (R \otimes_V K)^*$ tels que les $d\log u_i$ engendrent $\Omega^1_{R/V} \otimes_R K$ et que $\bar{R}$ puisse être "contrôlé" par $R\left[u_i^{p^{-\infty}}\right] \otimes_V \bar{V}$: construction par récurrence sur la dimension, utilisant les fibrations élémentaires d'Artin (SGA 4 XI). Certains arguments de [19] et [20] doivent être légèrement corrigés (notamment [19, III 1.1, 1.2, 3.3] et [20, VIII, b)]). Par ailleurs, la définition des transformations naturelles évoquées ci-dessus, et de leurs analogues dans le cadre de "Hodge-Tate" n'est pas explicitée. Compte tenu de l'importance de ces résultats, on ne peut que souhaiter qu'en paraisse au plus tôt une démonstration détaillée.

Ajoutons que, dans le cas des courbes modulaires, Faltings a établi une variante de la décomposition de Hodge-Tate à coefficients dans certains systèmes locaux [G. Faltings, Hodge-Tate structures and modular forms, Math. Ann. 278 (1987), 133-149]. Une généralisation a été proposée par Hyodo [38].

4. LA CONJECTURE C_{st}

4.1. L'opérateur de monodromie de Hyodo-Kato

4.1.1. Soit X un S-schéma *semi-stable*. On entend par là que, localement pour la topologie étale, X est isomorphe à $S[t_1, \cdots, t_m]/(t_1 \cdots t_r - \pi)$, où π est une uniformisante de V ; il revient au même de dire que X est régulier, X_η est lisse et la fibre spéciale $Y = X_s$ est un diviseur à croisements normaux réduit dans X.

Quand Y est singulier, et même si X/S est propre, la cohomologie cristalline (usuelle) de Y/W est pathologique. Hyodo et Kato ont défini dernièrement une cohomologie cristalline modifiée, possédant, elle, de bonnes propriétés. Leur construction s'inspire de celle des structures de Hodge limites de Steenbrink [69] (voir [29] pour un aperçu de cette théorie). Ils définissent un système projectif de W_n-modules, que nous noterons $H^*_{st}(Y/W_n)$ (bien qu'ils dépendent en fait de X), munis d'un endomorphisme de Frobenius φ, σ-linéaire, et d'un *opérateur de monodromie* N, linéaire, liés par la relation

$$N\varphi = p\varphi N \tag{4.1.1.1}$$

(à rapprocher de (1.1.1)) ; pour X/S lisse, $H^*_{st}(Y/W_n)$ est la cohomologie cristalline usuelle $H^*(Y/W_n)$, $\varphi = \varphi$ et $N = 0$. Posons $H^*_{st}(Y/W) := \varprojlim H^*_{st}(Y/W_n)$. Alors, si X/S est *propre*, $H^*_{st}(Y/W)$ est de type fini sur W, $\varphi \otimes \mathbf{Q}_p$ est bijectif, $N \otimes K_0$ est nilpotent, et Hyodo et Kato construisent, pour toute uniformisante π de V, un isomorphisme (K-linéaire)

$$\rho_\pi : H^*_{st}(Y/W) \otimes_W K \xrightarrow{\sim} H^*_{DR}(X_K/K). \tag{4.1.1.2}$$

La dépendance de ρ_π en π s'exprime par $\rho_\pi = \rho_{\pi u} \exp(\log(u)N)$, où $u \in V^*$ et log est le logarithme usuel. Quand X/S est lisse, (4.1.1.2) coïncide avec l'isomorphisme de Berthelot-Ogus (2.2.1.1) (et ne dépend pas de π). Noter aussi que, dans le cas général, l'endomorphisme N de $H^*_{DR}(X_K/K)$ déduit de l'endomorphisme N de $H^*_{st}(Y/W)$ via ρ_π ne dépend pas du choix de π.

4.1.2. La philosophie qui sous-tend les constructions de Hyodo-Kato est que, du point de vue du calcul différentiel, les morphismes "à réduction

semi-stable" se comportent à peu près comme les morphismes lisses, pourvu que l'on remplace les complexes de de Rham usuels par des complexes de de Rham à pôles logarithmiques appropriés. La théorie de Hodge mixte de Deligne ([12], [13]) a popularisé l'usage de tels complexes, mais ce n'est que depuis peu — essentiellement depuis l'article de Hyodo [39] — qu'on s'est rendu compte qu'on pouvait aussi les utiliser avec fruit dans des situations de caractéristique mixte. Le fait d'avoir à travailler alors avec des diviseurs à croisements normaux non nécessairement relatifs à une base, le souci d'obtenir des constructions stables par changement de base (à cet égard, la définition de "semi-stable" en 4.1.1 ne l'est pas!) ont amené à dégager des structures additionnelles permettant de définir de bons complexes logarithmiques. Les fondements de cette théorie sont exposés par Kato [47] ; elles généralisent des constructions proposées par Deligne [16] et Faltings [21]. Signalons d'ailleurs que les applications (*cf.* [49], [50])dépassent déjà largement la seule définition de H^*_{st} (nouveaux points de vue sur les dégénérescences de groupes p-divisibles et de variétés abéliennes, et sur les compactifications de Chai-Faltings [10]).

La définition de base est la suivante. Soit X un schéma muni de la topologie étale (on pourrait partir plus généralement d'un espace — voire d'un topos — localement annelé ...). Kato définit une *structure pré-logarithmique* sur X comme un couple (M, a) formé d'un faisceau de monoïdes (commutatifs, à élément unité) M sur X et d'un morphisme multiplicatif (transformant 1 en 1) $a : M \to \mathcal{O}_X$. Soit M' le sous-faisceau $a^{-1}(\mathcal{O}_X^*)$ de M ; on dit que (M, a) est une *structure logarithmique* (ou *log-structure*) si a induit un isomorphisme de M' sur $\mathcal{O}_X^*$. Un schéma muni d'une structure logarithmique s'appelle un *schéma logarithmique* (ou *log-schéma*). Les morphismes sont définis de la manière évidente. Il y a une notion naturelle de structure logarithmique associée à une structure pré-logarithmique, et d'image directe (resp. inverse) par $f : X \to Y$. La structure logarithmique initiale (ou triviale) (resp. finale) sur X est $(\mathcal{O}_X^* \hookrightarrow \mathcal{O}_X)$ (resp. $\mathcal{O}_X \xrightarrow{Id} \mathcal{O}_X$). Les exemples les plus utiles sont:

a) Supposons X noethérien régulier (resp. lisse sur Y), et soit $D \subset X$ un diviseur à croisements normaux réduit (resp. relatif à Y) : on prend

$M = \mathcal{O}_X \cap j_*\mathcal{O}_U^* \hookrightarrow \mathcal{O}_X$, où $j : U = X - D \to X$ est l'inclusion.

b) La donnée d'un monoïde P et d'un homomorphisme $u : P \to \Gamma(X, \mathcal{O}_X)$ définit une log-structure sur X, associée à la pré-log-structure $P_X \to \mathcal{O}_X$ déduite de u (où P_X est le faisceau constant de valeur P sur X). L'exemple a) est localement de ce type: $\mathbf{N}^r \to \Gamma(X, \mathcal{O}_X)$, $(n_i) \mapsto \prod t_i^{n_i}$, où $t_1 \cdots t_r$ est une équation locale de D.

On peut définir dans ce cadre les notions d'immersion fermée, de morphismes étale, lisse, etc., et les propriétés usuelles (telles que caractérisations infinitésimales) s'étendent ; la théorie obtenue contient celle des plongements toroïdaux [52].

Si $f : (X, L) \to (Y, M)$ est un morphisme de log-schémas, on définit un $\mathcal{O}_X$-module de différentielles logarithmiques $\Omega^1_{X/Y}(\log L/M)$ (noté aussi, en abrégé $\omega^1_{X/Y}$) et $d : \mathcal{O}_X \to \omega^1_{X/Y}$, $d\log : M \to \omega^1_{X/Y}$ liés par $a(u)d\log u = da(u)$, avec les propriétés et la caractérisation universelle qu'on devine. On en déduit un *complexe de de Rham* $\omega^{\cdot}_{X/Y}$, où $\omega^i_{X/Y} = \Lambda^i \omega^1_{X/Y}$, avec la différentielle extérieure définie de la manière habituelle. Par exemple, si M est la structure triviale, si le morphisme sous-jacent $X \to Y$ est lisse, et L est la log-structure associée à un diviseur à croisements normaux relatifs $D \subset X$ comme en a), $\omega^{\cdot}_{X/Y}$ est le complexe logarithmique usuel $\Omega^{\cdot}_{X/Y}(\log D)$. La formation de ces complexes de de Rham est compatible aux changements de base. En caractéristique p, on a une théorie d'isomorphismes de Cartier, généralisant ceux considérés dans [39], [44], [21].

Enfin, on peut définir des notions de site et topos cristallin d'un log-schéma, et généraliser les résultats fondamentaux de [4] sur la comparaison entre cohomologie cristalline et cohomologie de de Rham.

4.1.3. Revenons à la situation de 4.1.1. Munissons X (resp. $S = \operatorname{Spec} V$) de la log-structure M (resp. N) associée au diviseur Y (resp. $s = \operatorname{Spec} k$) (le morphisme $(X, M) \to (S, N)$ est alors "lisse"), et Y (resp. s) de la structure image inverse M_1 (resp. N_1). Notons d'autre part L_n la log-structure sur $\operatorname{Spec} W_n$ asscié à $\mathbf{N} \to W_n$, $1 \mapsto 0$. On a donc un morphisme "lisse" $(Y, M_1) \to (s, N_1)$ et une "immersion fermée" $(s, N_1) \to (\operatorname{Spec} W_n, L_n)$

(l'identité pour $n = 1$). On pose

$$H^*_{st}(Y/W_n) := H^*((Y, M_1)/(\operatorname{Spec} W_n, L_n), \mathcal{O}_{Y/W_n})$$

(cohomologie cristalline à valeurs dans le faisceau structural). On a ainsi

$$H^*_{st}(Y/k) \xrightarrow{\sim} H^*(Y, \omega^{\cdot}_{Y/s})$$

(avec les notations de 4.1.2). En général, on a

$$H^*_{st}(Y/W_n) \xrightarrow{\sim} H^*(Y, C_n),$$

où C_n est un certain complexe de W_n-modules sur Y, bien défini dans la catégorie dérivée (l'image directe dérivée du faisceau structural par la projection du topos cristallin de $(Y, M_1)/(W_n, L_n)$ sur le topos étale de Y). Supposons que X/S se déduise par changement de base par une immersion fermée $S \hookrightarrow \operatorname{Spec} W[t]$ de

$\mathcal{Z} = \operatorname{Spec} W[t_1, \cdots, t_m] \to \operatorname{Spec} W[t]$, $t \mapsto t_1 \cdots t_r$, soit $\mathcal{Y}/W$ déduit de $\mathcal{Z}$ par le changement de base $t \mapsto 0$, et $\mathcal{Y}_n = \mathcal{Y} \otimes \mathbf{Z}/p^n$ (donc $Y = \mathcal{Y}_1$) :

$$\begin{array}{ccccccccc} Y & \hookrightarrow & X & \hookrightarrow & \mathcal{Z} & \hookleftarrow & \mathcal{Y} & \hookleftarrow & \mathcal{Y}_n \\ \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\ s & \hookrightarrow & S & \hookrightarrow & \operatorname{Spec} W[t] & \hookleftarrow & \operatorname{Spec} W & \hookleftarrow & \operatorname{Spec} W_n; \end{array}$$

munissons $\mathcal{Z}$ (resp. $\operatorname{Spec} W[t]$) de la log-structure définie par le diviseur $(t_1 \cdots t_r)$ $(= \mathcal{Y})$ (resp. (t)), et $\mathcal{Y}_n$ (resp. W_n) de la log-structure image inverse (c'est donc L_n sur W_n). On a alors $C_n = \omega^{\cdot}_{\mathcal{Y}_n/(W_n, L_n)}$. En général, l'opérateur de monodromie N est défini comme l'opérateur bord relatif à un certain triangle distingué $C_n[-1] \to D_n \to C_n \to$. Dans la situation précédente, ce triangle est donné par la suite exacte

$$0 \longrightarrow \omega^{\cdot-1}_{\mathcal{Y}_n/(W_n, L_n)} \xrightarrow{d \log t \wedge} \omega^{\cdot}_{\mathcal{Y}_n/W_n} \longrightarrow \omega^{\cdot}_{\mathcal{Y}_n/(W_n, L_n)} \longrightarrow 0,$$

où, au centre, on considère la log-structure triviale sur W_n. Dans le cas général, la définition du triangle se fait par des techniques de descente plus ou moins standard. Hyodo et Kato donnent de tout ceci des descriptions

canoniques en termes de complexes de de Rham-Witt (généralisant [43]) ; voir [29] pour une introduction.

La construction de l'isomorphisme ρ_π (4.1.1.2) suit assez fidèlement celle de Berthelot-Ogus [6] ; un point-clé est que (sous des hypothèses de log-lissité convenables et sur des bases assez générales) l'endomorphisme de Frobenius de la cohomologie cristalline est une isogénie.

4.2. La conjecture C_{st}

4.2.1. Fixons une uniformisante π de V et notons B_{st} l'anneau de Fontaine correspondant (1.2.3). Soit X un S-schéma *propre* et *semi-stable* (4.1.1), soit X_K sa fibre générique. Le K_0-espace vectoriel de dimension finie

$$H^m_{st}(X_K) := H^m_{st}(Y/W) \otimes_W K_0$$

(notations de 4.1.1) est muni de l'opérateur σ-linéaire bijectif φ et de l'endomorphisme K_0-linéaire nilpotent N, liés par $N\varphi = p\varphi N$. L'isomorphisme (4.1.1.2) fait de $H^*_{st}(X_K)$ une K_0-structure sur $H^*_{DR}(X_K/K)$. Avec la filtration de Hodge Fil, elle définit sur $H^*_{st}(X_K)$ une structure de (φ, N)-module filtré (1.3.5).

Une structure analogue sur la réalisation de de Rham d'un 1-motif sur K à réduction semi-stable a été définie indépendamment par Raynaud, par des techniques rigides analytiques [60]. Toutefois, dans le cas d'un 1-motif associé à une courbe sur K à réduction semi-stable, la comparaison avec la construction de Hyodo-Kato reste à faire.

Fontaine a proposé la conjecture suivante :

Conjecture 4.2.2 (*Conjecture C_{st}*).— *Sous les hypothèses de* 4.2.1, *la représentation $H^*(X_{\bar\eta}, \mathbf{Q}_p)$ est semi-stable* (1.3.2), *et canoniquement associée* (1.3.7) *au (φ, N)-module filtré $H^*_{DR}(X_K/K)$ défini ci-dessus : il existe un isomorphisme fonctoriel*

$$\alpha_{st} : B_{st} \otimes_{K_0} H^*_{st}(X_K) \xrightarrow{\sim} B_{st} \otimes_{\mathbf{Q}_p} H^*(X_{\bar\eta}, \mathbf{Q}_p)$$

compatible aux structures naturelles des deux membres (action de G, φ, N, et filtrations après extension des scalaires à K).

La validité de cette conjecture entraînerait notamment que la structure de (φ, N)-module filtré $H^*_{DR}(X_K/K)$ ne dépend pas du "modèle" semi-stable X (contrairement au cas de bonne réduction [34], on ne sait pas le vérifier directement).

La méthode de Faltings n'a pas permis pour l'instant de prouver 4.2.2. Par contre, par une adaptation au cadre logarithmique de la méthode de Fontaine-Messing [31], Kato a réussi à établir le résultat suivant :

THÉORÈME 4.2.3 [48].— *La conjecture C_{st} est vraie si* $\dim X_K < (p-1)/2$.

De plus, H^*_{st} vérifie une dualité de Poincaré et l'isomorphisme α_{st} construit par Kato y est compatible.

4.2.4. Désignons maintenant par X un schéma propre et lisse sur K. Si l'on est optimiste, on peut espérer qu'il existe une extension finie K' de K telle que $X_{K'}$ admette un modèle propre et semi-stable $\mathcal{X}$ sur l'anneau des entiers de K'. C'est le cas si $\dim X \leq 1$, par le théorème de réduction semi-stable d'Artin-Deligne-Mumford ([18], [2]), et l'analogue en égale caractéristique nulle et dimension quelconque est vrai également par Mumford [52]. Compte tenu de 4.2.2, ceci amène à faire la conjecture suivante :

Conjecture 4.2.5 (*Conjecture de monodromie p- adique*).— *Pour X propre et lisse sur K, la représentation $H^*(X_{\bar{\eta}}, \mathbf{Q}_p)$ est potentiellement semi-stable, i.e. il existe une extension finie $L \subset \bar{K}$ de K telle que la représentation correspondante de* $\mathrm{Gal}(\bar{K}/L)$ *soit semi-stable.*

4.3. La méthode de Fontaine-Messing-Kato

4.3.1. Nous reprenons les hypothèses et notations de 4.2.1 et 4.1.3. Nous poserons en outre $V_n = V/p^nV$, $S_n = \mathrm{Spec}\, V_n$, $X_n = X \times_S S_n$, $\bar{X} = X \times_S \bar{S}$, $\bar{V}_n = \bar{V}/p^n\bar{V}$, $\bar{S}_n = \mathrm{Spec}\, \bar{V}_n$, $\bar{X}_n = \bar{X} \times_{\bar{S}} \bar{S}_n$ (et nous écrirons Y, $\bar{Y}$ au lieu de X_1, $\bar{X}_1$). La démonstration de 4.2.3 se fait en trois étapes.

4.3.2. *Interprétation cristalline de* $\left(B^+_{st} \otimes_{K_0} H^*_{st}(X_K)\right)_{N=0}$

Soit $\bar{N}$ la log-structure sur $\bar{S}$ limite inductive des images inverses des

log-structures canoniques (*i.e.* associées au point fermé) sur les Spec V', où V' parcourt les anneaux d'entiers d'extensions finies de K contenues dans $\bar{K}$. Soit $\bar{N}_n$ la log-structure image inverse de $\bar{N}$ sur $\bar{S}_n$ et $\bar{M}_n$ celle sur $\bar{X}_n$ déduite de M sur X par le changement de base $(\bar{S}_n, \bar{N}_n) \to (S, N)$. (Noter que, bien que $\bar{X}_n$ soit singulier du point de vue des log-schémas, $(\bar{X}_n, \bar{M}_n) \to (\bar{S}_n, \bar{N}_n)$ est un morphisme lisse !) Kato construit un isomorphisme canonique (G-équivariant)

$$(4.3.2.1) \qquad \left(B^+_{st} \otimes_{K_0} H^m_{st}(X_K)\right)_{N=0} \xrightarrow{\sim} \mathbf{Q} \otimes \varprojlim_n H^m((\bar{X}_n, \bar{M}_n)/W_n),$$

où l'indice $N = 0$ indique le noyau de N (opérant par $N \otimes 1 + 1 \otimes N$), et $H^m((\bar{X}_n, \bar{M}_n)/W_n)$ est la cohomologie cristalline (à valeurs dans le faisceau structural) du log-schéma $(\bar{X}_n, \bar{M}_n)$ relativement à W_n, muni de la log-structure triviale. Les ingrédients de la démonstration sont : a) une interprétation cristalline de B^+_{st} analogue à celle de B^+_{cris} signalée en 1.2.2 ; b) l'isomorphisme de Hyodo-Kato (4.1.1.2) (ou plutôt les techniques, évoquées en 4.1.3, permettant de le construire).

4.3.3. *Cycles évanescents et faisceaux* $s^{\log}_n(r)$

Dans la méthode de Fontaine-Messing [31], le coeur de la démonstration consiste en la construction de certains faisceaux $S_n(r)$ sur le site "syntomique-étale" de $\bar{X}$, servant de pont entre les faisceaux de Tate usuels $(\mathbf{Z}/p^n\mathbf{Z})(r)$ sur $X_{\bar{\eta}}$ et le noyau de $\varphi - p^r$ sur la cohomologie cristalline. Kato transpose ceci au cadre logarithmique. Pour $0 \leq r < p$, il construit un système projectif de complexes de G-faisceaux étales $s^{\log}_n(r)$ sur $\bar{X}$, concentrés sur $\bar{Y}$, donnant lieu à des triangles distingués

$$(4.3.3.1) \qquad s^{\log}_n(r) \longrightarrow Ru_* J^{[r]}_{\bar{X}_n/W_n} \xrightarrow{1-p^{-r}\varphi} Ru_* \mathcal{O}_{\bar{X}_n/W_n} \longrightarrow,$$

où u est le morphisme du topos cristallin de $(\bar{X}_n, \bar{M}_n)/W_n$ vers le topos étale de $\bar{X}$ et $J^{[r]}_{\bar{X}_n/W_n}$ désigne la r-ième puissance divisée de l'idéal $J_{\bar{X}_n/W_n} = \mathrm{Ker}(\mathcal{O}_{\bar{X}_n/W_n} \to \mathcal{O}_{\bar{X}_n})$. On a en particulier des suites exactes longues, G-équivariantes

$$(4.3.3.2) \qquad \begin{aligned} \cdots \longrightarrow H^m(\bar{X}, s^{\log}_n(r)) \longrightarrow H^m((\bar{X}_n, \bar{M}_n), J^{[r]}) \\ \xrightarrow{1-p^{-r}\varphi} H^m((\bar{X}_n, \bar{M}_n), \mathcal{O}) \longrightarrow \cdots \end{aligned}$$

Notons

$$\bar{Y} \overset{\bar{i}}{\hookrightarrow} \bar{X} \overset{\bar{j}}{\hookleftarrow} X_{\bar{\eta}}$$

les inclusions. Le point clé dans la comparaison avec la cohomologie étale de $X_{\bar{\eta}}$ est le résultat suivant :

THÉORÈME 4.3.3.3 [48].— *Pour $0 \leq r < p-1$, il existe un système projectif d'isomorphismes*

$$s_n^{\log}(r) \xrightarrow{\sim} \tau_{\leq r} \bar{i}_* \bar{i}^* R\bar{j}_*(\mathbf{Z}/p^n\mathbf{Z}(r))$$

dans la catégorie dérivée des G-faisceaux étales sur $\bar{X}$, où τ est la troncation canonique.

La variante "sans pôles logarithmiques" de 4.3.3.3 a été établie par Kurihara [53], à l'aide de résultats antérieurs de Bloch-Kato [7] et Kato [46] sur le calcul des cycles évanescents p-adiques. Dans le cas de réduction semi-stable, Kato utilise, à leur place, ceux de Hyodo [39].

Par le théorème de changement de base propre, on déduit de 4.3.3.3 un isomorphisme

$$H^m(\bar{X}, s_n^{\log}(r)) \xrightarrow{\sim} H^m(X_{\bar{\eta}}, \mathbf{Z}/p^n(r)) \tag{4.3.3.4}$$

pour $0 \leq m \leq r < p-1$. Cet isomorphisme est G-équivariant, et compatible aux produits (il y a un produit naturel $s_n^{\log}(r) \overset{L}{\otimes} s_n^{\log}(s) \to s_n^{\log}(r+s)$ pour $0 \leq r+s < p$).

4.3.4. *Définition de α_{st} et fin de la démonstration*

Soit $0 \leq m \leq r < p-1$. On déduit de (4.3.3.2) et (4.3.3.4) une flèche

$$H^m(X_{\bar{\eta}}, \mathbf{Z}/p^n(r)) \longrightarrow H^m((\bar{X}_n, \bar{M}_n)/W_n)_{\varphi=p^r},$$

d'où, par application de $\mathbf{Q} \otimes \varprojlim$, une flèche ($G$-équivariante)

$$H^m(X_{\bar{\eta}}, \mathbf{Q}_p)(r) \longrightarrow \mathbf{Q} \otimes \varprojlim H^m((\bar{X}_n, \bar{M}_n)/W_n)_{\varphi=p^r}.$$

Grâce à (4.3.2.1), cette flèche se récrit

$$H^m(X_{\bar{\eta}}, \mathbf{Q}_p)(r) \longrightarrow \left(B_{st}^+ \otimes_{K_0} H_{st}^m(X)\right)_{N=0, \varphi=p^r}.$$

Tensorisant par $\mathbf{Q}_p(-r)$ (*cf.* 1.2.2, 1.2.3), on obtient une flèche

$$H^m(X_{\bar{\eta}}, \mathbf{Q}_p) \longrightarrow \left(B_{st}^+ \otimes_{K_0} H_{st}^m(X)\right)_{N=0,\varphi=1}$$

(qui, pour m fixé, ne dépend pas du choix de r). Par extension des scalaires, on en déduit finalement

$$\beta_{st} : B_{st} \otimes_{\mathbf{Q}_p} H^m(X_{\bar{\eta}}, \mathbf{Q}_p) \longrightarrow B_{st} \otimes_{K_0} H_{st}^m(X), \tag{4.3.4.1}$$

compatible à φ, N, et à l'action de G. On vérifie que β_{st} est compatible à la dualité de Poincaré (ce qui nécessite l'hypothèse $2d < p-1$, où $d = \dim X_K$), d'où par l'argument habituel, la bijectivité de β_{st}. Une généralisation au cas logarithmique d'un résultat de Kato-Messing [51] permet de montrer que la flèche obtenue par extension des scalaires à B_{DR} est compatible aux filtrations, et cela termine la démonstration (α_{st} est l'inverse de β_{st}).

Problème 4.3.5.— On dispose, finalement, de plusieurs isomorphismes de périodes p-adiques, obtenus par diverses méthodes :

(1) la décomposition de Hodge-Tate (2.1.3.2) pour $m = 1$ et X une variété abélienne sur K, donnée par Tate [70] et Raynaud (*cf.* [9]) ;

(2) les décompositions analogues données par Fontaine [24] et Coleman [R.F. Coleman, Hodge-Tate periods and p-adic abelian integrals, Inv. math. 78 (1984), 351-379] ;

(3) la décomposition de Hodge-Tate (2.1.3.2) donnée par Bloch et Kato [7] pour X ayant bonne réduction ordinaire, et sa généralisation par Hyodo [39] au cas de réduction semi-stable ordinaire ;

(4) la décomposition de Hodge-Tate (2.1.3.2) donnée par Faltings [19] (l'inverse de l'isomorphisme β (3.5.2.3) dans le cas de bonne réduction) ;

(5) l'isomorphisme α_{cris} (2.2.2) construit par Fontaine et Messing [31], pour $\dim X < p$ et $K = K_0$;

(6) l'isomorphisme α_{cris} (2.2.2) construit par Faltings [20] (voir (3.6.1) ;

(7) l'isomorphisme α_{DR} (2.1.2) (voir 3.6.2) ;

(8) l'isomorphisme α_{st} (4.2.2) construit par Kato [48], pour X_K ayant réduction semi-stable et $2 \dim X_K < p-1$.

