Séminaire Bourbaki — Mars 2001
53$^{\rm e}$ année, 2000-2001, n$^{\rm o}$ 886

THÉORÈMES D'ALGÉBRICITÉ EN GÉOMÉTRIE DIOPHANTIENNE
d'après J.-B. Bost, Y. André, D. & G. Chudnovsky

par **Antoine CHAMBERT-LOIR**

1. INTRODUCTION

1.1. Certains problèmes géométriques ou arithmétiques se ramènent parfois à décider si une fonction analytique, voire une série formelle, est en fait une fonction algébrique, voire même une fraction rationnelle. On peut notamment penser à deux exemples :

1$^{\rm o}$) le problème de Schwarz (cf. [41]) consistant à déterminer les équations différentielles hypergéométriques de Gauß ayant une base de solutions formée de fonctions algébriques ;

2$^{\rm o}$) le théorème de É. Borel [15] affirmant qu'une série entière $f \in \mathbf{Z}[[x]]$ est le développement en série d'une fraction rationnelle si et seulement si c'est le développement de Taylor en l'origine d'une fonction *méromorphe* sur un disque de centre 0 et rayon strictement supérieur à 1. Une généralisation de ce critère a été utilisée par Dwork [21] dans sa démonstration de la rationalité de la fonction zêta d'une variété algébrique sur un corps fini.

Les travaux de D.V. et G.V. Chudnovsky [18] ont montré que les méthodes de transcendance fournissent une approche à ce genre de questions, en même temps qu'à d'autres problèmes a priori plus éloignés telle la conjecture d'isogénie. C'est là le sujet de notre exposé. Nous en donnerons de nombreuses applications, dont certaines remontent d'ailleurs à ces auteurs. Cette technique a toutefois été perfectionnée, notamment par Y. André ([3] et [4]) et, plus récemment, par un article de J.-B. Bost [17] qui fournit un critère permettant d'affirmer que certaines sous-variétés formelles d'une variété algébrique (c'est-à-dire « définies » par des séries formelles plutôt que des polynômes) sont en fait des sous-variétés algébriques. Celui-ci est écrit dans le langage de la géométrie d'Arakelov et j'espère convaincre le lecteur qu'elle fournit un cadre géométrique efficace pour les démonstrations d'approximation diophantienne.

Les théorèmes antérieurs des Chudnovsky et André (voir notamment [18, 3, 4]) établissaient l'algébricité d'une série formelle et les conséquences géométriques étaient alors obtenues après dévissage. Les résultats de Bost généralisent aussi un théorème de Graftieaux (voir [27, 28]) concernant les sous-groupes formels d'une variété abélienne, tout en en simplifiant notablement la démonstration.

1.2. Quel que soit le langage utilisé (approximation diophantienne classique, géométrie d'Arakelov,...), la « méthode de Chudnovsky » repose sur des techniques utilisées en théorie des nombres transcendants ; elle combine en effet des hypothèses de type arithmétique (contrôle des dénominateurs) et des hypothèses de type analytique (uniformisation).

L'irruption de l'arithmétique dans ces questions n'est pas nouvelle mais remonte — au moins — à la communication [23] d'Eisenstein où ce dernier établit le théorème suivant : *soit* $y = \sum_{n=0}^\infty a_n x^n \in \mathbf{Q}[[x]]$ *le développement en série de Taylor en l'origine d'une fonction algébrique. Alors, il existe un entier* $A \geqslant 1$ *tel que, pour tout entier* $n \geqslant 0$, $a_n A^{n+1}$ *est entier.* En particulier, les nombres premiers qui divisent les dénominateurs des rationnels a_n sont en nombre fini. Une conséquence immédiate de ce résultat, citée d'ailleurs par Eisenstein, est la transcendence des fonctions logarithme ou exponentielle, « mais aussi de beaucoup d'autres. »

1.3. Comme il m'est impossible de donner un aperçu des méthodes et des résultats en théorie des nombres transcendants, je me vois obligé de renvoyer le lecteur à l'immense littérature sur le sujet, à laquelle le petit ouvrage collectif [8] peut être une bonne introduction, quoiqu'un peu ancienne. Rappelons simplement que, classiquement, une « démonstration de transcendance » met successivement en jeu quatre ingrédients : on raisonne par l'absurde, puis

1°) on construit une *fonction auxiliaire* à l'aide du *lemme de Siegel* : celui-ci fournit à un système sous-déterminé d'équations linéaires à coefficients entiers une solution entière de petite taille, mais *non nulle*. L'*évaluation* de cette fonction auxiliaire fournit un entier ξ sur lequel va porter la contradiction ;

2°) un certain nombre d'estimations de nature analytique, telles que le *lemme de Schwarz* et l'inégalité d'Hadamard majorent $|\xi|$;

3°) le fait (trivial) qu'un entier non nul est de valeur absolue supérieure ou égale à 1 implique, si la majoration précédente est assez bonne, que $\xi = 0$. Dans les corps de nombres, ce principe est remplacé par la *formule du produit* ;

4°) un *lemme de zéros*, de nature généralement algébro-géométrique, montre qu'alors la fonction auxiliaire initiale est nulle, d'où la contradiction.

Cependant, la méthode des *déterminants d'interpolation* introduite par M. Laurent, cf. [36], ne fait pas intervenir le lemme de Siegel. En fait, plutôt que sur une solution du système linéaire, on peut raisonner directement sur les mineurs de sa matrice.

1.4. La *méthode des pentes*, introduite par Bost à propos d'un théorème de Masser et Wüstholz (voir l'exposé [16] à ce séminaire) est une version géométrique « intrinsèque » des déterminants d'interpolation. Sa formulation nécessite le langage de la géométrie d'Arakelov.

Plaçons-nous pour l'instant dans le cas le plus simple où les objets sont des réseaux euclidiens $\overline{E} = (E, q_E)$, où E est un $\mathbf{Z}$-module libre de rang fini et q_E une forme quadratique définie positive sur $E_{\mathbf{R}} = E \otimes_{\mathbf{Z}} \mathbf{R}$. À un tel objet, on peut associer un nombre réel $\widehat{\deg}\, \overline{E}$, son *degré arithmétique*, qui n'est autre que l'opposé du logarithme du covolume de E dans $E_{\mathbf{R}}$. En d'autres termes, $(e_1, \dots, e_d)$ est une $\mathbf{Z}$-base de E,

$$\widehat{\deg}\, \overline{E} = -\frac{1}{2} \log \det \big(q_E(e_i, e_j)\big)_{1 \leqslant i,j \leqslant d}. \tag{1.4.1}$$

On définit ensuite sa *pente* qui est tout simplement son degré divisé par son rang :

$$\mu(\overline{E}) = \widehat{\deg}\, \overline{E} / \operatorname{rang} E.$$

Dans ce contexte, on a aussi une notion de polygone de Harder-Narasimhan (cf. [46, 29, 16]) mais ne nous intéressera ici que sa *plus grande pente*, $\mu_{\max}(\overline{E})$: c'est le maximum des pentes des sous-réseaux de $\overline{E}$, c'est-à-dire des réseaux $\overline{F} = (F, q_E|_F)$ où F est un sous-$\mathbf{Z}$-module non nul de E.

Étant donnés deux tels réseaux euclidiens $\overline{E}$ et $\overline{F}$, un homomorphisme $\varphi \colon E \to F$ possède une *hauteur*, le logarithme de la norme de l'homomorphisme d'espaces euclidiens induit :

$$h(\varphi) = \log \|\varphi\| = \frac{1}{2} \log \sup_{e \in E_{\mathbf{R}} \setminus \{0\}} \frac{q_F(\varphi(e))}{q_E(e)}.$$

Si φ est *injectif*, on a alors une inégalité, dite *inégalité de pentes* :

$$\mu(\overline{E}) \leqslant \mu_{\max}(\overline{F}) + h(\varphi). \tag{1.4.2}$$

C'est essentiellement une reformulation de l'inégalité d'Hadamard. Le mérite de cette inégalité est de synthétiser les différentes étapes d'une preuve de transcendance : si le lemme de Siegel disparaît (en apparence seulement, voir plus bas), les estimées analytiques interviennent dans la majoration de $h(\varphi)$. Quand l'inégalité obtenue est absurde, le morphisme φ ne peut pas être injectif, et là intervient éventuellement le lemme de zéros.

1.5. Expliquons maintenant pourquoi, joint au théorème de Minkowski, le lemme de Siegel est, à des facteurs numériques près, un corollaire de l'inégalité de pentes (1.4.2). *Soit donc $\Phi = (a_{ij})$ une matrice à coefficients entiers à r lignes et n colonnes, avec $n > r$. Si $A = \max |a_{i,j}|$, le lemme de Siegel classique affirme qu'il existe un élément non nul $\mathbf{x} = {}^{\mathrm{t}}(x_1, \dots, x_n) \in \mathbf{Z}^n$ tel que $\Phi \cdot \mathbf{x} = 0$ et $|x_i| \leqslant (nA)^{r/(n-r)}$ pour tout $i \in \{1; \dots; n\}$.*

Soit alors $\overline{E}$ le réseau $\mathbf{Z}^n$ muni de la forme quadratique $q_E(x_1, \dots, x_n) = \sum_{i=1}^n x_i^2$, soit $\overline{F}$ le réseau analogue de rang r, et soit $\varphi \colon E \to F$ l'homomorphisme défini par la matrice Φ. Comme $n > r$, il n'est pas injectif et son noyau, muni de la norme euclidienne induite, est un sous-réseau saturé $\overline{E}_1$. On définit alors $\overline{E}_2 = \overline{E}/\overline{E}_1$ le réseau quotient, muni de la norme euclidienne quotient. Alors, φ induit un homomorphisme injectif $\varphi_2 \colon \overline{E}_2 \to \overline{F}$, si bien que l'inégalité de pentes (1.4.2) s'écrit

$$\mu(\overline{E}_2) \leqslant \mu_{\max}(\overline{F}) + h(\varphi_2). \tag{1.5.1}$$

Par construction,

$$h(\varphi_2) = h(\varphi) = \frac{1}{2} \log \sup_{\mathbf{x} \in E_{\mathbf{R}} \setminus \{0\}} \frac{q_F(\varphi(\mathbf{x}))}{q_E(\mathbf{x})} \leqslant \log(\sqrt{r} A). \tag{1.5.2}$$

De plus, les covolumes de réseaux sont multiplicatifs dans les suites exactes, donc les degrés arithmétiques sont additifs et

$$\mu(\overline{E}_2) = \operatorname{rang}(E_2)^{-1} \widehat{\deg} E_2 = \operatorname{rang}(E_2)^{-1} (\widehat{\deg} \overline{E} - \widehat{\deg} \overline{E}_1) = -\frac{\operatorname{rang}(E_1)}{\operatorname{rang}(E_2)} \mu(\overline{E}_1) \tag{1.5.3}$$

car $\widehat{\deg} \overline{E} = r \widehat{\deg}(\mathbf{Z}, \|\cdot\|) = 0$. De même, $\widehat{\deg} \overline{F} = 0$ et, plus généralement, le degré de tout sous-réseau de $\overline{F}$ est négatif ou nul : d'après la formule de Gram (cf. la formule (1.4.1)), le carré du covolume d'un tel sous-réseau de $\mathbf{Z}^n$ est en effet un entier non nul, si bien que $\mu_{\max}(\overline{F}) = 0$. Ainsi, utilisant que $d = \operatorname{rang} E_1 \geqslant n - r$, on a

$$\mu(\overline{E}_1) \geqslant -\frac{r}{n-r} \log(A\sqrt{r}) \tag{1.5.4}$$

Écrivons maintenant le théorème de Minkowski : il affirme que *si le volume (dans $E_{1,\mathbf{R}}$) de la boule B_t de rayon t est supérieur ou égal à 2^d fois le covolume de E_1, alors B_t contient au moins un point non nul de E_1*. Notons $\beta_d = \pi^{d/2}/\Gamma(d/2)$ le volume de la boule unité euclidienne en dimension d. Retranscrit en termes de pentes, le théorème de Minkowski affirme l'existence d'un point non nul $\mathbf{x} \in E_1$ tel que $q_E(\mathbf{x}) \leqslant t^2$ dès que

$$\mu(\overline{E}_1) \geqslant -\log t + \log(2\beta_d^{-1/d}). \tag{1.5.5}$$

Ainsi, il existe une solution non nulle $\mathbf{x} = {}^{\mathrm{t}}(x_1, \dots, x_n) \in \mathbf{Z}^n$ au système $\Phi \cdot \mathbf{x} = 0$ vérifiant

$$\|\mathbf{x}\| = \Big(\sum_{i=1}^n x_i^2\Big)^{1/2} \leqslant \big(A\sqrt{r}\big)^{r/(n-r)} 2\beta_d^{-1/d}. \tag{1.5.6}$$

De plus, la formule de Stirling montre que lorsque d tend vers $+\infty$,

$$2\beta_d^{-1/d} \simeq \sqrt{2d/e}.$$

1.6. Dans le même volume que celui où est publié [18], les Chudnovsky utilisent des techniques similaires pour débuter la théorie arithmétique des G-fonctions de Siegel, introduites dans [43]. Faute de place, nous ne dirons rien de cette théorie qui pourtant a vu récemment quelques développement majeurs, suite notamment aux travaux de Bombieri [13] et André. Citons ainsi une théorie géométrique des opérateurs différentiels de type G (André, Baldassarri [7]) ainsi que la généralisation en dimension supérieure, due à L. Di Vizio [20], du théorème des Chudnovsky affirmant qu'un opérateur différentiel minimal annulant une G-fonction est un G-opérateur. Enfin, signalons deux articles récents d'André [5, 6] consacrés à une « théorie Gevrey arithmétique » dont le théorème de Chudnovsky évoqué est un outil essentiel. Il en déduit de remarquables applications, par exemple une nouvelle preuve du théorème de Siegel-Shidlovsky et, inspiré par la preuve de Bézivin-Robba [10], deux (!) du théorème de Lindemann-Weierstraß.

