Université de Paris VI 2e semestre 2001-2002

Cours spécialisés du DEA "Méthodes algébriques"

MÉTHODES ARITHMÉTIQUES

pour les groupes algébriques et les équations différentielles.

Daniel BERTRAND

Plan

Sommaire

Comment reconnaître qu'une équation différentielle n'admet que des solutions algébriques ? qu'un sous-groupe analytique d'un groupe algébrique est en fait algébrique ? Ce cours passe en revue quelques solutions apportées par la théorie des nombres à ces questions. Une méthode de transcendance, introduite par G. et D. Chudnovsky et développée par Y. André et J-B. Bost, y joue un rôle clef.

CHAPITRE I

LE THÉORÈME DE KRONECKER

Il s'agit de l'énoncé suivant, où 'presque tout' signifie 'tout, à un nombre fini d'exceptions près'.

Théorème 0: *soient α un nombre algébrique, et K le corps $\mathbf{Q}(\alpha)$. On suppose que pour presque toute place finie v de K, il existe un entier rationnel a_v tel que $v(\alpha - a_v) > 0$. Alors, $\alpha \in \mathbf{Q}$.*

Nous allons en donner trois approches: par la théorie algébrique des nombres, par les équations différentielles, et par les groupes algébriques. Chacune correspond à une nouvelle formulation de l'énoncé, à l'origine des généralisations étudiées dans la suite du cours.

§1. Le théorème de Chebotarev

Pour tout corps de nombres K, on note $\mathcal{O}_K$ l'anneau des entiers de K, D_K son discriminant, M_K l'ensemble des places de K, M'_K l'ensemble des places finies; pour $v \in M'_K$, qu'on peut identifier à un idéal premier $\mathbf{p}_v$ (noté $\mathbf{p}$, quand le contexte est clair) de $\mathcal{O}_K$, on note $K(v)$ le corps résiduel, $N(v) = p^{f_v}$ son cardinal, K_v le complété de K en v, et $\mathcal{O}_v$ l'anneau des entiers de K_v.

Soient L/K une extension *galoisienne* finie, de groupe de Galois $G = Gal(L/K)$, et v un place finie de K ne divisant pas D_L. Toutes les places w de L au-dessus de v ont même degré résiduel $f_{w/v} = f_w/f_v$, et les groupes de décomposition $D_{w/v} = \{g \in G, g(\mathbf{p}_w) = \mathbf{p}_w\} \simeq Gal(L_w/K_v)$ sont conjugués dans G. Comme v est non ramifiée, le groupe d'inertie $I_{w/v} = \{g \in D_{w/v}, \forall x \in \mathcal{O}_w, w(g(x) - x) \geq 1\}$ est nul, et $D_{w/v}$ s'identifie à $Gal(L(w)/K(v))$. Il admet donc un générateur canonique $F_{w/v} := (\mathbf{p}_w, L/K)$, le *Frobenius en w*, défini par la condition $\forall x \in \mathcal{O}_K, F_{w/v}(x) - x^{N(v)} \in \mathbf{p}_w$, et dont la classe de conjugaison F_v dans G ne dépend que de v. On omet parfois l'un des deux indices v (par exemple quand $K = \mathbf{Q}$) ou w (par exemple quand L/K est abélienne).

Théorème 1 (Chebotarev): *Soit L/K une extension galoisienne finie, de groupe de Galois G, et soit C une partie de G stable par conjugaison. Alors,*

$$lim_{x \to +\infty} \frac{card\{v \in M'_K, v(D_L) = 0, N(v) \leq x, F_v \in C\}}{card\{v \in M'_K, N(v) \leq x\}} = \frac{card(C)}{card(G)}.$$

Démonstration: voir les livres de Serre (*Abelian ℓ-adic representations*), Lang (*Algebraic Number Th.*), Cassels-Fröhlich, Fried-Jarden, Neukirch. Le dénominateur de l'expression dont on prend la limite croît comme $x/Log(x)$. Dans le cas où $K = \mathbf{Q}, L = \mathbf{Q}(e^{2i\pi/m})$, on retrouve le théorème de Dirichlet: pour tout entier c premier à m, l'ensemble des nombres premiers $p \equiv c \bmod m$ est infini (et a pour densité $\frac{1}{\phi(m)}$).

Soient L/K une extension finie, R un ensemble fini (ou plus généralement, de densité nulle) de places de K, contenant les places ramifiées, et $S(L/K, R)$ l'ensemble des places $v \in M_K, v \notin R$ qui se décomposent totalement dans K. Si L/K est galoisienne, cette condition s'écrit: $F_{w/v} = id$, et $S(L/K, R)$ admet une densité, égale à $\frac{1}{[L:K]}$. Le théorème 0 découle du:

Corollaire 1: *soient $f \in \mathbf{Z}[X]$ un polynôme. On suppose que pour presque tout nombre premier p, le polynôme déduit de f par réduction modulo p se décompose en facteurs linéaires dans $\mathbf{F}_p$. Alors, f se décompose en facteurs linéaires dans $\mathbf{Q}$.*

Démonstration: soient L le corps de décomposition de f et R l'ensemble fini des nombres premiers divisant le discriminant de f ou son terme dominant, ou ne vérifiant pas l'hypothèse de l'énoncé. Pour $p \notin R$, f se décompose en facteurs linéaires dans $\mathbf{Q}_p$ (lemme de Hensel), de sorte que $L_{\mathbf{p}} = \mathbf{Q}_p$ pour tout idéal $\mathbf{p}$ de $\mathcal{O}_L$ divisant p. Ainsi, $S(L/K, R)$ est le complémentaire de l'ensemble fini R. Il a pour densité 1 , de sorte que $[L : K] = 1$.

Corollaire 2: *soient $f \in \mathbf{Z}[X]$ un polynôme* irréductible. *On suppose que pour presque tout nombre premier p, le polynôme déduit de f par réduction modulo p admet une racine dans $\mathbf{F}_p$. Alors, f admet une racine dans $\mathbf{Q}$ (et est donc linéaire) .*

Démonstration: soient L le corps de décomposition de f, et α une racine de f dans L. Posons $M = K(\alpha), G = Gal(L/K), H = Gal(L/M)$. Par hypothèse, il existe, pour tout nombre premier v hors d'un ensemble fini R, au moins une place u de M divisant v telle que $f_{u/v} = 1$, donc au moins une place w de L au-dessus de v telle que le sous-groupe $D_{w/v}$ de G fixe M, i.e. telle que $F_{w/v} \in H$. Pour ces places v, F_v appartient donc à la reunion C des classes de conjugaison des éléments de H, et leur densité ne peut valoir 1 que si $C = G$. Cela impose que H lui-même remplisse G.

Remarque 1: le corollaire 2 ne s'étend pas aux polynômes réductibles. Contre-exemples: $f(T) = T^8 - 16$, qui a une racine modulo n'importe quel nombre premier; de même pour $f(T) = (T^2 - a)(T^2 - b)(T^2 - c)$, où a, b, c sont trois entiers non carrés dont le produit abc est un carré.

§2. La conjecture de Grothendieck

Soit L un opérateur différentiel d'ordre n à coefficients dans $\mathbf{Q}(z)$. Pour tout nombre premier p suffisamment grand, on déduit de L, par réduction modulo p, un opérateur différentiel L_p à coefficients dans $\mathbf{F}_p(z)$. L'argument usuel du wronskien montre que l'équation différentielle $L_p(y) = 0$ a dans $\mathbf{F}_p(z)$ au plus n solutions linéairement indépendantes sur le corps des constantes $(\mathbf{F}_p(z))^p = \mathbf{F}_p(z^p)$ de $\mathbf{F}_p(z)$.

Conjecture (Grothendieck): *soit $L \in \mathbf{Q}(z)[d/dz]$ un opérateur différentiel d'ordre n. Les conditions suivantes sont équivalentes:*

i) l'équation différentielle $Ly = 0$ admet n solutions linéairement indépendantes sur $\overline{\mathbf{Q}}$, formées de fonctions algébriques sur $\mathbf{Q}(z)$;

ii) pour presque tout nombre premier p, l'équation différentielle $L_p y = 0$ admet dans $\mathbf{F}_p(z)$ n solutions linéairement indépendantes sur $\mathbf{F}_p(z^p)$.

L'implication i) $\Rightarrow$ ii), de nature élémentaire, se déduit du théorème d'Eisenstein ci-dessous. La conjecture ii) $\Rightarrow$ i) sera étudiée au chap. 3, mais nous allons voir dès maintenant que pour $n = 1$, elle équivaut au théorème de Kronecker.

Proposition 1 (Théorème d'Eisenstein). *Soit $f \in \mathbf{Q}[[z]]$ une série formelle à coefficients rationnels. Si f est algébrique sur $\mathbf{Q}(z)$, elle est globalement bornée.*
[Une série formelle $f(z) = \Sigma_{n\geq 0}\ a_n z^n \in \mathbf{Q}[[z]]$ est dite globalement bornée s'il existe deux entiers non nuls D_0, D tel que $D_0 f(Dz)$ soit une série convergente à coefficients entiers, autrement dit si pour toute place $v \in M_{\mathbf{Q}}$, le rayon de convergence v-adique $R_v(f)$ de $f \in \mathbf{Q}_v[[z]]$ est non nul, tandis que $f \in \mathbf{Z}_v[[z]]$ pour presque toute place $v \in M'_{\mathbf{Q}}$.]

Démonstration: puisque leurs coefficients sont des suites récurrentes linéaires, l'énoncé est clairement satisfait par les élements de $\mathbf{Q}(z)$. Il suffit donc de le vérifier sur n'importe quel générateur $g(z) = \Sigma_{n\geq 0}\ b_n z^n \in \mathbf{Q}[[z]]$ du corps de fonctions $\mathcal{K} = \mathbf{Q}(z)[f]$.

Soit C une courbe algébrique propre et lisse sur $\mathbf{Q}$ de corps de fonction $\mathcal{K}$. Sa fibre F_0 au dessus de $z = 0$ admet un point $\mathbf{Q}$-rationnel P_0 (correspondant au germe donné par la série f), et on déduit de Riemann-Roch l'existence d'un élément g de $\mathcal{K}$ de même degré que f, fini et non nul en P_0, tel que tous les points de F_0 distincts de P_0 soient des pôles de g. Alors, g vérifie une relation de dépendance algébrique sur $\mathbf{Q}(z)$ de la forme: $p_0(z)g(z)^m + ... + p_{m-1}(z)g(z) + p_m(z) = 0$, où les $p_i(z)$ sont des polynômes à coefficients dans $\mathbf{Q}$, qui s'annulent en 0 pour $i \leq m-2$, mais tels que $p_{m-1}(0) := D \neq 0$. Sans perte de généralité, on peut de plus supposer que $g(P_0) = b_0 \in \mathbf{Z}$, et $p_i \in \mathbf{Z}[z]$ pour tout i.

Il reste à vérifier que le développement en série $g(z) = \Sigma_{n\geq 0}\ b_n z^n \in \mathbf{Q}[[z]] \cap \mathcal{K}$ de g au voisinage de P_0 est globalement borné. Mais $Db_0 + p_m(0) = 0$, donc D divise $p_m(0)$,

et pour tout $i = 0, ..., m$, le polynôme $q_i(z) := \frac{1}{D} p_i(Dz) \in \mathbf{Z}[z]$, avec $q_{m-1}(0) = 1$. De la relation $-g(Dz) = \frac{q_m(z)}{q_{m-1}(z)} + \frac{q_{m-2}(z)}{q_{m-1}(z)} g(Dz)^2 + ... + \frac{q_0(z)}{q_{m-1}(z)} g(Dz)^m$, on déduit par récurrence que $D^n b_n \in \mathbf{Z}$ pour tout $n \geq 0$.

Proposition 2 (Grothendieck-Katz, repris par Honda) *Soit $R(z) \in \mathbf{Q}(z)$ telle que pour presque tout nombre premier p, l'équation différentielle $y' - R_p(z)y = 0$ obtenue en réduisant R modulo p admette une solution non nulle $y_p \in \mathbf{F}_p(z)$. Alors, l'équation différentielle $y' - R(z)y = 0$ admet une solution non nulle algébrique sur $\mathbf{Q}(z)$.*

Démonstration: pour p assez grand, tous les pôles de $R_p = \frac{y_p'}{y_p}$ sont simples, à résidus dans $\mathbf{Z}$. On en déduit d'abord que $R(z)$ s'écrit sous la forme $\Sigma_{j \in J} \frac{\epsilon_j}{z - \beta_j}$, où $L = \mathbf{Q}(\beta_j, \epsilon_j ; j \in J)$ est une extension galoisienne de $\mathbf{Q}$. Par ailleurs, pour presque toute place w de L, de caratéristique résiduelle p, les pôles β_j sont dans des classes résiduelles distinctes, et chaque résidu ϵ_j se réduit modulo w en le résidu correspondant de R_p. D'après le Théorème 0, ils sont donc bien tous rationnels. (Inversément, il est facile de déduire le Théorème 0 de la Proposition 2.)