Il serait intéressant de comparer ces isomorphismes. A la connaissance du rapporteur, les seules compatibilités à figurer dans la littérature sont la comparaison entre les deux décompositions (2) dans Coleman *loc. cit.*, et la comparaison entre (1) et (2) dans [24].

(Ajouté en juillet 1990) Faltings m'informe qu'il vient de vérifier les compatibilités entre (1), (4), (6) et (7) (celle entre (1) et (4) vient d'être également vérifiée, indépendamment, par Wintenberger).

BIBLIOGRAPHIE

[1] V.-A. ABRASHKIN - *Galois moduli of period p group schemes over a ring of Witt sectors*, Math. USSR Izvestia 31 (1988), 1-46.

[2] M. ARTIN and G. WINTERS - *Degenerate fibers and reduction of curves*, Topology 10 (1971), 373-383.

[3] A. BEILINSON - *Higher regulators and values of L-functions*, Soviet Math. 30 (1985), 2036-2070.

[4] P. BERTHELOT - *Cohomologie cristalline des schémas de caractéristique $p > 0$*, Lecture Notes in Math. 407, Springer-Verlag, 1974.

[5] P. BERTHELOT et A. OGUS - *Notes on crystalline cohomology*, Math. Notes, Princeton University Press, 1978.

[6] P. BERTHELOT and A. OGUS - *F-isocrystals and de Rham cohomology* I, Inv. Math. 72 (1983), 159-199.

[7] S. BLOCH and K. KATO - *p-adic étale cohomology*, Pub. Math. IHES 63 (1986), 107-152.

[8] S. BLOCH and K. KATO - *L-functions and Tamagawa numbers of motives*, à paraître dans Grothendieck Festschrift, Progress in Math., Birkhäuser, 1990.

[9] F. BOGOMOLOV - *Sur l'algébricité des représentations ℓ-adiques*, C.R.A.S. Paris 290 (1980), 701-703.

[10] C.-L. CHAI and G. FALTINGS - *Semi-abelian degeneration and compactification*, preprint, 1989.

[11] L. CLOZEL - *Nombres de Tamagawa des groupes semi-simples*, d'après

Kottwitz, Sém. Bourbaki, Nov. 1988, exp. n° 702, Astérisque 177-178 (1989), 61-82.

[12] P. DELIGNE - *Théorie de Hodge* II, Publ. Math. IHES 40 (1972), 5-57.

[13] P. DELIGNE - *Théorie de Hodge* III, Publ. Math. IHES 44 (1974), 5-77.

[14] P. DELIGNE - *Valeurs de fonctions L et périodes d'intégrales* Proc. Symp. Pure Math. 33 (1979), AMS, 313-346.

[15] P. DELIGNE - *Hodge cycles on abelian varieties* dans Hodge Cycles, Motives and Shimura Varieties, Lecture Notes in Math. 900, Springer-Verlag, 1982.

[16] P. DELIGNE - Lettre à L. Illusie, 1.6.1988.

[17] P. DELIGNE et L. ILLUSIE - *Relèvements modulo p^2 et décomposition du complexe de de Rham*, Inv. Math. 72 (1987), 247-270.

[18] P. DELIGNE et D. MUMFORD - *The irreducibility of the space of curves of given genus*, Publ. Math. IHES 36 (1969), 75-109.

[19] G. FALTINGS - *p-adic Hodge theory*, Journal of the AMS 1 (1988), 255-299.

[20] G. FALTINGS - *Crystalline cohomology and p-adic Galois representations*, preprint, 1988.

[21] G. FALTINGS - *F-isocrystals on open varieties, results and conjectures*, à paraître dans Grothendieck Festchrift, Progress in Math., Birkhäuser, 1990.

[22] J.-M. FONTAINE - *Modules galoisiens, modules filtrés et anneaux de Barsotti-Tate*, dans Journées de géométrie algébrique de Rennes (III), Astérisque 65 (1979), 3-80.

[23] J.-M. FONTAINE - *Sur certains types de représentations p-adiques du groupe de Galois d'un corps local ; construction d'un anneau de Barsotti-Tate*, Ann. of Math. 115 (1982), 529-577.

[24] J.-M. FONTAINE - *Formes différentielles et modules de Tate des variétés abéliennes sur les corps locaux*, Inv. Math. 65 (1982), 379-409.

[25] J.-M. FONTAINE - *Cohomologie de de Rham, cohomologie cristalline et représentations p-adiques*, dans Algebraic Geometry Tokyo-Kyoto, Lecture Notes in Math. 1016, Springer-Verlag (1983), 86-108.

[26] J.-M. FONTAINE - *Il n'y a pas de variété abélienne sur* **Z**, Inv. Math. 81 (1985), 515-538.

[27] J.-M. FONTAINE - *Le corps des périodes p-adiques*, preprint, à paraître dans [Bures].

[28] J.-M. FONTAINE - *Représentations p-adiques semi-stables*, preprint, à paraître dans [Bures].

[29] J.-M. FONTAINE et L. ILLUSIE - *p-adic periods, a survey*, Indo-French conf. on geometry, Bombay, 1989, à paraître.

[30] J.-M. FONTAINE et G. LAFFAILLE - *Construction de représentations p-adiques*, Ann. Sc. ENS 15 (1982), 547-608.

[31] J.-M. FONTAINE and W. MESSING - *p-adic periods and p-adic étale cohomology*, Contemporary Mathematics 67 (1987), 179-207.

[32] J.-M. FONTAINE et B. MAZUR - *Représentations ℓ-adiques potentiellement semi-stables*, preprint, à paraître dans [Bures].

[33] J.-M. FONTAINE et B. PERRIN-RIOU - *Cohomologie galoisienne et valeurs de fonctions L (autour de Bloch-Kato)*, en préparation.

[34] H. GILLET and W. MESSING - *Cycle classes and Riemann-Roch for crystalline cohomology*, Duke Math. J. 55 (1987), 501-538.

[35] B. GROSS - *On the periods of Abelian integrals and a formula of Chowla and Selberg*, Inv. Math. 45 (1978), 193-211.

[36] A. GROTHENDIECK - *Groupes de Barsotti-Tate et cristaux*, Actes Congrès Int. Math. Nice 1970, I, Gauthier-Villars, Paris, 1971.

[37] A. GROTHENDIECK - *Groupes de Barsotti-Tate et cristaux de Dieudonné*, Presses de l'Université de Montréal, 1974.

[38] O. HYODO - *On variation of Hodge-Tate structures*, preprint, 1987.

[39] O. HYODO - *A note on p-adic étale cohomology in the semi-stable reduction case*, Inv. Math. 91 (1988), 543-557.

[40] O. HYODO and K. KATO - *Semi-stable reduction and crystalline cohomology with logarithmic poles*, preprint, à paraître dans [Bures].

[41] L. ILLUSIE - *Report on crystalline cohomology*, Proc. Symp. Pure Math. XXIX (1975), 459-478.

[42] L. ILLUSIE - *Cohomologie cristalline, d'après P. Berthelot*, Sém. Bourbaki, exp. n° 456, Lecture Notes in Math. 514, Springer-Verlag, 1976.

[43] L. ILLUSIE - *Complexe de de Rham-Witt et cohomologie cristalline*, Ann. Sc. ENS 12 (1979), 501-661.

[44] L. ILLUSIE - *Réduction semi-stable et décomposition de complexes de de Rham à coefficients*, Duke Math. J. 60 (1990), 139-185.

[45] U. JANNSEN - *On the ℓ-adic cohomology of varieties over number fields and its Galois cohomology*, preprint, 1988.

[46] K. KATO - *On p-adic vanishing cycles (application of ideas of Fontaine-Messing)*, Advanced Studies in Pure Math. 10 (1987), 207-251.

[47] K. KATO - *Logarithmic structures of Fontaine-Illusie*, Algebraic analysis, Geometry and Number Theory, The Johns Hopkins Univ. Press (1989), 191-224.

[48] K. KATO - *Semi-stable reduction and p-adic étale cohomology*, preprint, à paraître dans [Bures].

[49] K. KATO - *Logarithmic degeneration and Dieudonné theory*, preprint, 1989.

[50] K. KATO - *Toric singularities*, preprint, 1990.

[51] K. KATO and W. MESSING - *Syntomic cohomology and p-adic étale cohomology*, preprint, 1989.

[52] G. KEMPF, F. KNUDSEN, D. MUMFORD and B. SAINT-DONAT - *Toroidal embeddings* I, Lecture Notes in Math. 339, Springer-Verlag, 1973.

[53] M. KURIHARA - *A note on p-adic étale cohomology*, Proc. Japan Academy 63 (1987), 275-278.

[54] B. MAZUR, J. TATE and J. TEITELBAUM - *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer*, Inv. Math. 84 (1986), 1-48.

[55] M. NAGATA - *Imbedding of an abstract variety in a complete variety*, J. Math. Kyoto 2 (1962), 1-10.

[56] A. OGUS - *Hodge cycles and crystalline cohomology*, dans Hodge Cycles, Motives and Shimura Varieties, Lecture Notes in Math. 900, Springer-Verlag, 1982.

[57] A. OGUS - *F-isocrystals and de Rham cohomology* II - *convergent isocrystals*, Duke Math. J. 51 (1984), 765-850.

[58] A. OGUS - *A p-adic analogue of the Chowla-Selberg formula*, preprint, 1990.

[59] M. RAYNAUD - *Anneaux locaux henséliens*, Lecture Notes in Math 169, Springer-Verlag, 1970.

[60] M. RAYNAUD - *Réalisation de de Rham des 1-motifs*, à paraître dans [Bures].

[61] M. RAPOPORT, N. SCHAPPACHER, P. SCHNEIDER (eds) - *Beilinson's conjectures on special values of L functions*, Perspectives in Math. 4, Academic Press, New York, 1988.

[62] S. SEN - *Lie algebras of Galois groups arising from Hodge-Tate modules*, Ann. of Math. 97 (1973), 160-170.

[63] J.-P. SERRE - *Sur les groupes de Galois attachés aux groupes p-divisibles*, Proc. of a Conf. on local fields, Driebergen 1966, Springer-Verlag (1967), 118-131.

[64] J.-P. SERRE - Résumé des cours 1965-66, dans Annuaire du Collège de France, Paris, 1967, 49-58.

[65] J.-P. SERRE - *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Inv. Math. 15 (1972), 259-331.

[66] J.-P. SERRE - *Groupes algébriques associés aux modules de Hodge-Tate*, Journées de géométrie algébrique de Rennes 1978, III, Astérisque 65 (1979), 155-188.

[67] J.-P. SERRE - *Motifs*, Journées arithmétiques de Luminy 1989, à paraître dans Astérisque.

[68] J.-P. SERRE and J. TATE - *Good reduction of abelian varieties*, Ann. of Math. 88 (1968), 492-517.

[69] J. STEENBRINK - *Limits of Hodge structures*, Inv. Math. 31 (1976), 229-257.

[70] J. TATE - *p-divisible groups*, dans Proc. of a conf. on local fields, Driebergen (1967), 158-183.

[71] J.-P. WINTENBERGER - *Torseur entre cohomologie étale p-adique et cohomologie cristalline ; le cas abélien*, soumis à Duke Math. J.

[72] J.-P. WINTENBERGER - *Théorème de comparaison p-adique pour les schémas abéliens*, en préparation.

[CL] J.-P. SERRE - *Corps locaux*, Hermann, Paris, 1962.

[SGA 1] *Revêtements étales et groupe fondamental*, Séminaire de Géométrie Algébrique du Bois-Marie 1960-61, dirigé par A. Grothendieck, Lecture Notes in Math. 224, Springer-Verlag, 1971.

[SGA 2] *Cohomologie locale des faisceaux cohérents et théorèmes de Lefschetz locaux et globaux*, Séminaire de Géométrie Algébrique du Bois-Marie 1961-62, dirigé par A. Grothendieck, North Holland Pub. Comp., Amsterdam, 1968.

[SGA 4] *Théorie des topos et cohomologie étale des schémas*, Séminaire de Géométrie Algébrique du Bois-Marie 1963-64, dirigé par M. Artin, A. Grothendieck et J.-L. Verdier, Lecture Notes in Math. 269, 270, 305, Springer-Verlag, 1972-73.

[SGA 7] *Groupes de monodromie en géométrie algébrique*, Séminaire de Géométrie Algébrique du Bois-Marie 1967-69, I, dirigé par A. Grothendieck, Lecture Notes in Math. 288, Springer-Verlag, 1972.

[SGA $4\frac{1}{2}$] *Cohomologie étale*, par P. Deligne, Lecture Notes in Math. 569, Springer-Verlag, 1977.

[Bures] *Périodes p-adiques*, Séminaire dirigé par J.-M. Fontaine à l'IHES, janvier-mai 1988, actes en préparation.

Luc ILLUSIE

Université de Paris-Sud
Arithmétique et géométrie algébrique
CNRS URA D0752
Bâtiment 425
F-91405 Orsay Cedex

Astérisque

JOSEPH OESTERLÉ

Empilements de sphères

Astérisque, tome 189-190 (1990), Séminaire Bourbaki,
exp. n° 727, p. 375-397

<http://www.numdam.org/item?id=SB_1989-1990__32__375_0>

© Société mathématique de France, 1990, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Séminaire BOURBAKI juin 1990
42ème année, 1989-90, n° 727

EMPILEMENTS DE SPHÈRES

par **Joseph OESTERLÉ**

Contrairement à l'usage en mathématiques, le mot "sphère" signifie ici "sphère pleine", *i.e.* est synonyme de "boule fermée".

Soit E un espace euclidien de dimension n. Un *empilement de sphères* dans E est une famille de sphères de même rayon d'intérieurs mutuellement disjoints. À tout réseau L de E, on associe un empilement de sphères : ces sphères ont pour centres les points de L et leur rayon commun est le plus grand pour lequel elles forment un empilement.

Soit (S_i) un empilement de sphères. Lorsque la limite

$$\lim_{R\to\infty} [\mathrm{vol}((\cup S_i) \cap B(0,R))/\mathrm{vol}(B(0,R))]$$

existe, on l'appelle la *densité de l'empilement.* Par exemple, l'empilement de sphères associé à un réseau L de E a pour densité

$$d(L) = \mathrm{vol}(B(0,r))/v = b_n\, r^n/v, \tag{1}$$

où r est le rayon commun des sphères, v le volume de E modulo L et $b_n = \pi^{n/2}/\Gamma\left(\frac{n+2}{2}\right)$ celui de la boule unité de E. Par abus de langage, on dit que $d(L)$ est la *densité du réseau* L.

Deux questions fondamentales concernant les empilements de sphères sont :

a) *Quelle est la densité maximale δ_n d'un empilement de sphères dans E ?*

b) *Quelle est la densité maximale d_n d'un réseau de E ?*

(Dans chacun des deux cas, on peut montrer que la densité maximale est effectivement atteinte ; par ailleurs, elle ne dépend que de n, puisque deux espaces euclidiens de même dimension sont isométriques. Enfin, il est clair que l'on a $d_n \leq \delta_n \leq 1$.)

Après quelques rappels sur l'état de ces questions, nous décrirons le procédé d'Elkies et Shioda qui , en utilisant l'arithmétique des courbes elliptiques sur les corps de fonctions, permet de retrouver (au moins en dimension ≤ 1000) la plupart des réseaux très denses connus et, pour certaines dimensions (par exemple 33, 54, 64, 80,...) d'en découvrir de nouveaux, plus denses.

La taille de cet exposé ne nous a pas permis d'aborder d'autres sujets pourtant fort intéressants : empilements de corps convexes, recouvrements par des sphères, nombre maximal de contacts entre sphères de même rayon (kissing number), applications à la géométrie des nombres, liens profonds entre la théorie du codage et celle des empilements de sphères, géométrie très riche des réseaux les plus denses connus, etc. Le lecteur intéressé pourra consulter le livre de Rogers ([Ro]), et celui de Conway et Sloane ([C,S]), qui contiennent d'excellentes bibliographies sur ces sujets.

1. EMPILEMENTS DE SPHÈRES

1.1. La dimension 2

La densité maximale d'un empilement de sphères en dimension 2 est $\delta_2 = \pi/2\sqrt{3} = 0,9068\ldots$. C'est la densité de l'empilement associé au réseau hexagonal :

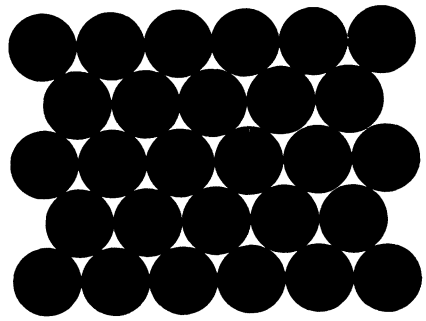


Figure 1.

Ce résultat, énoncé en 1882 par Thue ([Th]), n'a été démontré de façon complètement satisfaisante qu'en 1940 par Fejes ([Fe]). Une preuve élégante est due à Rogers ([Ro], ch. 7), qui démontre pour tout $n \geq 1$ l'inégalité

$$\delta_n \leq \sigma_n, \tag{2}$$

où σ_n est, dans un simplexe régulier à $n+1$ sommets de côté 2, la proportion du volume recouverte par les sphères de rayon 1 centrées aux sommets. (Pour $n = 2$, on a $\sigma_2 = \pi/2\sqrt{3}$ et (2) est une égalité car le plan peut être pavé par des triangles équilatéraux.)

1.2. La dimension 3

On ne connaît la densité maximale δ_n des empilements de sphères en dimension n pour aucun entier $n \geq 3$. Pour $n = 3$ par exemple, l'inégalité de Rogers $\delta_3 \leq \sigma_3 = \sqrt{2}(3 \operatorname{Arc\,cos} \frac{1}{3} - \pi) = 0,7796\ldots$ n'est pas une égalité. (On ne peut paver $\mathbf{R}^3$ par des tétraèdres réguliers car l'angle entre leurs faces, égal à $\operatorname{Arc\,cos} \frac{1}{3}$, ne divise pas 2π.) La majoration de Rogers a été légèrement améliorée par Lindsey: on a $\delta_3 < 0,7784\ldots$.

Considérons dans $\mathbf{R}^3$ le réseau

$$L = \{(n_1, n_2, n_3) \in \mathbf{Z} \mid n_1 + n_2 + n_3 \in 2\mathbf{Z}\}$$

(dit "cubique à faces centrées", car il s'obtient en répétant dans les trois directions le motif obtenu en plaçant des points aux sommets et aux centres des faces d'un cube) :

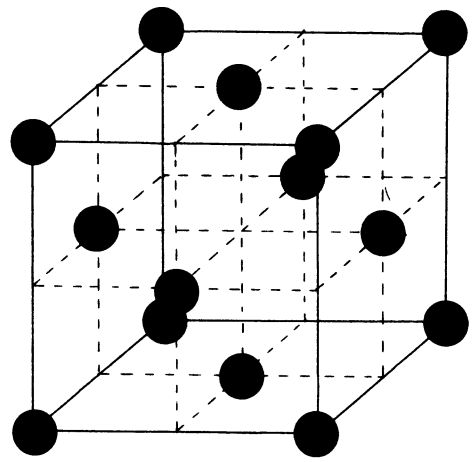


Figure 2.

L'empilement de sphères associé a pour densité $\pi/3\sqrt{2} = 0,7404\ldots$. Le réseau L est isométrique au réseau engendré par le système de racines A_3 : en effet, $(1,1,0)$, $(-1,0,1)$ et $(1,-1,0)$ forment une base de L par rapport à laquelle la matrice du produit scalaire de $\mathbf{R}^3$ est $\begin{pmatrix} 2 & -1 & 0 \\ -1 & 2 & -1 \\ 0 & -1 & 2 \end{pmatrix}$. C'est pourquoi on note A_3 le réseau L et l'empilement de sphères associé. Gauss a démontré que A_3 est le réseau le plus dense en dimension 3, c'est-à-dire que l'on a $d_3 = \pi/3\sqrt{2}$.

L'empilement A_3 est celui suivant lequel les épiciers empilent les oranges : il s'obtient en superposant des couches horizontales de sphères, les sphères de chaque couche étant réparties suivant un réseau carré et celles de la $n+1$-ième couche venant s'insérer dans les trous les plus profonds de la n-ième couche.

Lorsqu'on veut superposer de la même manière des couches horizontales dans lesquelles les sphères sont disposées suivant un réseau hexagonal (fig. 1), on peut poser la $n+1$-ième couche sur la n-ième de deux façons. Cela conduit à différents empilements possibles. L'un d'eux est encore

l'empilement A_3 (regarder la fig. 2 en prenant comme verticale une grande diagonale du cube), mais d'autres ne sont pas associés à des réseaux. Tous ces empilements ont la même densité $\pi/3\sqrt{2}$.

On ne connaît aucun empilement de sphères plus dense en dimension 3, d'où la célèbre phrase de Rogers : "Many mathematicians believe, and all physicists know, that the density cannot exceed $\pi/3\sqrt{2}$".

1.3. Les dimensions plus grandes

Pour certaines dimensions (par exemple $n = 10, 11, 13$), les empilements de sphères les plus denses connus actuellement ne sont pas associés à des réseaux. Il se pourrait que l'on ait $d_n < \delta_n$ pour ces dimensions.

Lorsque n est grand, la constante σ_n intervenant dans la majoration de Rogers est équivalente à $ne^{-1}\,2^{-n/2}$. Une meilleure majoration asymptotique de δ_n a été obtenue par Kabatiansky et Levenshtein [K,L] : pour n assez grand, on a $\delta_n \leq 2^{-0,599\,n}$.

Si l'on choisit un empilement de sphères *maximal* dans un espace euclidien E, on obtient un recouvrement de E en prenant les sphères de mêmes centres et de rayon double. De cette remarque élémentaire, on déduit aussitôt la minoration $\delta_n \geq 2^{-n}$. (On peut faire mieux : d'après Rogers ([Ro], th. 2.4), δ_n est supérieur à $\left(\frac{n}{2(n+1)}\right)^{n/2}\sigma_n$, qui est équivalent à $ne^{-3/2}\,2^{-n}$ lorsque n tend vers ∞.) Curieusement, personne n'a su jusqu'à présent exhiber "explicitement" pour une infinité de dimensions n, des empilements de sphères de densité $\geq 2^{-n}$; le mieux qui ait été fait dans cette direction est la construction explicite, par Rosenbloom et Tsfasman ([R,T]), d'empilements de sphères (associés à des réseaux) de densité $\geq 2^{-1,39\,n}$ pour une infinité de dimensions n.

1.4. Empilements aléatoires

Avant d'achever ce paragraphe, il convient de signaler le très joli chapitre 22 du livre de géométrie de Coxeter ([Co]) où sont décrits quelques faits expérimentaux concernant les empilements "aléatoires" en dimension 3. Coxeter mentionne en particulier les observations suivantes de G.D. Scott :

lorsqu'on remplit une grande boîte de petites billes identiques, en déversant les billes en vrac dans la boîte, on constate que la densité de l'empilement obtenu est d'environ $0,60$; si l'on agite la boîte pendant qu'on la remplit, l'empilement obtenu est plus dense et on constate que sa densité, remarquablement stable, est voisine de $0,6366$ (c'est-à-dire de $\frac{2}{\pi}$). Aucun modèle mathématique permettant d'expliquer ces observations n'existe à ce jour.

2. EMPILEMENTS DE SPHÈRES ASSOCIÉS À DES RÉSEAUX

2.1. Densité et constante d'Hermite

Soient E un espace euclidien de dimension n et L un réseau de E . Posons

$$m(L) = \inf_{\ell \in L, \ell \neq 0} \langle \ell, \ell \rangle. \tag{3}$$

Par abus de langage, les vecteurs $\ell \in L$ tels que $m(L) = \langle \ell, \ell \rangle$ sont appelés les *vecteurs minimaux* de L. Le nombre

$$\operatorname{disc}(L) = \det(\langle \ell_i, \ell_j \rangle), \tag{4}$$

où (ℓ_i) est une base de L, ne dépend pas de la base choisie et s'appelle le *discriminant* de L. Posons

$$\gamma(L) = m(L)/\operatorname{disc}(L)^{1/n}. \tag{5}$$

Le volume de E modulo L est $v = \sqrt{\operatorname{disc}(L)}$. L'empilement de sphères associé à L est formé de sphères de rayon $r = \frac{1}{2}\sqrt{m(L)}$ et sa densité est, d'après la formule (1)

$$d(L) = 2^{-n}\, b_n\, \gamma(L)^{n/2},$$

où $b_n = \pi^{n/2}/\Gamma\left(\frac{n+2}{2}\right)$ est le volume de la boule unité de E.

Le nombre $\gamma_n = \sup_L \gamma(L)$ est appelé la *constante d'Hermite* (en dimension n). Il est lié à la densité maximale d_n des réseaux de E par la relation

$$d_n = 2^{-n}\, b_n\, \gamma_n^{n/2}.$$

On a $\gamma_n \geq 1$: en effet si L est un réseau de E engendré par une base orthonormale de E, on a $m(L) = \mathrm{disc}(L) = \gamma(L) = 1$. Par ailleurs de l'inégalité $d_n \leq 1$ on déduit $\gamma_n = O(n)$.

Il est commode d'appeler *réseau euclidien* un $\mathbf{Z}$-module libre de rang fini L muni d'une application bilinéaire symétrique $B : L \times L \to \mathbf{R}$ "définie positive", *i.e.* possédant les propriétés équivalentes suivantes :

i) la forme bilinéaire sur $L \otimes_{\mathbf{Z}} \mathbf{R}$ qui prolonge B est définie positive ;

ii) la matrice de B dans une base de L est définie positive ;

iii) pour tout $c \geq 0$, il n'y a qu'un nombre fini d'éléments $\ell \in L$ tels que $B(\ell, \ell) \leq c$;

iv) il existe $c > 0$ tel que, pour tout $\ell \in L$, $\ell \neq 0$, on ait $B(\ell, \ell) > c$.

Sous ces hypothèses, $E = L \otimes_{\mathbf{Z}} \mathbf{R}$ est un espace euclidien et L un réseau de E ; cela permet de définir $m(L)$, $\mathrm{disc}(L)$, $\gamma(L)$, $d(L)$. Tout réseau dans un espace euclidien peut être considéré comme un réseau euclidien. Un réseau euclidien est dit *unimodulaire* si son discriminant est 1, *entier* si l'on a $B(L \times L) \subset \mathbf{Z}$, *pair* s'il est entier et que $B(\ell, \ell)$ est pair pour tout $\ell \in L$. Un réseau euclidien est dit *semblable* à (L, B) s'il est isomorphe à $(L, \lambda B)$ pour un nombre réel $\lambda > 0$.