Je remercie Y. André, D. Bertrand, J.-B. Bost et Y. Laszlo pour l'aide qu'ils m'ont apportée pendant la préparation de cet exposé. Je remercie aussi C. Gasbarri et A. Thuillier pour leur lecture attentive.

2. QUATRE THÉORÈMES

2.1. Les énoncés que nous présentons maintenant font intervenir des objets algébro-géométriques définis sur un corps de nombres (nombres, variétés algébriques, équations différentielles, sous-algèbres de Lie, etc.) vérifiant une propriété modulo p pour presque tout nombre premier p. Le sens de ce genre d'hypothèses est le suivant. Soit K un corps de nombres et soit $\mathfrak{o}_K$ son anneau d'entiers. Un objet algébro-géométrique sur K « de type fini » est défini par une famille finie d'éléments de K (par exemple, dans le cas d'une variété algébrique, les coefficients des équations polynomiales qui la définissent) ; ces éléments ont un dénominateur commun $D \in \mathbf{Z}$, si bien qu'en fait l'objet initial « vit » naturellement sur l'anneau $\mathfrak{o}_K[1/D]$. Il y a bien sûr des choix mais étant données deux structures entières sur $\mathfrak{o}_K[1/D]$ et $\mathfrak{o}_K[1/D']$, il existera un multiple commun à D et D', soit D'', tel que les structures entières coïncident, une fois regardées sur $\mathfrak{o}_K[1/D'']$. C'est bien sûr dans le langage des *schémas* que de telles considérations trouvent leur place naturelle.

Les idéaux maximaux d'un tel anneau $\mathfrak{o}_K[1/D]$ s'identifient naturellement à une partie de complémentaire fini de l'ensemble des idéaux maximaux de $\mathfrak{o}_K$ (ceux qui ne contiennent pas D). Réduire modulo p pour presque tout p signifie que, pour tout idéal maximal $\mathfrak{p}$ de $\mathfrak{o}_K[1/D]$ (sauf peut-être un nombre fini d'entre eux), on considère la structure entière modulo l'idéal $\mathfrak{p}$. On obtient ainsi une structure algébrique analogue à celle de départ, mais sur un corps fini. C'est sur ces structures « modulo p » que portent les hypothèses des théorèmes.

Nous donnerons volontairement les énoncés dans ce style informel, en en indiquant juste après la signification précise.

2.2. Théorème. — *Soit α un nombre algébrique tel que pour presque tout nombre premier p, la réduction modulo p de α est dans le sous-corps premier $\mathbf{F}_p$. Alors, α est un nombre rationnel.*

Autrement dit, α est un élément d'un corps de nombres K. Écrivons le β/D où D est un entier $\geqslant 1$ et β un entier algébrique. L'hypothèse signifie que pour presque tout idéal maximal $\mathfrak{p}$ de $\mathfrak{o}_K$, il existe un élément $n_\mathfrak{p} \in \mathbf{Z}$ tel que $\beta \equiv n_\mathfrak{p} D \pmod{\mathfrak{p}}$. La conclusion est alors que $\beta \in \mathbf{Z}$.

Ce résultat apparaît dans l'article [35] de Kronecker qui le dérive du comportement du logarithme de la fonction zêta de Dedekind du corps $\mathbf{Q}(\alpha)$ en $s = 1$.(1) Aujourd'hui, il apparaît souvent comme une conséquence du théorème de densité de Čebotarev. En lien avec le théorème 2.6 ci-dessous, les

(1)L'argument de Kronecker semble cependant incomplet. L'existence d'une densité de certains ensembles de nombres premiers, aujourd'hui conséquence du théorème de Čebotarev, est en effet utilisée sans justification.

Chudnovsky en fournissent une démonstration « diophantienne » dans [18], c'est-à-dire fondée sur les méthodes introduites par la théorie des nombres transcendants.

2.3. Théorème. — *Soit E et E' deux courbes elliptiques sur $\mathbf{Q}$. Alors, E et E' sont isogènes sur $\mathbf{Q}$ si et seulement si, pour presque tout nombre premier p, E et E' ont le même nombre de points sur $\mathbf{F}_p$.*

Donnons là encore une interprétation naïve : partant de deux courbes elliptiques E et E' sur $\mathbf{Q}$ on peut en trouver des équations (affines, sous forme de Weierstraß) $y^2 = 4x^3 + ax + b$ et $y^2 = 4x^3 + a'x + b'$, avec a, b, a', b' dans $\mathbf{Z}$. Pour tout nombre premier p sauf 2, 3 et ceux qui divisent le produit des discriminants $4a^3 + 27b^2$ et $4a'^3 + 27b'^2$, ces équations définissent des courbes elliptiques E_p et E'_p sur le corps fini $\mathbf{F}_p$.

Une $\mathbf{Q}$-isogénie entre E et E', c'est-à-dire en l'occurrence un morphisme non constant défini sur $\mathbf{Q}$ fournira pour tous ces nombres premiers (sauf quelques-uns, peut-être) une isogénie entre les courbes elliptiques E_p et E'_p. Il est alors connu que E_p et E'_p ont même nombre de points sur $\mathbf{F}_p$. La réciproque est le point difficile.

Démontré par Serre [42] si l'un des invariants $j(E)$ et $j(E')$ n'est pas entier, c'est un cas particulier du « théorème d'isogénie de Faltings », cf. [25], lequel fournit un énoncé analogue pour deux variétés abéliennes définies sur un corps de nombres. Dans [18], les Chudnovsky avaient donné une démonstration diophantienne du théorème 2.3. Cependant, leur démonstration nécessitait en outre le théorème de Cartier et Honda [30] reliant la fonction zêta de Hasse-Weil d'une $\mathbf{Q}$-courbe elliptique et le groupe formel de son modèle de Néron sur $\mathbf{Z}$. Dans [27], Graftieaux a donné une démonstration analogue du théorème d'isogénie pour les variétés abéliennes à multiplication réelle définies sur $\mathbf{Q}$. Cette preuve nécessite une généralisation du théorème de Cartier et Honda, démontrée par Deninger et Nart dans [19], qui fournit un isomorphisme entre les groupes formels des variétés abéliennes en question. Graftieaux démontre ensuite l'algébricité de cet isomorphisme, autrement dit l'algébricité du graphe, lequel est un sous-groupe formel du produit des deux variétés abéliennes. Graftieaux a ensuite établi dans [28] un critère général d'algébricité de sous-groupes formels d'une variété abélienne définie sur un corps de nombres. Ses résultats sont de plus effectifs : les hypothèses ne font intervenir qu'un nombre fini explicite de nombres premiers.

Plus généralement, on a le théorème suivant, dû à Bost.

2.4. Théorème. — *Soit G un groupe algébrique défini sur un corps de nombres K, soit $\mathfrak{g}$ son algèbre de Lie. Soit $\mathfrak{h}$ une sous-K-algèbre de Lie de $\mathfrak{g}$ vérifiant la propriété suivante : pour presque tout nombre premier p, la réduction de $\mathfrak{h}$ modulo p est une p-algèbre de Lie. Alors, il existe un sous-groupe algébrique H de G, défini sur K, dont $\mathfrak{h}$ est l'algèbre de Lie.*

L'ingrédient nouveau est la notion de p-algèbre de Lie. Si G est un groupe algébrique lisse sur un corps k, son algèbre de Lie $\mathfrak{g}$ est par définition le k-espace vectoriel des dérivations invariantes par translations sur G, muni du crochet $[D_1, D_2] = D_1D_2 - D_2D_1$. En effet, si D_1 et D_2 sont deux dérivations invariantes, leur commutateur en est encore une. De plus, si k est de caractéristique $p > 0$ et si D est une dérivation invariante, la formule du binôme montre que, pour tous germes de fonctions f et g, on a

$$D^p(fg) = \sum_{i=0}^{p} \binom{p}{i} D^i(f) D^{p-i}(g) = gD^p(f) + fD^p(g),$$

si bien que D^p est encore une dérivation. Cette opération de puissance p-ième donne naissance à la notion de p-algèbre de Lie, cf. [31], 5.7, [14], 1.3 ainsi que l'exposé [37] à ce séminaire. Étant donnée une telle p-algèbre de Lie $\mathfrak{g}$, une sous-p-algèbre de Lie est alors une sous-algèbre de Lie $\mathfrak{h}$ telle que pour tout $D \in \mathfrak{h}$, $D^p \in \mathfrak{h}$.

L'explicitation du « modulo p » se fait alors comme précédemment. Si $\mathfrak{o}_K$ est l'anneau des entiers de K, il existe un entier $N \geqslant 1$ et un schéma en groupes lisse $\mathscr{G}$ sur $\operatorname{Spec} \mathfrak{o}_K[1/N]$ dont la fibre générique $\mathscr{G} \otimes K$ est G. Son algèbre de Lie $\operatorname{Lie}(\mathscr{G})$ est une $\mathfrak{o}_K[1/N]$-algèbre de Lie telle que $\operatorname{Lie}(\mathscr{G}) \otimes K = \mathfrak{g}$. Pour tout idéal maximal $\mathfrak{p}$ de $\mathfrak{o}_K$ ne contenant pas N, on dispose alors d'un groupe algébrique lisse sur le corps fini $\mathbf{F}_\mathfrak{p} = \mathfrak{o}_K/\mathfrak{p}$ dont l'algèbre de Lie n'est autre que $\mathrm{Lie}(\mathscr{G}) \otimes \mathbf{F}_\mathfrak{p}$. Si l'on note p la caractéristique du corps $F_\mathfrak{p}$, c'est en particulier une p-algèbre de Lie.

Quitte à remplacer l'entier N par un multiple, une sous-algèbre de Lie $\mathfrak{h}$ de $\mathfrak{g}$ définit de même une sous-algèbre de Lie de $\mathrm{Lie}(\mathscr{G})$, et par conséquent, par réduction modulo $\mathfrak{p}$, des sous-algèbres de Lie de $\mathrm{Lie}(\mathscr{G}) \otimes \mathbf{F}_\mathfrak{p}$. L'hypothèse est donc que pour presque tout idéal maximal $\mathfrak{p}$, ces sous-algèbres de Lie sont des sous-p-algèbres de Lie.

2.5. Le théorème 2.4 est démontré par Bost dans [17]. Il avait été indépendamment conjecturé par Ekedahl et Shepherd-Barron dans leur article [24]. Il n'est peut-être pas inutile d'expliquer en quoi les deux théorèmes 2.2 et 2.3 en sont des cas particuliers.

2.5.1. Théorème de Kronecker. — Considérons le groupe algébrique $G_k = \mathbf{G}_m \times \mathbf{G}_m$ sur un corps k. On note x et y les coordonnées sur les deux produits, l'élément neutre étant $(1,1)$. Alors, une base de l'algèbre de Lie $\mathfrak{g}_k$ de G_k est constituée des champs de vecteurs $x\frac{\partial}{\partial x}$ et $y\frac{\partial}{\partial y}$. et $\mathfrak{g}_k$ est la k-algèbre de Lie commutative k^2.

Si k est de caractéristique positive p, déterminons l'opération de puissance p-ième sur $\mathfrak{g}_k$. Il suffit de la calculer dans le cas de $\mathbf{G}_m$, auquel cas on a

$$(x\frac{\partial}{\partial x})^p = x\frac{\partial}{\partial x}. \tag{2.5.2}$$

En effet, $x\frac{\partial}{\partial x}$ est l'unique dérivation invariante sur $\mathbf{G}_m$ qui envoie sur elle-même la fonction régulière x. Ainsi, utilisant le fait que l'algèbre de Lie de $(\mathbf{G}_m)^2$ est commutative,

$$(ax\frac{\partial}{\partial x} + by\frac{\partial}{\partial y})^p = a^p x\frac{\partial}{\partial x} + b^p y\frac{\partial}{\partial y}.$$

Pour établir le théorème 2.2, considérons un élément α d'un corps de nombres K et soit G le groupe $\mathbf{G}_m \times \mathbf{G}_m$ sur K, d'algèbre de Lie $\mathfrak{g} = K^2$. La droite $\mathfrak{h} = (1,\alpha)K$ est une sous-algèbre de Lie. Soit $\mathfrak{p}$ un idéal maximal de $\mathfrak{o}_K$ tel que α soit $\mathfrak{p}$-entier. La réduction modulo $\mathfrak{p}$ de $\mathfrak{h}$ est la sous-algèbre de Lie de $\mathfrak{h}_\mathfrak{p}$ engendrée par $(1, \alpha \mod \mathfrak{p})$ dans $(\mathfrak{o}_K/\mathfrak{p})^2$. C'est une sous-$p$-algèbre de Lie si et seulement si $(1^p, (\alpha \mod \mathfrak{p})^p)$ est colinéaire à $(1, \alpha \mod \mathfrak{p})$, c'est-à-dire si et seulement si $\alpha^p = \alpha \pmod{\mathfrak{p}}$, ou encore si $\alpha \mod \mathfrak{p}$ est dans le corps premier $\mathbf{F}_p$. Par suite, sous l'hypothèse du théorème de Kronecker, l'algèbre de Lie $\mathfrak{h}$ est l'algèbre de Lie d'un K-sous-groupe algébrique H de $\mathbf{G}_m \times \mathbf{G}_m$. Or, ceux-ci sont définis par une équation de la forme $x^m = y^n$ pour deux entiers m et n. L'algèbre de Lie d'un tel H est la droite d'équation $m\xi = n\eta$ dans le plan K^2 de coordonnées (ξ,η), donc est engendrée par le vecteur (n,m). On a ainsi $\alpha = m/n$.