Remarque 2: la proposition 2 énonce que si une différentielle $\xi = R(z)dz$ du corps de fonctions $\mathbf{Q}(z)$ est logarithmiquement exacte modulo presque tout nombre premier p, alors, un de ses multiples entiers non nuls $N\xi$ est logarithmiquement exacte (prendre $N = ppcm(den(\epsilon_j))$. On verra au chap. 2 les extensions qu'en ont données Chudnovsky et André aux corps de fonctions sur les courbes algébriques de genre > 0.

Remarque 3: pour $L \in \mathbf{Q}(z)[d/dz]$, soit S l'ensemble des singularités de L, Γ l'image de $\pi_1(\mathbf{P}_1(\mathbf{C}) \backslash S); x_0)$ par la représentation de mononodromie attachée à L, et pour tout $s \in S$, γ_s l'image du générateur standard du sous-groupe d'inertie en s, de sorte que Γ est engendré par les $\gamma_s, s \in S$. Le même argument que supra montre que si L vérifie la condition ii), les valeurs propres de γ_s sont toutes des racines de l'unité (du type $exp(2i\pi\epsilon_j)$); Katz (Nilpotent connections..., IHES 1970) montre de plus que l'ordre de nilpotence de γ_s est nul. Donc γ_s est d'ordre fini, et la conjecture est vérifiée dès que Γ est un groupe abélien. Idem pour la conjecture plus générale proposée par Katz sur le groupe de Galois différentiel de L, cf. chap. 3.

Remarque 4: revenons au sens facile i) $\Rightarrow$ ii). Dans le cas des séries entières solutions d'une équation d'ordre 1, le théorème d'Eisenstein revient à l'énoncé bien connu suivant: soit $f(z) = (1+z)^\alpha = \Sigma_{n \geq 0} \binom{\alpha}{n} z^n$, qui est algébrique si (et slt si) α est un nombre rationnel, et soit dans ce cas D son dénominateur; *pour tout nombre premier p ne divisant pas D, et tout entier $n \geq 0$, le nombre rationnel $\binom{\alpha}{n}$ est p-entier.*

La condition ii) de la conjecture de Grothendieck n'entraîne pas, *a priori*, que les séries formelles $f \in \mathbf{Q}[[z]]$ solutions de $Lf = 0$ soient globalement bornées, ni même que leurs rayons de convergence p-adiques $R_p(f)$ soient égaux à 1 pour p assez grand, mais seulement que le produit $\Pi_{v \in M_{\mathbf{Q}}} R_v(f)$ soit convergent(cf. chap. III, §2). Le Théorème 3 du § suivant donne néanmoins la clef de la preuve 'transcendante' de la Proposition 2 (et donc du Théorème 0) obtenue par Chudnovsky.

§3. La méthode de Chudnovsky pour le théorème d'isogénie.

Cette méthode a été considérablement généralisée par les travaux d'Y. André, puis de J-B. Bost (voir aussi A. Chambert-Loir; réf. en fin du chap. IV). Dans sa version la plus simple, elle énonce:

Théorème 2 (Chudnovsky, repris par M. Laurent) *Soient f et g deux éléments de $\mathbf{Q}[[z]]$, globalement bornés. On suppose qu'il existe un série localement convergente $\phi \in z\mathbf{C}[[z]]$, $\phi'(0) \neq 0$, telle que les séries $f \circ \phi, g \circ \phi$ soient les développement de Taylor de fonctions méromorphes sur $\mathbf{C}$, d'ordre fini. Alors, f et g sont algébriquement dépendantes sur $\mathbf{Q}$.*

Démonstration: on se ramène immédiatement au cas où $f, g \in \mathbf{Z}[[z]]$ et $\phi'(0) = 1$. On désigne par N un entier, par θ une fonction entière non nulle d'ordre fini telle que $\theta.f(\phi), \theta.g(\phi)$ le soient aussi, et que $\theta(0) = 1$, et par c_i des 'constantes' ne dépendent que de f, g, ϕ, θ.

Pour $N \geq c_1$, le principe des tiroirs fournit un polynôme non nul $P_N \in \mathbf{Z}[X, Y]$ de degré $\leq N$, de coefficients majorés en valeur absolue par $exp(c_2 N^{3/2})$, tel que la série $P_N(f, g)$ soit de valuation z-adique $\geq N^{3/2}$.

Supposons $P_N(f, g)$ non identiquement nulle, et soit $M \geq N^{3/2}$ sa valuation. La fonction $F_N(z) = (\frac{1}{z})^M \theta(z)^N P_N(f(\phi(z)), g(\phi(z)))$ prend donc en 0 une valeur $\frac{F_N^{(M)}(0)}{M!}$ *entière et non nulle.*

Or c'est une fonction entière d'ordre fini, disons $\rho = c_3$. En lui appliquant le principe du maximum sur le disque $|z| \leq (M/N)^{1/\rho}$, on obtient: $|\frac{F_N^{(M)}(0)}{M!}| \leq c_4^M N^{-M/2\rho}$. Pour $N > c_4^{2\rho}$, cela contredit la conclusion précédente, et l'on obtient la relation de dépendance algébrique $P_N(f, g) \equiv 0$ recherchée.

Remarque 5: on abrège l'hypothèse faite au Théorème 2 sur l'existence de ϕ en disant que f et g sont *simultanément uniformisables* sur $\mathbf{C}$ par des fonctions d'ordre fini. Il est facile de l'étendre au cas d'un corps de nombres K, en imposant l'existence d'uniformisations simultanées ϕ_v pour toute place archimédienne v de K, i.e. pour tout plongement σ de K dans $\mathbf{C}$ (une place suffirait, d'ailleurs). Pour $\alpha \in K$, les séries $f(t) = \Sigma_{n \geq 0} \binom{\alpha}{n} t^n$ et

$g(t) = 1 + t$ vérifient cette hypothèse: prendre $\phi_\sigma(z) = e^z - 1$, de sorte que $\sigma(f) \circ \phi_\sigma(z) = e^{\sigma(\alpha)z}$, $\sigma(g) \circ \phi_\sigma(z) = e^z$. Si α vérifie l'hypothèse du théorème 0, $\binom{\alpha}{n}$ est v-entier pour presque tout $v \in M'_K$; f et g sont donc globalement bornées, et le thm. 2 entraîne bien le thm. 0. Pour des généralisations *adéliques* du Théorème 2, voir [A'], et le chap. II.

Les théorèmes d'isogénie

Contrairement à celle de Faltings, les preuves qui suivent ne font *pas* appel au théorème de Chebotarev.

Corollaire 3 (Chudnovsky) : *Soient E et E' deux courbes elliptiques définies sur $\mathbf{Q}$. On suppose que pour presque tout nombre premier p, les courbes elliptiques sur $\mathbf{F}_p$ déduites de E, E' par réduction modulo p ont le même nombre de points $\mathbf{F}_p$-rationnels. Alors, E et E' sont isogènes sur $\mathbf{Q}$.*

Démonstration: selon un théorème de Cartier-Hill-Honda, l'hypothèse entraîne l'existence d'un isomophisme entre les groupes formels de E et E' sur $\mathbf{Z}$, décrit en terme d'un paramètre formel t sur E par une série $f(t) \in \mathbf{Z}[[t]]$. On applique alors le Théorème 2 aux séries $f(t), g(t) = t$, et $\phi(z) = exp_E(z)$: les séries composées s'étendent en des fonctions elliptiques, donc méromorphes d'ordre 2.

Les théorèmes de Bost [B] (voir chap. IV) sur la méthode de Chudnovsky permettent d'éviter le recours au théorème de Cartier et al. dans cette preuve. Ainsi:

Théorème 3 (J-B. Bost): *Soit G un groupe algébrique défini sur un corps de nombres K, d'algèbre de Lie $\mathbf{g}$, et $\mathbf{h}$ une sous-algèbre de Lie de $\mathbf{g}$, définie sur K. Les conditions suivantes sont équivalentes:*

i) $\mathbf{h}$ est l'algèbre de Lie d'un K-sous-groupe algébrique H de G;

ii) pour presque tout nombre premier p, et toute place v de K divisant p, la réduction de $\mathbf{h}$ modulo v est une p-sous-algèbre de Lie de la p-algèbre de Lie sur $K(v)$ déduite de $\mathbf{g}$ par réduction modulo v.

Outre le corollaire 3 (voir le chap. II, §1), et bien plus, ce théorème fournit une nouvelle démonstration du théorème de Kronecker : pour $G = \mathbf{G}_m \times \mathbf{G}_m$, la réduction modulo v de la K-sous algèbre de Lie $\mathbf{h}$ de $\mathbf{g}/K \simeq K \oplus K$ d'équation $y = \alpha x$ est p-restreinte ssi $v(\alpha^p - \alpha) > 0$, i.e. ssi α vérifie l'hypothèse du Théorème 0, tandis que $\mathbf{h}$ est une sous-algèbre de Lie algébrique ssi α est un nombre rationnel.

Remarque 6: le théorème de Chebotarev admet des versions effectives; voir Serre, Oeuvres, III, p. 571. Il en est de même des théorèmes de Chudnovky. Mais les estimations sont de natures différentes: discriminants et conducteurs d'un côté, hauteurs de l'autre.

CHAPITRE II

LE THÉORÈME DE CHUDNOVSKY-ANDRÉ

Il s'agit de l'énoncé suivant, où on reprend les notations de I, §1 (sur un corps de nombres noté maintenant k), et où 'courbe algébrique' sur k signifie courbe algébrique propre lisse et géométri-quement irréductible, définie sur k. Pour toute place v de k de norme assez grande, on note X_v la réduction de X modulo v.

Théorème 0: *soient k un corps de nombres, X une courbe algébrique sur k, et ξ une forme différentielle sur X, définie sur k. On suppose que pour presque toute place v de K, la forme différentielle ξ_v sur X_v déduite de ξ par réduction modulo v vérifie*

i) (Chudnovsky) *ξ_v est logarithmiquement exacte. Alors, il existe un entier rationnel $N \neq 0$ tel que $N\xi$ soit logarithmiquement exacte.*

ii) (André) *ξ_v est exacte. Alors, ξ est exacte.*

§1. Formes différentielles sur les courbes algébriques.

On suppose ici que k est un corps *algébriquement clos*, de caractéristique p, nulle on non. Soit $K = k(X)$ le corps de fonctions rationnelles sur la courbe algébrique X/k. Pour toute k-algèbre A, on note $\Omega_{A/k}$ le A-module des différentielles de Kähler sur k, et $dA = \{df, f \in A\}$ le k-ss-ev formé par les formes exactes. Par exemple, le K-ev $\Omega_{K/k}$ des formes différentielles rationnelles sur X est de dimension 1 sur K, engendré par dx où x est un élément séparant quelconque de K. Pour tout point P de $X(k)$, d'anneau local $\mathcal{O}_P$ et de paramètre local t_P, le $\mathcal{O}_P$-module $\Omega_{\mathcal{O}_P/k}$ est libre de rang 1, engendré par dt_P; le k-ev de dimension 1 $\Omega_{\mathcal{O}_P/k} \otimes_{\mathcal{O}_P} k \simeq (t_P)/(t_P)^2$ admet pour k-dual l'espace tangent $T_P(X)$ de X en P. Les $\Omega_{\mathcal{O}_P/k}$ sont les fibres du faisceau $\Omega_{X/k}$ des germes de formes différentielles régulières sur X, sous-faisceau du faisceau constant $\underline{\Omega}_{K/k}$ (de fibres $\Omega_{\mathcal{O}_P/k} \otimes_{\mathcal{O}_P} K = \Omega_{K/k}$).

Soit ξ une forme différentielle rationnelle sur X. On dit que ξ est logarithmiquement exacte (resp. exacte) s'il existe $f \in K$ telle que $\xi = df/f$ (resp. $\xi = df$). Pour tout point P de X, on note $ord_P(\xi)$ (resp. $res_P(\xi)$) l'ordre (resp. le résidu) de ξ en P, et on définit le diviseur (resp. le diviseur résidu) de ξ par

$$div(\xi) = \Sigma_{P \in X} ord_P(\xi).(P) \ ; \ div.res(\xi) = \Sigma_{P \in X} res_P(\xi).(P).$$

On note $Div(X), Div_0(X), Div_\ell(X)$ les groupes des diviseurs, div. de degré 0, div. lin. éq. à 0, sur X et $Pic(X), Pic_0(X)$ les quotients des premiers par $Div_\ell(X)$. D'après le théorème des résidus, $div.res(\xi) \in Div_\ell(X) \otimes_{\mathbf{Z}} k$ pour toute f. diff. ξ. Les diviseurs des f. diff. sur X définissent la même classe κ dans $Pic(X)$, dite (classe du) diviseur canonique.