2.2. Existence d'un réseau de densité maximale

Les réseaux de l'espace euclidien $\mathbf{R}^n$ sont paramétrés par l'ensemble $\mathrm{GL}_n(\mathbf{R})/\mathrm{GL}_n(\mathbf{Z})$: à une classe $g\mathrm{GL}_n(\mathbf{Z})$ correspond le réseau $g(\mathbf{Z}^n)$. On munit l'ensemble des réseaux de $\mathbf{R}^n$ de la topologie quotient de celle de $\mathrm{GL}_n(\mathbf{R})$; la fonction $L \mapsto \gamma(L)$ est continue sur cet ensemble. Les réseaux de $\mathbf{R}^n$ de densité maximale sont ceux en lesquels la fonction γ atteint son maximum. On a $\gamma(\lambda L) = \gamma(L)$ pour tout $\lambda > 0$. Pour étudier les maxima de γ, on peut donc se restreindre à l'ensemble des réseaux unimodulaires de $\mathbf{R}^n$, qui s'identifie à $\mathrm{SL}_n(\mathbf{R})/\mathrm{SL}_n(\mathbf{Z})$.

PROPOSITION 1.— *L'application* $\gamma : \mathrm{SL}_n(\mathbf{R})/\mathrm{SL}_n(\mathbf{Z}) \to]0, +\infty[$ *est propre.*

C'est une conséquence de la théorie de la réduction de Minkowski : toute classe $\bar{g} \in \mathrm{SL}_n(\mathbf{R})/\mathrm{SL}_n(\mathbf{Z})$ possède un représentant $g \in \mathrm{SL}_n(\mathbf{R})$ de la

forme kau, avec $k \in \mathrm{SO}_n(\mathbf{R})$, $a = \mathrm{diag}(t_1, \cdots, t_n)$ une matrice diagonale de déterminant 1 à coefficients positifs telle que $t_i \leq \frac{2}{\sqrt{3}} t_{i+1}$ pour $1 \leq i < n$, et u une matrice triangulaire supérieure unipotente dont les coefficients appartiennent à $[0,1]$. On a par définition $\gamma(\bar{g}) = \inf_{x \in \mathbf{Z}^n, x \neq 0} \langle gx, gx \rangle$, d'où $\gamma(\bar{g}) \leq \langle ge_1, ge_1 \rangle = t_1^2$. Il en résulte facilement que, pour tout $\varepsilon > 0$, l'image réciproque de $[\varepsilon, +\infty[$ par γ est une partie compacte de $\mathrm{SL}_n(\mathbf{R})/\mathrm{SL}_n(\mathbf{Z})$, d'où la proposition.

La prop. 1 est parfois appelée "critère de Mahler". On en trouvera une autre démonstration dans [B], ch. 8, p. 187 et des généralisations dans [G], n° 2.2.

COROLLAIRE.— *Il existe des réseaux L de $\mathbf{R}^n$ de densité maximale (i.e. tels que $\gamma(L) = \gamma_n$).*

En effet, $\gamma : \mathrm{SL}_n(\mathbf{R})/\mathrm{SL}_n(\mathbf{Z}) \to]0, +\infty[$ est une application continue, propre, majorée, donc atteint son maximum.

2.3. Réseaux extrêmes

DÉFINITION 1.— *Soit L un $\mathbf{Z}$-module libre de rang fini. Un sous-ensemble S de L est dit* parfait *si :*

i) *il existe une application bilinéaire symétrique $B : L \times L \to \mathbf{R}$ et une seule telle que $B(\ell, \ell) = 1$ pour $\ell \in S$;*

ii) *l'application B est définie positive et S est l'ensemble de ses vecteurs minimaux.*

Remarque.— Soit n le rang de L. L'espace vectoriel V des applications bilinéaires symétriques de $L \times L$ dans $\mathbf{R}$ est de dimension $n(n+1)/2$. Soit S un sous-ensemble parfait de L. De l'assertion d'unicité dans la condition i) de la définition, on déduit que l'espace vectoriel dual V^* est engendré par les formes linéaires $u \mapsto u(s,s)$, pour $s \in S$. En particulier, S contient au moins $\frac{n(n+1)}{2}$ paires de vecteurs opposés et l'on a $\mathrm{Card}(S) \geq n(n+1)$. Par ailleurs, si B est comme dans la définition, les coefficients matriciels de B dans une base de L s'obtiennent en résolvant un système d'équations linéaires à coefficients entiers. Ils sont donc rationnels.

Un réseau L d'un espace euclidien E de dimension n est dit *parfait* si l'ensemble S de ses vecteurs minimaux est parfait. (Dans ce cas, l'application B de la déf. 1 est l'application $(\ell, \ell') \mapsto \langle \ell, \ell' \rangle / m(L)$.) Le réseau L est dit *eutactique* si l'application identique de E peut s'écrire sous la forme $\sum_{s \in S} \lambda_s p_s$, où les λ_s sont des nombres réels > 0 et p_s désigne le projecteur orthogonal dans E d'image $\mathbf{R}s$.

Un réseau de E est dit *extrême* s'il correspond à un maximum local de la fonction γ. En étudiant, au voisinage d'un réseau L de E, le développement limité à l'ordre 2 de γ, on obtient la caractérisation suivante des réseaux extrêmes :

PROPOSITION 2 (Voronoï [Vo]).— *Un réseau de E est extrême si et seulement si il est parfait et eutactique.*

On en déduit, grâce à la remarque :

COROLLAIRE 1.—*Un réseau extrême de E a au moins $n(n+1)$ vecteurs minimaux.*

COROLLAIRE 2.—*Soit L un réseau extrême de E. La matrice du produit scalaire de E dans une base de L est proportionnelle à une matrice à coefficients rationnels. En particulier $\gamma(L)^n$ est rationnel.*

COROLLAIRE 3.—*La constante d'Hermite γ_n est la racine n-ième d'un nombre rationnel.*

Les classes modulo $GL_n(\mathbf{Z})$ de sous-ensembles parfaits de $\mathbf{Z}^n$ correspondent bijectivement aux classes de similitude de réseaux parfaits de rang n. Voronoï a démontré que ces classes sont en nombre fini et a donné un algorithme permettant (au moins en principe) d'en dresser la liste. D'après la prop. 2, l'algorithme de Voronoï fournit la liste (finie) des maxima locaux de γ et permet donc de calculer la constante d'Hermite γ_n.

En dimension 3, le seul réseau parfait (à similitude près) est A_3 (Gauss, 1831). Les réseaux parfaits en dimension 4 et 5 ont été déterminés par Korkine et Zolotareff ([K,Z],1877), en dimension 6 par Barnes (1957). En dimension 7, on connaît grâce à Stacey une liste de 33 réseaux parfaits

non semblables ; des calculs sur ordinateurs, effectués en ce moment par D.-O. Jaquet, en utilisant l'algorithme de Voronoï, devraient permettrent de prouver que cette liste est complète[1].

Pour une généralisation de ces résultats aux réseaux G-stables dans un espace euclidien muni d'un groupe fini d'automorphismes G, et des applications à la géométrie des nombres, on pourra consulter [B,M].

2.4. Quelques valeurs de la constante d'Hermite

Pour $n \leq 8$, on connaît la valeur de γ_n et on sait qu'il n'existe à similitude près qu'un seul réseau euclidien L de rang n tel que $\gamma(L) = \gamma_n$. (Pour $n \leq 6$, c'est une conséquence des résultats décrits à la fin du n° 2.3 ; pour $n = 7$ et $n = 8$, cela a été démontré par Blichfeldt.) On a la table suivante (où un symbole tel que D_4, par exemple, désigne le réseau engendré par le système de racines D_4) :

n	L	m(L)	disc(L)	γ_n	d_n
1	A_1	2	2	1	1
2	A_2	2	3	1,1547...	0,9068...
3	D_3	2	4	1,2599...	0,7404...
4	D_4	2	4	1,4142...	0,6168...
5	D_5	2	4	1,5157...	0,4652...
6	E_6	2	3	1,6653...	0,3729...
7	E_7	2	2	1,8114...	0,2952...
8	E_8	2	1	2	0,2536...

On ne connaît la valeur de γ_n pour aucun entier $n \geq 9$. On trouvera, pour $n \leq 24$ et pour certaines valeurs de n comprises entre 24 et 2^{20}, les réseaux de rang n les plus denses connus (avant les travaux d'Elkies et Shioda) dans les tables de [C,S], p. 15 à 17.

Pour n petit, les "réseaux laminés" jouent un rôle important. Ils sont définis par récurrence sur n ; un réseau L de rang n est dit laminé si :

[1] Ces calculs ont été achevés en juillet 1990, après 100 jours CPU de calcul sur VAX. Effectivement, la liste de Stacey est complète.

i) il contient un réseau laminé L' de rang $n-1$ tel que $m(L') = m(L)$;

ii) il est de densité maximale parmi les réseaux ayant la propriété i).

Pour $n \leq 25$, on connaît tous les réseaux laminés ([C,S], ch. 6) ; ils sont plus denses que les autres réseaux de rang n connus, sauf pour $n = 11$, 12, 13.

Nous avons indiqué ci-dessous quelques valeurs de n pour lesquelles un réseau particulièrement dense L est connu. Son influence se fait sentir dans les dimensions voisines : on trouve par exemple des réseaux denses de rang $n-1$ parmi ses sections hyperplanes.

n	L	découvert par	m(L)	disc(L)	$\gamma(L)$
12	K_{12}	Coxeter et Todd	4	3^6	$4/\sqrt{3}$
24	Λ_{24}	Leech	4	1	4
32	Q_{32}	Quebbemann	6	2^{16}	$3\sqrt{2}$

2.5. Réseaux de grand rang

Supposons $n \geq 2$. Comme au n° 2.2, l'ensemble X des réseaux unimodulaires de $\mathbf{R}^n$ s'identifie à $SL_n(\mathbf{R})/SL_n(\mathbf{Z})$. Il existe sur X une unique mesure μ de masse 1, invariante par $SL_n(\mathbf{R})$. D'après un théorème de Siegel ([Si]), on a pour toute fonction continue à support compact f sur $\mathbf{R}^n$

$$\int_{\mathbf{R}^n} f(x)dx_1 \cdots dx_n = \zeta(n) \int_X \Big(\sum_{\ell \in L^{\text{prim}}} f(\ell) \Big)\, d\mu(L), \tag{6}$$

où L^{prim} désigne l'ensemble des vecteurs primitifs de L (*i.e.* n'appartenant à mL pour aucun entier $m \geq 2$) et ζ la fonction zêta de Riemann.

Soit $r > 0$ un nombre réel tel que $\text{vol}(B(0,r)) < 2\zeta(n)$. Il existe une fonction continue à support compact $f : \mathbf{R}^n \to [0,1]$, égale à 1 sur $B(0,r)$, d'intégrale $< 2\zeta(n)$. En appliquant (6) à cette fonction, on voit qu'il existe un réseau unimodulaire de $\mathbf{R}^n$ tel que $\sum_{\ell \in L^{\text{prim}}} f(\ell) < 2$. Pour un tel réseau, on a $m(L) > r$, $\text{disc}(L) = 1$, d'où $d(L) > 2^{-n} \,\text{vol}(B(0,r))$. Nous avons ainsi démontré l'inégalité

$$d_n \geq 2^{1-n}\, \zeta(n). \tag{7}$$

(théorème de Minkowski). On ne sait pas construire explicitement des réseaux aussi denses pour n arbitrairement grand. Divers auteurs (Litsyn, Tsfasman, Quebbemann, Rosenbloom, etc.) ont cependant exhibé des suites de réseaux, dont le rang tend vers l'infini, et dont la densité satisfait une inégalité de la forme $d \geq c^n$ pour une constante c. (La meilleure constante c est pour l'instant $2^{-1,39}$; *cf.* [T,R]).

3. LES RÉSEAUX D'ELKIES ET SHIODA

Dans une conférence aux journées arithmétiques de Luminy au printemps 1989, Tsfasman signale l'intérêt pour les empilements de sphères de divers réseaux euclidiens intervenant en théorie des nombres et en géométrie algébrique. Cela donne l'idée à Elkies d'examiner la situation suivante : on choisit une courbe elliptique définie sur un corps global K, et on prend pour réseau euclidien le groupe $E(K)/E(K)_{\text{tors}}$, muni de la hauteur de Néron-Tate. Du point de vue des empilements de sphères, ces réseaux semblent peu intéressants lorsque K est un corps de nombres. (On ne sait même pas si, pour $K = \mathbf{Q}$, leur rang peut être arbitrairement grand.) Par contre, en prenant pour K un corps de fonctions d'une variable sur un corps fini et en choisissant E astucieusement, on découvre de nouveaux empilements de sphères plus denses que ceux connus auparavant.

Indépendamment et à la même époque, Shioda avait entrepris, dans une série d'articles ([Sh.1-6]), l'étude des liens entre la géométrie des surfaces elliptiques (sur un corps non nécessairement fini) et l'arithmétique des groupes de Mordell-Weil associés. La théorie des surfaces elliptiques est essentiellement équivalente à celle des courbes elliptiques sur les corps de fonctions d'une variable, quoique le dictionnaire pour passer de l'une à l'autre soit parfois délicat (*cf.* [Ta], §4). Au cours de son étude, Shioda obtient des résultats sur les empilements de sphères du même type que ceux d'Elkies ([Sh.6]).

3.1. Courbes elliptiques sur un corps de fonctions

Soient k un corps fini de cardinal $q = p^r$, et K un corps de fonctions d'une variable sur k : autrement dit, K est le corps des fonctions rationnelles d'une courbe projective lisse absolument irréductible X définie sur k. On définit une application $\deg : K \to \mathbf{N}$ en associant à une fonction rationnelle sur X son degré.

Considérons une courbe elliptique E définie sur K. Le groupe $E(K)$ est de type fini. Il existe une unique forme quadratique positive $h : E(K) \to \mathbf{R}$ possédant la propriété suivante : si $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ est un modèle de Weierstrass de E, l'application $P \mapsto h(P) - \frac{1}{2}\deg(x(P))$ de $E(K) - \{0\}$ dans $\mathbf{R}$ est bornée. (L'application h est, à un facteur multiplicatif $\log q$ près, la *hauteur de Néron-Tate* de E.) Le sous-groupe de torsion $E(K)_{\text{tors}}$ de $E(K)$ est formé des points P tels que $h(P) = 0$; il est fini. Posons $L = E(K)/E(K)_{\text{tors}}$. De l'application bilinéaire $(P, Q) \mapsto h(P+Q) - h(P) - h(Q)$ associée à h, on déduit par passage au quotient une application bilinéaire symétrique définie positive de $L \times L$ dans $\mathbf{R}$. Muni de cette application, L est un réseau euclidien que nous appellerons le *réseau de Mordell-Weil* de E. Pour étudier l'empilement de sphères associé à L, il convient de déterminer :

i) le rang n du $\mathbf{Z}$-module libre L ;

ii) le nombre $m(L) = \inf_{\ell \in L, \ell \neq 0} \langle \ell, \ell \rangle = 2 \inf_{P \in E(K) - E(K)_{\text{tors}}} h(P)$;

iii) le discriminant de L.

Le discriminant de L est l'un des ingrédients intervenant dans la conjecture de Birch et Swinnerton-Dyer (formulée pour les corps de fonctions par Tate dans [Ta]). Rappelons-en brièvement l'énoncé. Si v est une place de K (*i.e.* un point fermé de X), et si q_v est le cardinal du corps résiduel $k(v)$, le nombre de points à valeurs dans $k(v)$ d'un modèle de Weierstrass de E minimal en v est de la forme $1 + q_v - a_v$, avec $|a_v| \leq 2\sqrt{q_v}$. On pose $L_v(s) = (1 - a_v q_v^{-s} + q_v^{1-2s})^{-1}$ si E a bonne réduction en v et $L_v(s) = (1 - a_v q_v^{-s})^{-1}$ sinon. La série de Dirichlet $\prod_v L_v(s)$, appelée *fonction L de Hasse-Weil* de E sur K, est de la forme $L_{E/K}(q^{-s})$, où $L_{E/K}$ est une fonction rationnelle. La conjecture de Birch et Swinnerton-Dyer affirme que :

i) *la fonction rationnelle $L_{E/K}$ possède au point q^{-1} un zéro de multiplicité égale au rang n de $E(K)/E(K)_{\text{tors}}$;*

ii) *le groupe de Tate-Šafarevič $Ш(E/K)$, qui classifie les espaces principaux homogènes sous E possédant un point rationnel sur chacun des complétés K_v de K, est fini ;*

iii) *la fonction rationnelle $L_{E/K}(T)/(1-qT)^n$ prend au point q^{-1} la valeur*

$$q^{1-g}\,\frac{\operatorname{Card}(Ш(E/K))\operatorname{disc}(L)}{\operatorname{Card}(E(K)_{\text{tors}})^2}\prod_v c_v, \tag{8}$$

où g est le genre de X et où, pour chaque place v de K, c_v est le nombre des composantes connexes de la fibre géométrique en v du modèle de Néron de E, qui sont définies sur $k(v)$.

Fort heureusement, on dispose de nombreux résultats positifs dans cette direction :

a) *L'ordre n' de la fonction $L_{E/K}$ au point q^{-1} est toujours supérieur ou égal à n* (*cf.* [Ta], démonstration du th. 5.2).

b) *L'égalité $n' = n$ est équivalente à la finitude de $Ш(E/K)$ et implique la formule* (8). La "partie première à p" de cet énoncé a été démontrée par Tate ([Ta], th. 5.2), modulo une conjecture (*loc. cit.*, p. 13, conjecture (d)) qui a été prouvée par Gordon ([Go]). La "partie divisant p" de l'énoncé a été démontrée par Milne ([Mil.2]). Milne suppose $p \neq 2$ car il utilise un théorème de dualié plate pour les surfaces (Ann. Sci. ENS 9 (1976)), qui réfère (*loc. cit.*, p. 189) à un article de Bloch (IHES, vol. 47) ; en remplaçant cette dernière référence par un article d'Illusie (Ann. Sci. ENS 12 (1979)), on s'affranchit de l'hypothèse $p \neq 2$.

c) *La conjecture de Birch et Swinnerton-Dyer est démontrée lorsque la courbe elliptique E est constante* (*i.e.* provient par extension des scalaires d'une courbe elliptique définie sur k) ; un énoncé analogue vaut d'ailleurs pour les variétés abéliennes ([Mil.1], th. 3). Plus généralement :

d) *La conjecture de Birch et Swinnerton-Dyer est démontrée lorsque E est la tordue d'une courbe elliptique constante, i.e. lorsque $j(E)$ appartient à k.* En effet, il existe alors une extension galoisienne finie K' de K sur laquelle E devient une courbe elliptique constante. Le groupe

$Ш(E/K')$ est fini d'après c). Le noyau de l'homomorphisme canonique $Ш(E/K) \to Ш(E/K')$ est annulé par $[K';K]$ et tout sous-groupe de $Ш(E/K)$ d'exposant fini est fini. Par suite, $Ш(E/K)$ est fini et E satisfait à la conjecture de Birch et Swinnerton-Dyer, d'après b).

Ces résultats permettent, dans les exemples considérés par Elkies et Shioda, de déduire de la formule (8) des minorations du discriminant de L.

3.2. Cas où la courbe elliptique est constante

Nous allons expliciter les résultats du numéro précédent dans le cas particulier simple où la courbe elliptique considérée sur K est constante, c'est-à-dire provient par extension des scalaires de k à K d'une courbe elliptique E définie sur k.

Le groupe $E(K)$: il s'identifie au groupe $\mathrm{Mor}_k(X,E)$ des morphismes de X dans E (définis sur k). En effet, se donner un point de $E(K)$ équivaut à se donner une application rationnelle de X dans E, et une telle application se prolonge de façon unique en un morphisme de X dans E.

La forme quadratique $h : E(K) \to \mathbf{R}$: elle s'identifie à l'application $u \mapsto \deg u$ de $\mathrm{Mor}_k(X,E)$ dans $\mathbf{R}$.

Le sous-groupe de torsion $E(K)_{\mathrm{tors}}$: il est égal à $E(k)$ et s'identifie au sous-groupe de $\mathrm{Mor}_k(X,E)$ formé des morphismes constants de X dans E.

Le Z-module $L = E(K)/E(K)_{\mathrm{tors}}$: il est canoniquement isomorphe au groupe $\mathrm{Hom}_k(J(X),E)$ des morphismes de variétés abéliennes de $J(X)$ (la jacobienne de X) dans E,définis sur k. En effet, l'homomorphisme $u \mapsto u_*$ de $\mathrm{Mor}_k(X,E)$ dans $\mathrm{Hom}_k(J(X),E)$ (où u_* est déduit de u par fonctorialité d'Albanese) est surjectif, et son noyau est formé des morphismes constants de X dans E.

Le rang n **de** L. La variété abélienne $J(X)$ est k-isogène à un produit $A_1 \times \cdots \times A_m$ de variétés abéliennes simples sur k. Si s est le nombre de celles qui sont k-isogènes à E et si t est le rang du $\mathbf{Z}$-module $\mathrm{End}_k(E)$, on a $n = st$: en effet $\mathrm{Hom}_k(A_i,E)$ est de rang t si A_i est isogène à E et est nul sinon.

Nous allons décrire une autre façon de calculer n. Pour cela, considérons la fonction $Z(X,T)$ de la courbe X, définie par

$$Z(X,T) = \prod_v \left(1 - T^{[k(v):k]}\right)^{-1} \tag{9}$$

(où v parcourt l'ensemble des points fermés de X). C'est une fonction rationnelle en T, de la forme

$$Z(X,T) = \frac{\prod_{i=1}^{2g}(1-\alpha_i T)}{(1-T)(1-qT)} \tag{10}$$

où g est le genre de X et $\alpha_1, \cdots, \alpha_{2g}$ des nombres complexes de valeur absolue $q^{1/2}$. Écrivons de même

$$Z(E,T) = \frac{(1-\beta_1 T)(1-\beta_2 T)}{(1-T)(1-qT)}. \tag{11}$$

PROPOSITION 3.— *Le rang du* $\mathbf{Z}$*-module* $L = E(K)/E(K)_{\mathrm{tors}}$ *est le nombre de couples* (i,j)*, avec* $1 \leq i \leq 2g$, $1 \leq j \leq 2$ *tels que* $\alpha_i = \beta_j$.

Soit ℓ un nombre premier distinct de p. Les points de ℓ^∞-torsion de $J(X)$ et E permettent de définir des représentations ℓ-adiques de $\mathrm{Gal}(\bar{k}/k)$ dans des $\mathbf{Q}_\ell$-espaces vectoriels $V_\ell(J(X))$ et $V_\ell(E)$ de dimensions respectives $2g$ et 2. D'après un théorème de Tate, les $\mathbf{Q}_\ell$-espaces vectoriels $L \otimes_{\mathbf{Z}} \mathbf{Q}_\ell = \mathrm{Hom}_k(J(X),E) \otimes_{\mathbf{Z}} \mathbf{Q}_\ell$ et $\mathrm{Hom}_{\mathrm{Gal}(\bar{k}/k)}(V_\ell(J(X)), V_\ell(E))$ sont isomorphes. Leur dimension est le nombre de couples (i,j) tels que $\alpha_i = \beta_j$, car l'automorphisme de Frobenius $x \mapsto x^q$ de $\bar{k}$, qui engendre $\mathrm{Gal}(\bar{k}/k)$ topologiquement, opère sur $V_\ell(J(X))$ et $V_\ell(E)$ suivant des endomorphismes semi-simples, de polynômes caractéristiques respectifs $\prod_{i=1}^{2g}(T-\alpha_i)$ et $\prod_{j=1}^{2}(T-\beta_j)$.

Le nombre $m(L)$. Par définition, on a

$$m(L) = \inf_{\ell \in L, \ell \neq 0} \langle \ell, \ell \rangle = 2 \inf_u \deg u, \tag{12}$$

où la seconde borne inférieure est prise sur l'ensemble des morphismes non constants $u : X \to E$, définis sur k. Par ailleurs, il est clair que, pour toute extension finie k' de k, on a

$$\inf_u \deg u \geq \mathrm{Card}(X(k'))/\mathrm{Card}(E(k')). \tag{13}$$

Cela permet de minorer $m(L)$.

La fonction de Hasse-Weil de E sur K. Conservons les notations des formules (9), (10), (11). Soit v un point fermé de X. Notons $k(v)$ son corps résiduel et posons $q_v = \mathrm{Card}(k(v))$, $\deg v = [k(v) : k]$. Le cardinal de $E(k(v))$ est $1 - a_v + q_v$, avec $a_v = \beta_1^{\deg v} + \beta_2^{\deg v}$. On a $\beta_1\beta_2 = q$. La fonction de Hasse-Weil de E sur K, égale à $\prod_v (1 - a_v q_v^{-s} + q_v^{1-2s})^{-1}$, s'écrit donc $L_{E/K}(q^{-s})$, avec

$$
\begin{aligned}
L_{E/K}(T) &= \prod_v ((1 - (\beta_1 T)^{\deg v})(1 - (\beta_2 T)^{\deg v}))^{-1} \\
&= Z(X, \beta_1 T) Z(X, \beta_2 T) = Z\Big(X, \frac{qT}{\beta_1}\Big) Z\Big(X, \frac{qT}{\beta_2}\Big).
\end{aligned} \tag{14}
$$

On constate que, conformément à la conjecture de Birch et Swinnerton-Dyer (qui comme nous l'avons dit est ici un théorème de Milne), la fonction $L_{E/K}$ possède en q^{-1} un zéro de multiplicité égale au nombre de couples (i, j) tels que $\alpha_i = \beta_j$, c'est-à-dire (prop. 3) au rang n de $E(K)/E(K)_{\mathrm{tors}}$.

Le discriminant de L. Le théorème de Milne nous dit que la valeur en q^{-1} de $L_{E/K}(T)/(1 - qT)^n$ est

$$
\frac{q^{1-g}\,\mathrm{Card}\,(Ш(E/K))\,\mathrm{disc}\,(L)}{\mathrm{Card}\,(E(K)_{\mathrm{tors}})^2}.
$$

Compte tenu des relations (10), (14) et du fait que le groupe $E(K)_{\mathrm{tors}}$, égal à $E(k)$, a pour cardinal $(1 - \beta_1)(1 - \beta_2)$, on a

$$
\mathrm{Card}\,(Ш(E/K))\,\mathrm{disc}\,(L) = q^g \prod_{\alpha_i \neq \beta_j} \Big(1 - \frac{\alpha_i}{\beta_j}\Big). \tag{15}
$$

3.3. Un exemple

Soit q une puissance d'un nombre premier p. Considérons sur le corps $k = \mathbf{F}_{q^2}$ la courbe de Fermat X d'équation

$$
x^{q+1} + y^{q+1} + z^{q+1} = 0
$$

Lemme.— a) *Le genre de* X *est* $g = q(q-1)/2$.

b) *Le cardinal de* $X(k)$ *est* $q^3 + 1$.

c) *On a* $Z(X,T) = (1+qT)^{2g}/((1-T)(1-q^2T))$.

d) *Soit* π *l'endomorphisme de Frobenius (relatif à* k*) de la jacobienne de* X.