2.5.3. Théorème d'isogénie. — Pour commencer, soit E une courbe elliptique sur un corps k. Son algèbre de Lie est une k-algèbre de Lie de dimension 1, bien entendu commutative. De plus, on a une identification canonique $\mathrm{Lie}(E) = H^1(E, \mathscr{O}_E)$. Si k est de caractéristique positive p, l'opération de puissance p-ième sur $\mathrm{Lie}(E)$ se confond alors avec l'action du morphisme dit « Frobenius absolu » $F\colon E \to E$. Supposons de plus que k est le corps premier $\mathbf{F}_p$. Alors, F induit un endomorphisme p-linéaire, donc linéaire, de $H^1(E, \mathscr{O}_E)$; c'est ainsi une homothétie dont nous noterons $A \in \mathbf{F}_p$ le rapport (*invariant de Hasse*). On sait d'autre part depuis Hasse qu'il existe deux entiers algébriques α et β tels que $\#E(\mathbf{F}_p) = p+1-(\alpha+\beta)$ et $\alpha\beta = p$. De plus, modulo p, l'un des deux, disons α, s'interprète comme l'action de l'endomorphisme F sur $\mathrm{Lie}\, E$, tandis que β correspond à l'action du Verschiebung (défini par $FV = p$), c'est-à-dire A. Par suite $\#E(\mathbf{F}_p) \equiv 1 - A$ modulo p.

Plaçons-nous maintenant sous les hypothèses du théorème 2.3 et considérons le groupe algébrique $G = E \times E'$ sur $\mathbf{Q}$, d'algèbre de Lie $\mathfrak{g} = \mathrm{Lie}(E) \oplus \mathrm{Lie}(E')$. Soit $\mathfrak{h} \subset \mathfrak{g}$ une droite arbitraire se projetant surjectivement sur les deux facteurs. L'hypothèse que E et E' ont, pour presque tout nombre premier

p, même nombre de points modulo p implique que, modulo p pour presque tout p, $\mathfrak{h}$ définit une sous-p-algèbre de Lie de la réduction modulo p de $\mathfrak{g}$. C'est ainsi l'algèbre de Lie d'un sous-groupe algébrique $H \subset E \times E'$ défini sur $\mathbf{Q}$. Or, un tel sous-groupe fournit automatiquement une isogénie entre E et E' (considérer par exemple H comme une correspondance).

2.6. THÉORÈME. — *Soit X une variété algébrique lisse définie sur un corps de nombres et soit ω une forme différentielle sur X. On suppose que pour presque tout nombre premier p, ω est modulo p une forme différentielle exacte ($\omega = \mathrm{d}f$). Alors, ω est une forme différentielle exacte.*

On a un résultat similaire dans le cas logarithmique : si pour presque tout nombre premier p, ω est modulo p une forme logarithmique exacte ($\omega = \mathrm{d}\log f = \mathrm{d}f/f$), alors, il existe un entier $n \geqslant 1$ tel que $n\omega$ est une forme différentielle logarithmiquement exacte.

Ce théorème est démontré par André [3] dans le premier cas et par les Chudnovsky dans [18] dans le cas logarithmique. Il était conjecturé dans le premier cas par Ogus dans [39, §2] et, en liaison avec la conjecture de Grothendieck, par Katz dans [33, p. 2] pour le cas logarithmique.

Comme exemple d'application, montrons comment en déduire le théorème 2.2. Considérons la courbe $X = \mathbf{G}_m = \operatorname{Spec} K[x, x^{-1}]$ sur un corps de nombres K, et, si $\alpha \in K$, posons $\omega = \alpha x^{-1}\mathrm{d}x$. Si $\mathfrak{p}$ est un idéal maximal de $\mathfrak{o}_K$ et $n_\mathfrak{p} \in \mathbf{Z}$ un entier tel que $\alpha - n_\mathfrak{p} \in \mathfrak{p}$, ω modulo $\mathfrak{p}$ est égale à $n_\mathfrak{p} x^{-1}\mathrm{d}x$, donc est la différentielle logarithmique de $x^{n_\mathfrak{p}}$. D'après le théorème 2.6, il existe $n \geqslant 1$ tel que $n\alpha x^{-1}\mathrm{d}x$ est une forme différentielle logarithmiquement exacte, c'est-à-dire $n\alpha \in \mathbf{Z}$, d'où $\alpha \in \mathbf{Q}$.

Sur la droite projective, le théorème 2.6 admet le corollaire suivant : *soit $y \in \mathbf{Z}[[x]]$ une série formelle à coefficients entiers dont la dérivée est une fonction algébrique, alors y est une fonction algébrique.* La variante de cet énoncé où algébrique est remplacé par *rationnelle* a été démontrée par Pólya ; c'est une application classique du théorème de Borel [15]. Signalons d'ailleurs que ce critère a été généralisé par Bézivin et Robba dans [11] au cas d'opérateurs différentiels d'ordre supérieur. Cette généralisation leur a permis d'en déduire une nouvelle démonstration du théorème de Lindemann-Weierstrass.

F. Caligari en a donné une application aux courbes modulaires : joint au théorème de Manin-Drinfel'd, il implique en effet qu'une forme modulaire (non nécessairement cuspidale) de poids 2 qui pour presque tout nombre premier p est fixée par l'opérateur T_p modulo p est une combinaison linéaire de séries d'Eisenstein.

3. LA CONJECTURE DE GROTHENDIECK

3.1. La *conjecture de Grothendieck* est un critère arithmétique qui prédit qu'un système différentiel linéaire, disons de la forme

$$\frac{\mathrm{d}}{\mathrm{d}z}Y = A(z)Y, \qquad A(z) \in M_d(\mathbf{Q}(z)) \tag{3.1.1}$$

possède une base de solutions algébriques, c'est-à-dire dont les solutions holomorphes au voisinage d'un point $z_0 \in \mathbf{Q}$ qui n'est pas un pôle de A sont algébriques sur $\mathbf{Q}(z)$. La condition, conjecturalement suffisante, est que pour presque tout nombre premier p, le système différentiel obtenu par réduction modulo p ait une base de solutions algébriques sur $\mathbf{F}_p(z)$.

Le point fondamental, dû à Cartier et Honda, est que cette dernière condition est, pour p un nombre premier fixé, effectivement vérifiable. Pour rester élémentaire, définissons une suite (A_n) de matrices $n \times n$ à coefficients dans $\mathbf{Q}(z)$ par

$$A_0(z) = I_d, \quad A_1(z) = A(z), \quad A_{n+1}(z) = \frac{\mathrm{d}}{\mathrm{d}z}A_n(z) + A_n(z)A(z). \tag{3.1.2}$$

Si l'on peut réduire A modulo p, alors on a l'équivalence des propositions suivantes :

– le système différentiel (3.1.1) modulo p admet une base de solutions algébriques sur $\mathbf{F}_p(z)$;
– il admet une base de solutions dans $\mathbf{F}_p(z)$;
– il admet une base de solutions dans $\mathbf{F}_p((z))$;
– la matrice de « p-courbure » A_p est nulle modulo p.

Sous cette forme, cet énoncé est assez élémentaire. Si $Y(z)$ est une solution du système (3.1.1), on vérifie par récurrence que pour tout n, $\frac{\mathrm{d}^n}{\mathrm{d}z^n}Y(z) = A_n(z)Y(z)$. Si Y est une solution de ce système, par exemple dans $\mathbf{F}_p((z))$, on a $(\mathrm{d}^p/\mathrm{d}z^p)Y(z) = 0$. L'existence d'une *base* de solutions dans $\mathbf{F}_p((z))$ implique alors que $A_p(z) = 0$ modulo p. Dans l'autre sens, supposant pour simplifier que 0 n'est pas une singularité de A, on constate que la formule (de Taylor !)

$$Y(z) = \Big(\sum_{i=0}^{p-1} \frac{(-z)^i}{i!} A_i(z)\Big)^{-1} \tag{3.1.3}$$

fournit une matrice fondamentale de solutions dans $\mathbf{F}_p(z)$.

3.2. Ces considérations s'étendent à un contexte plus général que nous présentons maintenant. Soit X une variété algébrique lisse sur un corps de nombres K et soit E un $\mathscr{O}_X$-module localement libre de rang fini. Une connexion sur E est une application K-linéaire

$$\nabla \colon E \to E \otimes_{\mathscr{O}_X} \Omega^1_X \tag{3.2.1}$$

vérifiant $\nabla(fe) = f\nabla(e) + e \otimes \mathrm{d}f$ pour toutes sections locales f de $\mathscr{O}_X$ et e de E. Il sera pratique de considérer l'homomorphisme dual

$$\mathrm{T}X \to \mathit{End}(E), \qquad \partial \mapsto \nabla(\partial), \tag{3.2.2}$$

$\mathrm{T}X$ désignant le fibré tangent de X. On notera aussi E^∇ le faisceau des *sections horizontales* de E, c'est-à-dire des germes de sections locales e de E telles que $\nabla(e) = 0$. Par définition, E est *trivial* s'il est engendré par E^∇ comme $\mathscr{O}_X$-module. On dit aussi que la connexion ∇ est *intégrable* si l'homomorphisme (3.2.2) est un homomorphisme d'algèbres de Lie, c'est-à-dire si pour tous champs de vecteurs locaux ∂_1 et ∂_2,

$$[\nabla(\partial_1), \nabla(\partial_2)] = \nabla([\partial_1, \partial_2]). \tag{3.2.3}$$

C'est bien sûr équivalent au fait que la *courbure* $\psi(E, \nabla) = \nabla^2 \in \mathrm{End}(E) \otimes \Omega^2_X$ soit nulle.

Supposons ∇ intégrable. Si K est un corps de caractéristique positive p, $\mathrm{T}X$ et $\mathit{End}(E)$ sont des p-algèbres de Lie et on définit une *p-courbure* qui mesure le défaut pour l'homomorphisme (3.2.2) d'être un homomorphisme de p-algèbres de Lie :

$$\psi_p \colon \mathrm{T}_X \to \mathit{End}(E), \qquad \partial \mapsto \nabla(\partial)^p - \nabla(\partial^p). \tag{3.2.4}$$

C'est une application additive, p-linéaire :

$$\psi_p(f_1\partial_1 + f_2\partial_2) = f_1^p\psi_p(\partial_1) + f_2^p\psi_p(\partial_2).$$

Le théorème de Cartier affirme alors l'équivalence des propriétés suivantes (cf. [32], théorème 5.1) :

– pour toute section locale ∂ de $\mathrm{T}X$, $\psi_p(\partial) = 0$;
– l'homomorphisme (3.2.2) est un homomorphisme de p-algèbres de Lie ;
– le faisceau E est trivial.

3.3. Conjecture (Grothendieck). — *Soit X une variété lisse sur un corps de nombres K et (E, ∇) un module à connexion intégrable sur X. On suppose que pour presque tout nombre premier p, la réduction modulo p de (E, ∇) est à p-courbure nulle. Alors, il existe un revêtement étale $f \colon Y \to X$ tel que f^*E soit trivial.*

La condition pour un module à connexion intégrable (E, ∇) d'avoir (presque toutes) ses p-courbures nulles a été étudiée de manière approfondie par Katz. En particulier, il est établi dans [32] qu'alors, (E, ∇) est à singularités régulières et ses exposants sont des nombres rationnels, ce qui n'est d'ailleurs pas sans rapport avec le théorème 2.2 (voir aussi [22], III.6.1).

Il y a eu essentiellement deux approches de cette conjecture, l'une géométrique, l'autre arithmétique. Rappelons que les périodes d'une famille de variétés algébriques lisses sont gouvernées par une équation différentielle, dite de Picard-Fuchs. Pour celles-ci, et plus généralement, pour leurs facteurs, Katz [33] puis André [4] relient les p-courbures à la réduction modulo p de l'application de Kodaira-Spencer. C'est ainsi qu'est établie la conjecture de Grothendieck pour les équations hypergéométriques de Gauß (on retrouve la liste de Schwarz) ou les facteurs des connexions de Knizhnik-Zamolodchikov. L'approche arithmétique est au cœur de cet exposé. Elle a permis d'établir la conjecture pour les fibrés de rang 1 sur une courbe (Chudnovsky [18], le cas où E est trivial a été vu plus haut), lorsque (E, ∇) est extension de deux modules à connexion isotriviaux (André, [4]), et plus généralement, lorsque le *groupe de Galois différentiel* de (E, ∇) a une composante neutre résoluble (André, voir plus bas).

Le groupe de Galois différentiel « générique » d'un module à connexion (E, ∇) est défini par Katz dans [34] (voir aussi l'exposé [9] de Bertrand à ce séminaire). Sa définition la plus élégante est tannakienne et fournit un groupe algébrique sur le corps $K(X)$ des fonctions de X : c'est le sous-groupe de $\mathrm{GL}(E \otimes K(X))$ qui stabilise tout sous-module horizontal de toute construction tensorielle sur (E, ∇). Dans le cas singulier régulier, qui est en fin de compte celui qui nous importe le plus pour la conjecture de Grothendieck, on peut décrire peut-être plus concrètement une $\mathbf{C}$-forme de ce groupe. Étant donné un plongement de K dans $\mathbf{C}$, on peut considérer (E, ∇) comme un module à connexion intégrable sur la variété analytique $X(\mathbf{C})$. Le groupe de Galois différentiel « est » alors l'adhérence de Zariski du groupe de monodromie usuel de (E, ∇) ([34], Prop. 5.2). Dans tous les cas ([34], Prop. 4.5), la finitude du groupe de Galois différentiel de (E, ∇) équivaut à l'isotrivialité de (E, ∇), soit encore à l'existence d'une base de solutions algébriques.