Soit $g \geq 1$ le genre de X. On dit que ξ est de *première* espèce si $div(\xi)$ est effectif. Par Riemann-Roch, l'espace $D^1(X) \simeq H^0(X, \Omega_{X/k})$ des f. de première espèce sur X est de dimension g sur k. On dit que ξ est de *deuxième* espèce, et on note $\omega \in D^2(X)$ si $div.res(\xi) = 0$ (i.e., en caractéristique 0, si ξ est localement exacte en tout point). On dit que ξ est de *troisième* espèce si son diviseur polaire est formé de pôles simples, à résidus entiers (i.e. en car. 0, si elle est localement logarithmiquement exacte en tout point).

Le cas classique ($k = \mathbf{C}$).

Soit $H^1_{dR}(X/\mathbf{C}) \simeq D^2(X)/dK$ l'espace des classes de cohomologie de f. diff. rationnelles loc. exactes sur X. La suite exacte de faisceaux $0 \to \underline{\mathbf{C}} \to \underline{K} \xrightarrow{d} \Omega^{loc.exactes}_{K/k} \to 0$ fournit en cohomologie de Čech une suite exacte longue $0 \to dK \to D^2(X) \to H^1(X, \mathbf{C}) \to 0$. Ainsi, $H^1_{dR}(X/\mathbf{C})$ s'identifie au dual de $H_1(X, \mathbf{C})$, et on a 'un accouplement de périodes' non dégénéré

$$H^1_{dR}(X/\mathbf{C}) \times H_1(X, \mathbf{Z}) \to \mathbf{C} : (\xi, \gamma) \mapsto \int_\gamma \xi.$$

$H^1_{dR}(X/\mathbf{C})$ est donc un $\mathbf{C}$-ev. de dimension $2g$, qui contient naturellement $D^1(X)$. L'image Λ de $H_1(X, \mathbf{Z})$ dans le dual $V \simeq H^0(X, T_{X/\mathbf{C}}) \simeq H^1(X, \mathcal{O}_X)$ de $D^1(X) = H^0(X, \Omega_{X/\mathbf{C}})$ est un réseau; mieux, le tore complexe V/Λ est une variété abélienne $Jac(X)$ de dimension g, appelée jacobienne de X. En particulier, toute fonction rationnelle sur $Jac(X)$ s'écrit comme quotient de deux fonctions theta sur V (ce sont des fonctions entières d'ordre 2, vérifiant certaines propriétés de périodicité).

Fixons un point b_0 de X. L'application $f : X \to V/\Lambda : P \mapsto \int_{b_0}^P$ s'étend par linéarité en un homomorphisme $Div_0(X) \to J(X)$; d'après le *théorème d'Abel-Jacobi*, f passe au quotient par $Div_\ell(X)$, et définit un isomorphisme canonique $\Phi : Pic_0(X) \simeq Jac(X)$. Plus précisément, pour tout système non spécial $b = b_1 + ... + b_g$ sur X, l'application $(P_1, ...P_g) \mapsto \Phi((P_1 + ... + P_g - b_1 - ... - b_g))$ définit un isomorphisme birationnel de $Sym^g X = X^g/\mathcal{S}_g$ sur $Jac(X)$, qui induit un isomorphisme local au voisinage de b. En particulier, soient $x \in K$ un paramètre local commun aux points b_j et $\{\xi = f(x)dx = \omega_1,\ \omega_2, ..., \omega_g\}$ une base de $D^1(X)$. Alors, $\sigma_1(P_1, ..., P_g) = x(P_1) + ... + x(P_g), ..., \sigma_g(P_1, ..., P_g) = x(P_1)...x(P_g)$ sont des fonctions rationnelles sur $Sym^g(X)$, et le germe de fonction $\psi : \mathbf{C}^g \to \mathbf{C}^g$ défini pour les P_j proches des b_j par

$$\psi : (z_1 = \Sigma_{j=1,...g} \int_0^{x(P_j)} \omega_1, ..., z_g = \Sigma_{j=1,...g} \int_0^{x(P_j)} \omega_g) \mapsto (\sigma_k(P_1, ..., P_g))_{k=1,...,g}$$

est un difféomorphisme local, dont les applications cooordonnées sont des fonctions méromorphes sur $\mathbf{C}^g$, d'ordre 2. Noter également que $z(x) = \int_0^x f(x)dx$ est la restriction à la droite $\sigma_2 = ... = \sigma_g = 0$ de la première coordonnée $z_1(\sigma_1, ..., \sigma_g) = \Sigma_{j=1,...g} \int_{b_j}^{P_j} \xi$ de l'application réciproque de ψ.

Ces résultats s'étendent à l'étude des primitives de n'importe quelle forme différentielle $\xi \in \Omega_{K/\mathbf{C}}$, de diviseur polaire $-D$, avec $D > 0$, à condition de remplacer:

- g par la dimension $\gamma = g + deg(D) - 1 = \ell(\kappa + D)$ de $H^0(X, \Omega_X(-D))$;

- $Jac(X)$ par la jacobienne généralisée $J_D(X)$ de module D; c'est encore un groupe algébrique commutatif, extension de $Jac(X)$ par un groupe linéaire;

- les fonction theta par des dérivés de fonctions theta, des formes linéaires, et des exponentielles; ce sont donc encore des fonctions méromorphes d'ordre fini.

On dira que x et une série formelle $g(x) \in \mathbf{C}[[x]]$ sont *simultanément uniformisables à plusieurs variables* s'il existe un entier $\gamma \geq 1$, un difféomorphisme ψ de $(\mathbf{C}^\gamma; 0)$ et un polynôme G en $g(x_1), ..., g(x_\gamma)$, à coefficients entiers non tous nuls, tels que ψ et $G \circ \psi$ s'étendent en des applications méromorphes sur $\mathbf{C}^\gamma$ (sans imposer qu'elles soient d'ordre fini.) On peut donc énoncer:

Lemme 1: *Soient $f \in \mathbf{C}[[x]]$ une série entière algébrique sur $\mathbf{C}(x)$, et $y(x)$ la série formelle $exp(\int_0^x f(t)dt)$ (resp. $\int_0^x f(t)dt$). Alors x et $y(x)$ sont simultanément uniformisables à plusieurs variables.*

En caractéristique finie (disons $k = \overline{\mathbf{F}}_p$).

La condition sur les résidus ne suffit plus à caractériser les formes localement exactes (considérer $t^{p-1}dt$ sur $\mathbf{P}_1$), l'espace $D^2(X)/dK$ n'est plus de dimension $2g$, et $D^1(X)$ ne s'y injecte pas (courbes elliptiques supersingulières, cf. infra). En remplacant $D^2(X)$ par le sous-espace $D_2(X)$ des formes de 2e espèce dont tous les pôles sont d'ordre ≤ 2 (donc $= 2$), et dK par le sous-espace $(dK)_1$ des différentielles dont tous les pôles sont d'ordre 1, on peut toutefois retrouver un espace $D_2(X)/(dK)_1$ de dimension $2g$, dans lequel s'injecte $D^1(X)$.

Considérons maintenant le k-dual $H^1(X, \mathcal{O}_X)$, de dimension g, de $D^1(X)$. La suite exacte longue déduite de $O \to \mathcal{O}_X \to \underline{K} \to \underline{K}/\mathcal{O}_X \to 0$ l'identifie à $H^0(X, \underline{K}/\mathcal{O}_X)/K$, c'est-à-dire aux classes de répartitions $R/(R(0) + K)$ sur X, sur lesquelles la dualité avec $D^1(X)$ s'exprime par la formule $< r, \omega >= \Sigma_{P \in X} res_P(r_P \omega)$. Soit F l'endomorphisme de Frobenius $r \mapsto r^p$ de $R/(R(0)+K)$ (en termes de $H^1(X, \mathcal{O}_X)$, c'est l'élévation à la puissance p sur les fibres). Il est p-linéaire, et admet un transposé p^{-1}-linéaire $F' \in End(D^1(X))$, défini par la condition $< r^p, \omega >=< r, F'\omega >^p$ pour tout r. Cet opérateur est en fait la

restriction à $D^1(X)$ de l'*opérateur de Cartier* C, défini sur $\Omega_{K/k}$ tout entier de la façon suivante.

Soit x un élément séparant de K, de sorte que $1, x, .., x^{p-1}$ est une base de K sur K^p. Pour toute forme différentielle $\xi = f(x)dx$, on pose

$$C\xi := f_{p-1}dx, \quad \text{si } (f_{p-1})^p = -(d/dx)^{p-1}f$$

désigne la coordonnée de f relative à x^{p-1}. Alors, C ne dépend pas du choix de x (voir la formule de Jacobson, chap. III), annule les formes exactes, est additif et vérifie pour tout $f \in K$: $C(f^p\omega) = fC(\omega)$, $C(f^{p-1}df) = df$.

Lemme 2: *l'opérateur de Cartier C vérifie les propriétés suivantes. Pour tout $\xi \in \Omega_{K/k}$,*

i) $C\xi = 0$ si et seulement si ξ est exacte.

ii) $C\xi = \xi$ si et seulement si ξ est logarithmiquement exacte;

iii) le groupe $Pic_0(X)[p]$ des classes de diviseurs d'ordre divisant p est canoniquement isomorphe au sous-groupe des différentielles logarithmiquement exactes de $D^1(X)$.

Exemple: pour $\lambda \in k = \overline{\mathbf{F}}_p, \lambda \neq 0, 1$, soit $X := E_\lambda$ la courbe elliptique d'équation $y^2 = x(x-1)(x-\lambda)$. L'image sous C de la différentielle de première espèce $\omega = dx/y$ en est un mutiple $A^{1/p}\omega$. L'élément $A \in k$, appelé *invariant de Hasse* de E_λ, vaut $H_p(\lambda)$, où $H_p(X) := (-1)^N \Sigma_{i=0,...,N} \binom{N}{i}^2 X^i$, avec $N = \frac{p-1}{2}$. On dit que E_λ est supersingulière si $A = 0$, i.e. si ω est exacte. Cela arrive pour N valeurs de λ, (d'où $\sim p/12$ valeurs de $j(E_\lambda)$, toutes dans $\in \mathbf{F}_{p^2}$), et $E_\lambda[p]$ est alors réduit à 0. Dans le cas contraire, ce groupe est d'ordre p, et E_λ admet une forme différentielle de première espèce logarithmiquement exacte -mais en général pas définie sur son corps de définition $\mathbf{F}_p(\lambda)$.

Revenons au cas général (avec $g \geq 1$), et soit $b = b_1 + ... + b_g$ un diviseur non spécial sur X. Dans une base $r_1, ..., r_g$ de $R/R(0)+K$ adaptée à b, la matrice $A = (a_{i,j})$ représentative de F s'appelle la *matrice de Hasse-Witt* de X: pour tout $i = 1, ..., g$, $r_i^p - \Sigma_{j=1,..,g} a_{ij} r_j \in R(0) + K$. Soient alors $\mathbf{F}_q$ ($q = p^n$) le corps de définition de X, F_X l'endom. de Frobenius de $Jac(X)$, $\pi(T)$ la réduction mod. p du polynôme caractéristique "$deg(F_X - Tid)$" de F_X, et $\mathbf{A}$ la matrice $AA^{[p]}...A^{[p^{n-1}]}$. D'après un théorème de Manin, $\pi(T) = T^g det(\mathbf{A} - Tid)$. Si donc $E = E_\lambda$ désigne une courbe elliptique définie sur $\mathbf{F}_q$, d'invariant de Hasse A, le nombre $N_E = deg(F - id) = 1 - a_n + p^n$ de ses points $\mathbf{F}_q$-rationnels vérifie la congruence $a_n \equiv A^{\frac{p^n-1}{p-1}}$ mod. p; pour $n = 1$, on déduit alors des bornes de Hasse-Weil (et du fait que $2|N_E$) que ω elle-même n'est pas logarithmiquement exacte.

Soit enfin $Der(K/k)$ le K-ev des dérivations sur la courbe X. Il est stable sous

l'application $D \mapsto D^p$, et on déduit de la formule de Jacobson que

$$< C(\omega), D >^p = < \omega, D^p > - D^{p-1}(< \omega, D >)$$

pour tout $\xi \in \Omega_{K/k}$; on retrouve ainsi que sur la p-algèbre de Lie $Lie(E)$ d'une courbe elliptique, l'opération de puissance p-ième est transposée de l'endomorphisme $F' = C_{|D^1}$ de $D^1(X)$ décrit plus haut. En particulier, $D^p = AD$; cette propriété permet, comme promis, d'établir directement l'implication Thm. 3 $\Rightarrow$ Cor. 3 du chap I: la réduction modulo p d'une $\mathbf{Q}$-sous-algèbre de Lie de $Lie(E \times E')$ est p-restreinte si et seulement si $N_E \equiv N_{E'}$ mod p, ou encore, au vu des bornes de Weil pour $p > 2$, ssi $N_E = N_{E'}$.

§2. La méthode de Chudnovsky-André

[Pour simplifier, nous supposons ici encore que $k = \mathbf{Q}$.]