On a $\pi + q = 0$.

L'assertion a) résulte de ce que X est une courbe projective plane lisse de degré $q+1$.

Lorsque x décrit $k = \mathbf{F}_{q^2}$, x^{q+1} prend une fois la valeur 0 et $q+1$ fois chaque valeur dans $\mathbf{F}_q^\times$. On a des résultats analogues pour y et z. Un comptage élémentaire fournit alors l'assertion b).

La fonction rationnelle $Z(X,T)$ admet une expression de la forme $\prod_{i=1}^{2g}(1-\alpha_i T)/((1-T)(1-q^2T))$ et l'on a

$$\mathrm{Card}\,(X(k)) = 1 + q^2 - \sum_{i=1}^{2g} \alpha_i.$$

Par suite, d'après b), la somme des α_i est égale à $q^2 - q^3$, c'est-à-dire à $-2gq$. Comme les α_i sont de valeur absolue q, il sont égaux à $-q$.

Soit ℓ un nombre premier distinct de p. On sait que π opère sur $V_\ell(J(X))$ suivant un endomorphisme semi-simple, dont le polynôme caractéristique est $\prod_{i=1}^{2g}(T-\alpha_i) = (T+q)^{2g}$. Il en résulte que $\pi + q$ annule $V_\ell(J(X))$, donc que le noyau de $\pi + q$ contient tous les points de $J(X)$ d'ordre une puissance de ℓ. Cela entraîne l'égalité $\pi + q = 0$.

Choisissons une courbe elliptique E, définie sur k, telle que $E(k)$ ait $q^2 + 2q + 1$ éléments. (Il en existe ; par exemple, si q est un nombre premier ≥ 5, n'importe quelle courbe elliptique supersingulière définie sur $\mathbf{F}_q$ convient.) On a $Z(E,T) = (1+qT)^2/((1-T)(1-q^2T))$. Soit K le corps des fonctions de la courbe de X. Nous allons appliquer les résultats du numéro précédent au réseau de Mordell-Weil $L = E(K)/E(K)_{\mathrm{tors}}$.

PROPOSITION 4.— a) *Le rang* n *de* L *est* $4g = 2q(q-1)$.

b) *On a* $m(L) \geq 2(q-1)$.

c) *On a* $\mathrm{Card}\,(Ш(E/K))\,\mathrm{disc}\,(L) = q^{2g} = q^{q(q-1)}$.

d) *On a* $\gamma(L) \geq 2(q-1)/\sqrt{q}$.

L'assertion a) résulte de la prop. 3 (tous les α_i et β_j sont égaux à $-q$). On a

$$\mathrm{Card}(X(k))/\mathrm{Card}(E(k)) = (q^3+1)/(q+1)^2 > q-2,$$

donc b) résulte des formules (12) et (13). L'assertion c) est un cas particulier de la formule (15) ; elle implique l'inégalité $\mathrm{disc}(L) \leq q^{2g}$. Enfin, d) se déduit de ce qui précède, puisque l'on a $\gamma(L) = m(L)/\mathrm{disc}(L)^{1/n}$.

Pour obtenir de meilleures majorations du discriminant de L, il convient d'étudier le groupe $Ш(E/K)$. C'est ce qu'a fait Gross ([Gr], prop. 14.10) : il démontre que $Ш(E/K)$ est nul si q est égal à p ou à p^2, et non nul si p^3 divise q ; par exemple, pour $q = p^3$, on a $\mathrm{Card}(Ш(E/K)) \geq p^{p^3(p-1)^3/2}$.

Gross ([Gr]) construit et caractérise de façon purement algébrique les réseaux L ci-dessus. Il en tire des informations sur leur géométrie : lorsque $q = p^2$, par exemple, on a $\langle \ell, \ell' \rangle \in p\mathbf{Z}$ pour ℓ, ℓ' dans L, et $\left(L, \frac{1}{p}\langle\ ,\ \rangle\right)$ est un réseau entier unimodulaire pair.

Le réseau L construit dans ce numéro est isomorphe à D_4 pour $q = 2$, au réseau de Coxeter-Todd K_{12} pour $q = 3$, et semblable au réseau de Leech pour $q = 4$.

Remarque.— Les réseaux de Mordell-Weil que nous avons considérés ont un rang élevé parce que la courbe de Fermat X d'équation (16) satisfait aux conditions équivalentes c) et d) du lemme. D'autres courbes remplissent ces conditions (entre autres, les quotients de X) et fournissent également de bons empilements de sphères. Notons que l'équation (16) s'écrit $x\overline{x} + y\overline{y} + z\overline{z} = 0$ (avec $\overline{x} = x^q$), et se transforme, après un changement linéaire convenable de coordonnées, en $x\overline{y} + y\overline{x} - z\overline{z} = 0$. Donc $x + x^q = z^{q+1}$ est un modèle affine de X. Pour tout entier f qui divise $q+1$, $x + x^q = z^f$ est un modèle affine d'un quotient de X ; si de plus q est une puissance de 2, $u^2 + u = v^f$ est un modèle affine d'un quotient de X, comme on le voit en posant $u = x + x^2 + x^4 + \cdots + x^{q/2}$ et $v = z$.

Exemple.— Si l'on prend pour X la courbe d'équation $y^2 + y = x^{q+1}$ sur le

corps $k = \mathbf{F}_{q^2}$, avec $q = 2^r$, et pour E la même courbe elliptique qu'avant, le réseau de Mordell-Weil associé L est entier, pair, de rang $2q$. Elkies décrit explicitement un sous-réseau d'indice fini de L semblable au réseau de Barnes-Wall BW_{2q}. Pour $q = 16$, L est un réseau de rang 32 qui a la même densité que le réseau de Quebbemann Q_{32} ; il est probablement isomorphe à Q_{32}, mais cela n'a pas été prouvé pour l'instant ; l'étude de certains trous profonds de L a permis à Elkies de construire un réseau euclidien de rang 33 plus dense que ceux connus auparavant. Pour $q = 32, 64, \cdots, 512$, les réseaux L ou certains de leurs sous-réseaux améliorent les records de densité en dimension $64, 128, \cdots, 1024$.

3.4. Conclusion

Dans cet exposé, nous n'avons étudié que le cas des courbes elliptiques constantes. D'autres courbes elliptiques ont été utilisées par Elkies et Shioda pour construire de bons empilements de sphères. Celles qui s'avèrent intéressantes sont des courbes elliptiques dont l'invariant modulaire $j(E)$ appartient à k (*i.e.* qui sont tordues de courbes constantes), et plus particulièrement celles considérées dans [T,S] pour obtenir des groupes de Mordell-Weil de grand rang. Il est parfois utile d'étudier des sous-réseaux du réseau de Mordell-Weil : par exemple, celui provenant des points de $E(K)$ dont la réduction en chaque place appartient à la composante neutre du modèle de Néron.

Il serait intéressant de savoir ce que l'on obtient en remplaçant E par une variété abélienne A (en particulier lorsque A est la jacobienne d'une courbe définie sur $\mathbf{F}_{q^2}$, pour laquelle les conditions c), d) du lemme de 3.3 sont satisfaites).

Il ne semble pas pour l'instant que les constructions d'Elkies et Shioda soient susceptibles de fournir des suites de réseaux dont le rang n tend vers l'infini, et dont la densité d est supérieure à c^n, pour une constante c convenable. Elles ont seulement permis d'exhiber des suites pour lesquelles $\log d$ est équivalent à $-\frac{n \log n}{12}$.(*)

(*) Elkies m'a signalé après l'exposé qu'il sait remplacer la condition $\log d \sim -\frac{n \log n}{12}$ par $-\log d = \mathcal{O}(n \log n^{0.5+\varepsilon})$, pour tout $\varepsilon > 0$.

Voici la liste de quelques dimensions n pour lesquelles un réseau L plus dense que ceux connus auparavant a été construit par les méthodes d'Elkies et Shioda. Pour chacune de ces dimensions, nous avons indiqué une minoration de $\log_2 \delta$, où $\delta = d(L)/b_n$ est la densité centrée de L ; afin de permettre la comparaison, nous avons rappelé entre parenthèses l'ancien record, lorsque celui-ci figure dans les tables de [C,S], p. 16-17.

n	54	64	80	104	128
$\log_2 \delta \geq$	15,88	24,71	40,14	67,01	97,40
		(22)	(36)	(60)	(88)
référence	[E]	[E]	[Sh.6]	[Sh.6]	[E]

n	256	508	512	520	1024
$\log_2 \delta \geq$	294,80	745,62	797,12	770,37	2018,24
	(270,89)	(742,66)	(698)	(767,46)	
référence	[E]	[Sh.6]	[E]	[Sh.6]	[E](**)

(**) La minoration de $\log_2 \delta$ figurant dans [E] est 2012,24 ; elle peut être remplacée par 2018,24, si l'on tient compte que dans l'exemple considéré le groupe $Ш(E/K)$ est d'ordre $\geq 2^{12}$.

BIBLIOGRAPHIE

[B,M] A.M. BERGÉ et J. MARTINET - *Réseaux extrêmes pour un groupe d'automorphismes*, à paraître dans les actes des Journées Arithmétiques de Luminy, 1989, éditions Astérisque.

[B] N. BOURBAKI - *Éléments de mathématique, Intégration*, Act. Sci. et Ind., ed. Hermann, 1963.

[C,S] J.H. CONWAY and N.J.A. SLOANE - *Sphere packings, lattices and groups*, Grundlehren der mathematischen Wissenschaften 290, Springer Verlag, 1988.

[Co] H.S.M. COXETER - *Introduction to Geometry*, John Wiley & sons, 1961.

[E] N. ELKIES - Lettres électroniques à N.J. SLOANE, du 15 août et du 15 septembre 1989.

[Fe] J. FEJES - *Über einen geometrischen Satz*, Math. Z. 46 (1940), 79-83.

[G] R. GODEMENT - *Domaines fondamentaux des groupes arithmétiques*, Séminaire Bourbaki, mai 1963, exposé n° 257, Benjamin, volume 1962-63, New York, 1966.

[Go] W.J. GORDON - *Linking the conjectures of Artin-Tate and Birch-Swinnerton-Dyer*, Compositio math. 38 (1979), 163-199.

[Gr] B.H. GROSS - *Group representations and lattices*, preprint.

[K,L] G.A. KABATIANSKY and V.I. LEVENSHTEIN - *Bounds for packings on a sphere and in space*, Problems of Information Transmission 14, n° 1, 1978, 1-17.

[K,Z] A. KORKINE et G. ZOLOTAREFF - *Sur les formes quadratiques positives*, Math. Ann. 11 (1977), 242-292.

[Mil.1] J.S. MILNE - *The Tate-Šafarevič group of a constant Abelian variety*, Invent. math. 6 (1968), 91-105.

[Mil.2] J.S. MILNE - *On a conjecture of Artin and Tate*, Annals of math. 102 (1975), 517-533.

[Ro] C.A. ROGERS - *Packing and covering*, Cambridge tracts in mathematics and mathematical physics, vol. 54, Cambridge University Press, 1964.

[R,T] M.Y. ROSENBLOOM and M.A. TSFASMAN - *Multiplicative lattices in global fields*, à paraître dans Invent. math., 1990.

[Sh.1] T. SHIODA - *The Galois representation of type E_8 arising from certain Mordell-Weil groups*, Proc. Jap. Acad. 65, Ser. A (1989), 195-197.

[Sh.2] T. SHIODA - *Mordell-Weil lattices and Galois representation*, I, II, III, Proc. Jap. Acad. 65, Ser. A (1989), 268-271, 296-299, 300-303.

[Sh.3] T. SHIODA - *Construction of elliptic curves over $\mathbf{Q}(t)$ with high rank : a preview*, Proc. Jap. Acad. 66, Ser. A (1989), 57-90.

[Sh.4] T. SHIODA - *Construction of elliptic curves with high rank via the invariants of the Weyl groups*, preprint.

[Sh.5] T. SHIODA - *Mordell-Weil lattices of type E_8 and deformation of singularities*, preprint.

[Sh.6] T. SHIODA - *Mordell-Weil lattices and sphere packings*, preprint.

[Si] C.L. SIEGEL - *A mean value theorem in the geometry of numbers*, Ann. of math. 46 (1945), 340-347.

[Ta] J. TATE - *On the conjectures of Birch and Swinnerton-Dyer and a geometric analog*, Séminaire Bourbaki 1965/66, exposé n° 306.

[T,S] J. TATE and I.R. ŠAFAREVIČ - *The rank of elliptic curves*, Dokl. Akad. Nauk SSSR 175 (= Soviet Math. 8) (1967), 917-925.

[Th] A. THUE - *Om nogle geometrisk-taltheoretiske Theoremer*, Forhandlige ved de Skandinaviske Naturforskeres, 14 Møde, Kjøbenhavn, 1882, 352-353.

[Vo] G. VORONOÏ - *Sur quelques propriétés des formes quadratiques positives parfaites*, J. reine angew. Math. 133 (1908), 97-178.

Joseph OESTERLÉ

Université de Paris 6
Département de Mathématiques
Tour 45-46 - 5ème étage
4 place Jussieu
F-75230 Paris Cedex 05

Astérisque

DOUGLAS C. RAVENEL

The nilpotence and periodicity theorems in stable homotopy theory

Astérisque, tome 189-190 (1990), Séminaire Bourbaki,
exp. n° 728, p. 399-428

<http://www.numdam.org/item?id=SB_1989-1990__32__399_0>

© Société mathématique de France, 1990, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Séminaire BOURBAKI
42ème année, 1989–90, n° 728

juin 1990

THE NILPOTENCE AND PERIODICITY THEOREMS IN STABLE HOMOTOPY THEORY

by **Douglas C. RAVENEL**

1 Introduction and statement of theorems

In this paper we will outline some recent results in stable homotopy theory due to Devinatz, Hopkins and J. Smith ([DHS88], [Hop87] and [HS]) and conjectured by the author in [Rav84]. A more detailed account will appear in [Rav].

The theorems in question address one of the fundamental questions in algebraic topology: how to determine, by algebraic methods, when a continuous map from one topological space to another is homotopic to a constant map, i.e., a map that sends all of the source space to a single point in the target. This is the simplest case of the *homotopy classification problem*, which is to determine the set of homotopy classes of continuous maps from a space X to a space Y, and to classify spaces (satisfying various conditions) up to homotopy equivalence.

The basic strategy of algebraic topology is to study this problem by defining functors from the homotopy category (in which the objects are suitable topological spaces and the morphisms are homotopy classes of continuous maps) to various algebraic categories such as that of graded modules over graded rings. The most familiar examples are homotopy groups and ordinary homology and cohomology; in the latter case the functor is contravariant rather than covariant. A continuous map is essential (i.e., *not* homotopic to a constant map) if the functor carries it to a nontrivial homomorphism, but the converse is rarely true. In general there is a tradeoff between the computability of the functor and the amount of information it provides. When a functor that is easy to compute gives complete information about the homotopy class of a map, one considers it a great success.

Before stating the Nilpotence Theorem, we will indicate the modification of the homotopy classification problem that it addresses. First, the spaces under consideration are *finite CW-complexes*. The definition can be found in any textbook on algebraic

topology. This class of spaces includes all of those one commonly studies geometrically, e.g. compact manifolds, algebraic varieties and simplicial complexes. Moreover, it is especially convenient for homotopy theory.

Second, we consider such spaces and maps between them *up to suspension.* The suspension ΣX of a space X is the topological of the cylinder

$$X \times [0,1]$$

obtained by collapsing each end of the cylinder (i.e., the subspaces $X \times \{0\}$ and $X \times \{1\}$) to a single point. For example, the suspension of the n–sphere S^n (the space of unit vectors in $\mathbf{R}^{n+1}$) is S^{n+1}.

The suspension Σf of a map $f\colon X \longrightarrow Y$ can be similarly defined, and suspension can be iterated.

A map f is *stably null homotopic* if some suspension $\Sigma^i f$ is homotopic to a constant map. Otherwise it is said to be *stably essential.* When the spaces in question are finite CW–complexes, there is an upper bound (depending on the connectivity and dimension of the spaces) on the number of suspensions needed to settle the question.

One can define stable homotopy and the stable homotopy classification problem in an obvious way. Experience has shown that stabilizing a problem in homotopy theory in this way makes it much easier to study in most cases. (There are a few exceptions to this statement, e.g. it is much easier to study maps to the circle S^1 up ordinary homotopy than up to stable homotopy.)

A map of the form

$$X \xleftarrow{f} \Sigma^d X$$

for $d \geq 0$ is called a *self–map* of X. It can be iterated by considering the maps

$$X \xleftarrow{f} \Sigma^d X \xleftarrow{\Sigma^d f} \Sigma^{2d} X \xleftarrow{\Sigma^{2d} f} \Sigma^{3d} X \longleftarrow \cdots$$

and one can ask if any of these composites is stably null homotopic. If the answer is yes, we say the map f is *stably nilpotent*; otherwise we say it is *periodic.*

When X is a finite CW–complex, the adjective 'stably' here is redundant. If one of the composites above is stably null homotopic, there is another one (obtained by moving further to the right) which is null homotopic without suspending.

Now we can state the simplest form of the Nilpotence Theorem of Devinatz–Hopkins–Smith [DHS88].

Theorem 1.1 (Nilpotence Theorem, Self–map Form) *There is a functor MU_* such that a self–map f of a finite CW–complex X is stably nilpotent if and only if some iterate of $MU_*(f)$ is trivial.*

This is the first of three equivalent forms of the Nilpotence Theorem. The others are 3.7 and 5.2.

The functor MU_*, known as complex bordism theory, takes values in the category of graded modules over a certain graded ring L, which is isomorphic to $MU_*(\text{pt.})$. These modules come equipped with an action by a certain infinite group Γ, which also acts on L. The ring L and the group Γ are closely related to the theory of formal group laws. $MU_*(X)$ was originally defined in terms of maps from certain manifolds to X, but this definition sheds little light on its algebraic structure. It is the algebra rather than the geometry which is central to our discussion. We will discuss this in more detail in Section 2 and more background can be found in [Rav86, Chapter 4]. In practice, $MU_*(X)$ is not difficult to compute.

We can also say something about periodic self-maps.

Before doing so we must discuss localization at a prime p. In algebra one does this by tensoring everything in sight by $\mathbf{Z}_{(p)}$, the integers localized at the prime p; it is the subring of the rationals consisting of fractions with denominator prime to p. If A is a finite abelian group, then $A \otimes \mathbf{Z}_{(p)}$ is the p-component of A. $\mathbf{Z}_{(p)}$ is flat as a module over the integers $\mathbf{Z}$; this means that tensoring with it preserves exact sequences.

There is an analogous procedure in homotopy theory. The definitive reference is [BK72]; a less formal account can be found in [Ada75]. For each CW-complex X there is a unique $X_{(p)}$ with the property that for most algebraic functors E_*, $E_*(X_{(p)}) \cong E_*(X) \otimes \mathbf{Z}_{(p)}$. We call $X_{(p)}$ the *p-localization* of X. If X is finite we say $X_{(p)}$ is a *p-local finite CW-complex.*

Proposition 1.2 *Suppose X is a simply connected CW-complex such that $\overline{H}_*(X)$ (the ordinary reduced homology of X) consists entirely of torsion.*

(i) If this torsion is prime to p then $X_{(p)}$ is contractible.

(ii) If it is all p-torsion then X is p-local, i.e., $X_{(p)}$ is homotopy equivalent to X. (In this case we say that X is a p-torsion complex.)

(iii) In general X is homotopy equivalent to the one-point union of its p-localizations for all the primes p in this torsion.

The most interesting periodic self-maps occur when X is a finite p-torsion complex. In these cases it is convenient to replace MU_* by the *Morava K-theories* $K(n)_*$. These were invented by Jack Morava in the early '70's, but he has yet to publish his work. Algebraic topologists are generally reluctant to give a precise definition of them in public because doing so would require a prohibitively long technical discussion. An axiomatic approach would be desirable, but has yet to be formulated.

Despite the difficulties with the definition, $K(n)_*(X)$ is generally easier to compute than $MU_*(X)$, and it makes certain properties of X (having to do with periodic

self–maps) more readily apparent. The essential properties of Morava K–theory are contained in the following result, most of which is proved in [JW75]; a proof of (v) can be found in [Rav84].

Proposition 1.3 *For each prime p there is a sequence of functors $K(n)_*$ for $n \geq 0$ with the following properties. (We follow the standard practice of excluding p from the notation.)*

(i) $K(0)_*(X) = H_*(X; \mathbf{Q})$ *and* $K(0)_*(X) = K(0)_*(\text{pt.})$ *when X is a p–torsion complex.*

(ii) $K(1)_*(X)$ *is one of $p-1$ isomorphic summands of mod p complex K–theory.*

(iii) $K(0)_*(\text{pt.}) = \mathbf{Q}$ *and for $n > 0$,* $K(n)_*(\text{pt.}) = \mathbf{Z}/(p)[v_n, v_n^{-1}]$ *where the dimension of v_n is $2p^n - 2$. This ring is a graded field in the sense that every graded module over it is free. $K(n)_*(X)$ is a module over $K(n)_*(\text{pt.})$.*

(iv) There is a Künneth isomorphism

$$K(n)_*(X \times Y) \cong K(n)_*(X) \otimes_{K(n)_*(\text{pt.})} K(n)_*(Y).$$

(v) Let X be a p–local finite CW–complex. If

$$K(n)_*(X) = K(n)_*(\text{pt.}),$$

then

$$K(n-1)_*(X) = K(n-1)_*(\text{pt.}).$$

(vi) If X as above is not contractible then $K(n)_*(X)$ is nontrivial for n sufficiently large.

Definition 1.4 *A p–local finite complex X has* **type** *n if n is the smallest integer such that $K(n)_*(X)$ is nontrivial.*

Because of the Künneth isomorphism, $K(n)_*(X)$ is easier to compute than $MU_*(X)$. Again there are still many interesting spaces for which this has not been done. See [RW80] and [HKR]. A consequence of the Nilpotence Theorem (1.1) is that the Morava K–theories, along with ordinary homology with coefficients in a field, are essentially the only homology theories with Künneth isomorphisms.

The Morava K–theories are especially useful for detecting periodic self–maps. This is the subject of the second major result of this paper, the Periodicity Theorem of Hopkins–Smith [HS]. The proof is outlined in [Hop87].

Theorem 1.5 (Periodicity Theorem) *Let X and Y be p–local (noncontractible) finite CW–complexes of type n (1.4).*

(i) There is a self-map $f\colon \Sigma^d X \to X$ *such that* $K(n)_*(f)$ *is an isomorphism and* $K(m)_*(f)$ *is nilpotent for* $m > n$. *(We will refer to such a map as a* v_n**–map.**) *When* $n = 0$, $d = 0$ *and when* $n > 0$ *then* d *is a multiple of* $2p^n - 2$.

(ii) Suppose $h\colon X \to Y$ *is a continuous map where* Y *is another finite* p*-local* CW*-complex of type* n. *Let* $g\colon \Sigma^e Y \to Y$ *be a self-map as in (i). Then there are positive integers* i *and* j *with* $di = ej$ *such that the following diagram commutes up to homotopy.*

$$\begin{array}{ccc} \Sigma^{di}X & \xrightarrow{\Sigma^{di}h} & \Sigma^{di}Y \\ {\scriptstyle f^i}\downarrow & & {\scriptstyle g^j}\downarrow \\ X & \xrightarrow{h} & Y. \end{array}$$

There are two special cases of (ii) worth noting. The first is when $X = Y$ and h is the identity map. In that case, (ii) says that f is *assymptotically unique* in the following sense. Suppose g is another such periodic self–map. Then there are positive integers i and j such that f^i is homotopic to g^j.

The second case is when Y is a suspension of X and g is the corresponding suspension of f. Then (ii) shows that f is *assymptotically central* in that any map h commutes with some iterate of it. We will see below in 4.3 that a fixed iterate of f commutes with all h.

2 MU–theory and formal group laws

In this section we will discuss the functor MU_* used in the Nilpotence Theorem. $MU_*(X)$ is defined in terms of maps of manifolds into X as will be explained presently. Unfortunately the geometry in this definition does not appear to be relevant to the applications we have in mind. We will be more concerned with some algebraic properties of the functor which are intimately related to the theory of formal group laws.

Definition 2.1 *Let* M_1 *and* M_2 *be smooth closed* m*-dimensional manifolds and let*

$$f_i\colon M_i \to X$$

be continuous maps for $i = 1, 2$. *These maps are* **bordant** *if there is a map*

$$f\colon W \to X$$

where W *is a smooth manifold whose boundary is the disjoint union of* M_1 *and* M_2 *such that the restriction of* f *to* M_i *is* f_i. f *is a* **bordism** *between* f_1 *and* f_2.

Bordism is an equivalence relation and the set of bordism classes forms a group under disjoint union, called the m^{th} **bordism group of** X.

A manifold is **stably complex** if it admits a complex linear structure in its stable normal bundle, i.e., the normal bundle obtained by embedding in a large dimensional Euclidean space. A complex analytic manifold (e.g. a complex algebraic variety) is stably complex, but the notion of stably complex is far weaker than that of complex analytic.

Definition 2.2 *$MU_m(X)$, the m^{th}* **complex bordism group of** *X, is the bordism group obtained by requiring that all manifolds in sight be stably complex.*

The fact that these groups are accessible is due to some remarkable work of Thom in the 1950's [Tho54]. A general reference for cobordism theory is Stong's book [Sto68].

The groups $MU_*(X)$ satisfy all but one of the axioms used by Eilenberg–Steenrod to characterize ordinary homology. They fail to satisfy the dimension axiom, which describes the homology of a point. If X is a single point, then the map from the manifold to X is vacuous, and $MU_*(\text{pt.})$ is the group of bordism classes of stably complex manifolds, which we will denote simply by MU_*. It is a graded ring under Cartesian product and its structure was determined independently by Milnor [Mil60] and Novikov ([Nov60] and [Nov62]).

Theorem 2.3 *The complex bordism ring, MU_* is isomorphic to*

$$\mathbf{Z}[x_1, x_2, \ldots]$$

where $\dim x_i = 2i$.

It is possible to describe the generators x_i as complex manifolds, but this is more trouble than it is worth. The complex projective spaces $\mathbf{C}P^i$ serve as polynomial generators of $\mathbf{Q} \otimes MU_*$.