Katz a proposé ([34], Conj. 9.2) une généralisation de la conjecture de Grothendieck et prédit que l'algèbre de Lie du groupe de groupe de Galois différentiel de (E, ∇) est la plus petite sous-algèbre de Lie algébrique de $\mathfrak{gl}(E)$ qui « contient », pour presque tout p, les p-courbures $\psi_p(\partial)$. En fait, et c'est là l'objet principal de l'article [34], cette généralisation et la conjecture de Grothendieck sont équivalentes : la véracité de la conjecture de Grothendieck pour tout fibré à connexion intégrable implique celle de Katz.

Enfin, signalons qu'un « q-analogue » de la conjecture de Grothendieck-Katz (pour les équations aux q-différences) a été démontré par L. Di Vizio dans sa thèse (décembre 2000). La démonstration utilise le théorème 6.2 ci-dessous, l'un des R_v étant infini.

3.4. Exemples. — Revenons maintenant sur le théorème 2.6 concernant l'exactitude de formes différentielles. Soit X une courbe algébrique lisse sur un corps de nombres K et soit $\omega \in \Gamma(X, \Omega^1_X)$ une forme différentielle régulière sur X. On peut considérer deux modules à connexion (nécessairement intégrables puisque X est une courbe) :

$$E_1 = \mathscr{O}_X, \qquad \nabla f = \mathrm{d}f - f\omega \tag{3.4.1}$$

$$E_2 = \mathscr{O}_X^2, \qquad \nabla(f, g) = (\mathrm{d}f - \omega g, \mathrm{d}g). \tag{3.4.2}$$

L'existence d'une section horizontale non nulle de E_1 signifie ainsi exactement que ω est une différentielle logarithmiquement exacte. Si E_2 est engendré par ses sections horizontales, il existe une telle section (f, g) avec $g \neq 0$, donc g constante que l'on peut supposer égale à 1, et alors $\mathrm{d}f = \omega$, ce qui signifie que ω est une différentielle exacte. Dans les deux cas, l'hypothèse du théorème 2.6 sur la réduction modulo p de ω pour presque tout nombre premier p est, d'après le théorème de Cartier, équivalente à la nullité des p-courbures.

D'autre part, la définition même du groupe de Galois différentiel montre que c'est un sous-groupe de $\mathbf{G}_m$ dans le cas de (E_1, ∇), tandis que (E_2, ∇) ayant un sous-fibré horizontal (défini par $q = 0$), son groupe de Galois différentiel est un sous-groupe du groupe de Borel $\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)$. Ces deux groupes algébriques sont en particulier résolubles et résoudre la conjecture de Grothendieck pour les modules à connexion intégrable dont le groupe de Galois est résoluble démontre le théorème 2.6. Réciproquement, si le groupe de Galois différentiel est résoluble, des dévissages ramènent la conjecture de Grothendieck au cas du théorème 2.6, d'où le théorème ([4], §3, voir aussi [17], théorème 2.9) :

3.5. Théorème (André). — *Soit X une variété algébrique lisse sur un corps de nombre et (E, ∇) un fibré vectoriel à connexion intégrable sur X. Si la composante neutre du groupe de Galois différentiel de (E, ∇) est résoluble, alors (E, ∇) vérifie la conjecture de Grothendieck-Katz.*

4. FEUILLETAGES

4.1. Soit X une variété algébrique lisse sur un corps K et soit $F \subset T_X$ un sous-fibré vectoriel de son fibré tangent qui est *involutif*, c'est-à-dire stable par le crochet de Lie sur T_X. Si $K \subset \mathbf{C}$, un tel fibré involutif définit un feuilletage holomorphe sur la variété analytique $X(\mathbf{C})$: il existe dans un voisinage U_x de tout point $x \in X(\mathbf{C})$ une sous-variété analytique $Y \subset U_x$ telle que pour tout $y \in Y$, l'espace tangent $T_y Y$ à Y en y soit égal à $F_y \subset T_y X$ (théorème de Frobenius). Cependant, une telle *feuille* n'est en général pas un germe de sous-variété algébrique.

Si K est de caractéristique 0 et $x \in X(K)$ un point rationnel, la variante formelle du théorème de Frobenius fournit cependant une sous-variété formelle lisse de X complété le long de x, la *feuille formelle de F en x*.

Si K est de caractéristique p, on dira que F est *p-intégrable* si c'est un sous-fibré de $\mathrm{T}X$ stable par puissance p-ième.

Pour motiver cette définition, supposons maintenant que K soit un corps de nombres et que la feuille formelle $\widehat{Y}$ passant par un point rationnel $x \in X(K)$ soit le germe d'une sous-variété algébrique Y. Pour presque tout nombre premier p, on obtient par réduction modulo p une situation analogue (X, F, Y) sur un corps fini de caractéristique p. Comme les opérations de puissance p-ième sur T_Y et sur T_X sont compatibles, il en résulte que F est clos par puissance p-ième aux points de Y.

Réciproquement, la généralisation de la conjecture de Grothendieck aux feuilletages (formulée par Ekedahl et Shepherd-Barron dans [24], conjecture F) prédit que les feuilles formelles d'un tel sous-fibré involutif $F \subset T_X$ qui pour presque tout nombre premier p est p-intégrable sont des sous-variétés algébriques.

Avant d'énoncer le théorème de Bost, quelques rappels d'analyse complexe s'imposent.

4.2. Il est bien connu que toute fonction holomorphe bornée sur l'espace affine $\mathbf{C}^n$ est constante : c'est le théorème de Liouville. Plus généralement, toute fonction *plurisousharmonique* majorée sur $\mathbf{C}^n$ est constante. Rappelons qu'une fonction ψ sur une variété analytique complexe M à valeurs dans $\mathbf{R} \cup \{-\infty\}$ est dite plurisousharmonique si :

– elle est semicontinue supérieurement ;
– elle n'est identiquement $-\infty$ sur aucune composante connexe de M ;
– pour toute fonction holomorphe $f\colon D(0,1) \to M$ du disque unité fermé de $\mathbf{C}$ dans M, on a l'inégalité

$$\psi(f(0)) \leqslant \frac{1}{2\pi} \int_0^{2\pi} \psi(f(e^{\mathrm{i}\theta}))\, \mathrm{d}\theta. \tag{4.2.1}$$

Par exemple, pour toute fonction holomorphe φ non nulle, $\log|\varphi|$ est une fonction plurisousharmonique.

Suivant la terminologie de [17], nous dirons ainsi qu'une variété analytique complexe connexe M vérifie la *propriété de Liouville* si toute fonction plurisousharmonique majorée sur M est constante. Si X est une variété algébrique complexe connexe lisse, on peut démontrer que $X(\mathbf{C})$ satisfait la propriété de Liouville. Dans le cas compact, cela résulte du principe du maximum ; dans le cas général, on peut par exemple remarquer que le complémentaire d'un fermé analytique (strict) dans une variété qui satisfait la propriété de Liouville le satisfait aussi. Tout groupe de Lie complexe connexe vérifie la propriété de Liouville.

4.3. Théorème (Bost). — *Soit X une variété algébrique lisse sur un corps de nombres K contenu dans $\mathbf{C}$, soit F un sous-fibré involutif de $\mathrm{T}X$ et soit $x \in X(K)$ un point rationnel. Supposons que les deux conditions suivantes sont satisfaites :*

– pour presque tout nombre premier p, la réduction modulo p de F est un sous-fibré p-intégrable ;

– il existe une variété analytique complexe M satisfaisant la propriété de Liouville, un point $O \in M$, une application holomorphe ψ de M vers la feuille en x du feuilletage holomorphe induit par F sur $X(\mathbf{C})$ telle que $\psi(O) = x$ et telle que ψ soit biholomorphe d'un voisinage de O vers un voisinage de x dans cette feuille.

Alors, la feuille formelle de F passant par x est algébrique.

4.4. Les équations différentielles issues de fibrés vectoriels à connexion fournissent naturellement des feuilletages. Plus généralement, si G est un groupe algébrique sur un corps de nombres K, un G-fibré principal à connexion sur une K-variété algébrique lisse B est un G-fibré principal $X \to B$ (c'est-à-dire un G-torseur sur B) muni d'un scindage G-équivariant de la suite exacte de G-fibrés vectoriels sur X,

$$0 \to \mathrm{T}_{X/B} \to \mathrm{T}X \to \mathrm{T}B \to 0. \tag{4.4.1}$$

Dans ce cas, l'image de $\mathrm{T}B$ par la section fournit un feuilletage G-équivariant sur X.

À l'aide du théorème 4.3, on peut alors démontrer certains cas de la conjecture de Grothendieck, par exemple le théorème 2.6 ou le théorème 3.5, si l'on établit que la condition d'uniformisation est automatiquement remplie. Après dévissages, le théorème 3.5 se ramène au cas où la base B est une courbe et le groupe G connexe commutatif. Utilisant le morphisme d'addition $G^d \to G$, on peut alors étendre le G-fibré à connexion (X, ∇) sur B, en un autre (X_d, ∇) sur la puissance symétrique d-ième de B (qui contient B une fois fixé un point base). Le point est que pour d assez grand, le revêtement universel d'une telle puissance symétrique vérifie la propriété de Liouville.

4.5. Proposition. — *Soit C une courbe algébrique complexe lisse connexe. Pour tout entier d assez grand, le revêtement universel du produit symétrique $\mathrm{Sym}^d C$ satisfait la propriété de Liouville.*

Soit $\overline{C}$ la complétion projective lisse de C, g son genre et s le cardinal de $S = \overline{C} \setminus C$. Il est démontré dans [17] qu'il suffit de prendre $d \geqslant \max(2, g, g+s-1)$. Cependant, si $d > 2g-2+s$, $\mathrm{Sym}^d C$ est un fibré en espaces affines (projectifs si $s = 0$) au-dessus de la jacobienne généralisée $\mathrm{Jac}_S \overline{C}$ définie par le module S. Son revêtement universel est l'image réciproque par l'application exponentielle $\mathrm{Lie}\,\mathrm{Jac}_S \overline{C} \to \mathrm{Jac}_S \overline{C}$ de ce fibré affine (resp. projectif). Il vérifie la condition de Liouville. Si $S \neq \varnothing$, c'est même l'espace affine de dimension d.

4.6. Dans [38], Miyaoka démontre un théorème d'algébricité pour les feuilles de certains feuilletages algébriques. Il procède essentiellement en *construisant* des courbes rationnelles tangentes au feuilletage. Le point de départ de la démonstration est ainsi l'existence d'une famille dense de courbes le long desquelles le fibré involutif définissant le feuilletage a un degré strictement positif. Les feuilles obtenues sont faiblement rationnellement connexes : deux points quelconques peuvent être reliés par une suite de courbes rationnelles.

Le théorème 4.3 admet un analogue géométrique, découvert très récemment de manière indépendante par Bogomolov et McQuillan [12] d'une part, en liaison avec les travaux de Miyaoka, et par Bost, d'autre part. L'énoncé en est le suivant.

4.7. THÉORÈME. — *Soit k un corps, disons algébriquement clos et soit V_0 une sous-variété connexe projective lisse d'une variété quasi-projective X définie sur k. On suppose que V_0 n'est pas réduite à un point. Soit $\widehat{V}$ une sous-variété formelle lisse du complété formel de X le long de V_0 et contenant V_0.*[2] *On suppose que le fibré normal de V_0 dans $\widehat{V}$, $N_{V_0}\widehat{V}$ est ample. Alors, $\widehat{V}$ est algébrique : l'adhérence de Zariski de $\widehat{V}$ dans X a même dimension que $\widehat{V}$.*

Autrement dit, il existe une sous-variété algébrique Y de X contenant V_0 dont $\widehat{V}$ est l'une des « branches » le long de V_0.

La démonstration est étonnamment simple et, après tout, l'idée n'est pas si différente de celle qui conduira à la démonstration du théorème 4.3. Précisons un peu les analogies entre ces deux théorèmes. Dans le théorème 4.3, il faut interpréter la variété X sur le corps de nombres K comme un germe de variété $\mathscr{X}$ au-dessus de la « courbe arithmétique » Spec $\mathfrak{o}_K$. Le point rationnel x fournit alors une section, c'est-à-dire quelque chose comme une courbe tracée sur $\mathscr{X}$ qui est l'analogue arithmétique de la sous-variété V_0 du théorème 4.7. Dans le théorème 4.3, l'algébricité de la feuille est plus simple à concevoir : dans ce cas, il existe effectivement une variété algébrique dont le complété formel en x s'identifie à la feuille formelle passant par x.