Si $y = \Sigma_{n \geq 0} a_n z^n \in \mathbf{Q}[[x]]$ est une série formelle, on pose

$$\sigma(y) = \overline{lim}_{n \geq 0} \ (\frac{1}{n} \ Log \ ppcd(a_0, ..., a_n)),$$

où *ppcd* désigne le plus petit commun dénominateur; plus généralement, on considère pour tout $m \geq 1$:

$$\sigma_m(y) = \overline{lim}_{n \geq 0} \ (\frac{1}{n} \ Log \ ppcd(a_{i_1} ... a_{i_m}; \Sigma_{1 \leq k \leq m} i_k \leq n).$$

Pour m fixé, cette quantité contrôle le dénominateur commun des coefficients d'indice $\leq n$ des puissance d'ordre $\leq m$ de y. Si $\sigma(y) < \infty$, il en est de même de $\sigma_m(y)$ pour tout m, mais en général pas de façon uniforme. On écrira $\tilde{\sigma}(y) < \infty$ pour dire que la suite $\{\sigma_m(y); m \in \mathbf{N}\}$ est bornée. C'est le cas si y est globalement bornée, par exemple, si y est algébrique sur $\mathbf{Q}(x)$.

La démonstration du Théorème 0 se fait en deux étapes. On fixe un point k-rationnel $b_0 \in X$ assez général et un paramètre local $x \in K$, et on identifie ξ/dx à une fonction algébrique $f(x)$ non ramifiée en 0.

Théorème 1: *soient $\xi = f(x)dx$ une forme différentielle sur $X/\mathbf{Q}$ vérifiant l'hypothèse i) (resp. ii)) du Théorème 0. Alors, la série $y(x) = exp(\int_0^x f(t)dt)$ (resp. $y(x) = \int_0^x f(t)dt$) vérifie $\tilde{\sigma}(y) < \infty$.*

Théorème 2: *si x et $y(x) \in \mathbf{Q}[[x]]$ sont simultanément uniformisables à plusieurs variables, et si $\tilde{\sigma}(y) < \infty$, alors, x et $y(x)$ sont algébriquement dépendantes sur $\mathbf{Q}$.*

On conclut alors par le lemme 1, et par un argument de monodromie: dans le cas i), le groupe de Galois différentiel (cf. chap. III) de l'équation $\frac{dy}{dx} - fy = 0$ est un sous-groupe

d'ordre fini N de $\mathbf{G}_m$; un tel sous-groupe étant cyclique, y^N est invariant sous Galois, et $N\omega \in dLog(K)$. Dans le cas ii), le groupe de Galois différentiel de $(\frac{d}{dx} - dLog(f))\frac{d}{dx}y = 0$ est un sous-groupe de $\mathbf{G}_a$ fini, donc nul, et $\omega \in d(K)$.

Démonstration du Thm. 1

Son point clef ("$\tau(y) = 0$") sera démontré dans un cadre plus général au chap. III. Indiquons ici comment on s'y ramène. On pose $Log^+ = sup(0, Log)$. On identifie les places finies de $\mathbf{Q}$ à des nombres premiers p, ou à des valuations v, ou à des valeurs absolues, normalisées pour $a \in \mathbf{Q}^*$ par $|a|_v = p^{-v(a)}$ (i.e. $|p|_v = 1/p$). Pour $y = \Sigma_{n\geq 0} a_n x^n \in \mathbf{Q}[[x]]$ et $v \in M'_{\mathbf{Q}} := M'$, on pose

$$h_0(n, v) = sup_{0\leq m\leq n} Log^+ |a_m|_v,$$

de sorte que $Logppcd(a_0, ..., a_n) = \Sigma_{v\in M'} h_0(v, n)$ et

$$\rho_v(y) := \overline{lim}_{n\geq 0} \frac{1}{n} Log^+ |a_n|_v = \overline{lim}_{n\geq 0} \frac{1}{n} h_0(v, n)$$

est le logarithme de l'inverse du minimum de 1 et du rayon de convergence v-adique de la série y, vue dans $\mathbf{Q}_v[[x]]$. On définit le *rayon inverse global* $\rho(y)$ et la *taille* $\sigma(y)$ de y par les expressions (éventuellement infinies)

$$\rho(y) = \Sigma_{v\in M'} \overline{lim}_n \frac{1}{n} h_0(v, n) = \Sigma_v \rho_v(y) \qquad ; \qquad \sigma(y) = \overline{lim}_{n\geq 0} \Sigma_{v\in M'} \frac{1}{n} h_0(v, n).$$

On pose enfin

$$\tau(y) = inf_p \{\overline{lim}_{n\geq 0} \Sigma_{v\in M', p_v\geq p} \frac{1}{n} h_0(v, n)\}.$$

On étend ces symboles à des N-uplets de séries, c'est-à-dire à des éléments de $\mathbf{Q}^N[[x]]$, en munissant $\mathbf{Q}_v^N$ de la norme $|.|_v$ du sup des coordonnées. Pour $y \in \mathbf{Q}[[x]]$ et $m \geq 1$, $\sigma_m(y)$ est ainsi la taille de la famille $(1, y, ..., y^m)$; on note de même $\rho_m(y)$ son rayon inverse global, τ_m son "τ". Dans ces conditions:

Lemme 3: *Pour tout $y \in \mathbf{Q}[[x]]$ et $m \geq 1$, on a:*

i) $\sigma(y) \leq \rho(y) + \tau(y)$;

ii) si, pour tout $v \in M'$, la suite $\{\frac{1}{n} h_0(v, n)\}_{n\geq 0}$ converge, alors, $\rho(y) \leq \sigma(y)$;

iii) $\rho((d/dx)y) = \rho(y) = \rho(\int_0^x y dx)$; $\sigma((d/dx)y) \leq \sigma(y), \tau((d/dx)y) \leq \tau(y)$;

iv) $\sigma(\int_0^x y dx) \leq \sigma(y) + 1, \tau(\int_0^x y dx) \leq \tau(y) + 1$;

v) $\rho_m(y) \leq \rho(y)$; $\tau_m(y) \leq (\Sigma_{1\leq j\leq m} \frac{1}{j})\tau(y)$, *donc* $\sigma_m(y) \leq \rho(y) + (1 + Logm)\tau(y)$.

Démonstration: i), iii) et la première inégalité de v) sont élémentaires. ii) se déduit du lemme de Fatou: $\Sigma_v \underline{lim}_n x_{n,v} \leq \underline{lim}_n \Sigma_v x_{n,v}$ pour toute famille $\{x_{n,v} \geq 0\}$. (Attention: aucune relation ne lie en général $\rho(y)$ et $\sigma(y)$.) Pour iv), noter que $\overline{lim}_n \frac{1}{n} Logppcd(1, \frac{1}{2}, ..., \frac{1}{n})$

$= 1$, d'après le théorème des nombres premiers. Passons à v): pour tout $v \in M'$, et $\Sigma_{k=1,...,m} i_k = n' \leq n$ avec $i_1 \geq i_2 \geq ... \geq i_m$ (de sorte que $ki_k \leq n$), on a $Log^+|a_{i_1}...a_{i_m}|_v \leq \Sigma_{k=1,...,m} h_0(v,[n/k])$, d'où

$$\frac{1}{n} Log^+ Max_{\Sigma i_k = n'} |a_{i_1}...a_{i_m}|_v \leq \Sigma_{1 \leq k \leq m} \frac{1}{k} \frac{1}{[n/k]} h_0(v,[n/k]), \text{ et } \tau'_m(y) \leq (\Sigma_{1 \leq k \leq m} \frac{1}{k}) \tau(y).$$

Traduite en termes de p-coubures (cf. chap. III), l'hypothèse (i) (resp. (ii)) du théorème 1 entraîne que $\rho(y)$ est borné, et que $\tau(y) = 0$. Du lemme 3.v, on déduit alors bien que $\tilde{\sigma}(y) < \infty$.

Remarque 1: sous l'hypothèse (i), la propriété $\rho(y) < \infty$ suffit à entraîner que $\tilde{\sigma}(y) < \infty$. En effet, pour presque tout $v \in M'$, la solution $y = exp(\int_0^x f) \in \mathbf{Q}_v[[x]]$ de l'équation du premier ordre $y' = fy$ n'a pas de zéro dans son disque de convergence (que l'on suppose ici contenu dans $\{|z|_v < 1\}$). Son polygône de Newton n'a donc qu'un côté (infini), d'équation $Y = -\rho_v(y)X$, d'où $h_0(v,n) \leq n\rho_v(y)$ pour tout $n \geq 0$, et $\sigma(y) \leq \rho(y)$. De $y^m = exp(m \int_0^x f)$, on déduit immédiatement que $\sigma_m(y) \leq \sigma(y)$, ou, en reprenant le même argument, que $\sigma_m(y) \leq \rho_m(y) = \rho(y)$.

Démonstration du Thm. 2

On reprend les notations précédant le lemme 1. Sans perte de généralité, on peut supposer que le difféomorphisme local ψ de $(\mathbf{C}^\gamma, 0)$ sous-jacent à l'hypothèse d'uniformisation est tangent à l'identité, et on désigne par θ une fonction entière telle que $\theta.\psi, \theta.G \circ \psi$ soient entières et $\theta(0) = 1$. On note d'une lettre grasse les γ-uples de variables, et on désigne par c_i des 'constantes' ne dépendant que de f, G, ψ et θ; même convention pour les notations o, O. On fixe un entier $m \geq c_0$, et on note g le degré du polynôme G.

Pour tout entier $N \geq c_1$, le principe des tiroirs fournit m polynômes $P_0, ..., P_{m-1} \in \mathbf{Z}[\mathbf{x}]$ non tous nuls, de degrés $\leq D = \frac{2}{m^{1/\gamma}} N$, de coefficients majorés en valeur absolue par $exp((\sigma_{gm}(y) + \rho_\infty(y))N + o(N))$, tel que la série $R_N(\mathbf{x}) = \Sigma_{0 \leq k < m} P_k(\mathbf{x}) G^k(\mathbf{x}) := P(\mathbf{x}, G(\mathbf{x}))$ ait en $\mathbf{x} = 0$ un ordre $\geq N$.

Supposons R_N non identiquement nulle, et soit $\mathbf{m}$ un multi-indice de longueur $M \geq N$ minimale telle que le nombre (rationnel) $\xi = \frac{1}{\mathbf{m}!} \frac{\partial^M}{\partial \mathbf{x}^\mathbf{m}} R_N(0)$ soit non nul. Son dénominateur vérifie alors:

$$Log\ den(\xi) \leq (\sigma_{gm}(y) + \rho_\infty(y))M + o(M).$$

Considérons la fonction analytique sur $\mathbf{C}^\gamma$: $F_N(\mathbf{z}) = \theta(\mathbf{z})^D P(\psi(\mathbf{z}), G \circ \psi(\mathbf{z}))$. Comme ψ est tangent à l'identité et que $\theta(0) = 1$, on a $\frac{\partial^M}{\partial \mathbf{x}^\mathbf{m}} R_N(0) = \frac{\partial^M}{\partial \mathbf{z}^\mathbf{m}} F_N(0)$. Pour tout $R \geq c_2$, la formule de Cauchy sur le polydisque $|\mathbf{z}| = R$ entraîne dans ces conditions:

$$Log|\xi| \leq -(LogR)M + (\sigma_{gm}(y) + \rho_\infty(y))N + \chi(R)D + o(N),$$

où $\chi(R) = Log(sup_{|\mathbf{z}|=R}(|\theta|, |\theta.\psi|, |\theta.G \circ \psi|))$. Ainsi

$$0 \leq \frac{1}{M}(Log\ den(\xi) + Log|\xi|) \leq 2\tilde{\sigma}(y) + +\rho_\infty(y) + \frac{2}{m^{1/\gamma}}\chi(R) - LogR + o(1).$$

Pour $R = exp(3\tilde{\sigma}(y)+\rho_\infty(y))$, cela conduit à une contradiction dès que $m > (2\chi(R)/\tilde{\sigma}(y))^\gamma$. Ainsi, $P(\mathbf{x}, G(\mathbf{x})) \equiv 0$, et on obtient par spécialisation une relation de dépendance algébrique non triviale entre x et $y(x)$.

Remarque 2: soit E/k une courbe elliptique à multiplications complexes, et $\omega \neq 0$ une forme de première espèce définie sur k. L'ensemble des places de k où E a bonne réduction supersingulière a pour densité $1/2$. On ne peut donc remplacer, dans le Théorème 0.ii, l'hypothèse "pour presque tout place" par "pour un ensemble de places de densité > 0".

Remarque 3: dans la preuve ci-dessus, la place archimédienne a joué un rôle particulier. Pour des énoncés de nature adélique, voir Y. André [A'].