Note that $MU_*(X)$ is an MU_*–module as follows. Given $x \in MU_*(X)$ represented by $f\colon M \to X$ and $\lambda \in MU_*$ represented by a manifold N, λx is represented by the composite map

$$M \times N \longrightarrow M \xrightarrow{f} X.$$

Definition 2.4 *A* **formal group law** *over a commutative ring with unit R is a power series $F(x, y)$ over R that satisfies the following three conditions.*

(i) $F(x,0) = F(0,x) = x$ *(identity),*

(ii) $F(x,y) = F(y,x)$ *(commutativity) and*

(iii) $F(F(x,y),z) = F(x,F(y,z))$ *(associativity).*

(The existence of an inverse is automatic. It is the power series $i(x)$ determined by the equation $F(x,i(x)) = 0$.)

Example 2.5 *(i)* $F(x,y) = x + y$. *This is called the* **additive** *formal group law.*

(ii) $F(x,y) = x+y+xy = (1+x)(1+y)-1$. *This is called the* **multiplicative** *formal group law.*

The theory of formal group laws from the power series point of view is treated comprehensively in [Haz78]. A short account containing all that is relevant for the current discussion can be found in [Rav86, Appendix 2].

The following result is due to Lazard [Laz55a].

Theorem 2.6 (Lazard's Theorem) *(i) There is a universal formal group law defined over a ring L of the form*

$$G(x,y) = \sum_{i,j} a_{i,j} x^i y^j \quad \text{with } a_{i,j} \in L$$

such that for any formal group law F over R there is a unique ring homomorphism θ from L to R such that

$$F(x,y) = \sum_{i,j} \theta(a_{i,j}) x^i y^j.$$

(ii) L is a polynomial algebra $\mathbf{Z}[x_1, x_2, \ldots]$. If we put a grading on L such that $a_{i,j}$ has degree $2(1-i-j)$ then x_i has degree $-2i$.

The grading above is chosen so that if x and y have degree 2, then $G(x,y)$ is a homogeneous expression of degree 2. Note that L is isomorphic to MU_* except that the grading is reversed. There is an important connection between the two.

Associated to the covariant functor MU_* there is a contravariant functor MU^*. It bears the same relation to MU_* that ordinary cohomology bears to ordinary homology. The conventions in force in algebraic topology require that MU^*(pt.) (which we will denote by MU^*) be the same as MU_*(pt.) but with the grading reversed. Thus MU^* is isomorphic to the Lazard ring L.

This isomorphism is natural in the following sense. $MU^*(X)$, like $H^*(X)$, comes equipped with cup products, making it a graded algebra over MU^*. Of particular interest is the case when X is the infinite-dimensional complex projective space $\mathbf{C}P^\infty$. We have

$$MU^*(\mathbf{C}P^\infty) \cong MU^*[[x]]$$

where $\dim x = 2$, and

$$MU^*(\mathbf{C}P^\infty \times \mathbf{C}P^\infty) \cong MU^*[[x \otimes 1, 1 \otimes x]].$$

The space $\mathbf{C}P^\infty$ is an abelian topological group, so there is a map

$$\mathbf{C}P^\infty \times \mathbf{C}P^\infty \xrightarrow{f} \mathbf{C}P^\infty$$

with certain properties. ($\mathbf{C}P^\infty$ is also the classifying space for complex line bundles and the map in question corresponds to the tensor product.) Since MU^* is contravariant we get a map

$$MU^*(\mathbf{C}P^\infty \times \mathbf{C}P^\infty) \xleftarrow{f^*} MU^*(\mathbf{C}P^\infty)$$

which is determined by its behavior on the generator $x \in MU^2(\mathbf{C}P^\infty)$. The power series

$$f^*(x) = F(x \otimes 1, 1 \otimes x)$$

can easily be shown to be a formal group law over MU^*. Hence by Lazard's Theorem (2.6) it corresponds to a ring homomorphism $\theta\colon L \to MU^*$. The following was proved by Quillen [Qui69] in 1969.

Theorem 2.7 (Quillen's Theorem) *The homomorphism $\theta\colon L \to MU^*$ above is an isomorphism. In other words, the formal group law associated with complex cobordism is the universal one.*

Given this isomorphism (and ignoring the reversal of the grading), we can regard $MU_*(X)$ as an L–module.

Now we define a group Γ which acts in an interesting way on L.

Definition 2.8 *Let Γ be the group of power series over $\mathbf{Z}$ having the form*

$$\gamma = x + b_1x^2 + b_2x^3 + \cdots$$

where the group operation is functional composition. Γ acts on the Lazard ring L of 1.5 as follows. Let $G(x,y)$ be the universal formal group law as above and let $\gamma \in \Gamma$. Then $\gamma^{-1}(G(\gamma(x),\gamma(y)))$ is another formal group law over L, and therefore is induced by a homomorphism from L to itself. Since γ is invertible, this homomorphism is an automorphism, giving the desired action of Γ on L.

For reasons too difficult to explain here, Γ also acts naturally on $MU_*(X)$ compatibly with the action on $MU_*(\text{pt.})$ defined above. That is, given $x \in MU_*(X)$, $\gamma \in \Gamma$ and $\lambda \in L$, we have

$$\gamma(\lambda x) = \gamma(\lambda)\gamma(x)$$

and the action of Γ commutes with homomorphisms induced by continuous maps.

For algebraic topologists we can offer some explanation for this action of Γ. It is analogous to the action of the Streenrod algebra in ordinary cohomology. More precisely, it is analogous to the action of the group of multiplicative cohomology operations, such as (in the mod 2 case) the total Streenrod square, $\sum_{i\geq 0} \mathrm{Sq}^i$. Such an operation is determined by its effect on the generator of $H^1(\mathbf{R}P^\infty; \mathbf{Z}/(2))$. Thus the group of multiplicative mod 2 cohomology operations embeds in $\Gamma_{\mathbf{Z}/(2))}$, the group of power series over $\mathbf{Z}/(2)$ analogous to Γ over the integers.

Definition 2.9 *Let* $\mathbf{C}\Gamma$ *denote the category of finitely presented* L*–modules equipped with an action of* Γ *compatible with its action on* L *as above, and let* $\mathbf{FH}$ *denote the category of finite CW–complexes and homotopy classes of maps between them.*

Thus we can regard MU_* as a functor from $\mathbf{FH}$ to $\mathbf{C}\Gamma$. The latter category is much more accessible. We will see that it has some structural features which reflect those of $\mathbf{FH}$ very well. The Nilpotence and Periodicity Theorems are examples of this.

In order to study $\mathbf{C}\Gamma$ further we need some more facts about formal group laws. Here are some power series associated with them.

Definition 2.10 *For each integer* n *the* n**-series** $[n](x)$ *is given by*

$$\begin{aligned} [1](x) &= x, \\ [n](x) &= F(x,[n-1](x)) \qquad \text{for } n>1 \text{ and} \\ [-n](x) &= i([n](x)). \end{aligned}$$

These satisfy

$$\begin{aligned} [n](x) &\equiv nx \mod (x^2), \\ [m+n](x) &= F([m](x),[n](x)) \qquad \text{and} \\ [mn](x) &= [m]([n](x)). \end{aligned}$$

For the additive formal group law (2.5), we have $[n](x) = nx$, and for the multiplicative formal group law, $[n](x) = (1+x)^n - 1$.

Of particular interest is the p–series. In characteristic p it always has leading term ax^q where $q = p^h$ for some integer h. This leads to the following.

Definition 2.11 *Let* $F(x,y)$ *be a formal group law over a ring in which the prime* p *is not a unit. If the mod* p *reduction of* $[p](x)$ *has the form*

$$[p](x) = ax^{p^h} + \textit{higher terms}$$

then we say that F *has* **height h at** p*. If* $[p](x) \equiv 0 \mod p$ *then the height is infinity.*

For the additive formal group law we have $[p](x) = 0$ so the height is ∞. The multiplicative formal group law has height 1 since $[p](x) = x^p$.

The following classification theorem is due to Lazard [Laz55b].

Theorem 2.12 (Lazard's Classification Theorem) *Two formal group laws over the algebraic closure of* $\mathbf{F}_p$ *are isomorphic if and only if they have the same height.*

Let $v_n \in L$ denote the coefficient of x^{p^n} in the p–series for the universal formal group law; the prime p is omitted from the notation. This v_n is closely related to the v_n in the Morava K–theories (1.3). It can be shown that v_n is an indecomposable element in L, i.e., it could serve as a polynomial generator in dimension $2p^n - 2$. Let $I_{p,n} \subset L$ denote the prime ideal $(p, v_1, \dots v_{n-1})$.

The following result is due to Morava [Mor85] and Landweber [Lan73a].

Theorem 2.13 (Morava–Landweber Theorem) *The only prime ideals in L which are invariant under the action of Γ are the $I_{p,n}$ defined above, where p is a prime integer and n is a nonnegative integer, possibly ∞. ($I_{p,\infty}$ is by definition the ideal $(p, v_1, v_2, \dots)$ and $I_{p,0}$ is the zero ideal.)*

Moreover in $L/I_{p,n}$ for $n > 0$ the subgroup fixed by Γ is $\mathbf{Z}/(p)[v_n]$. In L itself the invariant subgroup is $\mathbf{Z}$.

This shows that the action of Γ on L is very rigid. L has a bewildering collection of prime ideals, but the only ones we ever have to consider are the ones listed in the theorem. This places severe restriction on the modules in $\mathbf{C}\Gamma$.

Recall that a finitely presented module M over a Noetherian ring R has a finite filtration

$$F_1M \subset F_2M \subset \cdots F_kM = M$$

in which each subquotient $F_iM/F_{i-1}M$ is isomorphic to R/I_i for some prime ideal $I_i \subset R$. Now L is not Noetherian, but it is coherent, which means that finitely presented modules over it admit similar filtrations. For a module in $\mathbf{C}\Gamma$, the filtration can be chosen so that the submodules, and therefore the prime ideals, are all invariant under Γ. The following result is due to Landweber [Lan73b].

Theorem 2.14 (Landweber's Filtration Theorem) *Every module M in $\mathbf{C}\Gamma$ admits a finite filtration by submodules in $\mathbf{C}\Gamma$ as above in which each subquotient is isomorphic to a suspension of $L/I_{p,n}$ for some prime p and some finite n.*

The following are easy consequences of the Landweber Filtration Theorem.

Corollary 2.15 *Suppose M is a p–local module in $\mathbf{C}\Gamma$.*

(i) Then if $v_n^{-1}M = 0$, i.e., if each element in M is annihilated by some power of v_n, then $v_{n-1}^{-1}M = 0$.

(ii) If M is nontrivial, then so is $v_n^{-1}M$ for n sufficiently large.

(iii) If $v_{n-1}^{-1}M = 0$, then there is a positive integer k such that multiplication by v_n^k in M commutes with the action of Γ.

The first two statements should be compared to the last two statements in 1.3. In fact the functor $v_n^{-1}MU_*(X)_{(p)}$ is trivial on a finite p–local CW–complex X if and only if $K(n)_*(X)$ is. One could replace $K(n)_*$ by $v_n^{-1}MU_{(p)*}$ in the statement of the Periodicity Theorem. The third statement above is an algebraic analogue of the Periodicity Theorem.

Now we need to consider certain full subcategories of $\mathbf{C\Gamma}$ and $\mathbf{FH}$.

Definition 2.16 *A full subcategory* $\mathbf{C}$ *of* $\mathbf{C\Gamma}$ *is* **thick** *if it satisfies the following two axioms:*

(i) If

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

is a short exact sequence in $\mathbf{C\Gamma}$ *in which two of the three modules are in* $\mathbf{C}$*, then so is the third.*

(ii) If $M \oplus N$ *is in* $\mathbf{C}$ *then so are* M *and* N*.*

We want to define the corresponding notion for a subcategory of $\mathbf{FH}$, so we need analogs of short exact sequences and direct sums. Given a map $f : X \to Y$, the *cofibre* C_f of f is the quotient of

$$X \times [0,1] \cup Y$$

obtained by collapsing $X \times \{0\}$ to a single point, and identifying $(x,1)$ for $x \in X$ with $f(x) \in Y$. It is easy to show that the cofibre of the map $Y \to C_f$ is homotopy equivalent to ΣX. A *cofibre sequence* is a sequence of maps of the form

$$X \xrightarrow{f} Y \longrightarrow C_f \longrightarrow \Sigma X \longrightarrow \cdots.$$

The composite

$$X \xrightarrow{f} Y \longrightarrow C_f$$

is the homotopy theoretic analog of a short exact sequence. The analog of a direct sum is the *wedge* $X \vee Y$, which is the quotient of $X \cup Y$ obtained by identifying one point in X with one point in Y.

Definition 2.17 *A full subcategory* $\mathbf{F}$ *of* $\mathbf{FH}$ *is* **thick** *if it satisfies the following two axioms:*

(i) If

$$X \xrightarrow{g} Y \longrightarrow C_f$$

is a cofibre sequence in which two of the three spaces are in $\mathbf{F}$*, then so is the third.*

(ii) If $X \vee Y$ *is in* $\mathbf{F}$ *then so are* X *and* Y*.*

Thick subcategories were called *generic subcategories* by Hopkins in [Hop87].

Using the Landweber Filtration Theorem, one can classify the thick subcategories of $\mathbf{C\Gamma}_{(p)}$.

Theorem 2.18 *Let* $\mathbf{C}$ *be a thick subcategory of* $\mathbf{C\Gamma}_{(p)}$ *(the category of all* p*–local modules* $\mathbf{C\Gamma}$*). Then* $\mathbf{C}$ *is either all of* $\mathbf{C\Gamma}_{(p)}$*, the trivial subcategory (in which the only object is the trivial module), or consists of all* p*–local modules* M *in* $\mathbf{C\Gamma}$ *with* $v_{n-1}^{-1}M = 0$*. We denote the latter category by* $\mathbf{C_{p,n}}$.

There is an analogous result about thick subcategories of $\mathbf{FH}_{(p)}$, which is a very useful consequence of the Nilpotence Theorem.

Theorem 2.19 (Thick Subcategory Theorem) *Let* $\mathbf{F} \subset \mathbf{FH}_{(p)}$ *be a thick subcategory of the category of* p*–local finite* CW*–complexes. Then* $\mathbf{F}$ *is either all of* $\mathbf{FH}_{(p)}$*, the trivial subcategory (in which the only object is a point) or consists of all* p*–local finite* CW*–complexes* X *with* $v_{n-1}^{-1}MU_*(X)$ *trivial. We denote the latter category by* $\mathbf{F_{p,n}}$.

Thus we have two nested sequences of thick subcategories,

$$\mathbf{FH}_{(p)} = \mathbf{F}_{p,0} \supset \mathbf{F}_{p,1} \supset \mathbf{F}_{p,1} \cdots \{\text{pt.}\}$$

and

$$\mathbf{C\Gamma}_{(p)} = \mathbf{C}_{p,0} \supset \mathbf{C}_{p,1} \supset \mathbf{C}_{p,1} \cdots \{0\}.$$

The functor $MU_*(\cdot)$ sends one to the other. Until 1983 it was not even known that the $\mathbf{F}_{p,n}$ were nontrivial for all but a few small values of n. Mitchell [Mit85] first showed that all of the inclusions of the $\mathbf{F}_{p,n}$ are proper. Now it is a corollary of the Periodicity Theorem.

In Section 3 we will derive the Thick Subcategory Theorem from another form of the Nilpotence Theorem. This is easy since it uses nothing more than elementary tools from homotopy theory.

In Section 4 we will sketch the proof of the Periodicity Theorem. It is not difficult to show that the collection of complexes admitting periodic self maps for given p and n forms a thick subcategory. Given the Thick Subcategory Theorem, it suffices to find just one nontrivial example of a complex of type n with a periodic self–map. This involves some hard homotopy theory. There are two major ingredients in the construction. One is the Adams spectral sequence, a computational tool that one would expect to see used here. The other is a novel application of the modular representation theory of the symmetric group described in as yet unpublished work of Jeff Smith.

3 The proof of the Thick Subcategory Theorem

In this section we will derive the Thick Subcategory Theorem from the Nilpotence Theorem with the use of some standard tools from homotopy theory, which we must introduce before we can give the proof. The proof itself is identical to the one given by Hopkins in [Hop87].

First we have to introduce the category of spectra. Since the category was introduced around 1960 [Lim60], it has taken on a life of its own, as will be seen later in this paper. Most of the theorems in this paper that are stated in terms of spaces are really theorems about spectra that we have done our best to disguise. However we cannot keep up this act any longer.

Definition 3.1 *A* **spectrum** E *is a collection of spaces* $\{E_n : n \gg 0\}$ *and maps* $\Sigma E_n \to E_{n+1}$. *The* **suspension spectrum** *of a space* X *is defined by* $E_n = \Sigma^n X$ *with each map being the identity. The* i^{th} *suspension* $\Sigma^i E$ *of* E *is defined by*

$$(\Sigma^i E)_n = E_{n+i}$$

for any integer i. *Thus any spectrum can be suspended or desuspended any number of times.*

The homotopy groups of E *are given by*

$$\pi_k(E) = \varinjlim \pi_{n+k}(E_n)$$

and other invariants such as homology and cohomology can be similarly defined.

A spectrum X *is* **connective** *if its homotopy groups are bounded below, i.e., if*

$$\pi_{-k}(X) = 0 \text{ for } k \gg 0.$$

It has **finite type** *if* $\pi_k(X)$ *is finitely generated for each* k.

Example 3.2 (Sphere spectrum) *The spectrum* S^k *is defined by setting* $(S^k)_n = S^{k+n}$. *(The abuse of notation here is standard. Hopefully the context will make it clear whether we are talking about a spectrum or a space.)*

Example 3.3 (Mod p Eilenberg–Mac Lane spectrum) *The spectrum* $H/(p)$ *is defined by setting* $H/(p)_n$ *equal to the Eilenberg–Mac Lane space* $K(\mathbf{Z}/(p), n)$.

One of the original motivations for the definition of spectra is the following example.

Example 3.4 (Complex cobordism spectrum) *The spectrum MU is defined by setting* MU_{2n} *equal to the Thom space for the universal* $\mathbf{C}^n$*-bundle over* $BU(n)$, *the classifying space for the unitary group* $U(n)$. MU_{2n+1} *defined to be* ΣMU_{2n}. *Then* $\pi_*(MU)$ *is isomorphic to the complex cobordism ring* MU_* *discussed above. MU is a ring spectrum (see 4.1 below).*

The homotopy groups of spectra are much more manageable than those of spaces. For example, one has

$$\pi_k(\Sigma^i E) = \pi_{k-i}(E)$$

for all k and i.

Next we need to discuss smash products. For spaces the definition is as follows.

Definition 3.5 *Let X and Y be spaces equipped with base points x_0 and y_0. The* **smash product** *$X \wedge Y$ is the quotient of $X \times Y$ obtained by collapsing $X \times \{y_0\} \cup \{x_0\} \times Y$ to a single point. The k-fold iterated smash product of X with itself is denoted by $X^{(k)}$. For $f: X \to Y$, $f^{(k)}$ denote the evident map from $X^{(k)}$ to $Y^{(k)}$. The map f is* **smash nilpotent** *if $f^{(k)}$ is null homotopic for some k.*

The k-fold suspension $\Sigma^k X$ is the same as $S^k \wedge X$. For CW-complexes X and Y there is an equivalence

$$\Sigma(X \times Y) \simeq (\Sigma X) \vee (\Sigma Y) \vee \Sigma(X \wedge Y).$$

If either of the spectra E or F is a suspension spectrum, then there is an obvious definition of their smash product $E \wedge F$. In particular, smashing E with the sphere spectrum S^0 (3.2) leaves E unchanged. However the general definition of the smash product of two spectra is very difficult; we refer the interested reader to Adams [Ada74].

Definition 3.6 *For a spectrum E the* **E-homology of X** *is defined by*

$$E_*(X) = \pi_*(E \wedge X).$$

The **E-cohomology of X**, *$E^*(X)$, is the graded group of homotopy classes of maps from X to E, i.e.,*

$$E^i(X) = [X, \Sigma^i E]$$

In the case $E = MU$, this is equivalent to the definition given above, 2.2.

The Nilpotence Theorem can be stated in terms of smash products as follows.

Theorem 3.7 (Nilpotence Theorem, Smash Product Form) *Let*

$$F \xrightarrow{f} X$$

be a map of spectra where F is finite. Then f is smash nilpotent if $MU \wedge f$ (i.e., the evident map $MU \wedge F \to MU \wedge X$) is null homotopic.

This can be shown to be equivalent to 1.1. A more useful form of this for our purposes is the following.

Corollary 3.8 *Let W, X and Y be p-local finite spectra with $f: X \to Y$. Then $W \wedge f^{(k)}$ is null homotopic for $k \gg 0$ if $K(n)_*(W \wedge f) = 0$ for all $n \geq 0$. (In particular, W could be S^0, in which case $W \wedge f = f$.)*

It is from this result that we will derive the Thick Subcategory Theorem.

Next we need to discuss Spanier–Whitehead duality, which is treated in more detail in [Ada74].

Theorem 3.9 (Spanier–Whitehead Duality) *For a finite spectrum X there is a unique finite spectrum DX (the* **Spanier–Whitehead dual** *of X) with the following properties.*

(i) For any spectrum Y, the graded group $[X, Y]_*$ is isomorphic to $\pi_*(DX \wedge Y)$. We say that the maps $S^n \to DX \wedge Y$ and $\Sigma^n X \to Y$ that correspond under this isomorphism are **adjoint** *to each other. In particular when $Y = X$, the identity map on X is adjoint to a map $e: S^0 \to DX \wedge X$.*

(ii) For $Y = X$ this isomorphism is reflected in Morava K-theory, namely

$$K(n)_*(X))$$

is isomorphic to $K(n)_*(DX \wedge X)$. In particular $K(n)_*(e) \neq 0$ when $K(n)_*(X) \neq 0$.

(iii) $DDX \simeq X$.

(iv) For a homology theory E_*, there is a natural isomorphism between $E_k(X)$ and $E^{-k}(DX)$. (These groups are defined in 3.6.)

(v) Spanier–Whitehead duality commutes with smash products, i.e., for finite spectra X and Y, $D(X \wedge Y) = DX \wedge DY$.

The basic geometric idea behind Spanier–Whitehead duality is as follows. A finite spectrum X is the suspension spectrum of a finite CW-complex, which we also denote by X. It can always be embedded in some Euclidean space $\mathbf{R}^N$ and hence in S^N. Then DX is a suitable suspension of the suspension spectrum of the complement $S^N - X$. 3.9(iv) is a generalization of the classical Alexander Duality Theorem, which says that $H_k(X)$ is isomorphic to $H^{N-1-k}(S^N - X)$. A simple example of this is the case where $X = S^k$ and it it linearly embedded in S^N. Then its complement is homotopy equivalent to S^{N-1-k}. The Alexander Duality Theorem says that the complement has the same cohomology as S^{N-1-k} even when the embedding of S^k in S^N is not linear, e.g. when $k = 1$, $n = 3$ and $S^1 \subset S^3$ is knotted.

Before we can proceed with the proof of the Thick Subcategory Theorem we need an elementary lemma about Spanier–Whitehead duality. For a finite spectrum X, let $f: W \to S^0$ be the map such that

$$W \xrightarrow{f} S^0 \xrightarrow{e} DX \wedge X$$

is a cofibre sequence. In the category of spectra, such maps always exist. W in this case is finite, and $C_f = DX \wedge X$.

Lemma 3.10 *With notation as above, there is cofibre sequence*

$$C_{f^{(k)}} \longrightarrow C_{f^{(k-1)}} \longrightarrow \Sigma W^{(k-1)} \wedge C_f$$

for each $k > 1$.

Proof. A standard lemma in homotopy theory says that given maps

$$X \xrightarrow{f} Y \xrightarrow{g} Z$$

there is a diagram

$$\begin{array}{ccccc} C_f & \longrightarrow & \text{pt.} & \longrightarrow & \Sigma C_f \\ \uparrow & & \uparrow & & \uparrow \\ Y & \xrightarrow{g} & Z & \longrightarrow & C_g \\ {\scriptstyle f}\uparrow & & \| & & \uparrow \\ X & \xrightarrow{gf} & Z & \longrightarrow & C_{gf} \end{array}$$

in which each row and column is a cofibre sequence. Setting $X = W^{(k)}$, $Y = W^{(k-1)}$, $Z = S^0$ and $g = f^{(k-1)}$, this diagram becomes

$$\begin{array}{ccccc} W^{(k-1)} \wedge C_f & \longrightarrow & \text{pt.} & \longrightarrow & \Sigma W^{(k-1)} \wedge C_f \\ \uparrow & & \uparrow & & \uparrow \\ W^{(k-1)} & \xrightarrow{f^{(k-1)}} & S^0 & \longrightarrow & C_{f^{(k-1)}} \\ {\scriptstyle W^{(k-1)} \wedge f}\uparrow & & \| & & \uparrow \\ W^{(k)} & \xrightarrow{f^{(k)}} & S^0 & \longrightarrow & C_{f^{(k)}} \end{array}$$

and the right hand column is the desired cofibre sequence. ∎

Now we are ready to prove the Thick Subcategory Theorem. Let $\mathbf{F} \subset \mathbf{FH}_{(p)}$ be a thick subcategory. Choose n to be the smallest integer such that $\mathbf{F}$ contains a p–local finite spectrum X with $K(n)_*(X) \neq 0$. We want to show that $\mathbf{F} = \mathbf{F}_n$. It is clear from the choice of n that $\mathbf{F} \subset \mathbf{F}_n$, so it suffices to show that $\mathbf{F} \supset \mathbf{F}_n$.

Let Y be a p–local finite CW–spectrum in $\mathbf{F}_n$. From the fact that $\mathbf{F}$ is thick, it follows that $X \wedge F$ is in $\mathbf{F}$ for any finite F, so $X \wedge DX \wedge Y$ (or $C_f \wedge Y$ in the notation of 3.10) is in $\mathbf{F}$. Thus 3.10 implies that $C_{f^{(k)}} \wedge Y$ is in $\mathbf{F}$ for all $k > 0$.

It follows from 3.9(ii) that $K(i)_*(f) = 0$ when $K(i)_*(X) \neq 0$, i.e., for $i \geq n$. Since $K(i)_*(Y) = 0$ for $i < n$, It follows that $K(i)_*(Y \wedge f) = 0$ for all i. Therefore by 3.8 (a corollary to the Nilpotence Theorem), $Y \wedge f^{(k)}$ is null homotopic for some $k > 0$.

Now the cofibre of a null homotopic map is equivalent to the wedge of its target and the suspension of its source, so we have

$$Y \wedge C_{f^{(k)}} \simeq Y \vee \Sigma Y \wedge W^{(k)}.$$

Since $\mathbf{F}$ is thick and contains $Y \wedge C_{f^{(k)}}$, it follows that Y is in $\mathbf{F}$, so $\mathbf{F}$ contains $\mathbf{F}_n$ as desired.