Remplaçons X par l'adhérence de Zariski de $\widehat{V}$, c'est-à-dire la plus petite sous-variété algébrique contenant V_0 et dont le complété formel le long de V_0 contient $\widehat{V}$. Notons $N = N_{V_0}\widehat{V}$, $v_0 = \dim V_0$ et $v = \dim \widehat{V} = v_0 + \operatorname{rang} N$, de sorte que la conclusion du théorème est que $v = \dim X$. Soit L la restriction à X du fibré en droites $\mathscr{O}(1)$ sur l'espace projectif. L'hypothèse que X est l'adhérence de Zariski de $\widehat{V}$ signifie que pour tout entier $D \geqslant 0$, l'opération de restriction des sections de L^D de X à $\widehat{V}$ définit une injection de k-espaces vectoriels

$$\Gamma(X, L^D) \hookrightarrow \Gamma(\widehat{V}, L^D). \tag{4.7.1}$$

Nous allons filtrer l'espace vectoriel $E_D = \Gamma(\widehat{V}, L^D)$ par l'ordre d'annulation le long de V_0. Si n est un entier $\geqslant 1$, notons V_n le voisinage infinitésimal d'ordre n de V_0 dans $\widehat{V}$. Notons $E_0^D = E^D$ et, si $n \geqslant 1$, soit E_n^D l'ensemble des sections de E_0^D dont la restriction à V_{n-1} est nulle. Une section s de E_n^D possède un *jet d'ordre* n le long de V_0 ; c'est une section sur V_0 de $L_{V_0}^D \otimes \operatorname{Sym}^n N^\vee$, nulle si et seulement si s appartient à E_{n+1}^D. Par passage aux sous-quotients, on déduit de l'injection (4.7.1) des injections, pour tous n et D,

$$E_n^D / E_{n+1}^D \hookrightarrow \Gamma(V_0, L|_{V_0}^D \otimes \operatorname{Sym}^n N^\vee) = \Gamma(\mathbf{P}(N^\vee), \pi^* L|_{V_0}^D \otimes \mathscr{O}_{\mathbf{P}(N^\vee)}(n)), \tag{4.7.2}$$

où l'on a noté $\pi \colon \mathbf{P}(N^\vee) \to V_0$ le fibré projectif associé à $N^\vee$ au-dessus de V_0. Comme $\mathbf{P}(N^\vee)$ est une variété projective sur k de dimension $v-1$, il existe une constante c telle que pour tous D et n, on ait la majoration

$$\dim_k \Gamma(\mathbf{P}(N^\vee), \pi^* L^D \otimes \mathscr{O}_{\mathbf{P}(N^\vee)}(n)) \leqslant c(1+n+D)^{v-1}. \tag{4.7.3}$$

D'autre part, l'hypothèse d'amplitude sur N et le théorème d'annulation de Serre impliquent qu'il existe un entier $\lambda \geqslant 1$ tel que si $n \geqslant \lambda D$ et $D \geqslant \lambda$,

$$\Gamma(V_0, L|_{V_0}^D \otimes \operatorname{Sym}^n N^\vee) = 0. \tag{4.7.4}$$

[2] Lorsque $k = \mathbf{C}$ est le corps des nombres complexes, une sous-variété analytique V d'un voisinage ouvert U de $V_0(\mathbf{C})$ dans $X(\mathbf{C})$ contenant $V_0(\mathbf{C}) \cap U$ en fournit un excellent exemple.

Il en résulte que pour tout entier $D \geqslant \lambda$, on a l'inégalité

$$\dim_k \Gamma(X, L^D) = \sum_{n=0}^{\infty} \dim_n E_n^D / E_{n+1}^D \leqslant \sum_{n=0}^{\lambda D-1} c_1(1+n+D)^{v-1} \leqslant c\lambda(1+\lambda)^{v-1} D^v. \tag{4.7.5}$$

Par suite, $\dim_k \Gamma(X, L^D) = \mathrm{O}(D^v)$. D'après le théorème de Hilbert, on a $\dim X = v$, ainsi qu'il fallait démontrer.

5. FRAGMENTS DE THÉORIE D'ARAKELOV

Nous résumons maintenant les quelques définitions et résultats de théorie d'Arakelov dont nous aurons besoin. Le lecteur intéressé trouvera des compléments importants dans les références [47, 45, 16, 44].

5.1. Soit K un corps de nombres ; notons $\mathfrak{o}_K$ son anneau d'entiers. Les valeurs absolues sur K sont de deux types. Celles qui sont non-archimédiennes (on dit aussi finies) sont associées à un idéal premier $\mathfrak{p}$ de $\mathfrak{o}_K$; on note $v_\mathfrak{p} : K^\times \to \mathbf{Z}$, la valuation associée et $|\cdot|_\mathfrak{p}$ la valeur absolue correspondante, normalisées de sorte que, si π est une uniformisante, $v_\mathfrak{p}(\pi) = 1$ et $\log |\pi|_\mathfrak{p} = -\log \#(\mathfrak{o}_K/\mathfrak{p})$. Si $K_\mathfrak{p}$ désigne le complété $\mathfrak{p}$-adique de K et p la caractéristique du corps résiduel $\mathfrak{o}_K/\mathfrak{p}$, on a ainsi

$$\log |p|_\mathfrak{p} = -[K_\mathfrak{p} : \mathbf{Q}_p] \log p. \tag{5.1.1}$$

Les valeurs absolues archimédiennes (ou infinies) sont associées à un plongement $\sigma \colon K \hookrightarrow \mathbf{C}$, mais deux plongements conjugués fournissent la même valeur absolue. Si $\sigma \colon K \hookrightarrow \mathbf{C}$ est un tel plongement, on définit $\varepsilon_\sigma = 1$ si σ est réel et 2 sinon, et on a, si $x \in K$,

$$\log |x|_\sigma = \varepsilon_\sigma \log |\sigma(x)| . \tag{5.1.2}$$

On notera aussi $K_\sigma = \mathbf{R}$ ou $\mathbf{C}$ suivant que σ est réel ou complexe. On a ainsi $\varepsilon_\sigma = [K_\sigma : \mathbf{R}]$.

Notons Σ_K l'ensemble des valuations sur K ainsi définies ; on notera aussi $\Sigma_{K,f}$ et $\Sigma_{K,\infty}$ les ensembles de valuations non-archimédiennes et archimédiennes respectivement. Avec ces normalisations, on a la *formule du produit* :

$$\text{si } x \in K \setminus \{0\}, \qquad \prod_{v \in \Sigma_K} |x|_v = 1. \tag{5.1.3}$$

Définition 5.1. — *Un $\mathfrak{o}_K$-fibré vectoriel hermitien $\overline{E} = (E, \|\sigma\|)$ est la donnée d'un $\mathfrak{o}_K$-module projectif de rang fini E, ainsi que pour tout $\sigma \in \Sigma_{K,\infty}$, d'une norme hermitienne sur l'espace vectoriel $E_\sigma = \mathbf{C} \otimes_{\mathfrak{o}_K,\sigma} E$, invariante par la conjugaison complexe si σ est réelle.*

Il revient au même de considérer une norme hermitienne invariante par conjugaison sur l'espace vectoriel complexe $\mathbf{C} \otimes_\mathbf{Z} E$.

Soit $\overline{E}$ un $\mathfrak{o}_K$-fibré vectoriel hermitien. Si $\mathfrak{p}$ est un idéal premier de $\mathfrak{o}_K$, on peut aussi définir une norme $\mathfrak{p}$-adique sur l'espace vectoriel $E_\mathfrak{p} = K_\mathfrak{p} \otimes_{\mathfrak{o}_K} E$: par définition, si $e \in E_\mathfrak{p}$,

$$\|e\|_\mathfrak{p} = \inf\{|a|_\mathfrak{p} \; ; \; a \in K_\mathfrak{p}^\times, \quad ae \in \mathfrak{o}_\mathfrak{p} \otimes_{\mathfrak{o}_K} E\}. \tag{5.1.4}$$

5.2. Plus généralement, si $\mathscr{X}$ est un $\mathbf{Z}$-schéma de type fini et plat, un *fibré vectoriel hermitien* $\overline{E} = (E, \|\|)$ sur $\mathscr{X}$ est la donnée d'un fibré vectoriel E sur $\mathscr{X}$ ainsi que d'une *métrique hermitienne* sur le fibré vectoriel holomorphe $E_{\mathbf{C}}$ sur l'espace analytique complexe $\mathscr{X}(\mathbf{C})$, supposée invariante par conjugaison complexe.

On peut effectuer, sur ces fibrés vectoriels hermitiens, un certain nombre de constructions standard : image réciproque par un morphisme $\mathscr{X}' \to \mathscr{X}$; somme directe, munie de la norme somme directe orthogonale ; sous-fibré, muni de la norme induite ; fibré quotient, muni de la norme quotient ; modules d'homomorphismes, en particulier duaux ; produit tensoriel, puissances symétriques et extérieures (toutes deux *quotients* du produit tensoriel).

5.3. Soit $\mathscr{X}$ un $\mathfrak{o}_K$-schéma de type fini et plat. Si σ est un plongement de K dans $\mathbf{C}$, notons $\mathscr{X}_\sigma(\mathbf{C}) = \mathscr{X} \otimes_{\mathfrak{o}_K,\sigma} \mathbf{C}$, de sorte que $\mathscr{X}(\mathbf{C})$ est la réunion disjointe des $\mathscr{X}_\sigma(\mathbf{C})$. Si $\overline{E}$ est un fibré vectoriel hermitien sur $\mathscr{X}$ et si $\mathscr{X}$ est propre, $\Gamma(\mathscr{X}, E)$ est un $\mathfrak{o}_K$-module projectif de rang fini. On peut le munir d'une structure de $\mathfrak{o}_K$-fibré vectoriel hermitien comme suit. Fixons μ une mesure « de Lebesgue » sur $\mathscr{X}(\mathbf{C})$ (voir [17] pour la définition précise ; quand $\mathscr{X}(\mathbf{C})$ est lisse de dimension complexe d c'est une mesure qui, en coordonnées locales $z_j = x_j + \mathrm{i}y_j$, s'écrit $\omega(x)\mathrm{d}x_1\mathrm{d}y_1 \dots \mathrm{d}x_d\mathrm{d}y_d$ où ω est une fonction $\mathscr{C}^\infty$ strictement positive). Alors, on définit pour tout $e \in \Gamma(\mathscr{X}, E)$ et tout plongement complexe $\sigma\colon K \hookrightarrow \mathbf{C}$,

(5.3.1) $$\|e\|_\sigma = \left(\int_{\mathscr{X}_\sigma(\mathbf{C})} \|e(x)\|_\sigma^2 \,\mathrm{d}\mu(x) \right)^{1/2}.$$

On définit aussi une *norme sup.* :

(5.3.2) $$\|e\|_{\infty,\sigma} = \sup_{x \in \mathscr{X}_\sigma(\mathbf{C})} \|e(x)\|_\sigma .$$

Un lemme élémentaire relie ces deux normes.

5.4. Lemme. — *Si de plus $\overline{E}$ est un fibré en droites hermitien sur $\mathscr{X}$, il existe une constante C telle que pour tout $\sigma\colon K \hookrightarrow \mathbf{C}$, tout entier $D \geqslant 1$ et tout $e \in \Gamma(\mathscr{X}, E^D)$, on ait l'encadrement*

(5.4.1) $$\|e\|_\sigma \leqslant C \|e\|_{\infty,\sigma} \leqslant C^D \|e\|_\sigma .$$

5.5. Un $\mathfrak{o}_K$-fibré vectoriel hermitien $\overline{E}$ de rang 1 possède un *degré*, défini par

(5.5.1) $$\widehat{\deg}\,\overline{E} = \log \#(E/\mathfrak{o}_K e) - \sum_{\sigma\colon K \hookrightarrow \mathbf{C}} \log \|e\|_\sigma ,$$

e étant un élément non nul quelconque de E ; le fait que la formule n'en dépende pas résulte de la formule du produit. Plus généralement, pour tout élément non nul $e \in E_K$, on a

(5.5.2) $$\widehat{\deg}\,\overline{E} = - \sum_{v \in \Sigma_K} \log \|e\|_v .$$

On définit plus généralement le degré d'un $\mathfrak{o}_K$-fibré vectoriel hermitien $\overline{E}$ de rang $d \geqslant 1$ comme celui de sa puissance extérieure maximale $\bigwedge^d \overline{E}$. On définit aussi la *pente* de $\overline{E}$, notée $\widehat{\mu}(\overline{E})$, comme le quotient de son degré par son rang.

Si $\overline{E}$, $\overline{E}'$ et $\overline{F}$ sont trois $\mathfrak{o}_K$-fibrés vectoriels hermitiens, $\overline{F}$ étant un sous-fibré de $\overline{E}$, on a les formules

(5.5.3) $$\widehat{\deg}\,\overline{E}^\vee = - \widehat{\deg}\,\overline{E},$$

(5.5.4) $$\widehat{\deg}\,\overline{E} = \widehat{\deg}\,\overline{F} + \widehat{\deg}(\overline{E}/\overline{F}),$$

(5.5.5) $$\widehat{\mu}(\overline{E} \otimes \overline{E}') = \widehat{\mu}(\overline{E}) + \widehat{\mu}(\overline{E}').$$

D'après le théorème des facteurs invariants et la théorie des déterminants de Gram, si $(e_1,\dots,e_d)$ est une famille linéairement indépendante d'éléments de E, on a

$$\widehat{\deg}\,\overline{E} = \log \#(E/(\mathfrak{o}_K e_1 + \cdots + \mathfrak{o}_K e_d)) - \frac{1}{2} \sum_{\sigma\colon K\hookrightarrow \mathbf{C}} \log\det\big(\langle e_j, e_k\rangle_\sigma\big). \tag{5.5.6}$$

En utilisant l'inégalité d'Hadamard, on en déduit que pour toute famille génératrice $(e_1,\dots,e_r)$ de $K\otimes E$,

$$\widehat{\mu}(\overline{E}) \geqslant -\sum_{v\in\Sigma_K} \log \max_{1\leqslant j\leqslant r} \|e_j\|_v\,. \tag{5.5.7}$$

5.6. Proposition. — *Soit $\mathscr{X}$ un $\mathfrak{o}_K$-schéma propre et plat et soit $\overline{L}$ un fibré en droites hermitien sur $\mathscr{X}$. Si D est un entier $\geqslant 0$, notons $\overline{E}_D$ le $\mathfrak{o}_K$-fibré vectoriel hermitien défini par $\Gamma(\mathscr{X}, L^D)$. Si L est ample, il existe une constante $c\in\mathbf{R}$ telle que pour tout entier $D\geqslant 0$, on ait*

$$\widehat{\mu}(\overline{E}_D) \geqslant -cD. \tag{5.6.1}$$

Pour la démonstration, combiner l'inégalité (5.5.7), le lemme 5.4 et le fait que la K-algèbre graduée $\bigoplus_D \Gamma(\mathscr{X}_K, L^D)$ est de type fini.