CHAPITRE III

LA CONJECTURE DE GROTHENDIECK-KATZ

Sous sa forme la plus élémentaire, la conjecture de Grothendieck énonce:

Conjecture 0: *soit $L \in \mathbf{Q}(z)[d/dz]$ un opérateur différentiel d'ordre n. Les conditions suivantes sont équivalentes:*

i) l'équation différentielle $Ly = 0$ admet n solutions linéairement indépendantes sur $\overline{\mathbf{Q}}$, formées de fonctions algébriques sur $\mathbf{Q}(z)$;

ii) pour presque tout nombre premier p, l'équation différentielle $L_p y = 0$ (déduite de L par réd. mod. p) admet dans $\mathbf{F}_p(z)$ n solutions linéairement indépendantes sur $\mathbf{F}_p(z^p)$.

La généralisation qu'en a proposée Katz [K'] sera décrite au §3. Elle met en jeu le *groupe de Galois différentiel* de L (au lieu de l'hypothèse i), et les p-courbures des L_p (au lieu de l'hypothèse ii), que nous décrivons maintenant dans le cadre des modules à connexions.

§1. Connexions et p-courbures

Soient K un corps muni d'une dérivations ∂, de corps de constantes $C = K^{\partial} := \{x \in K, \partial x = 0\}$, $\Omega \subset \Omega_{K/C}$ le K-dual du K-espace vectoriel $\Delta = K.\partial$ de dérivations sur K engendré par ∂, $d : K \to \Omega$ l'application canonique, et V un K-espace vectoriel de dimension finie. Une *connexion* sur V est une application $\nabla : V \to V \otimes_K \Omega$ C-linéaire et vérifiant la formule de Leibniz $\nabla(fv) = f\nabla(v) + v \otimes df$. Elle munit V d'une action $\nabla_\theta : V \to V$ des dérivations $\theta \in \Delta$, donnée par la contraction $V \otimes \Omega \otimes \Delta \to V$. Plus généralement, si $\mathcal{D}_K = K[\partial]$ désigne l'anneau des opérateurs différentiels engendré sur K par ∂, une connexion sur V revient à la donnée d'une structure de $\mathcal{D}_K$-module à gauche sur V: $(\Sigma_{i=0,...,N} a_i \partial^i)v = \Sigma_{i=0,...,N} a_i (\nabla_\partial)^i(v)$.

Dans une base $\underline{e} = (e_1, ..., e_n)$ de V sur K, ∇_∂ s'identifie à l'opérateur $D : K^n \to K^n$: $DY = \partial Y - AY$, où A est la matrice n, n à coefficients dans K définie par $\nabla_\partial(\underline{e}) = -\underline{e}A$. Dans une seconde base $\underline{e}' = \underline{e}P, P \in GL_n(K)$, ∇_∂ est alors représentée par la matrice $A_P = P^{-1}AP - P^{-1}\partial P$, et les systèmes différentiels $\partial Y = AY, \partial Z = A_P Z$ sont dits *équivalents*.

Le K-dual $\check{V}$, les puissances symétriques $Sym^m V$, et plus généralement, toutes les constructions tensorielles E formées sur V et $\check{V}$ sont naturellement munies de connexions déduites de ∇. Ainsi, la connexion ∇_E de $E = V \otimes_K \check{V} \simeq End_K(V)$ est donnée en termes matriciels par $D_E Q = \partial Q - [A, Q]$. Plus généralement, deux vectoriels à connexions $(V_1, \nabla_1), (V_2, \nabla_2)$ étant donnés, $Hom_K(V_1, V_2) \simeq V_2 \otimes \check{V}_1$ admet une connexion naturelle $\nabla_{1,2} = \nabla_2 \otimes \check{\nabla}_1$ définie par $\nabla_{1,2}(\phi)(v_1) = \nabla_2(\phi(v_1)) - \phi(\nabla_1(v_1))$. On dit que ∇_1 et ∇_2 sont isomorphes s'il existe un K-isomormorhisme $\phi : V_1 \to V_2$ tel que $\nabla_{1,2}(\phi) = 0$.

Pour toute extension différentielle (H, ∂) de (K, ∂), on munit $V_H = V \otimes_K H$ de la connexion $\nabla = \nabla_H : v \otimes h \mapsto v \otimes dh + \nabla v \otimes h$. Les *vecteurs horizontaux* de ∇ (à valeur dans H) sont les éléments u de V_H tels que $\nabla_H(u) = 0$. Ils forment un H^∂-sous-espace vectoriel $(V_H)^\partial$ de V_H. Leur recherche revient à la résolution (dans H^n) du système différentiel $\partial Y = AY$ (tandis que les vecteurs horizontaux de la connexion duale $\check{\nabla}$ correspondent aux solutions du système $\partial Z = -{}^t AZ$). Du lemme du wronskien (rappelé ci-dessous sous sa forme classique), on déduit que pour tout H, l'injection de $(V_H)^\partial$ dans V_H s'étend en un H-homomorphisme *injectif*

$$(V_H)^\partial \otimes_{H^\partial} H \to V_H.$$

On dit que (V, ∇) est *soluble* dans H si cette injection est un isomorphisme, autrement dit s'il existe une "matrice fondamentale de solutions" $U \in GL_n(H)$ telle que $\partial U = AU$. On dit que H est une *extension de Picard-Vessiot* de K pour ∇ si les conditions suivantes sont satisfaites: i) $H^\partial = K^\partial$; ii) ∇ est soluble dans H; iii) H est engendré sur K par les coordonnées de U.

Lemme 1: *soient $f_1, ..., f_m$ des éléments d'un corps différentiel (K, ∂), de corps de constantes C. Alors, $f_1, ..., f_m$ sont linéairement indépendants sur C si et seulement si leur déterminant wronskien $W(f_1, ..., f_m)$ est non nul.*

Pour C algébriquement clos de caractéristique nulle, et Δ de dimension 1 comme ci-dessus, toute K-connexion ∇ admet une extension de Picard-Vessiot. Lorsqu'on remplace Δ par une sous-algèbre de Lie de $Der(K/C)$ de dimension > 1, cela ne reste vrai, d'après le théorème de Frobenius, que si ∇ est une connexion *intégrable*, i.e. de courbure ψ^∇ nulle: $\psi^\nabla(\partial_1, \partial_2) := [\nabla_{\partial_1}, \nabla_{\partial_2}] - \nabla_{[\partial_1, \partial_2]} = 0$ pour tout couple $\partial_1, \partial_2 \in \Delta$. Un phénomène similaire apparaît en caractéristique p, où nous nous plaçons jusqu'à la fin de ce § (en supposant de nouveau Δ de dimension 1). Dans ce cas, ∂^p est encore une dérivation de K. Supposant Δ p-restreinte, on définit (l'image d'une dérivation $\theta \in \Delta$ sous) *la p-courbure de la connexion* ∇ sur le K-vectoriel V par la formule:

$$\psi_p(\theta) := \psi_p^\nabla(\theta) = (\nabla_\theta)^p - \nabla_{\theta^p} : V \to V.$$

On vérifie immédiatement que $\psi_p(\theta)$ est un opérateur K-linéaire sur V, et qu'il est horizontal pour la connexion de $End_K(V)$. De plus, ψ_p est p-linéaire en θ: $\psi_p(f\partial) = f^p\psi_p(\partial)$ pour tout $f \in K$, de sorte que ψ_p est nulle si et slt si $\psi_p(\partial) = 0$. Pour $(K, \partial) = (\mathbf{F}_p(z), d/dz)$, et ∇ représentée par une matrice A comme ci-dessus, $\psi_p(\partial)$ est l'endomorphisme de K^n de matrice représentative $A_p \in gl_n(K)$ définie par la relation de récurrence

$$A_1 = -A,\ A_2 = \partial A_1 + A_1.A_1,\ ...,\ A_{k+1} = \partial A_k + A_1.A_k.$$

(On a $D^m Y = \Sigma_{k=0,...,m} \begin{pmatrix} m \\ k \end{pmatrix} A_k \partial^{m-k} Y$ pour tout m, et $(d/dz)^p(K) = 0$.)

La formule de Jacobson sur les dérivations d'un annneau commutatif quelconque R de caractéristique p:

$$\forall \theta \in Der(R),\ \forall u \in R,\ u^{p-1}\theta^p u = (\theta u)^p + \theta^{p-1}(u^{p-1}\theta u)$$

montre que pour $n = 1, \partial^p(K) = 0$ et $\nabla_\partial e_1 = ae_1$, $\psi_p(\partial)$ est l'homothétie de rapport (constant) $a_p = \partial^{p-1}(a) + a^p \in K^p$. (Voir le chap. II, §2, pour d'autres applications.)

La p-courbure de la connexion $\nabla_1 \otimes \nabla_2$ sur un produit tensoriel $V_1 \otimes V_2$ est donnée par $\psi_p^{\nabla_1} \otimes id_{V_2} + id_{V_1} \otimes \psi_p^{\nabla_2}$. Enfin, si $V = \mathcal{D}_K/\mathcal{D}_K L$ pour un opérateur différentiel $L \in \mathcal{D}_K$, et si ∇_∂ est la connexion sur V déduite de sa structure naturelle de $\mathcal{D}_K$-module à gauche, les solutions de l'équation différentielle $Ly = 0$ correspondent aux vecteurs horizontaux de la connexion duale $\check{\nabla}$, qui vérifie $\psi_p^{\check{\nabla}} = -{}^t\psi_p^{\nabla}$. Sa p-courbure est nulle si et seulement si ∂^p est divisible à droite par L dans $\mathcal{D}_K$.

Lemme 2: *soient K un corps de fonctions d'une variable sur un corps fini de caractéristique p, et (V, ∇) un vectoriel à connexion sur K. Alors, ∇ est soluble dans K si et seulement si sa p-courbure ψ_p^{∇} est nulle.*

Démonstration: si V est soluble dans (un corps différentiel arbitraire) K, il existe une base de V sur K dans laquelle ∇ est représentée par la matrice 0, et $\psi_p(\partial)$ est repésentée par $\partial^p - \partial^p = 0$. Inversément, soit z un élément séparant du corps de fonctions K, et ∂ la dérivation de K telle que $\partial z = 1$, de sorte que $K = K^p(z)$, où $C = K^\partial = K^p$ est le corps de constantes du corps différentiel (K, ∂). Soient V^∂ le C-sous-espace des vecteurs horizontaux de $D = \nabla_\partial$, et W le K-sous-espace vectoriel de V formé par le noyau de l'opérateur $\psi_p(\partial) = D^p$. Alors, l'application $v \mapsto P(v) = \Sigma_{i=0,..,p-1} \frac{(-z)^i}{i!} D^i(v)$ envoie W dans V^∂, tandis que l'application $T : V \to V$:

$$v \mapsto T(v) = \Sigma_{k=0,...,p-1} \frac{z^k}{k!} P(D^k(v))$$

induit l'identité sur W. Comme $v \in W \Rightarrow D^k(v) \in W$, tout élément de W est donc combinaison linéaire à coefficients dans K d'éléments de V^∂. Ainsi, $W = V^\partial \otimes_C K$, et ce dernier remplit tout V si $\psi_p(\partial) = 0$.

Remarque 1: soient $\hat{K}$ le complété de K en une place de ce corps de fonctions, et $\hat{\partial}$ l'unique dérivation continue de $\hat{K}$ prolongeant ∂. Son corps de constantes $\hat{K}^p$ vérifie $\hat{K} = K \otimes_{K^p} \hat{K}^p$, et la même démonstration montre que la connexion $\nabla_{\hat{K}}$ de $\hat{V} = V \otimes_K \hat{K}$ est soluble dans $\hat{K}$ si et seulement si ∇ est soluble dans K. L'hypothèse ii) de la conjecture de Grothendieck équivaut donc à demander que L_p admette dans $\mathbf{F}_p((z))$ (donc *a fortiori* dans la clôture algébrique de $\mathbf{F}_p(z)$ dans ce corps), n solutions linéairement indépendantes sur $\mathbf{F}_p((z^p))$.