4 The proof of the Periodicity Theorem

In this section we will outline the proof of the Periodicity Theorem, which falls into two parts. The first, which is relatively easy, is to show that the category of spectra admitting self-maps as in the Periodicity Theorem is thick (4.6). Thus by the Thick Subcategory Theorem, this category is either $\mathbf{F}_n$, as asserted in the Periodicity Theorem, or it is trivial. The second and harder step in the proof is to construct a nontrivial example. This relies on some unpublished work of Jeff Smith.

First we need a definition.

Definition 4.1 *A* **ring spectrum** E *is a spectrum equipped with maps* $\eta: S^0 \to E$, *called the* **unit map**, *and* $m: E \wedge E \to E$, *called the* **multiplication map**, *such that the composites*

$$\begin{array}{ccccc} E = S^0 \wedge E & \xrightarrow{\eta \wedge E} & E \wedge E & \xrightarrow{m} & E \quad \textit{and} \\ E = E \wedge S^0 & \xrightarrow{E \wedge \eta} & E \wedge E & \xrightarrow{m} & E \end{array}$$

are each the identity on E *(this is analogous to the unitary condition on a ring), and the following diagram commutes up to homotopy.*

$$\begin{array}{ccc} E \wedge E \wedge E & \xrightarrow{m \wedge E} & E \wedge E \\ {\scriptstyle E \wedge m}\downarrow & & {\scriptstyle m}\downarrow \\ E \wedge E & \xrightarrow{m} & E. \end{array}$$

This is an associativity condition on m. *The multiplication* m *need not be commutative up to homotopy, but it is in most cases.*

A **module spectrum** M *over* E *is one equipped with a map*

$$E \wedge M \xrightarrow{\mu} M$$

such that the following diagram commutes up to homotopy.

$$\begin{array}{ccc} E \wedge E \wedge M & \xrightarrow{m \wedge M} & E \wedge M \\ {\scriptstyle E \wedge \mu}\downarrow & & {\scriptstyle \mu}\downarrow \\ E \wedge M & \xrightarrow{\mu} & M. \end{array}$$

We begin by observing that a self-map $f: \Sigma^d X \to X$ is adjoint to $\hat{f}: S^d \to DX \wedge X$. We will abbreviate $DX \wedge X$ by R. Now R is a ring spectrum. The unit is the map $e: S^0 \to DX \wedge X$ adjoint to the identity map on X (3.9). Since $DDX = X$ and Spanier–Whitehead duality commutes with smash products, e is dual to

$$X \wedge DX \xrightarrow{De} S^0.$$

The multiplication on R is the composite

$$DX \wedge X \wedge DX \wedge X \xrightarrow{DX \wedge De \wedge X} DX \wedge S^0 \wedge X = DX \wedge X.$$

We will use $\hat{f}_*$ to denote the element induced by $\hat{f}$ in both $\pi_*(R)$ and $K(n)_*(R)$.

Lemma 4.2 *For a v_n–map f as above, there is an i such that $K(n)_*(f^i)$ is multiplication by some power of v_n.*

Proof. The ring $K(n)_*(R)$ is a finite–dimensional $K(n)_*$–algebra, so the ungraded quotient $K(n)_*(R)/(v_n - 1)$ is a finite ring with a finite group of units. It follows that the group of units in $K(n)_*(R)$ itself is an extension of the group of units of $K(n)_*$ by this finite group. Therefore some power of the unit $\hat{f}_*$ is in $K(n)_*$, and the result follows. ∎

Lemma 4.3 *For a v_n–map f as above, there is an $i > 0$ such that $\pi_*(\hat{f}^i)$ is in the center of $\pi_*(R)$.*

Proof. Let A be a noncommutative p–torsion ring, such as $\pi_*(R)$. Given $a \in A$ we define a map

$$\mathrm{ad}(a)\colon A \longrightarrow A$$

by

$$\mathrm{ad}(a)(b) = ab - ba.$$

Thus a is in the center of A if $\mathrm{ad}(a) = 0$.

There is a formula relating $\mathrm{ad}(a^i)$ to $\mathrm{ad}^j(a)$, the j^{th} iterate of $\mathrm{ad}(a)$, namely

$$\mathrm{ad}(a^i)(x) = \sum_{j \le i} \binom{i}{j} \mathrm{ad}^j(a)(x) a^{i-j}.$$

Now suppose $\mathrm{ad}(a)$ is nilpotent and we set $i = p^N$ for some large N. Then the terms on the right for large j are zero because $\mathrm{ad}(a)$ is nilpotent, and the terms for small j vanish because the binomial coefficient is divisible by a large power of p. Hence $\mathrm{ad}(a^i) = 0$ so a^i is in the center of A.

To apply this to the situation at hand, define

$$\Sigma^d R \xrightarrow{\mathrm{ad}(f)} R$$

to be the composite

$$S^d \wedge R \xrightarrow{f \wedge R} R \wedge R \xrightarrow{1-T} R \wedge R \xrightarrow{m} R$$

where T is the map that interchanges the two factors. Then for $x \in \pi_*(R)$,

$$\pi_*(\mathrm{ad}(f))(x) = \mathrm{ad}(\hat{f})(x).$$

By 4.2 (after replacing f by a suitable iterate if necessary), we can assume that $K(n)_*(f)$ is multiplication by a power of v_n, so $K(n)_*(\hat{f})$ is in the center of $K(n)_*(R)$ and $K(n)_*(\mathrm{ad}(f)) = 0$. Hence the Nilpotence Theorem tells us that $\mathrm{ad}(f)$ is nilpotent and the argument above applies to give the desired result. ∎

Lemma 4.4 (Uniqueness of v_n–maps) *If X has two v_n–maps f and g then there are integers i and j such that $f^i = g^j$.*

Proof. Replacing f and g by suitable powers if necessary, we may assume that they commute with each other and that $K(m)_*(f) = K(m)_*(g)$ for all m. Hence $K(m)_*(f - g) = 0$ so $f - g$ is nilpotent. For $K \gg 0$ we also have

$$0 = (f-g)^{p^K} \equiv f^{p^K} - g^{p^K}$$

modulo any given power of p, so $f^{p^K} = g^{p^K}$ as claimed. ■

Lemma 4.5 *If X and Y have v_n–maps f and g and $h: X \to Y$, then there are integers i and j such that the following diagram commutes.*

$$\begin{array}{ccc} \Sigma^t X & \xrightarrow{h} & \Sigma^t Y \\ {\scriptstyle f^i}\downarrow & & {\scriptstyle g^j}\downarrow \\ X & \xrightarrow{h} & Y. \end{array}$$

Note that 4.4 is the special case of this where h is the identity map on X.

Proof. Let $W = DX \wedge Y$, so h is adjoint to an element $\hat{h} \in \pi_*(W)$. W has two v_n–maps, namely $DX \wedge g$ and $Df \wedge Y$, so by 4.4,

$$DX \wedge g^j \simeq Df^i \wedge Y$$

for suitable i and j.

Now hf^i is adjoint to $(Df^i \wedge Y)\hat{h}$ and $g^j h$ is adjoint to $(DX \wedge g^j)\hat{h}$. Since these are homotopic, the diagram commutes. ■

Theorem 4.6 *The category $\mathbf{C} \subset \mathbf{FH}_{(p)}$ of finite p–local CW–spectra admitting v_n–maps is thick.*

Proof. Suppose $X \vee Y$ is in $\mathbf{C}$ and

$$\Sigma^d(X \vee Y) \xrightarrow{f} X \vee Y$$

is a v_n–map. By 4.3 we can assume that f commutes with the idempotent

$$X \vee Y \longrightarrow X \longrightarrow X \vee Y$$

and it follows that the composite

$$\Sigma^d X \longrightarrow \Sigma^d(X \vee Y) \xrightarrow{f} X \vee Y \longrightarrow X$$

is a v_n–map, so X is in $\mathbf{C}$.

Now suppose $h: X \to Y$ where X and Y have v_n–maps f and g. By 4.5 we can assume that $hf \simeq gh$, so there is a map

$$\Sigma^d C_h \xrightarrow{\ell} C_h$$

making the following diagram commute.

$$\begin{array}{ccccc} X & \xrightarrow{h} & Y & \longrightarrow & C_h \\ {\scriptstyle f}\uparrow & & {\scriptstyle g}\uparrow & & {\scriptstyle \ell}\uparrow \\ \Sigma^d X & \xrightarrow{h} & \Sigma^d Y & \longrightarrow & \Sigma^d C_h \end{array}$$

The 5–lemma implies that $K(n)_*(\ell)$ is an isomorphism.

We also need to show that $K(m)_*(\ell) = 0$ for $m \neq n$. This is *not* implied by the facts that $K(m)_*(f) = 0$ and $K(m)_*(g) = 0$. However, an easy diagram chase shows that they do imply that $K(m)_*(\ell^2) = 0$, so ℓ^2 is the desired v_n–map on C_h. ∎

Having proved 4.6, we need only to construct one nontrivial example of a v_n–map in order to complete the proof of the Periodicity Theorem. This requires extensive use of the Adams spectral sequence and the Steenrod algebra. We will not describe these details here because they are quite technical. They will be described in [Rav]. However we will outline a new construction due to Jeff Smith which uses modular (characteristic p) representations of the symmetric group, and which is the most interesting part of the proof.

Suppose X is a finite spectrum, and $X^{(k)}$ is its k–fold smash product. The symmetric group Σ_k acts on $X^{(k)}$ by permuting coordinates. Since we are in the stable category, it is possible to add maps, so we get an action of the group ring $\mathbf{Z}[\Sigma_k]$ on $X^{(k)}$. If X is p–local, we have an action of the p–local group ring $S = \mathbf{Z}_{(p)}[\Sigma_k]$. Now suppose e is an idempotent element ($e^2 = e$) in this group ring. Then $1 - e$ is also idempotent. For any S–module M (such as $\pi_*(X^{(k)})$) we get a splitting

$$M \cong eM \oplus (1 - e)M.$$

There is a standard construction in homotopy theory which gives a similar splitting of $X^{(k)}$ or any other spectrum on which S acts, which we write as

$$X^{(k)} \simeq eX^{(k)} \vee (1 - e)X^{(k)}.$$

In some cases one of the two summands may be trivial.

Thus each idempotent element $e \in \mathbf{Z}_{(p)}[\Sigma_k]$ leads to a splitting of the smash product $X^{(k)}$ for any X. We will use this to construct a finite spectrum Y of type n that can be shown to admit a v_n–self map, starting with a well known X.

Now suppose V is a finite dimensional vector space over a field of characteristic p. (The example we have in mind is $H^*(X; \mathbf{Z}/(p))$.) Then $W = V^{\otimes k}$ is an S–module so we have a splitting

$$W \cong eW \oplus (1 - e)W$$

and the rank of eW is determined by that of V. There are enough idempotents e to give the following.

Theorem 4.7 (J. Smith) *For each positive integer r there is an idempotent*

$$e_r \in \mathbf{Z}_{(p)}[\Sigma_k]$$

(where the number k depends on r) such that the rank of eW above is nonzero if and only if the rank of V is at least r.

Now for $V = H^*(X; \mathbf{Z}/(p))$ there is a technical problem when p is odd and $H^*(X)$ is not concentrated in even dimensions. The action of Σ_k on $H^*(X^{(k)}; \mathbf{Z}/(p)) = V^{\otimes k}$ is not the expected permutation of coordinates, because a minus sign is introduced whenever two odd-dimensional elements are interchanged. Smith has proved a generalization of 4.7 that takes this into account.

For any spectrum Y, $H^*(Y; \mathbf{Z}/(p))$ is a module over the mod p Steenrod algebra A; the best reference for its properties is the classic [SE62]. Using the Adams spectral sequence, it can be shown that if Y is finite and its mod p cohomology is free as a module over a certain subalgebra of A, then Y has type n and admits a v_n-map.

To obtain such a Y, one starts with a finite spectrum X satisfying much milder conditions. An appropriate skeleton of the classifying space of the group with p elements, $B\mathbf{Z}/(p)$, will do. Then one applies a suitable Smith idempotent to a smash power of X. The cohomology of the resulting spectrum Y can be shown to satisfy the required conditions.

This completes our outline of the proof of the Periodicity Theorem.

5 The proof of the Nilpotence Theorem

In this section we will outline the proof of the Nilpotence Theorem. We have previously stated it in two different guises, in terms of self-maps (1.1) and in terms of smash products (3.7). For our purposes here it is convenient to give a third statement, but first we need another definition.

Definition 5.1 *For a ring spectrum E, the* **Hurewicz map** $h: \pi_*(X) \to E_*(X)$ *is the homomorphism induced by*

$$X \simeq S^0 \wedge X \xrightarrow{\eta \wedge X} E \wedge X$$

where $\eta: S^0 \longrightarrow E$ is the unit map for E (4.1).

Theorem 5.2 (Nilpotence Theorem, Ring Spectrum Form) *Let R be a connective ring spectrum of finite type (3.1 and 4.1) and let*

$$\pi_*(R) \xrightarrow{h} MU_*(R)$$

be the Hurewicz map. Then $\alpha \in \pi_*(R)$ is nilpotent if $h(\alpha) = 0$

To see that this implies 1.1, let X be a finite complex and let $R = X \wedge DX$. Recall that a self-map $f: \Sigma^d X \to X$ is adjoint to a map $\hat{f}: S^d \to R$. Then $h(\hat{f})$ is nilpotent if and only if $MU_*(f)$ is.

In proving this we will make use of certain spectra $X(n)$. They are constructed in terms of vector bundles and Thom spectra. Let SU denote the infinite special unitary group, i.e., the union of all the $SU(n)$'s. The Bott Periodicity Theorem gives us a homotopy equivalence

$$\Omega SU \xrightarrow{\simeq} BU$$

where BU is the classifying space of the infinite unitary group. Composing this with the loops on the inclusion of $SU(n)$ into SU, we get a map

$$\Omega SU(n) \longrightarrow BU.$$

This defines an infinite-dimensional vector bundle over $\Omega SU(n)$. The resulting Thom spectrum is $X(n)$. A routine calculation gives

$$H_*(X(n); \mathbf{Z}) = \mathbf{Z}[b_1, \ldots b_{n-1}]$$

where $|b_i| = 2i$. For $n = \infty$, this is the usual description of $H_*(MU)$.

$X(n)$ is a ring spectrum so we have a Hurewicz map

$$\pi_*(R) \xrightarrow{h(n)} X(n)_*(R).$$

In particular $X(1) = S^0$ so $h(1)$ is the identity map. The map $X(n) \to MU$ is a homotopy equivalence through dimension $2n - 1$. It follows that if $h(\alpha) = 0$, then $h(n)(\alpha) = 0$ for large n. Hence, the Nilpotence Theorem will follow from

Theorem 5.3 *With notation as above, if $h(n+1)(\alpha) = 0$ then $h(n)(\alpha)$ is nilpotent.*

The hypothesis that $h(n+1)(\alpha) = 0$ could be replaced by the condition that it is nilpotent, since we could replace α by a suitable power of it.

The element $\alpha \in \pi_*(R)$ is represented by a map

$$S^d \xrightarrow{\alpha} R.$$

Smashing both sides with R and using the multiplication in R, we get a self-map

$$\Sigma^d R = S^d \wedge R \xrightarrow{\alpha \wedge R} R \wedge R \xrightarrow{m} R,$$

which we also designate by α.

Definition 5.4 *Let $\alpha^{-1}R$ denote the homotopy direct limit of*

$$R \xrightarrow{\alpha} \Sigma^{-d}R \xrightarrow{\alpha} \Sigma^{-2d}R \xrightarrow{\alpha} \cdots.$$

This is called the **telescope** *associated with α.*

Lemma 5.5 *If $\alpha^{-1}R \wedge X(n)$ is contractible then $h(n)_*(\alpha)$ is nilpotent.*

Proof. The map $\alpha: S^d \to R$ induces a self-map Σ^d. The spectrum $\alpha^{-1}R \wedge X(n)$ is by definition the homotopy direct limit of

$$R \wedge X(n) \longrightarrow \Sigma^{-d}R \wedge X(n) \longrightarrow \Sigma^{-2d}R \wedge X(n) \longrightarrow \cdots$$

It follows that each element of $X(n)_*(R)$, including $h(n)(\alpha)$, is annihilated after a finite number of steps, so $h(n)(\alpha)$ is nilpotent. ∎

In studying questions of this sort, the following notion is convenient.

Definition 5.6 *Two spectra E and F are* **Bousfield equivalent** *if $E \wedge X$ is contractible if and only if $F \wedge X$ is. The resulting equivalence class is denoted by $\langle E \rangle$, called the* **Bousfield class** *of E. We say*

$$\langle E \rangle \geq \langle F \rangle$$

if $E \wedge X$ is contractible implies that $F \wedge X$ is contractible.

Under this partial ordering, the largest Bousfield class is, $\langle S^0 \rangle$ while the smallest is $\langle \text{pt.} \rangle$.

The following is straightforward.

Lemma 5.7 *Let*

$$\Sigma^d X \xrightarrow{f} X \longrightarrow Y$$

be a cofibre sequence, and let $f^{-1}X$ be the telescope associated with f. Then

$$\langle X \rangle = \langle Y \vee f^{-1}X \rangle$$

Now we need to study the spectra $X(n)$ more closely. Consider the diagram

$$\begin{array}{ccccc} \Omega SU(n) & \longrightarrow & \Omega SU(n+1) & \longrightarrow & \Omega S^{2n+1} \\ \| & & \uparrow & & \uparrow \\ \Omega SU(n) & \longrightarrow & B_k & \longrightarrow & J_k S^{2n} \end{array} \tag{5.8}$$

in which each row is a fibration. The top row is obtained by looping the fibration

$$SU(n) \longrightarrow SU(n+1) \xrightarrow{e} S^{2n+1}$$

where e is the evaluation map which sends a matrix $m \in SU(n+1)$ to mu where $u \in \mathbf{C}^{n+1}$ is fixed unit vector.

$J_k S^{2n}$ is the k^{th} space in the James construction [Jam53] on S^{2n}. This is the same thing as the $2nk$–skeleton of ΩS^{2n+1}. It is a CW–complex with one cell in every $2n$ dimensions; it can also be described as a certain quotient of the Cartesian product $(S^{2n})^k$. The space B_k is the pullback, i.e., the $\Omega SU(n)$–bundle over $J_k S^{2n}$ induced by the inclusion map into ΩS^{2n+1}.

Recall that $H_*(\Omega SU(n)) = \mathbf{Z}[b_1, b_2, \dots b_{n-1}]$. $H_*(B_k) \subset H_*(\Omega SU(n+1))$ is the free module over it generated by b_n^i for $0 \leq i \leq k$.

Now the composite map

$$B_k \longrightarrow \Omega SU(n+1) \longrightarrow BU \tag{5.9}$$

gives a stable bundle over B_k and we denote the Thom spectrum by F_k. We will be especially interested in F_{p^j-1}, which we will denote by G_j. These spectra interpolate between $X(n)$ and $X(n+1)$. Thus we have $G_0 = X(n)$ and $G_\infty = X(n+1)$.

The following two lemmas clearly imply 5.3 and hence the Nilpotence Theorem. Their proofs will occupy the rest of this section.

Lemma 5.10 *Let $\alpha^{-1}R$ be the telescope associated with $\alpha \in \pi_*(R)$ (5.4). If $h(n+1)_*(\alpha) = 0$ then $G_j \wedge \alpha^{-1}R$ is contractible for large j.*

The following is the harder of the two and is the heart of the Nilpotence Theorem.

Lemma 5.11 *For each $j > 0$, $\langle G_j \rangle = \langle X(n) \rangle$. In particular $\langle G_j \rangle = \langle G_{j+1} \rangle$.*

We will now outline the proof of 5.10. It requires the use of the Adams spectral sequence for a generalized homology theory. It would take too long to define this here. The interested reader can find all the needed definitions in [Rav86]. Fortunately all we require of it here is certain formal properties; we will not have to make any detailed computations.

We need to look at the Adams spectral sequence for $\pi_*(G_j \wedge R)$ based on $X(n+1)$–theory. It has the following properties:

(i) $E_2^{s,t}$ can be identified with a certain Ext group related to $X(n+1)$–theory.

(ii) $E_2^{s,t}$ vanishes unless s and t are both nonnegative.

(iii) α corresponds to an element $x \in E_2^{s,s+d}$ for some $s > 0$.

(iv) $E_2^{s,t}$ vanishes for all (s,t) above a certain line (called a *vanishing line*) of slope

$$\frac{1}{1 + p^{j+1}(n-1)},$$

i.e., $E_2^{s,t} = 0$ whenever

$$s(1 + p^{j+1}(n-1)) > t + c$$

for some constant c.

Hence the slope of the vanishing line can be made arbitrarily small by making j large, and j can be chosen so that some power of x lies above the vanishing line. This means that $G_j \wedge \alpha$ is nilpotent, and 5.10 follows.

We now turn to the more difficult proof of 5.11. We need to show that $\langle G_j \rangle = \langle X(n) \rangle$. Recall that $G_j = F_{p^j-1}$, and $H_*(F_k)$ is the free module over $H_*(X(n))$ generated by b_n^i for $0 \leq i \leq k$. One has inclusion maps

$$X(n) = F_0 \hookrightarrow F_1 \hookrightarrow F_2 \hookrightarrow \cdots$$

with cofibre sequences

$$F_{k-1} \longrightarrow F_k \longrightarrow \Sigma^{2kn} X(n).$$

From this it follows immediately that

$$\langle F_k \rangle \leq \langle X(n) \rangle$$

for all $k \geq 0$.

It can also be shown that (after localizing at p) there is a cofibre sequence

$$F_{kp^j-1} \longrightarrow F_{(k+1)p^j-1} \longrightarrow \Sigma^{2nkp^j} G_j.$$

In particular we have

$$G_j = F_{p^j-1} \hookrightarrow F_{2p^j-1} \hookrightarrow \cdots F_{(p-1)p^j-1} \hookrightarrow F_{p^{j+1}-1} = G_{j+1}$$

where the cofibre of each map is a suspension of G_j. This shows that

$$\langle G_j \rangle \geq \langle G_{j+1} \rangle. \tag{5.12}$$

It is also straightforward to show that there is a cofibre sequence

$$G_j \longrightarrow G_{j+1} \longrightarrow \Sigma^{2np^j} F_{(p-1)p^j-1}$$

which induces a short exact sequence in homology. Thus we can form the composite

$$f_{n,j}\colon G_{j+1} \longrightarrow \Sigma^{2np^j} F_{(p-1)p^j-1} \longrightarrow \Sigma^{2np^j} G_{j+1}$$

in which the first map is surjective in homology while the second is monomorphic. We denote the cofibre of $f_{n,j}$ by $Y_{n,j}$.

In order to understand these spectra, it is useful to consider the simplest case, i.e., $n = 1$ and $j = 0$. Then $G_0 = S^0$, G_1 has p cells and $Y_{1,0}$ is 2–cell complex of the form

$$S^1 \cup e^{2p}$$

so there is a cofibre sequence

$$S^{2p-1} \xrightarrow{b_{1,0}} S^1 \longrightarrow Y_{1,0}. \tag{5.13}$$

(At an odd prime these complexes are actually wedges of spheres, but is is best to ignores this fact for now.)

In the general case one replaces the cells above by copies of G_j, and there is a diagram

$$\begin{array}{ccccc} & & G_j & & \\ & & {\scriptstyle i}\downarrow & & \\ \Sigma^{-1}Y_{n,j} & \longrightarrow & G_{j+1} & \xrightarrow{f_{n,j}} & \Sigma^{2np^j}G_{j+1} \end{array}$$

where the bottom row is a cofibre sequence and i is the inclusion. The composite $f_{n,j}i$ is null, so i lifts to $\Sigma^{-1}Y_{n,j}$ This gives us the following cofibre sequence generalizing (5.13)

$$\Sigma^{2np^{j+1}-2}G_j \xrightarrow{b_{n,j}} G_j \longrightarrow \Sigma^{-1}Y_{n,j}. \tag{5.14}$$

Since $Y_{n,j}$ is the cofibre of a self–map of G_{j+1}, we have

$$\langle G_{j+1}\rangle \geq \langle Y_{n,j}\rangle. \tag{5.15}$$

Using 5.7, we see that *if the telescope* $b_{n,j}^{-1}G_j$ *is contractible* then we will have

$$\begin{array}{rcll} \langle Y_{n,j}\rangle & = & \langle G_j\rangle & \text{so} \\ \langle G_{j+1}\rangle & = & \langle G_j\rangle & \text{by (5.15) and (5.12)} \end{array}$$

Thus we have reduced the Nilpotence Theorem to the following.

Lemma 5.16 *Let*

$$\Sigma^{2np^{j+1}-2}G_j \xrightarrow{b_{n,j}} G_j$$

be the map of (5.14). It has a contractible telescope for each n and j.

This is equivalent to the statement that for each finite skeleton of G_j, there is an iterate of $b_{n,j}$ whose restriction to the skeleton is null.

Proof. We need to look again at (5.8) for $k = p^j - 1$. The map

$$J_{p^j-1}S^{2n} \longrightarrow \Omega S^{2n+1}$$

is known (after localizing at p) to the be inclusion of the fibre of a map

$$\Omega S^{2n+1} \xrightarrow{H} \Omega S^{2np^j+1}.$$

Thus the diagram (5.8) can be enlarged to

$$\begin{array}{ccccc} & & \Omega S^{2np^j+1} & = & \Omega S^{2np^j+1} \\ & & \uparrow & & {\scriptstyle H}\uparrow \\ \Omega SU(n) & \longrightarrow & \Omega SU(n+1) & \longrightarrow & \Omega S^{2n+1} \\ \| & & \uparrow & & \uparrow \\ \Omega SU(n) & \longrightarrow & B_{p^j-1} & \longrightarrow & J_{p^j-1}S^{2n} \\ & & \uparrow & & \uparrow \\ & & \Omega^2 S^{2np^j+1} & = & \Omega^2 S^{2np^j+1} \end{array} \tag{5.17}$$

in which each row and column is a fibre sequence.

Of particular interest is the map

$$\Omega^2 S^{2np^j+1} \longrightarrow B_{p^j-1}$$

We can think of the double loop space $\Omega^2 S^{2np^j+1}$ as a topological group acting on the space B_{p^j-1}, so there is an action map

$$\Omega^2 S^{2np^j+1} \times B_{p^j-1} \longrightarrow B_{p^j-1}. \tag{5.18}$$

Recall that G_j is the Thom spectrum of a certain stable vector bundle over B_{p^j-1}. This means that (5.18) leads to a stable map

$$\Sigma^\infty \Omega^2 S^{2np^j+1}_+ \wedge G_j \xrightarrow{\mu} G_j. \tag{5.19}$$

Here we are skipping over some technical details which can be found in [DHS88].