En appliquant l'inégalité (5.5.7) au fibré dual $\overline{E}^\vee$, on démontre que lorsque $\overline{F}$ parcourt les sous-fibrés vectoriels hermitiens de $\overline{E}$, l'ensemble des pentes $\widehat{\mu}(\overline{F})$ est majoré. La borne supérieure (en fait, un maximum) est la *plus grande pente* de $\overline{E}$ et est notée $\widehat{\mu}_{\max}(\overline{E})$. Le comportement précis de $\widehat{\mu}_{\max}$ par produit tensoriel est délicat. Si $\overline{E}$ et $\overline{L}$ sont deux $\mathfrak{o}_K$-fibrés vectoriels hermitiens, $\overline{L}$ étant de rang 1, on a

$$\widehat{\mu}_{\max}(\overline{E}\otimes\overline{L}) = \widehat{\mu}_{\max}(\overline{E}) + \widehat{\deg}\,\overline{L} \tag{5.6.2}$$

Pour des puissances symétriques, on établit le comportement asymptotique :

5.7. Lemme. — *Soit $\overline{E}$ un $\mathfrak{o}_K$-fibré vectoriel hermitien. Il existe une constante $c\in\mathbf{R}$ telle que pour tout entier $k\geqslant 0$,*

$$\widehat{\mu}_{\max}(\operatorname{Sym}^k \overline{E}) \leqslant ck. \tag{5.7.1}$$

Soit $\overline{F}$ un sous-fibré de $\operatorname{Sym}^k\overline{E}$. Il correspond par dualité à un quotient $\overline{G}$ du fibré hermitien $(\operatorname{Sym}^k\overline{E})^\vee$, lequel s'identifie au sous-fibré hermitien $\Gamma^k\overline{E}^\vee$ de $(\overline{E}^\vee)^{\otimes k}$ fixé par l'action du groupe symétrique $\mathfrak{S}_k$. Soit $(e_1,\dots,e_r)$ une base de $E_K^\vee$. Si $\mathbf{n}=(n_1,\dots,n_r)\in\mathbf{N}^r$ avec $\sum_{i=1}^r n_i = k$, soit $f_{\mathbf{n}}$ l'orbite du tenseur $e_1^{n_1}\otimes\cdots\otimes e_r^{n_r}$ sous l'action de $\mathfrak{S}_k$. Pour toute place finie v de K, on a ainsi

$$\|f_{\mathbf{n}}\|_v \leqslant \max(\|e_1\|_v,\dots,\|e_r\|_v)^k$$

tandis que pour toute place archimédienne v,

$$\|f_{\mathbf{n}}\|_v \leqslant \frac{k!}{n_1!\dots n_r!}\max(\|e_1\|_v,\dots,\|e_r\|_v)^k \leqslant r^k \max(\|e_1\|_v,\dots,\|e_r\|_v)^k.$$

Les $f_{\mathbf{n}}$ forment une base de $\Gamma^k E_K^\vee$. L'inégalité (5.5.7) appliquée à leurs images dans $\overline{G}$ jointe à l'égalité $\widehat{\mu}(\overline{G}) = -\widehat{\mu}(\overline{F})$ implique ainsi que

$$\widehat{\mu}(\overline{F}) \leqslant k\left([K:\mathbf{Q}]\log r + \sum_{v\in\Sigma_K}\log\max(\|e_1\|_v,\dots,\|e_r\|_v)\right),$$

comme il fallait démontrer.

5.8. Remarque. — En utilisant les résultats de Zhang [48] qui fournissent une « presque-base orthonormée » de $\overline{E}$, Bost a donné une version explicite du lemme 5.7, cf. [27]. Par ailleurs, dans la situation de la proposition 5.6, l'existence et le calcul de la limite de $\widehat{\mu}(\overline{E}_D)/D$, lorsque $D\to+\infty$, est le *théorème de Hilbert-Samuel arithmétique*, cf. [26, 1, 40].

5.9. Soit $\overline{E}$ et $\overline{F}$ deux $\mathfrak{o}_K$-fibrés vectoriels hermitiens et soit $\varphi\colon E_K \to F_K$ une application K-linéaire injective. Pour toute valuation $v \in \Sigma_K$, définissons la *hauteur de* φ *en* v par

(5.9.1)
$$h_v(\varphi) = \log \|\varphi\|_v = \log \sup_{e \in E_v \setminus \{0\}} \frac{\|\varphi(e)\|_v}{\|e\|_v}.$$

Pour tout v sauf pour un nombre fini, $h_v(\varphi) = 0$, si bien qu'on peut définir la *hauteur* (globale) de φ par la formule

(5.9.2)
$$h(\varphi) = \sum_{v \in \Sigma_K} h_v(\varphi).$$

En combinant les définitions et l'inégalité de Hadamard, on établit alors *l'inégalité de pentes* sur laquelle toute l'histoire qui va suivre est fondée :

(5.9.3)
$$\widehat{\mu}(\overline{E}) \leqslant \widehat{\mu}_{\max}(\overline{F}) + h(\varphi).$$

Plus précisément, nous aurons besoin de la variante « filtrée » de cette inégalité de pentes, dont la démonstration est immédiate à partir de l'inégalité précédente et de la formule (5.5.4).

5.10. Proposition. — *Soit $\overline{E}$ et $(\overline{G}^{(n)})_{n \geqslant 0}$ des $\mathfrak{o}_K$-fibrés vectoriels hermitiens. Soit F_K un K-espace vectoriel muni d'une filtration décroissante séparée $(F_K^{(n)})_{n \geqslant 0}$ et, pour tout entier $n \geqslant 0$, un isomorphisme $F_K^{(n)}/F_K^{(n+1)} \simeq G_K^{(n)}$.*

Soit $\varphi\colon E_K \to F_K$ une application linéaire injective. Pour tout $n \geqslant 0$, soit $\overline{E}^{(n)}$ le $\mathfrak{o}_K$-fibré vectoriel hermitien défini par $E^{(n)} = \varphi^{-1}(F_K^{(n)})$, muni des normes induites par $\overline{E}$ et soit $\varphi_K^{(n)}$ l'application linéaire induite $E_K^{(n)} \to G_K^{(n)}$.

Alors, on a l'inégalité

(5.10.1)
$$\widehat{\deg}\,\overline{E} \leqslant \sum_{n=0}^{\infty} \operatorname{rang}(E^{(n)}/E^{(n+1)}) \left(\widehat{\mu}_{\max}(\overline{G}^{(n)}) + h(\varphi^{(n)})\right).$$

(C'est une somme finie si l'on convient que l'expression entre parenthèses est nulle lorsque que $E^{(n)} = E^{(n+1)}$.)

6. UN PREMIER THÉORÈME D'ALGÉBRICITÉ

L'article d'André [4] (voir aussi [3]) repose sur un théorème d'algébricité d'une série formelle, sorte d'analogue du théorème de Borel-Dwork. Nous donnons ici une démonstration de ce théorème qui utilise le formalisme introduit au chapitre précédent. Pour alléger les notations, nous nous contentons d'une variable quoique la généralisation du critère de Pólya cité à la fin du chapitre 2 en nécessite plusieurs.

6.1. Soit K un corps de nombres et soit $y = \sum_{n=0}^{\infty} a_n x^n$ une série formelle à coefficients dans K. On définit trois invariants, ρ, σ et τ :

(6.1.1)
$$\rho(y) = \sum_{v \in \Sigma_K} \overline{\lim_{n \to \infty}} \frac{1}{n} \sup_{m \leqslant n} \log^+ |a_m|_v\,,$$

(6.1.2)
$$\sigma(y) = \overline{\lim_{n \to \infty}} \sum_{v \in \Sigma_K} \frac{1}{n} \sup_{m \leqslant n} \log^+ |a_m|_v\,,$$

(6.1.3)
$$\tau(y) = \inf_{\substack{S \subset \Sigma_K \\ S \text{ finie}}} \overline{\lim_{n \to \infty}} \sum_{v \in \Sigma_K \setminus S} \frac{1}{n} \sup_{m \leqslant n} \log^+ |a_m|_v\,.$$

(Si $x \in \mathbf{R}$, $\log^+(x) = \log \max(1, x)$.) Si S est une partie de Σ_K, $\rho_S(y)$ et $\sigma_S(y)$ désigneront les quantités analogues à $\rho(y)$ et $\sigma(y)$ où seules les places de S sont prises en compte. Par exemple, il vient ainsi

$\tau(y) = \inf_S \sigma_S(y)$. Notons de plus $R_v(y)$ le rayon de convergence v-adique de la série y ; on a pour toute ensemble S de places l'égalité $\rho_S(y) = \sum_{v\in S} \log^+ R_v(y)^{-1}$.

S'il existe un ensemble fini de places $S \subset \Sigma_K$ telles que les coefficients de y soient S-entiers, on a $\tau(y) = 0$. Dans ce cas, $\rho(y) < \infty$ si et seulement si pour toute place $v \in S$, le rayon de convergence v-adique de la série y n'est pas nul.

Soit v une place de K. Une *uniformisation v-adique simultanée* de x et y dans le disque « ouvert » $D(0, R_v) \subset \overline{K}_v$ est la donnée de deux fonctions méromorphes v-adiques φ et ψ vérifiant

– $\varphi(0) = 0$ et $\varphi'(0) = 1$;
– $y(\varphi(z))$ est le germe en l'origine de la fonction méromorphe $\psi(z)$.

C'est ainsi, en quelque sorte, une uniformisation (méromorphe) du graphe de y par le disque $D(0, R_v)$. (Par définition, une fonction méromorphe sur $D(0, R_v)$ est le quotient de deux fonctions analytiques sur ce disque.)

On parle d'*uniformisation triviale* si de plus φ est l'identité.

La première partie du théorème suivant est due à André ([4], théorème 2.3.1), la seconde est essentiellement le critère de Borel-Dwork.

6.2. Théorème. — *Soit $y \in K[[x]]$ telle que $\tau(y) = 0$ et $\rho(y) < \infty$. On suppose que pour toute place v de K, il existe une uniformisation v-adique simultanée de x et y dans un disque $D(0, R_v)$. Si $\prod R_v > 1$, alors y est une fonction algébrique.*

Si de plus les uniformisations sont triviales pour tout v, alors y est une fonction rationnelle.

La fin de ce chapitre est consacrée à la démonstration du théorème 6.2.

6.3. Soit d et D deux entiers $\geqslant 1$ et soit $E_{d,D} \subset \mathfrak{o}_K[X, Y]$ le $\mathfrak{o}_K$-module libre des polynômes de degrés $\leqslant d$ en X et $\leqslant D$ en Y. On le munit des normes hermitiennes induites par la base standard aux places archimédiennes, d'où un $\mathfrak{o}_K$-fibré vectoriel hermitien $\overline{E}_{d,D}$ de rang $(d+1)(D+1)$ et de degré arithmétique nul.

Soit $F_K = K[[x]]$ et soit $\varphi\colon E_{d,D;K} \to F_K$ l'application linéaire définie par $P \mapsto P(x, y(x))$. En filtrant $K[[x]]$ par l'ordre d'annulation en l'origine, soit $F_K^{(k)} = x^k K[[x]]$, on est dans la situation de la proposition 5.10, où pour tout $k \geqslant 0$, $\overline{G}^{(k)} = \mathfrak{o}_K$ muni de la norme triviale $\|1\|_\sigma = 1$; en particulier, $\widehat{\deg}\, \overline{G}^{(k)} = \widehat{\mu}_{\max}(\overline{G}^{(k)}) = 0$.