On dit souvent qu'une connexion ∇/K est triviale si elle est soluble dans K, et isotriviale s'il existe une extension finie séparable K'/K telle que $\nabla_{K'}$ soit triviale. Comme on vient de le voir (ou comme on le déduit plus directement du calcul de $\psi_p^{\nabla_1 \otimes \nabla_2}$), ces deux notions coïncident en caractéristique p, et on peut réécrire la conjecture 0 (étendue à un corps de nombres k) sous la forme

Conjecture 1 (Grothendieck): *une connexion $\nabla/k(z)$ est isotriviale si et seulement si pour presque toute place finie v de k, sa réduction $\nabla_v/k(v)(z)$ modulo v est (iso)triviale.*

En caractéristique p, *la nullité de la p-courbure est ainsi une propriété invariante par extension* finie séparable du corps des "scalaires" K (i.e. par image inverse sous un revêtement étale π). Elle l'est aussi par *restriction des scalaires* (i.e. par image directe sous π). Rappelons brièvement en quoi consiste cette construction. Soient donc K/K_0 une extension séparable de degré d fini, K_s la clôture séparable de K, ∂ une dérivation non triviale de K_0 (et son -unique- extension à K), et ∇ une connexion sur un K-espace vectoriel V de dimension n finie. Alors, $\nabla_0 = Res_{K/K_0} \nabla = \pi_* \nabla$ est la connexion sur le K_0-espace vectoriel $V_0 = Res_{K/K_0} V$ déduite de ∇ par le procédé suivant. Tout d'abord, V/K équivaut à la donnée de la représentation $V(K_s)$, de degré n, de $Gal(K_s/K)$. On note alors $V_0(K_s)$ la représentation induite $Ind_{Gal(K_s/K)}^{Gal(K_s/K_0)} V(K_s)$ du groupe $Gal(K_s/K_0)$, dont $Gal(K_s/K)$ est un sous-groupe d'indice d, et cela définit V_0/K_0. Si $V = \oplus K e_i$ et $K = \oplus K_0 \alpha_j$, V_0 admet pour base $\{e_i.\alpha_j\}_{i,j}$ sur K_0 (la surjection K-linéaire $\gamma : V_0 \otimes_{K_0} K \to V : \gamma(e_i.\alpha_j \otimes \alpha) = \alpha \alpha_j e_i$ vérifie la propriété universelle suivante: pour tout K_0-esp. vect. W et tout $\phi \in Hom_{K-lin}(W \otimes_{K_0} K, V)$, il existe un unique $\psi \in Hom_{K_0}(W, V_0)$ tel que $\phi = \gamma \circ \psi$.) Dans ces conditions, ∇_0 est la connexion sur V_0/K_0 définie par $(\nabla_0)_\partial(e_i.\alpha_j) = (\nabla_\partial e_i).\alpha_j + e_i.\partial\alpha_j$. Si ∇ est triviale et les e_i horizontaux, et si $\{\beta_k\}$ désigne la base duale de $\{\alpha_j\}$ relativement à Tr_{K/K_0}, un système fondamental de vecteurs horizontaux de $(\nabla_0)_{K^s}$ sera donné par les $E_i^\sigma = \Sigma_k e_i.\alpha_k \otimes \beta_k^\sigma$, où σ parcourt $Gal(K_s/K_0)/Gal(K_s/K)$. Ainsi, ∇ est isotriviale si et seulement si ∇_0 l'est, et en caractéristique p: $\psi_p^\nabla = 0 \Leftrightarrow \psi_p^{\nabla_0} = 0$.

§2 G-opérateurs.

Soient k un corps de nombres, et $M_k = M_k' \cup M_k^\infty$ l'ensemble de ses places (finies, et infinies). Pour tout $v \in M_k$, au-dessus d'une place $p(v)$ de $\mathbf{Q}$, on note $|.|_v$ la valeur absolue qui prolonge la valeur absolue $p(v)$-adique usuelle de $\mathbf{Q}$. Ainsi, $|x|_v = p(v)^{-v(x)/e_v}$ si $v \in M_k'$ admet $e_v = \frac{[k_v:\mathbf{Q}_{p(v)}]}{f_v}$ pour indice de ramification et $\mathbf{Z}$ pour groupe de valeurs. Les valeurs absolues normalisées définies par

$$||x||_v = |x|_v^{\frac{[k_v:\mathbf{Q}_{p(v)}]}{[k:\mathbf{Q}]}} = |N_{k_v/\mathbf{Q}_{p(v)}} x|_{p(v)}^{\frac{1}{[k:\mathbf{Q}]}}$$

vérifient alors la formule du produit $\Pi_{v\in M_k}||x||_v = 1$ pour $x \in k^*$; l'expression $h(x) = \Sigma_{v\in M_k} Log^+||x||_v$ s'appelle la hauteur logarithmique absolue de x, et $[k:\mathbf{Q}]\Sigma_{v\in M_k'} Log^+||x||_v$ est le logarithme du ppcd des coefficients du polynôme caractéristique de x relativement à $k/\mathbf{Q}$.

Si $y(z) = \Sigma_{i=0,...,d} a_i z^i \in k[z]$, on définit la norme de Gauss de y relativement à la place finie v par: $||y||_v = sup_{i=0,...,d}||a_i||_v$; d'après le lemme de Gauss, elle est mutiplicative et s'étend donc sans ambiguïté au corps des fractions $K = k(z)$ de $k[z]$. Pour un N-uplet $\mathbf{x} = (x_1, ..., x_N) \in k^N$, on pose de même $||\mathbf{x}||_v = sup_{i=1,...,N}||x_i||_v$, $h(\mathbf{x}) = \Sigma_{v\in M_k} Log^+||\mathbf{x}||_v$. (Ne pas confondre avec la hauteur sur l'espace projectif $\mathbf{P}_{N-1}(k)$, définie par $\hat{h}(\mathbf{x}) = \Sigma_{v\in M_k} Log||\mathbf{x}||_v$: par exemple, $h(x) = \hat{h}((1,x))$ pour tout x dans k.) Si $\mathbf{y}(z) \in K^N$ est un N-uplet de fractions rationnelles, sa norme de Gauss en une place finie v est définie par $||\mathbf{y}(z)||_v = sup_{i=1,...,N}||y_i(z)||_v$.

Enfin, si $\mathbf{y}(z) = \Sigma_{k\geq 0}\mathbf{a}_s z^s \in k^N[[z]]$ est un N-uplet de séries entières, on pose:

$$h_0(\mathbf{y}; s, v) = h_0(s, v) = sup_{0\leq m\leq s} Log^+||\mathbf{a}_m||_v; \rho_v(\mathbf{y}) := \overline{lim}_{s\geq 0}\frac{1}{s}h_0(v, s);$$
$$\rho(\mathbf{y}) = \Sigma_{v\in M_k'}\rho_v(\mathbf{y}); \rho^\infty(\mathbf{y}) = \Sigma_{v\in M_k^\infty}\rho_v(\mathbf{y})$$
$$\sigma(\mathbf{y}) = \overline{lim}_{s\geq 0}\Sigma_{v\in M_k'}\frac{1}{s}h_0(v, s); \tau(\mathbf{y}) = inf_p\{\overline{lim}_{s\geq 0}\Sigma_{v\in M', p(v)\geq p}\frac{1}{s}h_0(v, s)\}.$$

Ces quantités vérifient encore les propriétés énoncées au Lemme 3 du chapitre II. On va maintenant les préciser, en supposant que $\mathbf{y}$ est une matrice fondamentale de solutions d'un système différentiel rationnel sur $\mathbf{P}_1$, sans singularité en 0.

Soient $K = k(z)$ le corps de fonctions rationnelles sur $\mathbf{P}_1/k$, muni de la dérivation $\partial = \frac{d}{dz}$, et $\nabla =$ une connexion sur un K-e.v. V de dimension n finie. Dans une base de V sur K, ∇_∂ est représenté par l'opérateur $DY = \partial Y - AY$, et on définit une (nouvelle) suite de matrices $A_s \subset gl_n(K)$ par les relations:

$$A_0 = I_n, A_1 = A, A_2 = \partial A_1 + A_1.A_1, ..., A_{s+1} = \partial A_s + A_s.A_1.$$

(En transposant cette dernière suite, on obtient la suite définie au §1, mais relativement à la connexion *duale.*) Si U est une matrice fondamentale de solutions de $\partial Y = AY$, alors $\partial^s U = A_s U$ pour tout $s \geq 0$, de sorte que la série formelle $R_x(z) = \Sigma_{s\geq 0} \frac{1}{s!} A_s(x)(z-x)^s \in K^{n^2}[[z-x]]$ est la résolvante du système différentiel $\partial Y = AY$; lorsque ses coeff. sont définis en x et qu'elle converge, elle exprime en z la matrice fondamentale de solutions définie par la condition initiale $R(x) = I_n$. On pose alors (avec les normes de Gauss)

$$h_x(\nabla; s, v) = h_x(s, v) = sup_{0\leq m\leq s} Log^+ || \tfrac{1}{m!} A_m ||_v;$$

et on définit des invariants indépendants de la base choisie par les formules

$$\rho_v(\nabla) := \overline{lim}_{s\geq 0} Log^+ \tfrac{1}{s} || \tfrac{1}{s!} A_s ||_v = \overline{lim}_{s\geq 0} \tfrac{1}{s} h_x(v, s) \ ; \ \rho(\nabla) = \Sigma_{v\in M'_k} \rho_v(\nabla);$$
$$\sigma(\nabla) = \overline{lim}_{s\geq 0} \Sigma_{v\in M'_k} \tfrac{1}{s} h_x(v, s) \ ; \ \tau(\nabla) = inf_p \{ \overline{lim}_{s\geq 0} \Sigma_{v\in M', p(v)\geq p} \tfrac{1}{s} h_x(v, s) \}.$$

Théorème 1: *i) pour tout* $v \in M'_k$, $\rho_v(\nabla) := lim_{s\geq 0} \frac{1}{s} h_x(v, s)$.
ii) $\sigma(\nabla) = \rho(\nabla) + \tau(\nabla)$*, et si l'un de ces invariants est fini, les deux autres le sont aussi.*

Démonstration: i) Comme v est fixée, on reprend ici la valeur absolue usuelle $|.|_v$, norme de Gauss comprise, et on pose $p(v) = p$. On vérifie aisément que la limite supérieure définissant $\rho_v(\nabla)$ est finie (et même $\leq \frac{1}{p-1} Logp$ pour v asssez grand). Reste à la majorer par la limite inférieure. En calculant $\partial^m A_s U$, on voit que pour pour tout $s, m \geq 0$, $\frac{A_{s+m}}{(s+m)!} = \Sigma_{i+j=m} \frac{s!m!}{(s+m)!} \frac{\partial^i}{i!} (\frac{A_s}{s!}) . \frac{A_j}{j!}$. Mais les opérateurs $\frac{\partial^i}{i!}$ sont de norme 1 sur K, de sorte que $Log^+ | \frac{A_{s+m}}{(s+m)!} |_v \leq Log^+ | \frac{A_s}{s!} |_v + h_x(m, v) - log | \begin{pmatrix} s+m \\ s \end{pmatrix} |_v$. En itérant, on obtient $Log^+ | \frac{A_{s+qm}}{(s+qm)!} |_v \leq Log^+ | \frac{A_s}{s!} |_v + q h_x(m, v) - Log | \frac{(s+qm)!}{s!(m!)^q} |_v$ pour tout $q \geq 1$. Pour $s \leq m$, le terme binomial est majoré par $Logs + Logp + q(Logp + Logm)$, et on obtient en définitive: $Log^+ | \frac{A_{s+qm}}{(s+qm)!} |_v \leq (q+1)(h_x(m, v) + Logp + Logm)$. Effectuant la division euclidienne de tout entier N par m, on en déduit $Log^+ | \frac{A_N}{N!} |_v \leq \frac{N+m}{m} (h_x(m, v) + Logp + Logm)$, d'où $\rho_v(\nabla) \leq \frac{1}{m} (h_x(m, v) + logp + Logm)$ pout tout m, et $\rho_v(\nabla) \leq \underline{lim}_{m\geq 0} \frac{1}{m} h_x(m, v)$.

ii) Soient M un entier arbitrairement grand. D'après i), $\overline{lim}_{s\geq 0} \Sigma_{p(v)\leq M} \frac{1}{s} h_x(v, s) = \Sigma_{p(v)\leq M} \overline{lim}_{s\geq 0} \frac{1}{s} h_x(v, s)$, d'où

$$\sigma(\nabla) = \Sigma_{p(v)<M} \rho_v(\nabla) + \overline{lim}_{s\geq 0} \Sigma_{p(v)\geq M} \frac{1}{s} h_x(v, s)$$

et la valeur de la dernière somme décroissant avec M: $\sigma(\nabla) = \rho(\nabla) + \tau(\nabla)$. Donc la finitude de σ entraîne celle de ρ (et évidemment, de τ). Comme $\rho_v(\nabla)$ est fini pour tout v, celle de τ entraîne celle de σ, donc de ρ. Pour la troisième implication (que nous vérifierons plus bas dans un cas particulier), nous faisons appel au théorème de Dwork-Robba (Trans.

AMS 259, 1980, 559-577), en vertu duquel on a pour tout $s \geq n$:

$$|\frac{A_s}{s!}|_v \leq \ (sup_{0\leq j\leq n-1}\ |\frac{A_j}{j!}|_v)\ .\ R_v^{-s}\ .\ \{s, n-1\}_p,$$

où $R_v = e^{-\frac{[k:\mathbf{Q}]}{[k_v:\mathbf{Q}_{p(v)}]}\rho_v(\nabla)}$ désigne le rayon de convergence générique (calculé en norme usuelle), et

$$\{s, n-1\}_p = sup_{1\leq d_1<d_2<\ldots d_{n-1}\leq s}|\frac{1}{d_1\ldots d_{n-1}}|_p.$$

Cette expression est majorée par s^{n-1} si $p \leq s$, *et par* 1 *si* $p > s$, de sorte que

$$\frac{1}{s}h_x(s,v) \leq \rho_v(\nabla) + \frac{1}{s}h_x(n-1,v) + \frac{[k_v:\mathbf{Q}_{p(v)}]}{[k:\mathbf{Q}]}\begin{pmatrix}(n-1)(Logs)/s\ ,\ \text{si}\ p(v)\leq s\\ 0\ ,\ \text{si}\ p(v)>s\end{pmatrix}.$$

Mais $h_x(n-1,v) = 0$ dès que v est assez grand, tandis que $\Sigma_{p(v)\leq X}\frac{[k_v:\mathbf{Q}_{p(v)}]}{[k:\mathbf{Q}]} \sim \frac{X}{LogX}$ par le théorème des nombres premiers. Ainsi *toute connexion* ∇ *vérifie*

$$\sigma(\nabla) \leq \rho(\nabla) + n - 1,$$

et $\rho(\nabla) < \infty \Rightarrow \sigma(\nabla) < \infty \Rightarrow \tau(\nabla) \leq n-1$.