The space $\Omega^2 S^{2np^j+1}$ was shown by Snaith [Sna74] to have a stable splitting, i.e., the suspension spectrum $\Sigma^\infty \Omega^2 S^{2np^j+1}_+$ is homotopy equivalent to an infinite wedge of finite spectra. After localizing at p, this splitting has the form

$$\Sigma^\infty \Omega^2 S^{2np^j+1}_+ \simeq (S^0 \vee S^{2np^j-1}) \wedge \bigvee_{m\geq 0} \Sigma^{m|b_{n,j}|} D_m \tag{5.20}$$

where each D_m is a certain finite complex (independent of n and j) with bottom cell in dimension 0. Moreover there are maps

$$S^0 = D_0 \longrightarrow D_1 \longrightarrow D_2 \longrightarrow \cdots$$

of degree 1 on the bottom cell, and the limit, $\lim_{\rightarrow} D_m$, is known to be the mod p Eilenberg–Mac Lane spectrum $H/(p)$ (3.3).

Our map $b_{n,j}$ is the composite

$$\Sigma^{|b_{n,j}|}G_j \longrightarrow \Sigma^{|b_{n,j}|}D_1 \wedge G_j \longrightarrow \Sigma^\infty \Omega^2 S^{2np^j+1}_+ \wedge G_j \xrightarrow{\mu} G_j.$$

and $b^m_{n,j}$ is the composite

$$\Sigma^{m|b_{n,j}|}G_j \longrightarrow \Sigma^{m|b_{n,j}|}D_m \wedge G_j \longrightarrow \Sigma^\infty \Omega^2 S^{2np^j+1}_+ \wedge G_j \xrightarrow{\mu} G_j.$$

Thus we get a diagram

$$\begin{array}{ccccccc} G_j & \longrightarrow & D_1 \wedge G_j & \longrightarrow & D_2 \wedge G_j & \longrightarrow \cdots \\ \| & & \downarrow & & \downarrow & \\ G_j & \xrightarrow{b_{n,j}} & \Sigma^{-|b_{n,j}|}G_j & \xrightarrow{b_{n,j}} & \Sigma^{-2|b_{n,j}|}G_j & \longrightarrow \cdots \end{array}$$

This means that the map

$$G_j \longrightarrow b_{n,j}^{-1}G_j$$

factors through $G_j \wedge M/(p)$.

Now consider the diagram

$$\begin{array}{ccccc} G_j & \longrightarrow & G_j \wedge H/(p) & \longrightarrow & b_{n,j}^{-1}G_j \\ {\scriptstyle b_{n,j}}\downarrow & & {\scriptstyle b_{n,j}}\downarrow & & \| \\ \Sigma^{-|b_{n,j}|}G_j & \longrightarrow & \Sigma^{-|b_{n,j}|}G_j \wedge H/(p) & \longrightarrow & b_{n,j}^{-1}G_j \\ \downarrow & & \downarrow & & \downarrow \\ \vdots & & \vdots & & \vdots \end{array}$$

The middle vertical map is null because $b_{n,j}$ induces the trivial map in homology. Passing to the limit, we get

$$b_{n,j}^{-1}G_j \longrightarrow \text{pt.} \longrightarrow b_{n,j}^{-1}G_j$$

with the composite being the identity map on the telescope $b_{n,j}^{-1}G_j$. This shows that the telescope is contractible as desired. ∎

References

[Ada74] J. F. Adams. *Stable Homotopy and Generalised Homology.* University of Chicago Press, Chicago, 1974.

[Ada75] J. F. Adams. *Localisation and Completion. Lecture Notes in Mathematics,* University of Chicago, Department of Mathematics, 1975.

[BK72] A. K. Bousfield and D. M. Kan. *Homotopy Limits, Completions and Localizations.* Volume 304 of *Lecture Notes in Mathematics,* Springer–Verlag, 1972.

[DHS88] E. Devinatz, M. J. Hopkins, and J. H. Smith. Nilpotence and stable homotopy theory. *Annals of Mathematics*, 128:207–242, 1988.

[Haz78] M. Hazewinkel. *Formal Groups and Applications.* Academic Press, New York, 1978.

[HKR] M. J. Hopkins, N. J. Kuhn, and D. C. Ravenel. Generalized group characters and complex oriented cohomology theories. To appear.

[Hop87] M. J. Hopkins. Global methods in homotopy theory. In J. D. S. Jones and E. Rees, editors, *Proceedings of the 1985 LMS Symposium on Homotopy Theory*, pages 73–96, 1987.

[HS] M. J. Hopkins and J. H. Smith. Nilpotence and stable homotopy theory II. To appear.

[Jam53] I. M. James. Reduced product spaces. *Annals of Mathematics*, 62:170–197, 1953.

[JW75] D. C. Johnson and W. S. Wilson. BP–operations and Morava's extraordinary K–theories. *Mathematische Zeitschrift*, 144:55–75, 1975.

[Lan73a] P. S. Landweber. Annihilator ideals and primitive elements in complex cobordism. *Illinois Journal of Mathematics*, 17:273–284, 1973.

[Lan73b] P. S. Landweber. Associated prime ideals and Hopf algebras. *Journal of Pure and Applied Algebra*, 3:175–179, 1973.

[Laz55a] M. Lazard. Lois de groupes et analyseurs. *Ann. Écoles Norm. Sup.*, 72:299–400, 1955.

[Laz55b] M. Lazard. Sur les groupes de Lie formels á une paramètre. *Bull. Soc. Math. France*, 83:251–274, 1955.

[Lim60] E. L. Lima. Stable Postnikov invariants and their duals. *Summa Brasil. Math.*, 4:193–251, 1960.

[Mil60] J. W. Milnor. On the cobordism ring Ω^* and a complex analogue, Part I. *American Journal of Mathematics*, 82:505–521, 1960.

[Mit85] S. A. Mitchell. Finite complexes with $A(n)$–free cohomology. *Topology*, 24:227–248, 1985.

[Mor85] J. Morava. Noetherian localizations of categories of cobordism comodules. *Annals of Mathematics*, 121:1–39, 1985.

[Nov60] S. P. Novikov. Some problems in the topology of manifolds connected with the theory of Thom spaces. *Soviet Mathematics Doklady*, 1:717–720, 1960.

[Nov62] S. P. Novikov. Homotopy properties of Thom complexes (Russian). *Mat. Sb. (N. S.)*, 57 (99):407–442, 1962.

[Qui69] D. G. Quillen. On the formal group laws of oriented and unoriented cobordism theory. *Bulletin of the American Mathematical Society*, 75:1293–1298, 1969.

[Rav] D. C. Ravenel. The chromatic point of view in homotopy theory. To appear.

[Rav84] D. C. Ravenel. Localization with respect to certain periodic homology theories. *American Journal of Mathematics*, 106:351–414, 1984.

[Rav86] D. C. Ravenel. *Complex Cobordism and Stable Homotopy Groups of Spheres.* Academic Press, New York, 1986.

[RW80] D. C. Ravenel and W. S. Wilson. The Morava K–theories of Eilenberg–Mac Lane spaces and the Conner–Floyd conjecture. *American Journal of Mathematics*, 102:691–748, 1980.

[SE62] N. E. Steenrod and D. B. A. Epstein. *Cohomology Operations.* Volume 50 of *Annals of Mathematics Studies*, Princeton University Press, Princeton, 1962.

[Sna74] V. P. Snaith. Stable decomposition of $\Omega^n\Sigma^n X$. *Journal of the London Mathematical Society*, 7:577–583, 1974.

[Sto68] R. E. Stong. *Notes on Cobordism Theory.* Princeton University Press, Princeton, 1968.

[Tho54] R. Thom. Quelques propriétés globales des variétés differentiables. *Commentarii Mathematici Helvetici*, 28:17–86, 1954.

Douglas C. RAVENEL

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF ROCHESTER
ROCHESTER, NEW YORK 14627
USA

Astérisque

LUCIEN SZPIRO

Sur les solutions d'un système d'équations polynomiales sur une variété abélienne

Astérisque, tome 189-190 (1990), Séminaire Bourbaki,
exp. n° 729, p. 429-446

<http://www.numdam.org/item?id=SB_1989-1990__32__429_0>

© Société mathématique de France, 1990, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Séminaire BOURBAKI juin 1990
42ème année, 1989-90, n° 729

SUR LES SOLUTIONS D'UN SYSTÈME D'ÉQUATIONS POLYNOMIALES SUR UNE VARIÉTÉ ABÉLIENNE

[d'après **G. Faltings et P. Vojta**]

par **Lucien SZPIRO**

Dans un manuscrit récent, G. Faltings démontre un résultat bien plus général que la "conjecture de Mordell" (Théorème 1 ci-dessous). Nous analysons ce travail en nous organisant comme suit :

1. **Points rationnels** des variétés algébriques
2. **L'index** d'une section d'un fibré en droites en un point
   2.1. Le théorème du produit
   2.2. Section dérivées
3. **Fibrés amples**
   3.1. Un morphisme fini
   3.2. Le fibré $L(-\varepsilon, s_1 \cdots s_m)$
   3.3. Degré d'Arakelov de $L(-\varepsilon, s_1 \cdots s_m)$
4. **Une approximation** trop grande
   4.1. Points d'un réseau non dans un sous-réseau
   4.2. Sections d'index très petit
   4.3. Degré d'Arakelov et index
5. **Autres résultats**

En 1) nous indiquons le théorème principal et les raisons qui rendent "naturelles" ses hypothèses. En 2) nous introduisons la notion technique d'index qui sous-tend tout ce travail. En 3) les ressources de la géométrie algébrique (notamment le théorème de Nakaï-Moishezon-Kleiman) sont mises à profit pour trouver "l'invariant numérique" qui contrôle la situa-

tion. En 4) un peu d'arithmétique due à Minkowski permet de finir la démonstration.

Les manuscrits de G. Faltings ne m'ont jamais semblé aisés. Sans l'aide de M. Flexor et E. Ullmo, je n'aurais sans doute pas réussi à saisir celui-ci. Je tiens à les en remercier chaleureusement.

1. POINTS RATIONNELS DES VARIÉTÉS ALGÉBRIQUES

Soit C une courbe algébrique définie sur un corps de nombres K. La nature du cardinal de l'ensemble $C(K)$ de ses points rationnels sur K ne dépend que d'un invariant topologique de C : son genre. La situation est la suivante :

i) genre 0 : Aucun ou une infinité de points dans $C(K)$;

ii) genre 1 : $C(K)$ est vide ou est un $\mathbf{Z}$-module de type fini (théorème de Mordell sur $\mathbf{Q}$ généralisé par Weil aux variétés abéliennes et aux corps de nombres quelconques) ;

iii) genre au moins 2 : $C(K)$ est fini (conjecturé par Mordell, ce résultat a été prouvé par Faltings [F1], *cf.* aussi les exposés 616 et 619 de ce Séminaire).

Il est raisonnable de se poser la question de la finitude de l'ensemble $X(K)$ des points rationnels d'une variété algébrique X de dimension quelconque sur un corps de nombres K. On ne veut pas que X contienne de droite projective ou de variété abélienne. Par exemple, une variété abélienne ne contient aucune droite projective. G. Faltings, en comprenant la géométrie algébrique d'une nouvelle démonstration de iii) annoncée par P. Vojta, a obtenu le résultat suivant :

THÉORÈME 1.— *Soit A une variété abélienne sur un corps de nombres K. Soit X une sous-variété algébrique fermée de A, ne contenant sur la clôture algébrique $\bar{K}$ de K aucun translaté d'une sous-variété abélienne de dimension non nulle de A. Alors, l'ensemble des points rationnels de X sur K est fini.*

Exemple 1.— Une courbe projective, lisse, connexe sur K de genre $g \geq 2$ se

plonge (morphisme d'Abel) dans sa jacobienne qui est une variété abélienne de dimension g.

Exemple 2.— Si A est une variété abélienne simple — *i.e.* ne contenant aucune sous-variété abélienne — alors, toute sous-variété algébrique propre de A satisfait aux hypothèses du théorème.

Exemple 3.— Si C est une courbe hyperelliptique de genre au moins quatre, ou plus généralement si C n'est pas un revêtement double d'une courbe elliptique, l'image de $C \times C$ dans la jacobienne J de C (qui à (x, y) fait correspondre la classe de $x + y - D$ où D est un diviseur de degré deux choisi à l'avance) satisfait aux hypothèses du théorème.

Avant d'exposer la partie technique de la démonstration, rappelons la méthode pratiquement toujours utilisée dans les théorèmes de finitude :

On associe à un plongement projectif adéquat $X \hookrightarrow \mathbf{P}_K^N$ une *hauteur*. C'est une fonction sur $X(\bar{K})$ telle que l'ensemble des points sur $X(\bar{K})$, de hauteur bornée et défini sur un corps de degré borné, est un ensemble fini (théorème de Northcott). On sait, en géométrie algébrique, associer biunivoquement à un plongement projectif un faisceau inversible "très ample". Quand on munit ce faisceau inversible d'un modèle entier sur $\mathcal{O}_K$, anneau des entiers de K, et de métriques pour tout plongement de K dans $\mathbf{C}$, Arakelov [A] nous a appris à construire une hauteur de la façon suivante :

Soit $X \xrightarrow{f} \operatorname{Spec} \mathcal{O}_K$ un modèle entier de la variété projective $X \hookrightarrow \mathbf{P}_K^N$ et soit L_K un fibré inversible sur X muni de métriques hermitiennes $\| \|_\sigma$ pour chaque plongement $\sigma : K \to \mathbf{C}$. Soit $P \in X_K(K)$ un point rationnel, et soit $\mathbf{s}_P : \operatorname{Spec} \mathcal{O}_K \to X$ la section de f correspondant à P. Si t est un élément non nul de $\mathbf{s}_P^* L$, on pose le degré d'Arakelov de L en P égal à :

$$\log (\# \mathbf{s}_P^* L / t\mathcal{O}_K) - \sum_\sigma \log \|t(P)\|_\sigma$$

(ce nombre est indépendant de t).

Un travail du chapitre 3 sera de mettre en évidence une certaine catégorie de fibrés en droites, dont une puissance fournit une immersion

fermée dans un espace projectif. Munis de métriques à courbures plates sur A, ils permettent de calculer, au chapitre 4, des degrés d'Arakelov "trop petits".

2. L'INDEX D'UNE SECTION D'UN FIBRÉ EN DROITE EN UN POINT

Dans ce chapitre, nous apprenons à "dériver" les sections d'un fibré en droites qui s'annulent sur une sous-variété, pour obtenir une autre section du même fibré restreint à la sous-variété. L'idée est simple : soit X une variété algébrique, Y une sous-variété algébrique de X, L un fibré inversible sur X, s une section L et D un opérateur différentiel d'ordre un sur X (*i.e.* $D(fg) = gDf + fDg \quad f, g \in \mathcal{O}_X$). Si on identifie sur un ouvert s à une fonction sur X, on veut que $Ds_{|Y}$ ait un sens si s s'annule sur Y. Pour cela, il suffit de remarquer que si u, f sont des fonctions sur un ouvert et que $f_{|Y} = 0$, $(D(uf))_{|Y} = u(Df)_{|Y}$ et donc Ds est une section de $L_{|Y}$ (recollement par les mêmes cocycles !). De même si s s'annule à l'ordre m sur Y, et si $D = D_1 \cdots D_m$ est un opérateur différentiel, produit d'opérateurs de degré un, alors $Ds_{|Y}$ a un sens et est une section de $L_{|Y}$.

DÉFINITION 2.0.— *Soit $P = \mathbf{P}^{n_1} \times \cdots \times \mathbf{P}^{n_m}$ un produit d'espaces projectifs sur un corps K de caractéristique zéro, soit $L = \mathcal{O}(d_1, \cdots, d_m)$, $d_i > 0$, le fibré inversible sur P, dont les sections sont les polynômes de multidegré indiqué. Soit s une section globale de L. Alors pour un point $x \in P$ l'indice $i(x, s)$ de s en x est le plus grand nombre rationnel σ tel que :*

Si $D = D_1 \cdots D_m$ est un opérateur différentiel sur P tel que chaque D_i soit un opérateur différentiel sur $\mathbf{P}^{n_i}$ de degré j_i, avec

$$\frac{j_1}{d_1} + \frac{j_2}{d_2} + \cdots + \frac{j_m}{d_m} < \sigma$$

alors, $D(s)$ s'annule en x.

La "formule de Taylor" nous montre que l'index d'une section non nulle est fini. Il mesure, de façon pondérée, l'ordre du zéro de s en x.

2.1. Le théorème du produit

Notons Z_σ le fermé de P où l'index de s est au moins égal à σ. Le théorème qui suit, découverte de G. Faltings, donne de l'éclat à la notion que nous venons d'introduire.

THÉORÈME 2.1.— *Pour tout $\varepsilon > 0$, il existe r, tel que, si $d_i/d_{i+1} \geq r$ pour tout i, et si Z est une composante irréductible de $Z_{\sigma+\varepsilon}$ ainsi que de Z_σ, alors on a :*

i) *$Z = Z_1 \times \cdots \times Z_m$ est un produit de sous-variétés Z_i de $\mathbf{P}^{n_i}$;*

ii) *le degré de chaque Z_i est borné en fonction de ε.*

Soit $Z \subset \mathbf{P}^{n_i} \times \cdots \times \mathbf{P}^{n_m} = P$ et soit Z_i la projection de Z sur le facteur $\mathbf{P}^{n_i}$. Notons δ_i la dimension de Z_i. Si Z est un fermé irréductible réduit de P et si $\sum \delta_i = \dim Z$, il est clair que $Z = Z_1 \times \cdots \times Z_m$. Appliquons cette remarque simplette à notre situation et posons $L_i = pr_i^* \mathcal{O}(1)$ ($= \mathcal{O}(a_1, \cdots a_m)$ avec $a_j = \delta_{j,i}$) et essayons de voir quelles sont les intersections

$$\left(Z \cdot L_1^{e_1} \cdot \cdots \cdot L_m^{e_m}\right)$$

où L_i^a est l'intersection a-fois de L_i avec lui-même. Le fermé Z_σ étant défini par des équations de multidegré $(d_1, \cdots, d_m)$ si Z est une composante de Z_σ de multiplicité ρ, on voit facilement que $(Z \cdot L_1^{e_1} \cdot \cdots \cdot L_m^{e_m}) \leq \frac{1}{\rho} L^{\operatorname{codim} Z} \cdot (L_1^{e_1} \cdot \cdots \cdot L_m^{e_m})$, où $L = L_1^{\otimes d_1} \otimes L_2^{\otimes d_2} \otimes \cdots \otimes L_m^{\otimes d_m}$. Le seul terme non nul à droite de l'inégalité est obtenu à partir de

$$\left(L_1^{\otimes d_1}\right)^{n_1 - e_1} \cdot \left(L_2^{\otimes d_2}\right)^{n_2 - e_2} \cdots \left(L_m^{\otimes d_m}\right)^{n_m - e_m} \cdot L_1^{e_1} \cdot \cdots \cdot L_m^{e_m}.$$

On a donc :

$$(Z \cdot L_1^{e_1} \cdot \cdots \cdot L_m^{e_m}) \leq O\left(\frac{1}{\rho} \prod_i d_i^{n_i - e_i}\right).$$

Si on montre (*cf.* plus bas) :

$$(*) \qquad \rho = \text{multiplicité de } Z \text{ dans } Z_\sigma \geq O\left(\prod_i d_i^{n_i - \delta_i}\right).$$

on aura :

$$(Z \cdot L_1^{e_1} \cdot \cdots \cdot L_m^{e_m}) \leq O\left(\prod d_i^{\delta_i - e_i}\right).$$

D'autre part, il est clair que $(Z \cdot L_1^{e_1} \cdot \cdots \cdot L_m^{e_m})$ est nul si $e_i > \delta_i$, donc les $\eta_{m-j} = \delta_m + \delta_{m-1} + \cdots + \delta_{m-j} - (e_m + e_{m-1} + \cdots + e_{m-j})$ sont positifs et on a :

$$(Z \cdot L_1^{e_1} \cdot \cdots \cdot L_m^{e_m}) \leq O(r^{-\eta}),$$

où $\eta = \sum \eta_j \geq 0$. Si comme dans l'hypothèse du théorème $d_i/d_{i-1} \leq 1/r$ où r est assez grand, la seule possibilité pour que $(Z \cdot L_1^{e_1} \cdot \cdots \cdot L_m^{e_m})$ soit non nul (c'est toujours un entier positif ou nul) est que $\eta = 0$ *i.e.* $\delta_i = e_i$; comme $\sum e_i = \dim Z$, on a le résultat cherché. Il reste à prouver l'inégalité (*) quand Z est aussi une composante de $Z_{\sigma+\varepsilon}$. Soient $(X_{i,j} = 0)$, $j = 1, \cdots, n_i - \delta_i$ des équations locales de Z_i dans $\mathbf{P}^{n_i}$ en un point assez général. Une équation de la forme $g = \prod_{i,j} X_{i,j}^{\alpha_{i,j}} \cdot f$ (f équation non nulle au point) avec $\sum_i \frac{1}{d_i}(\sum_j \alpha_{i,j}) < \varepsilon$ est telle qu'il existe un opérateur $D = D_1 \cdots D_m$, D_i opérateurs différentiels sur $\mathbf{P}^{n_i}$ tels que $\sum_i \frac{\deg D_i}{d_i} \leq \varepsilon$, avec $D(g)$, n'appartient pas à l'idéal $(X_{i,j} = 0)$. On voit qu'une équation de Z_σ doit s'écrire $\prod_{i,j} X_{i,j}^{\alpha_{i,j}} \cdot f$ avec $\sum \frac{1}{d_i} \sum \alpha_{i,j} \geq \varepsilon$. Une puissance a d'un $X_{i,j}$ introduisant a de plus à la multiplicité, on voit que la multiplicité ρ de Z dans Z_σ, quand Z est une composante de Z_σ et $Z_{\sigma+\varepsilon}$, est au moins égale au nombre d'entiers $\alpha_{i,j}$ tels que $\sum_{i=1}^m \frac{1}{d_i} \sum_{j=1}^{n_i - \delta_i} \alpha_{ij} < \varepsilon$. Ceci prouve l'inégalité (*). La partie ii) se montre en faisant un peu plus attention aux résultats des calculs.

2.2. Sections dérivées

Si on envoie une variété X_i dans $\mathbf{P}^{\dim X_i} = P_i$ avec un morphisme fini bien choisi et si G_i est une équation (de degré calculable) qui annule $\Omega^1_{X_i|P_i}$ définissant un fermé Z_i dans X_i, $X_i - Z_i \to \mathbf{P}^{\dim X_i}$ est alors quasi-fini étale. Prenons une sous-variété fermée $Y \subset X_1 \times \cdots \times X_m \to P_1 \times \cdots \times P_m$ telle que $pr_i(Y)$ soit non contenue dans Z_i pour tout i. Fixant des entiers $d_1 \cdots d_m$, on définit l'index $i(Y, f)$ d'une section f de $O(d_1, \cdots, d_m)$ sur Y à partir d'opérateurs différentiels $D = D_1 \cdots D_m$ sur P en multipliant D_i par $G_i^{\deg D_i}$ pour qu'il ait un sens sur X_i. $D(f)$ devient alors une section

de

$$O(d_1, \cdots, d_m) \otimes \bigotimes_i O(\deg G_i \cdot \deg D_i).$$

L'indice de f en Y sera bien sûr celui de f en l'image de Y dans P, multiplié par le degré de Y sur son image.

3. FIBRÉS AMPLES

On met en évidence dans ce chapitre un ensemble de fibrés en droites qui permettront au chapitre 4 de calculer des hauteurs. Le choix d'une bonne hauteur sera essentiel à l'argument. Ceci rappelle que l'introduction de la "hauteur modulaire" dans [F1] a été une des grandes nouveautés utilisées. C'est P. Vojta qui dans [V] a introduit des fibrés amples "astucieux" pour la situation.

3.1. Un morphisme fini

Le lemme suivant, très utile dans la suite, a sans doute été influencé par les lemmes 10 et 11 de [H].

Lemme 3.1.— *Soit A une variété abélienne sur un corps algébriquement clos de caractéristique zéro. Soit X une sous-variété irréductible de A ne contenant aucun translaté d'une sous-variété abélienne de A. Alors pour m entier assez grand, le morphisme $\alpha_m : X^m \to A^{m-1}$ défini par $\alpha_m(x_1, \cdots, x_m) = (2x_1 - x_2, 2x_2 - x_3, \cdots, 2x_{m-1} - x_m)$ est fini.*

La projection $X^{m+1} \to X^m$ sur les premiers facteurs induit une immersion fermée d'une fibre de α_{m-1} dans une fibre de α_m. Soit d la limite inférieure des maxima de dimensions des fibres des α_m quand m croît. On veut montrer que $d = 0$. Fixons un fibré ample symétrique L sur A pour calculer les degrés. Le nombre et le maximum des degrés des composantes irréductibles de dimension d des fibres de α_m pour $m \geq m_0$ décroissent aussi, donc deviennent constants. Remarquons que si Z est une composante irréductible d'une fibre, $2^n Z$ aussi, donc son degré est borné indépendamment de n. Soit G le groupe algébrique des g dans A tels que

$g + Z = Z$. On a

$$\text{degré}\,(Z \to 2^n Z) \cdot \text{degré}\,(2^n Z) = \deg([2n]^* L)_{|Z} = \deg(L^{\otimes 4^n})^d_{|Z} = 4^{nd} \deg(Z)$$

($[2^n]^* L = L^{\otimes 4^n}$ car L est symétrique). Le degré de $Z \to 2^n Z$ se calcule au point générique de Z et est donc égal au cardinal de $\text{Ker}\,([2^n] : G \to G)$. On voit ainsi que 4^{nd} deg $Z/\sharp\text{Ker}\,([2^n] : G \to G)$ est borné et donc que $\text{Ker}\,[2^n] : G \to G$ est de l'ordre de 4^{nd}. Ceci implique deux choses :

i) G est de dimension d ;

ii) la composante connexe de G est une variété abélienne.

Si $z \in Z$, $z + G = Z$ car Z est irréductible, de dimension d, et que par définition $z + G \subset Z$. Donc G est connexe et Z est le translaté d'une variété abélienne, donc $d = 0$, CQFD.

COROLLAIRE 3.1.— *Si m est assez grand et si X satisfait aux hypothèses du lemme* 3.1, *alors le faisceau inversible*

$$\bigotimes_{i=1}^{m-1} \left(2^{m-i} x_i - 2^{m-i-1} x_{i+1}\right)^* (L)$$

est ample sur X^m quand L est ample sur A.

On a pris bien entendu $\left(2^{m-i} x_i - 2^{m-i-1} x_{i+1}\right) : A^m \longrightarrow A$ qui envoie $(x_1 \cdots x_m)$ sur $2^{m-i} x_i - 2^{m-i-1} x_{i+1}$. On en déduit que

$$\otimes\, (2^{m-i} x_i - 2^{m-i-1} x_{i+1})^* L = \alpha_m^* \otimes [2^{m-i-1}]^*\, pr_i^*(L).$$

3.2. Le fibré $L(-\varepsilon, s_1, \cdots, s_m)$

Nous sommes maintenant prêts à définir le fibré inversible important de ce travail et à montrer, en utilisant les chapitres 1 et 2 qu'il est ample sous certaines hypothèses.