On raisonne par l'absurde. Supposons que y n'est pas une fonction algébrique. Alors, pour tous d et D, l'application linéaire φ est injective. Si y n'est pas une fonction rationnelle, l'application φ est injective pour $D = 1$ et tout entier $d \geqslant 1$. L'inégalité de pentes de la proposition 5.10 s'écrit ainsi

$$0 \leqslant \sum_{n=0}^{\infty} \operatorname{rang}(E_{d,D}^{(n)}/E_{d,D}^{(n+1)}) h(\varphi^{(n)}). \tag{6.3.1}$$

Le reste de la démonstration consiste à majorer convenablement $h(\varphi^{(n)})$ de sorte à contredire l'inégalité précédente. Pour cela, on utilise deux types d'estimations : 1°) pour presque toute place, une majoration « triviale » (lemme 6.7) qui repose sur les hypothèses $\tau(y) = 0$ et $\rho(y) < \infty$, et 2°) pour un nombre fini de places, une majoration fondée sur le lemme de Schwarz, sous la forme :

6.4. Lemme. — *Soit v une place de K et soit f une fonction analytique bornée sur le disque $D(0, R_v) \subset \overline{K}_v$. Si f s'annule à l'ordre n en 0, on a*

$$\left| \frac{1}{n!} f^{(n)}(0) \right|_v \leqslant R_v^{-n} \|f\|_{R_v} .$$

6.5. Plaçons-nous dans le cas d'une uniformisation triviale en une place v de K et supposons qu'il existe une fonction méromorphe φ sur le disque $D(0, R_v)$ dont y soit le développement de Taylor en l'origine. Si $R'_v < R_v$, il existe alors des fonctions analytiques bornées sur le disque $D(0, R'_v)$ telles que $\varphi = f/g$ et $g(0) = 1$. Soit $n \geqslant 0$ et soit $P \in E_{d,D}^{(n)}$. Si $P = \sum_{i=0}^{D} P_i(X)Y^i$, où pour tout i, $\deg P_i \leqslant d$, définissons une fonction analytique bornée h sur $D(0, R'_v)$ par

$$h(x) = g(x)^D P(x, y(x)) = \sum_{i=0}^{D} P_i(x) f(x)^i g(x)^{D-i}.$$

Comme $g(0) = 1$ et comme $P(x, y(x))$ est supposé être d'ordre au moins n en l'origine, on a

$$\varphi^{(n)}(P) = \frac{1}{n!} \frac{\partial^n}{\partial x^n} P(x, y(x))|_{x=0} = \frac{1}{n!} \frac{\partial^n}{\partial x^n} h(x)|_{x=0}.$$

D'après le lemme de Schwarz, on a alors

$$\left|\varphi^{(n)}(P)\right|_v \leqslant R_v'^{-n} R_v'^{d} \max(\|f\|_{R'_v}, \|g\|_{R'_v})^D \|P\|_v$$

multiplié par $\operatorname{rang} E_{d,D}$ si v est une place archimédienne. On en déduit qu'il existe une constante C_v telle que l'on ait pour tous n, d, D, l'inégalité

$$h_v(\varphi^{(n)}) \leqslant (d - n) \log R'_v + DC_v \tag{6.5.1}$$

auquel il faut ajouter $\log \operatorname{rang} E_{d,D}$ si v est archimédienne.

6.6. Dans le cas d'une uniformisation simultanée générale, le même raisonnement fournit l'existence pour tout réel $R'_v < R_v$ d'une constante C_v telle que l'on ait pour tous n, d, D, l'inégalité

$$h_v(\varphi^{(n)}) \leqslant -n \log R'_v + (d + D)C_v \tag{6.6.1}$$

auquel il faut encore ajouter $\log \operatorname{rang} E_{d,D}$ si v est archimédienne.

6.7. Lemme. — *Pour tout ensemble de places $T \subset \Sigma_K$, et pour tout $\varepsilon > 0$, il existe une constante $C_T(\varepsilon)$ telle que l'on ait la majoration*

$$\sum_{v \in T} h_v(\varphi^{(n)}) \leqslant n\big(\rho_T(y) + \varepsilon(1 + \log D)\big) + C_T(\varepsilon) + [K : \mathbf{Q}] \log \operatorname{rang} E_{d,D} + [K : \mathbf{Q}](D + 1) \log n.$$

(On peut omettre les deux derniers termes si T ne contient pas de places archimédiennes.)

Si $j \geqslant 0$, introduisons le développement en série de y^j, $y = \sum_{m=0}^{\infty} a_m^{(j)} x^m$, où les $a_m^{(j)}$ sont dans K. Constatons que l'application $\varphi^{(n)}$ associe à un polynôme $P \in E_{d,D;K}$ tel que $P(x, y(x)) \in x^n K[[x]]$ le coefficient de x^n dans $P(x, y(x))$. Ainsi, si v est une place finie, on a l'estimée évidente :

$$h_v(\varphi^{(n)}) \leqslant \sup_{\substack{m \leqslant n \\ j \leqslant D}} \log^+ \left|a_m^{(j)}\right|_v. \tag{6.7.1}$$

Lorsque v est une place archimédienne, il faut rajouter $\log \operatorname{rang} E_{d,D} + (D + 1) \log n$.

Par suite, pour toute place v de K,

$$\overline{\lim} \frac{1}{n} h_v(\varphi^{(n)}) \leqslant \sup_{j \leqslant D} \overline{\lim_{n}} \sup_{m \leqslant n} \frac{1}{n} \log^+ \left|a_m^{(j)}\right|_v \leqslant \sup_{j \leqslant D} \log^+ R_v(y^j)^{-1},$$

$R_v(y^j)$ désignant le rayon de convergence v-adique de la série y^j. Mais ce rayon n'est autre que celui de y, si bien que

$$\overline{\lim} \frac{1}{n} h_v(\varphi^{(n)}) \leqslant \log^+ R_v(y)^{-1}.$$

D'autre part, si v est une place finie de K et si $j \leqslant D$, $a_m^{(j)}$ est majoré par le maximum des produits $a_{m_1} \dots a_{m_j}$, pour $m_1 + \dots + m_j = j$. Si ce maximum est atteint en $(m_1, \dots, m_j)$, on peut supposer $m_1 \geqslant m_2 \geqslant \dots \geqslant m_j$, si bien que pour tout $i \leqslant j$, $m_i \leqslant j/i$. On en déduit la majoration

$$\sup_{\substack{m \leqslant n \\ j \leqslant D}} \log^+ \left| a_m^{(j)} \right|_v \leqslant \sum_{j=1}^{D} \sup_{r \leqslant n/j} \log^+ |a_r|_v \, .$$

d'où finalement

$$\frac{1}{n} h_v(\varphi^{(n)} \leqslant \sum_{j=1}^{D} \frac{1}{n} \sup_{m \leqslant n/j} \log^+ |a_m|_v \, . \tag{6.7.2}$$

Soit T_1 une partie finie de T contenant les places archimédiennes. En décomposant la somme sur les places $v \in T$ suivant T_1 et son complémentaire, on obtient

$$\overline{\lim} \, \frac{1}{n} \sum_{v \in T} h_v(\varphi^{(n)}) \leqslant \sum_{v \in T_1} \log^+ R_v(y)^{-1} + \sum_{j=1}^{D} \frac{1}{j} \, \overline{\lim} \, \frac{1}{n} \sum_{v \in T \setminus T_1} \sup_{m \leqslant n} \log^+ |a_m|_v \, ,$$

c'est-à-dire

$$\overline{\lim} \, \frac{1}{n} \sum_{v \in T} h_v(\varphi^{(n)}) \leqslant \rho_{T_1}(y) + \left(\sum_{j=1}^{D} \frac{1}{j} \right) \sigma_{T \setminus T_1}(y).$$

Prenant T_1 arbitrairement grand et utilisant le fait que $\tau(y) = \inf_S \sigma_S(y) = 0$, on obtient la majoration voulue.

6.8. Démontrons maintenant le théorème d'algébricité. Soit $S \subset \Sigma_K$ un ensemble fini de places contenant les places archimédiennes. Par souci d'allègement, on note $E = E_{d,D}$. On note aussi $C'_v = \log \operatorname{rang} E$ pour v archimédienne et $C'_v = 0$ pour v finie.

Compte tenu du lemme 6.7 et de la majoration (6.6.1) pour toute place $v \in S$, l'inégalité de pentes (6.3.1) entraîne

$$0 \leqslant \sum_{v \in S} \sum_{n=0}^{\infty} \operatorname{rang}(E^{(n)}/E^{(n+1)}) \left(-n \log R'_v + (d+D) C_v + C'_v \right) \\ + C_S(\varepsilon) \operatorname{rang} E + \sum_{n=0}^{\infty} n \operatorname{rang}(E^{(n)}/E^{(n+1)}) (\rho_S(y) + \varepsilon(1 + \log D)),$$

d'où, utilisant que $\sum_n \operatorname{rang}(E^{(n)}/E^{(n+1)}) = \operatorname{rang} E$,

$$\sum_{n=0}^{\infty} n \operatorname{rang}(E^{(n)}/E^{(n+1)}) \log \prod_{v \in S} R'_v \\ \leqslant \left((d+D) \sum_{v \in S} C_v + C_S(\varepsilon) + [K : \mathbf{Q}] \log \operatorname{rang} E \right) \operatorname{rang} E \\ + \sum_{n=0}^{\infty} n \operatorname{rang}(E^{(n)}/E^{(n+1)}) (\rho_S(y) + \varepsilon(1 + \log D)). \tag{6.8.1}$$

Nous pouvons minorer $\Delta = \sum n \operatorname{rang}(E^{(n)}/E^{(n+1)})$ de la façon suivante. Par construction, $\operatorname{rang}(E^{(n)}/E^{(n+1)}) \leqslant \operatorname{rang} G^{(n)} = 1$. Il en résulte que $\operatorname{rang} E^{(n)} \geqslant \operatorname{rang} E - n$ et par suite,

$$\begin{aligned}\sum_{n=0}^{\infty} n \operatorname{rang}(E^{(n)}/E^{(n+1)}) &= \sum_{n=1}^{\infty} \operatorname{rang} E^{(n)} \\ &\geqslant \sum_{n=1}^{\operatorname{rang} E} (\operatorname{rang} E - n) = \frac{1}{2} \operatorname{rang} E (\operatorname{rang} E - 1). \end{aligned} \tag{6.8.2}$$

Faisons maintenant tendre d vers $+\infty$, D restant fixe. On a ainsi $\Delta \gg d^2 D^2$, si bien que $\operatorname{rang} E \log \operatorname{rang} E = \mathrm{o}(\Delta)$ et

$$\overline{\lim} \frac{(d+D) \operatorname{rang} E}{\Delta} \leqslant \frac{2}{D+1}.$$

En divisant les deux membres de l'inégalité (6.8.1) par $\sum n \operatorname{rang}(E^{(n)}/E^{(n+1)})$, on obtient l'inégalité

$$\log \prod_{v \in S} R'_v \leqslant \rho_S(y) + \varepsilon(1 + \log D) + \frac{1}{D} \sum_{v \in S} C_v.$$

On peut alors faire tendre ε vers 0, puis D vers l'infini, et enfin R'_v vers R_v dans cette inégalité et l'on obtient

$$\log \prod_{v \in S} R_v \leqslant \rho_S(y). \tag{6.8.3}$$

Comme $\rho(y) < \infty$, le membre de droite peut être rendu arbitrairement petit quitte à augmenter S, mais ceci contredit alors l'hypothèse que $\prod_{v \in \Sigma_K} R_v > 1$.

6.9. Pour démontrer la seconde partie du théorème, on fixe encore un ensemble fini $S \subset \Sigma_K$ contenant les places archimédiennes. On raisonne par l'absurde en supposant que y n'est pas rationnelle. Si $D = 1$, l'application linéaire φ est donc injective pour tout entier $d \geqslant 1$. On introduit un nouveau paramètre N et on utilise la majoration de $h_v(\varphi^{(n)})$ fournie par le lemme 6.7 si $v \notin S$ ou si $n < N$ et par l'estimée (6.5.1) sinon. On obtient ainsi l'inégalité

$$\begin{aligned} 0 \leqslant{} & C_{\complement S}(\varepsilon) \operatorname{rang} E + (\rho_{\complement S}(y) + \varepsilon) \sum_{n=0}^{\infty} n \operatorname{rang}(E^{(n)}/E^{(n+1)}) \\ & + \sum_{v \in S} \sum_{n \geqslant N} ((d-n) \log R'_v + D C_v + C'_v) \operatorname{rang}(E^{(n)}/E^{(n+1)}) \\ & + \sum_{n<N} \operatorname{rang}(E^{(n)}/E^{(n+1)})(C_S(\varepsilon) + [K:\mathbf{Q}] \log \operatorname{rang} E + 2[K:\mathbf{Q}] \log n) \\ & + (\rho_S(y) + \varepsilon) \sum_{n<N} n \operatorname{rang} E^{(n)}/E(n+1). \end{aligned} \tag{6.9.1}$$

Compte tenu de la majoration $\operatorname{rang}(E^{(n)}/E^{(n+1)}) \leqslant 1$, on a la majoration

$$\Delta_N = \sum_{n<N} n \operatorname{rang}(E^{(n)}/E^{(n+1)}) \leqslant \sum_{n<N} n = N(N-1)/2.$$

On fixe un paramètre λ et on pose $N = \lfloor 2\lambda d \rfloor$. Lorsque d tend vers l'infini, mais bien sûr, $D = 1$, de sorte que $\operatorname{rang} E = 2(d+1)$ et $N \sim \lambda \operatorname{rang} E$. Puisque

$$\Delta = \sum_{n=0}^{\infty} n \operatorname{rang}(E^{(n)}/E^{(n+1)}) \geqslant \frac{1}{2} \operatorname{rang} E(\operatorname{rang} E - 1),$$

on a $\overline{\lim}\,(\Delta_N/\Delta) \leqslant \lambda^2$. De plus, si $\lambda \leqslant 1/2$, on a $N \leqslant d$ et on constate que $\operatorname{rang} E^{(N)} = \operatorname{rang} E - N$, si bien que

$$\overline{\lim_{d\to+\infty}} \frac{d \operatorname{rang} E^{(N)}}{\Delta} \leqslant 1 - \lambda.$$

Après division des deux membres par Δ et passage à la limite, l'inégalité (6.9.1) devient

$$0 \leqslant (\rho_{\complement S}(y) + \varepsilon) + \lambda^2(\rho_S(y) + \varepsilon) + (\lambda^2 - \lambda)\log \prod_{v\in S} R'_v,$$

d'où, si ε tend vers 0 et R'_v vers R_v,

$$\lambda(1-\lambda)\log \prod_{v\in S} R_v \leqslant \rho_{\complement S}(y) + \lambda^2 \rho_S(y).$$

Comme $\rho_S(y) \leqslant \rho(y)$, cette inégalité contredit l'hypothèse $\prod_{v\in\Sigma_K} R_v > 1$, lorsque S est assez grand.