On dit que ∇ *est une G-connexion* si $\rho(\nabla)$ (ou donc $\tau(\nabla)$, ou $\sigma(\nabla)$) est fini, Toute connexion ∇ vérifie $||A||_v \leq 1$ pour v suffisamment grand, et l'on peut alors considérer sa réduction ∇_v modulo v. On notera ψ_v^∇ la $p(v)$-courbure de ∇_v ; d'après les formules du §1 (en particulier la relation $\psi_v^{\check{\nabla}} = -{}^t\psi_v^\nabla$), elle est nulle si et seulement si $||A_p||v < 1$.

Théorème 2: *soit* ∇ *une connexion définie sur* $k(z)$*, et telle que* $\psi_v^\nabla = 0$ *pour presque toute place* $v \in M_k'$*. Alors:*

i) toutes les singularités de ∇ *sont régulières, et les monodromies locales autour de chaque singularité de* ∇ *sont d'ordre fini;*

ii) ∇ *est une G-connexion, et* $\tau(\nabla) = 0$.

Démonstration: i) Voir [K], et Chapitre I, Remarque 3. Il suffit d'ailleurs, pour la première (resp. la seconde) assertion de supposer que $\psi_v^\nabla = 0$ pour une infinité de places $v \in M_k'$ (resp. pour un ensemble de places $v \in M_k'$ de densité 1 - et ceci vaut aussi pour ii);

ii) L'idée de base est de montrer que pour toute place $v \in M_k'$ telle que $||A||_v \leq 1$ et $||A_p||_v < 1$, on a $R_v(\nabla) \geq p^{-\frac{1}{p-1}+\frac{1}{e_v p}}$. Comme $e_v = 1$ pour $p(v) >> 0$, la série définissant $\rho(\nabla)$ est alors, à une constante près, majorée par $\Sigma_p(\frac{1}{p-1} - \frac{1}{p})Logp << \Sigma_p \frac{1}{p^2}Logp$, qui converge, et ∇ est bien une G-connexion. Plus précisément, soit $S = S_k(\nabla)$ l'ensemble des places v vérifiant ces hypothèses, qui entraînent qu'en norme usuelle $|A_p|_v \leq p^{-1/e_v}$,

et que $|A_s|_v$ est une fonction décroissante de s. Pour $v \in S$, on déduit par récurrence de la relation $A_{p(s+1)} = \Sigma_{i=0,\dots,p} \frac{p!}{i!(p-i)!}(\partial^i A_{ps})A_{p-i}$ que $|A_{ps}|_v \leq p^{-s/e_v}$. L'assertion sur $R_v(\nabla)$ en résulte, et ∇ est bien un G-connexion. Mieux, $h_x(s,v) \leq \frac{[k_v:\mathbf{Q}_{p(v)}]}{[k:\mathbf{Q}]} \frac{sLogp}{p(v)(p(v)-1)}$ pour $e_v = 1$, et comme $|\frac{1}{s!}|_v = 1$ pour $p(v) > s$, on a pour tout entier $X > Discr(k/\mathbf{Q})$ et tout s: $\Sigma_{v\in S, p(v)>X} \frac{1}{s} h_x(s,v) \leq \Sigma_{v\in S, X<p(v)\leq s} \frac{[k_v:\mathbf{Q}_{p(v)}]}{[k:\mathbf{Q}]} \frac{Logp}{p(v)(p(v)-1)} \leq \Sigma_{p>X} \frac{Logp}{p(p-1)}$. Ainsi, $\frac{1}{s}\Sigma_{v\in S} h_x(s,v) \leq \Sigma_{v\in S, p(v)\leq X} \frac{1}{s} h_x(s,v) + \Sigma_{p>X} \frac{Logp}{p(p-1)}$. En faisant tendre s, puis X vers l'infini, et en ajoutant la contribution de l'ensemble fini $M_k \setminus S_k(\nabla)$, on obtient finalement $\sigma(\nabla) \leq \rho(\nabla)$, et $\tau(\nabla) = 0$.

[On est en fait ici sous les hypothèses du théorème de convergence dominée de Lebesgue: il existe une fonction *intégrable* $g(v)$ sur M_k' telle que la suite de fonctions $f_s(v) := \frac{1}{s} h_x(s,v)$, qui converge partout vers la fonction $\rho(v) := \rho_v(\nabla)$, soit *majorée* par $g(v)$. Donc $\int_v \rho(v) = lim_s \int_v f_s(v) := \sigma(\nabla)$. Dans le même esprit, on peut, comme dans [A], déduire l'inégalité générale $\rho(\nabla) \leq \sigma(\nabla)$ du lemme de Fatou: $\int_v \underline{lim}_s f_s(v) \leq \underline{lim}_s \int_v f_s(v)$.]

Remarque 2: pour des énoncés bien plus précis, liant $\tau(\nabla)$ à la distribution des places v de k suivant l'ordre de nilpotence de ψ_v^∇, voir Dwork [D'], André [A'], et L. di Vizio (thèse Paris 6, 2001). Ainsi, lorsqu'on suppose seulement que les p-coubures de ∇ sont presque toutes *nilpotentes*, les monodromies locales sont quasi-unipotentes, et $\tau(\nabla) \leq 1 + \frac{1}{2} + \dots + \frac{1}{n-1}$; cette borne est par exemple atteinte par l'équation différentielle du $(n-1)$-ième polylogarithme.

Application: fin de la démonstration du Théorème 1 du Chapitre II.

Notons tout d'abord que si ∇_0 est une connexion vérifiant l'hypothèse du théorème 2 ci-dessus, et si $\nabla_{0,d/dz}$ n'a pas de singularité en $z = 0$, elle n'en a pas sur le disque $|z|_v < 1$ pour toute place v suffisamment grande. Sa résolvante formelle $R_x(z)$, spécialisée en $x = 0$, fournit donc une matrice fondamentale de solutions $U(z) = \Sigma_{s\geq 0} \frac{1}{s!} A_s(0) z^s \in k^{n^2}[[z]]$ qui vérifie $||A_s(0)||_v \leq ||A_s||$ pour tout $s \geq 0$. En particulier, tout vecteur solution $\mathbf{y}(z)$ de $\partial Y = AY$ vérifie alors $\rho(\mathbf{y}) < \infty$, et $\tau(\mathbf{y}) = 0$.

Soit maintenant ∇ la connexion sur le corps de fonctions $K = k(X)$ attachée à la forme différentielle ξ considérée au Chap. I, thm. 2, et soit π un morphisme non constant de X vers $\mathbf{P}_1$, non ramifié au dessus de 0, tel que $\pi^{-1}(0)$ ne rencontre pas les pôles de ξ. L'hypothèse de ce théorème, jointe à la remarque 1 du §1, entraîne que presque toutes les p-courbures de la connexion $\nabla_0 = \pi_* \nabla = Res_{K/k(z)} \nabla$ sont nulles. Les solutions $\mathbf{y}(z)$ de l'équation correspondante (qui n'a, par construction, pas de singularité en 0) vérifient donc $\rho(\mathbf{y}) < \infty$, et $\tau(\mathbf{y}) = 0$. Comme ∇ est facteur direct de $\pi^*\pi_*(\nabla) = \nabla_0 \otimes_{k(z)} K$, il en est de même de la solution $y(x)$ étudiée au chap. II, qui vérifie donc bien $\tau(y) = 0$, et (comme promis !) $\tilde{\sigma}(y) < \infty$.

§3 Groupes de Galois différentiels et p-courbures.

Soient $K = \mathbf{C}(z)$ le corps des fonctions rationnelles sur la sphère de Riemann $\mathbf{P}_1$, muni de sa dérivation $\partial = d/dz$, ∇ une connexion sur un K-espace vectoriel V de dimension finie n, $DY = \partial Y - AY$ une représentation matricielle de l'opérateur différentiel ∇_∂, et S l'ensemble de ses singularités. Pour $\omega \notin S$, notons $H = H_\omega$ l'extension de Picard-Vessiot de ∇ engendrée par une matrice fondamentale U de solutions de $\partial Y = AY$ dans $\hat{K} = \mathbf{C}((z-\omega))$; autrement dit, H est le corps de définition de l'ensemble $V^\partial_{\hat{K}} = V^\partial_H$ des vecteurs horizontaux de $\nabla_{\hat{K}}$. On appelle groupe de Galois différentiel de ∇ (en ω) le groupe (abstrait)

$$Gal^\omega(\nabla) = G = Aut_\partial(H/K) := \{\sigma \in Aut(H/K), \sigma\partial = \partial\sigma\}$$

des automorphismes de l'extension H/K qui commutent à la dérivation. Pour tout tel σ, $\partial(\sigma(Y)) = \sigma(\partial(Y)) = \sigma(AY) = \sigma(A)\sigma(Y) = A\sigma(Y)$. Il existe donc une matrice inversible $\rho(\sigma) \in GL_n(\mathbf{C})$ telle que $\sigma(U) = U\rho(\sigma)$, et $\sigma \mapsto \rho(\sigma)$ est une représentation fidèle de G, qu'on peut voir comme un sous-groupe de $GL_n(\mathbf{C}) \simeq GL_{\mathbf{C}}(V^\partial_H)$. Comme on va le voir, c'en est un sous-groupe *algébrique*, dont on note $gal^\omega(\nabla) = LieG$ l'algèbre de Lie. En parfaite analogie avec son analogue classique, la théorie de Galois différentielle établit un dictionnaire entre les extensions différentielles intermédiaires $H' = H^{G'}$ de H/K et les sous-groupes algébriques $G' = Aut_\partial(H/H')$ de G, où les sous-groupes distingués correspondent aux extensions de Picard-Vessiot de K: voir livres de Magid, de Singer-van der Put (à paraître), exposés 750, 849, 884 du Sém. Bourbaki, etc.

Lorsque l'extension H/K est algébrique (c'est-à-dire lorsque ∇ est isotriviale), tous ses automorphismes commutent à la dérivation, et $G = Gal(H/K)$, qui est un groupe fini; de façon équivalente, $LieG = 0$. Plus généralement, le corps fixé par la composante neutre G^0 de G est la fermeture algébrique de K dans H; bien entendu, $LieG^0 = gal^\omega(\nabla)$.

Le prolongement analytique des solutions le long d'un lacet de base ω dans $\mathbf{P}_1 \setminus S$ fournit un automorphisme de H/K commutant à ∂, d'où un morphisme de $\pi_1(\mathbf{P}_1 \setminus S; \omega)$ dans $Gal^\omega(\nabla)$, dont l'image s'appelle le *groupe de monodromie* Γ de ∇. Supposons que ∇ n'ait que des singularités *régulières*, i.e. que ses solutions aient une croissance modérée dans tout secteur centré en un point de S. Comme une fonction holomorphe sur $\mathbf{P}_1 \setminus S$ à croissance modérée en S est une fonction rationnelle, le sous-corps de H fixé par Γ coïncide avec K, et le dictionnaire galoisien entraîne que G *est l'adhérence de Zariski de* Γ. Pour H/K fini, ils sont égaux, et on retrouve ainsi la correspondance bien connue entre groupe de Galois et groupe de monodromie d'un revêtement.

La conjecture de Katz met en jeu le groupe algébrique $G \otimes_{\mathbf{C}} K$ déduit de G par extension des scalaires de $\mathbf{C}$ à K, ou plus exactement la K-forme 'intrinsèque' suivante

G^K de ce groupe. Considérons l'ensemble des constructions tensorielles E déduites de V et de son dual: chaque E est munie de sa connexion naturelle ∇_E (cf. §1), et les éléments de $Aut_K(V)$ agissent naturellement sur E par la représentation tensorielle correspondante. Soit $\mathbf{X}(\nabla)$ l'ensemble des sous-espaces W de ces différents E tels que $\nabla_{E,\partial} W \subset W$. On pose alors

$$G^K = Gal^K(\nabla) := \{g \in GL_K(V),\ \forall\ W \in \mathbf{X}(\nabla),\ gW = W\}.$$

C'est clairement un sous-groupe algébrique de $GL_K(V)$. On déduit du lemme du wronskien que c'est l'image, par conjugaison dans $GL_H(V_H)$ par la matrice fondamentale de solutions U, de l'extension des scalaires à K du $\mathbf{C}$-groupe algébrique $G^\omega = \{g \in GL_{\mathbf{C}}(V_H^\partial),\ \forall\ W \in \mathbf{X}(\nabla)\ ,\ gW_H^\partial = W_H^\partial\}$, et que l'ensemble des points complexes de ce dernier groupe coïncide avec $Gal^\omega(\nabla)$. Ainsi, G est bien un groupe algébrique, G^K est isomorphe, sur une extension de K, à $G \otimes_{\mathbf{C}} K$, et il en est de même des sous-algèbres de Lie $LieG^K := gal^K(\nabla)$ et $Lie(G \otimes_{\mathbf{C}} K) = gal^\omega(\nabla) \otimes_{\mathbf{C}} K$ de $gl_K(V) \simeq gl_n(K)$.