DÉFINITION.— *Soit L un fibré inversible sur A et soient $\varepsilon, s_1, \cdots, s_m$ des nombres rationnels positifs, le* **Q** *fibré en droite, $L(-\varepsilon, s_1, \cdots, s_m)$ sur A^m est défini par :*

$$L(-\varepsilon, s_1, \cdots, s_m) = \bigotimes_i pr_i^* \left(L^{\otimes \varepsilon s_i^2}\right) \otimes \bigotimes_i (s_i x_i - s_{i+1} x_{i+1})^* (L)$$

Comme plus haut, $(s_i x_i - s_{i+1}x_{i+1})^*(L)$ dénote l'objet suivant : Soit a un entier tel que as_i soit entier pour tout i. alors l'application $(x_i \cdots x_m) \to as_i x_i - as_{i+1}x_{i+1}$ de A^m dans A est bien définie, et l'image réciproque L par ce morphisme est la puissance tensorielle a^2-ième de $(s_i x_i - s_{i+1}x_{i+1})^*(L)$.

Dans ce rapport, nous considérerons toujours le cas où L est ample et symétrique sur A. Notons $P_{i,j} = (x_i + x_j)^* L \otimes pr_i^* L^{\otimes -1} \otimes pr_j^* L^{\otimes -1}$ le fibré de Poincaré d'indice i,j et $L_i = pr_i^* L$, $L(-\varepsilon, s) = L(-\varepsilon, s_1, \cdots, s_m)$. On voit que $L(-\varepsilon, s)$ est une combinaison linéaire à coefficients rationnels des L_i et des $P_{i,j}$. En fait

$$L(-\varepsilon, s) = \bigotimes_i L_i^{\otimes s_i^2(1-\varepsilon)} \otimes \bigotimes_i P_{i,i+1}^{\otimes -s_i s_{i+1}}.$$

THÉORÈME 3.2.— *Choisissons un entier m comme dans le lemme* 3.1 ; *alors il existe ε_0 réel positif tel qu'il existe un réel r, tel que : $L(-\varepsilon, s_1, \cdots, s_m)$ est ample dès que $\varepsilon < \varepsilon_0$ et $s_i/s_{i+1} \geq r$.*

Remarquons que $L(0, 2^{m-1}, 2^{m-2}, \cdots, 2^0)$ est le faisceau inversible considéré au corollaire 3.1 ; on sait donc déjà que celui-ci est ample sur X^m.

Lemme 3.2.1.— *Soit $Y = Y_1 \times \cdots \times Y_m$ une variété produit dans A^m ; alors comme fonction des s_i, $(L(-\varepsilon, s)^{\dim Y} \cdot Y)$ est proportionnel à $\prod s_i^{2 \dim Y_i}$.*

COROLLAIRE 3.2.1.— *Il existe $\varepsilon_0 > 0$ tel que si $\varepsilon < \varepsilon_0$ et si Y est une variété produit dans X^m, alors $L(-\varepsilon, s)^{\dim Y} \cdot Y$ est strictement positif.*

Ceci résulte du corollaire 3.1. Pour ε petit et $s_i = 2^{m-i}$, le résultat est donc aussi établi par le lemme 3.2.1, il est donc vrai pour les mêmes ε et $s_1 \cdots s_m$ positifs quelconques.

On montre maintenant par récurrence que, pour tout N entier, et pour un produit $Y = Y_1 \times \cdots \times Y_m$ dans X^m avec $\deg Y_i \leq N$, il existe r_0 (dépendant de ε et N) tel que $L(-\varepsilon, s)$ soit ample sur Y si $s_i/s_{i+1} \geq r_0$. On fait une récurrence sur la dimension de Y (Y étant toujours un produit). Par le théorème de Kleiman ([K]), $L(-\varepsilon, s)$ est dans la fermeture du cône ample si, restreint à toute courbe irréductible C dans Y, il est de degré positif ou nul. En diminuant un peu ε, il sera ample. Pour montrer la

positivité du degré de $L(-\varepsilon, s)$ sur C, nous allons **A)** d'abord trouver une section de $L(-\varepsilon, s)^{\otimes d}$ sur Y ; **B)** ensuite, montrer que si l'index du point générique de C est assez grand, par le théorème 2.1 C sera contenu dans un produit plus petit; **C)** enfin, si l'index au point générique de C est petit et si $0 < \varepsilon' \leq \varepsilon_0$, ε_0' bien choisi, alors $L(-\varepsilon', s)$ a une section sur C.

A) Si d est assez grand $\chi(Y, L(-\varepsilon, s)^{\otimes d}$ est positif (corollaire 3.2.1). Il nous suffira donc, pour avoir $H^0(Y, L(-\varepsilon, s)^{\otimes d} \neq 0$, de vérifier que pour $d \gg 0$ $H^i(Y, L(-\varepsilon, s)^{\otimes d}) = 0$ $i \geq 2$. Or, si H est une section hyperplane, et si d est assez grand,

$$H^i(H, L(-\varepsilon, s)^{\otimes d}(H)_{|H}) = 0 \qquad \text{pour } i \geq 1.$$

La suite exacte longue de cohomologie donne que

$$H^i(Y, L(-\varepsilon, s)^{\otimes d}) \longrightarrow H^i(Y, L(-\varepsilon, s)^{\otimes d}(H))$$

est un isomorhisme pour $i \geq 2$. L'ennui, c'est que le d choisi dépend de H. Un travail un peu plus fin permet quand même de conclure dans le même esprit :

$$H^i(Y, L(-\varepsilon, s)^{\otimes d}) \longrightarrow H^i(Y, L(-\varepsilon, s)^{\otimes d}(NH))$$

est un isomorphisme $i \geq 2$, $N \gg 0$. Donc chacun de ces groupes est nul.

B) On choisit une courbe C dans Y et on définit l'index $i(C)$ de la section trouvée dans **A)** en un point générique de C comme dans 2.2 quand C n'est pas contenu dans le lieu de ramification $Z_1 \times \cdots \times Z_m$ de morphismes raisonnablement choisis $Y_i \to \mathbf{P}^{\dim Y_i}$. (Si C était contenu dans $Z_1 \times \cdots \times Z_m$, l'hypothèse de récurrence s'appliquerait.) Choisissons σ assez petit et supposons $i(C) \geq \sigma$. Dans $\mathbf{P}^{n_1} \times \cdots \times \mathbf{P}^{n_m} = P$ $n_i = \dim Y_i$ les $(Z_{\sigma i/\dim P})$ $i = 1, 2, \cdots \dim P$ ont des composantes de dimension strictement comprise entre 0 et dim P ($Z_{\sigma i/\dim P}$ contient le point générique de l'image de C et aucun ne peut être P en entier car la section est non nulle). Par le théorème du produit un des $Z_{\sigma i/\dim P}$ est un produit quand $s_i/s_{i+1} \geq r$ et r assez grand. La courbe C elle-même est donc contenue dans un fermé produit plus petit et l'hypothèse de récurrence s'applique.

C) $i(D) < \sigma$. La théorie de 2.2 montre qu'on a ainsi une constante λ telle que $L(\lambda \deg(C \to D)\sigma - \varepsilon, s)_{|C}$ a une section non nulle (dérivée de celle de $L(-\varepsilon, s)$ sur Y). Choisissant σ assez petit pour que $\lambda \deg(C \to D)\sigma + \varepsilon$ soit plus petit que ε_0, alors, pour s assez grand, le degré cherché est non nul.

Le théorème d'amplitude est donc démontré. Il reste à voir le profit qu'on peut tirer de la forme explicite de $L(-\varepsilon, s)$ pour calculer son degré d'Arakelov en un point de X^m.

3.3. Le degré d'Arakelov de $L(-\varepsilon, s_1, \cdots, s_m)$

Si on a pris soin de prendre L symétrique cubiste et très ample, on sait que le degré d'Arakelov de $L_{|E}$ où E est la section du modèle de Néron de A sur $\mathcal{O}_K$ correspondant à un point rationnel P de A sur K, on a :

il existe une constante C telle que

$$\left| \frac{1}{K : \mathbf{Q}} \deg L_{|E} - \langle P \cdot P \rangle \right| < C$$

où $\langle P \cdot P \rangle$ est le carré scalaire pour l'accouplement de Néron-Tate qui est bilinéaire pour l'addition dans A. De même

$$\left| \frac{1}{K : \mathbf{Q}} \deg P_{1,2|E_1 \times E_2} - 2\langle P_1 \cdot P_2 \rangle \right| < \text{constante}$$

si $P_{1,2}$ est le fibré de Poincaré (*cf.* par exemple [M.B.])

Comme $L(-\varepsilon, s) = \otimes_i L_i^{s_i^2}(1-\varepsilon) \otimes \otimes_i P_{i,i+1}^{\otimes -s_i s_{i+i}}$ si $(x_1, \cdots, x_m) \in X^m$ et si $\left| \|x_i\|^2 - \frac{1}{s_i^2} \right| < \alpha$, α très petit, et si $\langle x_i \cdot x_{i+1} \rangle \geq (1 - \varepsilon/2) \|x_i\| \, \|x_{i+1}\|$, on a

$$\frac{1}{K : \mathbf{Q}} \deg L(-\varepsilon, s_1, \cdots, s_m)^{\otimes d}_{|E_1 \times \cdots \times E_m} \leq$$

$$\sum s_i^2(1-\varepsilon)(\|X_i\|^2 + C)d - s_i s_{i+1}(2\langle X_i \cdot X_{i+1} \rangle - C)d$$

et donc il existe une constante C' telle que

$$\deg L(-\varepsilon, s_1, \cdots, s_m)^{\otimes d}_{|E_1 \times \cdots \times E_m} \leq -d\varepsilon/2\,m + C'(\Sigma\, d s_i^2).$$

4. UNE APPROXIMATION TROP GRANDE

Dans cette partie, nous faisons enfin intervenir l'arithmétique de la situation. Nous commençons par un lemme sur les points d'un réseau n'appartenant pas à un sous-réseau et de "norme contrôlée". Nous utiliserons ce lemme pour trouver une section d'un des fibrés amples de la partie 3 qui soit d'indice petit en un point.

4.1. Un lemme de Siegel revisité

Soit V un espace vectoriel réel de dimension v et M un réseau dans V. On suppose V muni d'une norme notée $\| \ \|$. Si on note B la boule unité de V et λ_i le plus petit λ tel qu'il existe dans M un ensemble de i vecteurs linéairement indépendants de norme au plus λ, Minkowski [Mi] a montré qu'on a :

$$\mathrm{vol}(V/M)\, 2^v/v! \leq \lambda_1 \cdots \lambda_v \ \mathrm{vol}(B) \leq 2^v \,\mathrm{vol}(V/M).$$

On s'intéresse maintenant à borner "les λ_i" du noyau d'une application linéaire. De manière naturelle, l'énoncé précédent de Minkowski implique

Lemme 4.1.— *Soit* $0 \longrightarrow U \longrightarrow V \xrightarrow{\alpha} W$ *une suite exacte d'espaces vectoriels sur* $\mathbf{R}$ *de dimensions respectives* u, v, w. *Soient* M *un réseau de* V *et* N *un réseau de* W. *Supposons que* $\alpha(M)$ *soit contenu dans* N. *Soient, de plus, données des normes sur* V *et* W *et soit* C *un réel supérieur ou égal à deux, tel que* :

a) α *est de norme au plus* C ;

b) M *est engendré par des vecteurs de normes au plus* C ;

c) *tout élément non nul de* M *ou* N *a une norme au moins égale à* C^{-1}.

Alors, munissant U *de la norme induite par celle de* V, *on a* :

$$\lambda_{i+1}(U \cap M, U) \leq (C^{3v} \cdot v!)^{1/v-i}.$$

4.2. Sections de $L(\sigma-\varepsilon, s_1, \cdots, s_m)$ d'indice moins grand que σ en un point

Soit K un corps de nombres, $\mathcal{O}_K$ son anneau d'entiers, $\bar{K}$ une clôture algébrique de K. Soit A un schéma *projectif* sur $\mathcal{O}_K$ dont la fibre est une variété abélienne A_K. Soit X_K une sous-variété irréductible, fermée de A_K telle que $X_{\bar{K}}$ ne contienne aucun translaté d'une sous-variété abélienne de $A_{\bar{K}}$. Soit $X \hookrightarrow A$ un modèle de X_K sur $\mathcal{O}_K$. Choisissons m comme dans le lemme 3.1, L un fibré très ample sur A symétrique sur A_K et un modèle normal B de A_K^m, dominant A^m tel que les fibrés de Poincaré $P_{i,j,K}$ s'étendent en des fibrés en droites $P_{i,j}$ sur B. On appellera Y la fermeture de X^m dans B. Le théorème technique suivant permet de trouver des sections d'indice au plus σ, "holomorphes" sur Y, pour les fibrés amples considérés en 3.2. On veut de plus connaître la "grandeur" d'une telle section. Pour ceci, on munit l'espace des sections holomorphes $\mathbf{C} \otimes H^0(X_K, L(-\varepsilon, s_1 \cdots s_m))$ de la norme sup déduite des métriques à courbure invariante par translation qu'on peut naturellement mettre sur les L_i et les P_{ij} (*cf.* par exemple l'exposé de L. Moret-Bailly [M-B]).

THÉORÈME 4.2.— *Avec les notations ci-dessus introduites, soit $(x_1, \cdots, x_m)$ un point lisse de X_K^m et soient $0 < \sigma < \varepsilon < \varepsilon_0$ des réels et soient s_i/s_{i+1} des quotients assez grands comme dans le théorème* 3.2. *Alors, pour d suffisamment grand, on peut trouver un élément de $H^0(Y, L(\sigma-\varepsilon, s_1, \cdots, s_m)^{\otimes d})$ d'indice strictement plus petit que σ dont la norme aux places à l'infini est bornée par $\exp(C \sum_i d s_i^2)$ (où C est une constante ne dépendant que de σ et ε).*

Pour montrer ce théorème, établissons d'abord une situation comparable à celle du lemme 4.1. La suite exacte sera celle déduite d'un "complexe de Koszul" :

$$0 \longrightarrow \Gamma(X_K^m, L(-\varepsilon, s_1, \cdots, s_m)^{\otimes d}) \longrightarrow \Gamma(X_K^m, \bigotimes_i L_i^{\otimes 4ds_i^2})^n \longrightarrow \Gamma(X_K^m, \bigotimes_i L_i^{\otimes 12ds_i^2})^{n(n-1)/2}.$$

Pour "voir" la première application, notons qu'en partant des sections de L (très ample), on met en évidence des injections de $L(-\varepsilon, s_1, \cdots, s_m)$ dans

$\otimes_i L_i^{\otimes 4ds_i^2}$ sans zéro commun.

Quitte à envoyer encore $L(-\varepsilon, s_1, \cdots, s_m)^{\otimes d}$ dans $\otimes L_i^{\otimes 4ds_i^2}$, les trois premiers termes du "complexe de Koszul"

$$0 \longrightarrow L(-\varepsilon, \mathbf{s})^{\otimes d} \longrightarrow \mathcal{O}_{X_k}^n \otimes \bigotimes_i L_i^{\otimes 4ds_i^2} \longrightarrow \left(\overset{2}{\Lambda} \mathcal{O}_{X_k}^n\right) \otimes \bigotimes_i L_i^{\otimes 8ds_i^2} \otimes L(-\varepsilon, s)^{\otimes -d}$$

donnent la suite exacte annoncée.

On a envie de prendre les sections sur Y des "mêmes" faisceaux comme réseaux formant une suite exacte (pour pouvoir appliquer le lemme de Siegel). En fait, on montre qu'il existe une constante C ne dépendant que de ε telle que :

a) *la suite* $O \to \Gamma(Y, L(-\varepsilon, \mathbf{s})^{\otimes d}) \to \Gamma(Y, \otimes L_i^{\otimes 4ds_i^2}) \to \Gamma(Y, \otimes L_i^{\otimes 12ds_i^2})$ *est un complexe à cohomologie de torsion annulé par* $\exp(C \Sigma d s_i^2)$.

On démontre ensuite l'existence d'une constante C ne dépendant que de σ et ε telle que :

b) *l'injection* $\Gamma(Y, L(-\varepsilon, \mathbf{s})^{\otimes d}) \to \Gamma(Y, \otimes_i L_i^{\otimes 4ds_i^2})^n$ *est de norme bornée par* $\exp(C \Sigma d s_i^2)$.

(chacun de ces deux réseaux est muni de normes sup).

Des généralités sur les métriques sur les fibrés en droites et les normes sup sur leurs sections permettent alors d'établir :

c) *Il existe une constante* C *ne dépendant que de* σ *et* ε *telle que les normes des éléments de* $\Gamma(Y, \otimes_i L_i^{\otimes 4ds_i^2})$ *et de* $\Gamma(Y, \otimes_i L_i^{\otimes 12ds_i^2})$ *sont bornés inférieurement par* $\exp(C \Sigma d s_i^2)$.

L'anneau multigradué $\oplus_{\mathbf{n}} \Gamma(Y, \otimes_i L_i^{\otimes n_i})$ étant de type fini sur l'anneau des polynômes multigradué $\oplus_{\mathbf{n}} \Gamma((\mathbf{P}^n)^m, \otimes \mathcal{O}_{\mathbf{P}}(n_i))$, on a :

d) *Il existe une constante* C *telle que* $\Gamma(Y, \otimes_i L_i^{\otimes 4ds_i^2})$ *est engendré par des éléments de norme au plus* $\exp(C \Sigma d s_i^2)$.

Notons que la dimension de $\Gamma(X_K^m, L(-\varepsilon, s)^{\otimes d})$ est un $O(\prod_i (ds_i^2)^{\dim X_K})$. Pour montrer le théorème 4.2, on veut calculer l'ordre de grandeur de la codimension de l'espace des sections de $L(\sigma - \varepsilon, \mathbf{s})$ ayant un index supérieur ou égal à σ en $(x_1, \cdots, x_m)$, dans $\Gamma(X_K^m, L(-\varepsilon, \mathbf{s}))$. Comme le faisceau $L(-\varepsilon, \mathbf{s})$ est ample pour $\varepsilon < \varepsilon_0$ et s_i/s_{i+1} assez grand (théorème 3.2),

on voit que cette codimension est bornée inférieurement par un multiple positif de $\prod_i (ds_i^2)^{\dim X_K}$. (Compter le nombre de conditions imposées par "index $\geq \sigma$".) Le lemme 4.1 montre qu'asymptotiquement, il existe dans $\Gamma(Y, L(-\varepsilon, \mathbf{s})^{\otimes d})$ un sous-espace de dimension un de plus que l'espace cité plus haut engendré par des éléments de norme au plus $\exp(C \Sigma d s_i^2)$. On en déduit le théorème 4.2.

4.3. Degré d'Arakelov et index

Nous montrons enfin dans ce paragraphe le théorème 1. Nous prenons un entier m comme dans 3.1 et, pour tout $i = 1, \cdots m$, choisissons une projection

$$X_K \xrightarrow{\pi_i} \mathbf{P}^{\dim X} = P_i.$$

Pour chaque i, il existe une hypersurface Z_i d'équation G_i dans P_i, telle que G_i annule Ω^1_{X/P_i}. De cette façon, si D est un opérateur différentiel sur P_i, $G_i D$ est un opérateur différentiel sur X. En raisonnant par récurrence sur $\dim X$, on peut supposer qu'on a une infinité de points de $X_K(K)$ non dans $\pi_i^{-1}(Z_i)$ pour tout i. Par le théorème de Mordell-Weil, $A_K(K) \otimes_{\mathbf{Z}} \mathbf{R}$ est un espace vectoriel de dimension finie. Cet espace vectoriel est muni d'un accouplement "de Néron-Tate" qui est non dégénéré noté $\langle\ ,\ \rangle$. On sait que la hauteur d'un point définie à partir d'un fibré très ample symétrique L sur A ne diffère de son "carré scalaire pour Néron-Tate" que par une constante (*cf.* par exemple [Ma]). Si on a une infinité de points rationnels sur K dans l'intersection des $X_K - \pi^{-1}(Z_i)$, on peut, choisissant s et ε comme dans le théorème 3.2, trouver dans cette intersection m points $x_1, \cdots, x_m$ de hauteurs $h_1, \cdots, h_m$ tels que :

i) h_1 est très grand ;

ii) $h_{i+1}/h_i > s^2$;

iii) $\langle x_i \cdot x_{i+1} \rangle \geq (1 - \varepsilon/2) \|x_i\| \ \|x_{i+1}\|$.

En choisissant des rationnels s_i très proches de $h_i^{-1/2}$, on voit que $L(\sigma - \varepsilon, s_1, \cdots, s_m)^{\otimes d}$ a un degré d'Arakelov sur la section de Y correspondant au point $x_1, \cdots, x_m$ borné supérieurement par

$$(*) \qquad d((\sigma - \varepsilon/2)m + (\text{constante}) \cdot (\Sigma d s_i^2)$$

(même calcul qu'en 3.3.). D'autre part, par définition du degré d'Arakelov, la section du faisceau métrisé $L(\sigma-\varepsilon, s_1, \cdots, s_m)^{\otimes d}$ trouvée au théorème 4.2 donne si elle est non nulle en $\mathbf{x}$, une borne inférieure : $-$(constante) $\cdot$ $(\Sigma\, d\, s_i^2)$. Prenant au départ $\sigma = \varepsilon/4$, par exemple, on en déduit que la section due au théorème 4.2 est nulle en $\mathbf{x}$. C'est cet argument appliqué aux "dérivées" de la section qui permettra de montrer que son index est trop petit. Quitte à prendre ses précautions en chassant les dénominateurs, on voit que si $D = D_1 \cdots D_m$, D_i opérateur différentiel sur P_i tel que $\sum \frac{\deg D_i}{4ds_i^2} \leq i(x, f)$ (f section de $L(\sigma-\varepsilon, \mathbf{s})^{\otimes d}$ trouvée en 4.2)

$$\prod N(G_i)^{\deg D_i} \cdot \prod \frac{D_i}{\left(\prod_j \alpha_{i,j}!\right)}(f)$$

est "entier" en $(x_1, \cdots, x_m)$ par la formule de Taylor (où $D_i = \prod \frac{\partial^{\alpha_{i,j}}}{\partial X_j^{\alpha_{i,j}}}$ sur P_i).

On obtient ainsi une section de

$$L(\sigma-\varepsilon, s_1, \cdots, s_m)^{\otimes d} \otimes \bigotimes_i L_i^{\deg D_i \deg G_i}.$$

Nous établissons plus bas une borne supérieure pour la norme de cette section en chaque place à l'infini. Mais notons déjà que la section ainsi obtenue, si on choisit bien D, ne s'annule pas en $x_1 \cdots x_m$, et que le degré d'Arakelov de ce faisceau restreint à la section correspondant à $(x_1 \cdots x_m)$ est borné supérieurement par $d(C_1\sigma - \varepsilon/2)m + C_2 \cdot (\Sigma\, d\, s_i^2)$ (C_1 et C_2 constantes). Donc si on arrive à montrer que la norme aux places à l'infini de cette section est au plus $C_3(\Sigma\, d\, s_i^2)$, C_3 ne dépendant (comme C_2) que de σ et ε, et si on a pris soin de choisir $C_1\sigma \leq \varepsilon/4$, on aura une contradiction et le théorème 1 sera prouvé.

Il nous reste donc à majorer les "dérivées" d'une section de $L(\sigma - \varepsilon, \mathbf{s})$. La formule de Cauchy permet de borner $\frac{1}{a!}\frac{\partial^a}{\partial X^a}(f)$ par $\frac{1}{r^a}$ sup $|f|$ sur le disque de rayon r. Prenant autour du point X_i une boule de rayon $|G_i(x_i)| = r_i$ ou plus, on voit qu'on a une borne de la forme $\|f\|\, C^{ds_1^2+\cdots ds_m^2}$ $\prod_i r_i^{-\deg D_i}$, C constante, pour $D_1 \cdots D_m(f)$. Remarquons qu'on a deg $D_i \leq 4\sigma\, ds_i^2$. On obtient ainsi la borne $C_3(\Sigma\, d\, s_i^2)$ pour $\|D_1 \cdots D_m(f)\|$.

5. AUTRES RÉSULTATS

S. Lang a, de manière bien naturelle, demandé si l'hypothèse X fermée dans A variété abélienne était nécessaire (en supposant que X ne rencontre pas de translaté de sous-variété abélienne). À ma connaissance, on ne sait pas la réponse à cette question. G. Faltings a cependant, en poussant les méthodes exposées ici, réussi à montrer la conjecture de S. Lang suivante : Soit A une variété abélienne, H un diviseur ample sur A. Alors, $A - H$ ne contient qu'un nombre fini de points entiers.

Les résultats exposés ici ne sont pas effectifs, *i.e.* on n'a pas de borne explicite pour la hauteur des points considérés. On consultera avec profit un séminaire à paraître incessamment dans la revue Astérisque sur le sujet de l'effectivité.

On vient de me communiquer un manuscrit de E. Bombieri reprenant, en dimension un au moins, les arguments de P. Vojta dans un vocabulaire et une technique plus proches des œuvres de Siegel.

BIBLIOGRAPHIE

[A] S.J. ARAKELOV - *Intersection theory on arithmetic surfaces*, Math USSR Izvestia, vol. 8 (1974), n° 6, 1167-1180.

[F1] G. FALTINGS - *Endlichkeitssätze für Abelsche Varietäten über Zahlkörpern*, Inv. Math. Vol. 73, Fasc. 3 (1983), 349-366.

[F2] G. FALTINGS - *Diophantine approximation on Abelian varieties*, prépublication, 1989-1990.

[H] M. HINDRY - *Autour d'une conjecture de Lang*, Inv. Math. Vol. 94 (1988), 575-603.

[K] S.L. KLEIMAN - *Towards a numerical theory of ampleness*, Annals of Maths 84 (1966), 293-344.

[Ma] Y.I. MANIN - *Mordell-Weil theorem*, appendix II dans D. Mumford "Abelian varieties", Oxford University Press, 1970.

[Mi] H. MINKOWSKI - *Geometrie der Zahlen*, New York, Chelsea, 1953.

[M-B] L. MORET-BAILLY - *Métriques permises*, dans "Séminaire sur les

pinceaux arithmétiques : la conjecture de Mordell", Astérisque 127 (1985).

[V] P. VOJTA - *An extension of the Thue-Siegel-Dyson-Gel'fand theorem*, prépublication, 1989.

Lucien SZPIRO

CNRS URA 213
Institut Henri Poincaré
11 rue Pierre et Marie Curie
F-75005 PARIS