Supposons maintenant que ∇ soit définie sur un corps de nombres k. La même définition que supra fournit une groupe algébrique $G^K(\nabla)$, défini cette fois sur le corps $K := k(z)$, et une sous-algèbre de Lie algébrique $gal^K(\nabla)$ de $gl_K(V)$. On retrouve l'algèbre de Lie précédente en étendant les scalaires de k à $\mathbf{C}$ au moyen d'une place archimédienne de k. Par ailleurs, pour toute place finie v de k suffisamment grande, on peut réduire V et ∇ modulo v; la $p(v)$-courbure ψ_v^∇ de la connexion réduite $\nabla_v/k(v)(z)$ sur V_v est alors un élément de $gl_{k(v)}(V_v)$. On définit par noetherianité l'*algèbre de Lie des p-courbures de* ∇ comme la plus petite sous-algèbre de Lie algébrique $courb(\nabla)$ de $gl_K(V)$ dont la réduction modulo v contienne ψ_v^∇ pour presque toute place finie v de k. Puisque ψ_v^∇ est un vecteur horizontal pour $End_{k(v)}(V_v) = gl_{k(v)}(V_v)$ (cf. §1), il laisse stable W_v pour tout $W \in \mathbf{X}(\nabla)$. Par conséquent, ψ_v^∇ appartient à la réduite de $gal^K(\nabla)$ modulo v pour presque toute v, et $courb(\nabla) \subset gal^K(\nabla)$.

Conjecture 2 (Katz): *Pour toute connexion ∇/K, les K-sous-algèbres de Lie algébriques $courb(\nabla)$ et $gal^K(\nabla)$ de $gl_K(V)$ coïncident.*

Supposons que les p-courbures de ∇ soient presque toutes nulles. Alors, $courb(\nabla) = 0$, et la conjecture 2 prédit que $gal^K(\nabla)$, donc aussi $gal^\omega(\nabla)$, est nul, autrement dit que $Gal^\omega(\nabla)$ est un groupe fini, ou encore que ∇ est isotriviale. La conjecture 0/1 de Grothendieck est donc conséquence de la conjecture 2 de Katz. On trouvera dans les références citées plus haut un tableau de l'état actuel des connaissances sur la question. Pour des constructions plus générales, voir dans le cas linéaire Y. André (Ann. ENS, 34, 2001, 685-739), et, dans le cas non linéaire, B. Malgrange (Ens. math.), A. Pillay, etc.

CHAPITRE IV

LE THÉORÈME DE BOST

Dans [B], J-B. Bost établit un critère général d'algébricité pour les feuilles formelles d'un sous-fibré involutif du fibré tangent d'une variété algébrique, autrement dit pour les sous-variétés intégrales du champ de directions correspondant. Nous nous contenterons dans ce dernier chapitre d'en vérifier la conséquence suivante (cf. chap. 1, thm. 3).

Théorème (Bost): *Soit G un groupe algébrique défini sur un corps de nombres k, d'algèbre de Lie $\mathbf{g}$, et $\mathbf{h}$ une sous-algèbre de Lie de $\mathbf{g}$, définie sur k. Les conditions suivantes sont équivalentes:*

i) $\mathbf{h}$ *est l'algèbre de Lie d'un k-sous-groupe algébrique H de G;*

ii) pour presque toute place v de k, la réduction de $\mathbf{h}$ modulo v est une $p(v)$-sous-algèbre de Lie de la $p(v)$-algèbre de Lie sur $k(v)$ déduite de $\mathbf{g}$ par réduction modulo v.

L'implication $i) \Rightarrow ii)$ est ici encore élémentaire (pour plus de détails sur les p-algèbres de Lie, voir O. Mathieu, Sém. Bourbaki, exp. No 858, 1999). La *démonstration* [B] de l'implication $ii) \Rightarrow i)$ suit la méthode de Chudnovsky et André (cf. chap. 2, thm. 2), mais remplace le principe des tiroirs par l'*inégalité des pentes* de Bost, appliquée au morphisme $\phi_{M,D}$ d'évaluation des sections de la puissance D-ième d'un fibré hermitien ample sur un modèle $\mathbf{G}$ de G sur $Spec\mathcal{O}_k$, en les voisinages infinitésimaux d'ordre M le long de $\mathbf{h}$ de la section neutre de $\mathbf{G}$. Nous la donnons ici dans le formalisme de Chudnovsky-André.

Préparatifs: soient $exp_G : \mathbf{g} \to G$ l'application exponentielle de G, vue comme un morphisme formel au voisinage de l'élément neutre e de G, et τ_P la translation par un point P sur G. Puisque l'adhérence de Zariski du sous-groupe formel $\mathcal{H} = exp_G(\mathbf{h})$ est un sous-groupe algébrique de G, on peut sans perte de généralité supposer $\mathcal{H}$ Zariski-dense dans G, et il s'agit alors de montrer que $\mathcal{H} = G$, i.e., si $d \leq \delta$ désignent les dimensions respectives de $\mathbf{h}$ et de $\mathbf{g}$, que $d = \delta$.

Notons $D_1, ..., D_d$ une base de $\mathbf{h}$ sur k, et $x_1, ..., x_\delta$ des éléments k-algébriquement indépendants de $k(G)$, définis et nuls en e, tels que $D_i = (\frac{\partial}{\partial x_i})_e$ pour $i = 1, ..., \delta$. Alors, $\mathbf{x} = (x_1, ..., x_d)$ définit un paramétrage local de $\mathcal{H}$, et les solutions formelles $\overline{f} = (f_{d+1}, ..., f_\delta) \in k^{\delta-d}[[\mathbf{x}]]$ du système d'EDP: $\forall i = 1, ..., d,\ (\frac{\partial}{\partial x_i})(\mathbf{x}, \overline{f}(\mathbf{x})) \in (\tau_{P(\mathbf{x})})_*(\mathbf{h})$ expriment dans les coordonnées $\mathbf{x}$ la restriction à $\mathcal{H}$ des fonctions rationnelles $x_{d+1}, ..., x_\delta$.

Si v est une place de k de caractéristique $p >> 0$, l'hypothèse $D_i^p \in \mathbf{h} + \mathbf{p}_v$ Lie $\mathbf{G}$ pour tout $i = 1, ..., d$ entraîne que $(\frac{\partial}{\partial x_i})^p(\overline{f}) \in (\mathbf{p}_v.\mathcal{O}_v[[x_1, ..., x_d]])^{\delta - d}$. On en déduit comme au chap. 3, théorème 2, que pour $p >> 0$, les coefficients de $\overline{f}(\mathbf{x}) = \Sigma_{\mathbf{s} \in \mathbf{N}^d} \frac{1}{\mathbf{s}!} \frac{\partial^{|\mathbf{s}|}\overline{f}}{\partial \mathbf{x}^{\mathbf{s}}}(0)\ \mathbf{x}^{\mathbf{s}}$ vérifient:

$$v(\frac{1}{\mathbf{s}!}\frac{\partial^{|\mathbf{s}|}\overline{f}}{\partial \mathbf{x}^{\mathbf{s}}}(0)) \geq \Sigma_{i=1,...,d}([\frac{s_i}{p}] - v(s_i!)) \geq -\frac{|\mathbf{s}|}{p(p-1)}, \qquad (*)$$

et que les coefficients des monômes en les f_j, de degré D arbitraire, vérifient la même inégalité.

On désigne par $c_1, ...$ des nombres réels > 0 ne dépendant que de G, $\mathbf{h}$, k, et du choix des fonctions $x_1, ..., x_\delta$.

Premier pas: Soient $N \geq c_1$ et D deux entiers tels que $\frac{D^\delta}{\delta!} \sim 2[k : \mathbf{Q}]\frac{N^d}{d!}$. Le principe des tiroirs (lemme de Siegel) et les inégalités (*) permettent de construire un polynôme non nul $P_N \in \mathbf{Z}[X_1, ..., X_\delta]$ de degré $\leq D$, de coefficients majorés en valeurs absolues par $exp(c_2 N + o(N))$ tel que la série formelle en d variables $R_N(\mathbf{x}) = P(\mathbf{x}, \overline{f}(\mathbf{x}))$ s'annule à un ordre $\geq N$ en 0.

Deuxième pas: Comme $\mathcal{H}$ est Zariski dense dans G, R_N n'est pas identiquement nulle, et son ordre $M \geq N$ en 0 est fini. Soit $\mathbf{m} = (m_1, ..., m_d)$ un d-uplet de longueur M tel que $\xi := \frac{1}{\mathbf{m}!}\frac{\partial^M}{\partial \mathbf{x}^{\mathbf{m}}}R_N(0) \neq 0$.

Troisième pas: les inégalités (*) et une estimation grossière aux petites places finies de k montrent que $\Sigma_{v \in M_k'} Log||\xi||_v \leq c_3 M + c_4 D$.

Quatrième pas: soit σ un plongement complexe de k. Alors, exp_G^σ est le développement de Taylor de l'application exponentielle du groupe de Lie $G^\sigma(\mathbf{C})$, et pour $\mathbf{z} = (z_1, ..., z_d)$, $\phi(\mathbf{z}) := \mathbf{x} \circ exp_G^\sigma(z_1 D_1 + ... + z_d D_d) \in \mathbf{C}^d[[z_1, ..., z_d]]$ est un difféomorphisme local, qui s'étend en une application méromorphe sur $\mathbf{C}^d$; de même, $f_j(\phi(\mathbf{z})) = x_j(exp_G^\sigma(z_1 D_1 + ... + z_d D_d))$ est, pour tout $j = d+1, ..., \delta$, une fonction méromorphe sur $\mathbf{C}^d$. Notons θ un "dénominateur" commun de ces fonctions valant 1 en 0, et considérons la fonction analytique sur $\mathbf{C}^d$: $F_N(\mathbf{z}) = \theta(\mathbf{z})^D P_N(\phi(\mathbf{z}), \overline{f}(\phi(\mathbf{z}))$. On a $\frac{\partial^M}{\partial \mathbf{x}^{\mathbf{m}}}R_N(0) = \frac{\partial^M}{\partial \mathbf{z}^{\mathbf{m}}}F_N(0)$, et on déduit de Cauchy: $Log|\sigma(\xi)| \leq -M LogR + c_5 N + \chi(R)D + o(N)$ pour tout $R > c_6$, où $\chi(R)$ ne dépend que de R.

Conclusion: chosissons $LogR = 2(c_3 + c_5)$. Les deux derniers pas, combinés à la formule du produit, montrent que pour tout N suffisamment grand, $N \leq M \leq c_7 D < c_8 N^{\frac{d}{\delta}}$. Donc $d \geq \delta$, et $\mathcal{H} = G$.

Remarque: on peut, au moyen d'un *lemme de zéros*, majorer M en fonction de D, et rendre ainsi effective la preuve ci-dessus. Pour une application de ce principe aux théorèmes d'isogénie, voir P. Graftieaux, Duke Math. J., 106, 2000, 81-121.

Bibliographie

[A] Y. André: *G-functions and geometry*; Vieweg, 1989.

[A'] Y. André: *Sur la conjecture des p-courbures de Grothendieck-Katz*; Prépubl. Inst. math. Jussieu, no 134, 0ct. 1997.

[B] J-B. Bost: *Algebraic leaves of algebraic foliations over number fields*; Publ. Math. IHES 93, 2001, 161-221.

[C] A. Chambert-Loir: *Théorèmes d'algébricité en géométrie diophantienne*; Sém. Bourbaki No 886, 2001.

[Ch] D. et G. Chudnovsky: *Padé approximations and diophantine geometry*; Proc. N'al Ac. Sc. USA 82, 1985, 2212-16.

[D] B. Dwork, G. Gerotto, F. Sullivan: *An introduction to G-functions*; Princeton UP, Ann. Math. Study 133, 1994.

[D'] B. Dwork: *On the size of differential modules*; Duke Math. J., 2002.

[K] N. Katz: *Nilpotent connections and the monodromy theorem:... Turrittin*; Publ. Math. IHES 39, 1970, 175-232.

[K'] N. Katz: *A conjecture in the arithmetic theory of differential equations*; Bull. SMF, 110, 1982, 203-239 et 347-8.

Juin 02

D. Bertrand
Institut de Mathématiques de Jussieu
bertrand@math.jussieu.fr