(Il n'est pas certain que cette démonstration du théorème de Borel-Dwork soit plus simple que la démonstration originelle, cf. [15], [21] ou [2].)

7. ALGÉBRICITÉ DE SOUS-VARIÉTÉS FORMELLES

7.1. Nous voulons maintenant indiquer la démonstration du théorème 4.3. Rappelons la situation : X est une variété algébrique lisse sur un corps de nombres K, P est un point de $X(K)$ et F est un sous-fibré involutif de $\mathrm{T}X$ qui, modulo p pour presque tout nombre premier p, est stable par puissance p-ième. On suppose de plus qu'il existe un plongement $\sigma_0 \colon K \hookrightarrow \mathbf{C}$ tel que la feuille passant par P du feuilletage holomorphe de $X_{\sigma_0}(\mathbf{C})$ induit par F est « uniformisée par l'espace affine ». C'est une hypothèse plus contraignante que celle du théorème 4.3 mais suffisante pour établir le théorème 2.4.

On veut alors en déduire que ladite feuille est une sous-variété algébrique de X, ou encore, si $\widehat{V}$ désigne la feuille formelle de F en P, qu'il existe une sous-variété algébrique V de X dont $\widehat{V}$ est le complété en P.

Soit Y l'adhérence de Zariski de $\widehat{V}$ dans X, c'est-à-dire la plus petite sous-variété algébrique de X dont le complété en P contient $\widehat{V}$. Il suffit de démontrer que $\dim Y = \dim \widehat{V}$ car cette hypothèse implique que Y est automatiquement lisse et une feuille du flot F. On peut aussi supposer que X est projective (mais X n'est alors lisse que dans un voisinage de P) ; Y est alors projective. Soit L un fibré inversible ample sur X. L'hypothèse que Y est l'adhérence de $\widehat{V}$ signifie que pour tout entier $D \geqslant 0$, l'homomorphisme de restriction à $\widehat{V}$,

$$\varphi_D \colon \Gamma(Y, L^D) \to \Gamma(\widehat{V}, L^D) \tag{7.1.1}$$

est injectif.

Sous l'hypothèse que $\widehat{V}$ n'est pas algébrique, c'est-à-dire que $\dim Y > \dim \widehat{V}$, nous voulons contredire cette injectivité. Nous allons pour cela utiliser l'inégalité de pentes (prop. 5.10). Plaçons-nous ainsi dans le contexte du chapitre 5. Choisissons des modèles entiers de toute la situation :

– un $\mathfrak{o}_K$-schéma propre et plat $\mathscr{X}$ tel que $\mathscr{X} \otimes K = X$;
– une section $\varepsilon_P \colon \operatorname{Spec} \mathfrak{o}_K \to \mathscr{X}$ prolongeant $P \in X(K)$;
– l'adhérence schématique $\mathscr{Y}$ de $\widehat{V}$ (ou de Y) dans $\mathscr{X}$;
– un fibré inversible $\mathscr{L}$ sur $\mathscr{X}$ dont la restriction à X est égale à L.

On note $\mathrm{t}^\vee$ l'image de $\varepsilon_P^*\Omega^1_{\mathscr{Y}/\mathfrak{o}_K}$ dans $\Omega^1_{Y/K,P}$; c'est un $\mathfrak{o}_K$-module projectif de rang $\dim Y$. Choisissons aussi

– une métrique hermitienne sur le fibré holomorphe induit par L sur $X(\mathbf{C})$;
– une mesure de Lebesgue positive sur $Y(\mathbf{C})$;

– une métrique hermitienne sur l'espace tangent en P à $\widehat{V}$, ou par dualité, sur $\mathrm{t}^\vee$;

toutes invariantes par la conjugaison complexe.

7.2. Pour tout entier $D \geqslant 1$, on notera $\overline{E}_D = \Gamma(\mathscr{Y}, L^D)$, muni de sa structure naturelle de $\mathfrak{o}_K$-fibré vectoriel hermitien définie comme au paragraphe 5.3. Le K-espace vectoriel $\Gamma(\widehat{V}, L^D)$ est filtré par l'ordre d'annulation en P, les sous-quotients successifs s'identifient aux fibres génériques des $\mathfrak{o}_K$-fibrés vectoriels hermitiens

$$\mathrm{Sym}^n \,\overline{\mathrm{t}}^\vee \otimes_{\mathfrak{o}_K} \varepsilon_P^* \overline{\mathscr{L}}^D. \tag{7.2.1}$$

Si $\overline{E}_D^{(n)}$ désigne l'image inverse de cette filtration par l'homomorphisme d'évaluation φ_D, l'application

$$\varphi_D^{(n)} \colon E_D^{(n)}/E_D^{(n+1)} \to \mathrm{Sym}^n \,\mathrm{t}_K^\vee \otimes L_P^D \tag{7.2.2}$$

s'identifie à l'application « jet d'ordre n en P ». L'homomorphisme $\overline{E}_D \to \Gamma(\widehat{V}, L^D)$ est injectif par construction. L'inégalité de pentes de la proposition 5.10 s'écrit alors

$$\widehat{\deg}\,\overline{E}_D \leqslant \sum_{n\geqslant 0} \mathrm{rang}(E_D^{(n)}/E_D^{(n+1)}) \left(\widehat{\mu}_{\max}(\mathrm{Sym}^n \,\overline{\mathrm{t}}^\vee \otimes_{\mathfrak{o}_K} \varepsilon_P^* \overline{\mathscr{L}}^D) + h(\varphi_D^{(n)})\right). \tag{7.2.3}$$

Dans [17], $h(\varphi_D^{(n)})$ est majorée par la proposition suivante.

7.3. Proposition. — *Rappelons l'hypothèse :*

– *pour presque tout nombre premier p, la réduction de F modulo p est stable par puissance p-ième ;*

– *il existe une variété complexe M vérifiant la propriété de Liouville, un point $O \in M$, un plongement complexe $\sigma_0 \colon K \hookrightarrow \mathbf{C}$ et une application holomorphe ψ de M vers la feuille en P du feuilletage holomorphe induit par F sur $X_{\sigma_0}(\mathbf{C})$ telle que $\psi(O) = P$ et telle que ψ soit biholomorphe d'un voisinage de O vers un voisinage de P dans cette feuille.*

Alors, pour tout $\rho > 0$, il existe un réel $C(\rho)$ tel que pour tous les entiers D et $n \geqslant 1$, on ait

$$h(\varphi_D^{(n)}) \leqslant -n\rho + DC(\rho). \tag{7.3.1}$$

Pour démontrer le théorème 2.4, il suffit de traiter le cas où $M = \mathbf{C}^d$ dans lequel l'analyse aux places archimédiennes peut être présentée de façon relativement élémentaire (voir le paragraphe 7.5).

7.4. Tirons maintenant la contradiction de ces estimations. En insérant dans l'inégalité (7.2.3) la majoration (7.3.1), les conclusions de la proposition 5.6 et du lemme 5.7 ainsi que la formule (5.6.2), on obtient l'inégalité, valable pour tout $\rho > 0$,

$$-c_1 D \,\mathrm{rang}\, E_D \leqslant \sum_{n\geqslant 0} \mathrm{rang}(E_D^{(n)}/E_D^{(n+1)})\,(nc_2 + Dc_3 + DC(\rho) - n\rho), \tag{7.4.1}$$

soit encore

$$(\rho - c_2) \sum n \,\mathrm{rang}(E_D^{(n)}/E_D^{(n+1)}) \leqslant (c_3 + c_1 + C(\rho)) D \,\mathrm{rang}\, E_D. \tag{7.4.2}$$

Or, d'après l'algèbre linéaire, si $d = \dim \widehat{V}$,

$$\mathrm{rang}(E_D^{(n)}/E_D^{(n+1)}) \leqslant \mathrm{rang}\,\mathrm{Sym}^n \,\mathrm{t}^\vee = \binom{n+d-1}{d-1} \tag{7.4.3}$$

$$\mathrm{rang}\, E_D^{(n)} \geqslant \mathrm{rang}\, E_D - \sum_{k=0}^{n-1} \binom{k+d-1}{d-1} = \mathrm{rang}\, E_D - \binom{n+d-1}{d} \tag{7.4.4}$$

tandis que le théorème de Hilbert garantit que

$$\mathrm{rang}\, E_D \simeq c_4 D^{\dim Y}. \tag{7.4.5}$$

Il en résulte que, si N est un entier $\geqslant 1$ arbitraire,

$$\sum_{n=0}^{\infty} n \operatorname{rang}(E_D^{(n)}/E_D^{(n+1)}) = \sum_{n=1}^{\infty} \operatorname{rang} E_D^{(n)} \geqslant \sum_{n=1}^{N} \operatorname{rang} E_D^{(n)}$$
$$\geqslant N \operatorname{rang} E_D - \binom{N+d}{d+1}.$$

Supposons par l'absurde que $\dim Y > d$ et choisissons $N = \lfloor D^\alpha \rfloor$ pour un réel α tel que $1 < \alpha < \dim Y/d$. Il en résulte que $D = \mathrm{o}(N)$ et $N^d = \mathrm{o}(D^{\dim Y})$. Par suite, $\binom{N+d}{d+1} = \mathrm{o}(N \operatorname{rang} E_D)$. En passant à la limite dans l'inégalité (7.4.2), on obtient alors

$$\rho - c_2 \leqslant 0. \tag{7.4.6}$$

Comme ρ est arbitraire, on a une contradiction.

7.5. Il reste à établir l'inégalité (7.3.1), et pour cela, nous allons majorer $h_v(\varphi_D^{(n)})$ pour toute place v de Σ_K. Lorsque v est une place finie, il s'agit essentiellement de « contrôler les dénominateurs » qui apparaissent dans le théorème de Frobenius.

Notons s la dimension de X et fixons des coordonnées locales (pour la topologie étale) $x_1, \ldots, x_s$ sur X au point P, de sorte qu'autour de P, $\mathrm{T}X$ est libre de base $\frac{\partial}{\partial x_1}, \ldots, \frac{\partial}{\partial x_s}$. Les x_i définissent aussi un isomorphisme formel $\widehat{\alpha}_0 \colon \widehat{X}_P \simeq \widehat{\mathbf{A}}^s$. Quitte à renuméroter les x_i, il est possible de trouver une base $D_1, \ldots, D_d$ des sections de F dans un voisinage de P de la forme

$$D_i = \frac{\partial}{\partial x_i} + \sum_{j=d+1}^{s} a_{i,j} \frac{\partial}{\partial x_j}, \tag{7.5.1}$$

où les $a_{i,j}$ sont des séries formelles. Soit $\widehat{\alpha} \colon \widehat{X}_P \to \widehat{\mathbf{A}}^d$ le morphisme déduit de $\widehat{\alpha}_0$ par projection sur les d premières coordonnées. On a ainsi $\widehat{\alpha}_*(D_i) = \frac{\partial}{\partial x_i}$ et

$$\widehat{\alpha}_*([D_i, D_j]) = [\widehat{\alpha}_*(D_i), \widehat{\alpha}_*(D_j)] = [\frac{\partial}{\partial x_i}, \frac{\partial}{\partial x_j}] = 0$$

si bien que $[D_i, D_j]$ est une combinaison linéaire des $\frac{\partial}{\partial x_k}$ pour $k > d$. Comme F est involutif, $[D_i, D_j] \in F$. Il en résulte que $[D_i, D_j] = 0$: les champs de vecteurs $D_1, \ldots, D_d$ commutent.

Ainsi, $\widehat{V}$ est la feuille passant par $P = (0, \ldots, 0)$ du « flot formel », $\Phi \colon \widehat{\mathbf{A}}^d \times \widehat{\mathbf{A}}^s \to \widehat{\mathbf{A}}^s$,

$$\begin{aligned} ((t_1, \ldots, t_d), (x_1, \ldots, x_s)) &\mapsto \exp\big(\sum_{i=1}^{d} t_i e_i\big) \cdot (x_1, \ldots, x_s) \\ &= \sum_{n_1, \ldots, n_d \geqslant 0} \frac{t_1{}^{n_1}}{n_1!} \cdots \frac{t_d^{n_d}}{n_d!} e_1{}^{n_1} \cdots e_d^{n_d} \cdot (x_1, \ldots, x_s). \end{aligned} \tag{7.5.2}$$

Pour tout multi-indice $n = (n_1; \ldots; n_d)$ et tout entier $i \in \{1; \ldots; s\}$, notons $P_{n,i}$ la série formelle $\frac{1}{n_1! \ldots n_d!} e_1^{n_1} \cdots e_d^{n_d}(x_i)$, de sorte que $\widehat{V}$ admet la paramétrisation formelle

$$(t_1, \ldots, t_d) \mapsto \sum_{n \in \mathbf{N}^d} t_1^{n_1} \cdots t_d^{n_d} (P_{n,1}(0), \ldots, P_{n,s}(0)).$$

7.6. Lemme. — *Pour toute place finie v de K, de caractéristique résiduelle p, il existe un réel $C_v \geqslant 0$ tel que pour tous $n \in \mathbf{N}^d$ et tout $i \in \{1; \ldots; s\}$,*

$$-\log \left|P_{n,i}(0)\right|_v \leqslant (n_1 + \cdots + n_d) C_v.$$

De plus, pour presque tout v, on peut choisir

$$C_v = [K:\mathbf{Q}]\frac{\log p}{p(p-1)}.$$

L'existence d'un tel C_v équivaut à la convergence v-adique du flot formel dans un polydisque.

De plus, pour presque toute place finie v, les coordonnées locales x_i s'étendent en des coordonnées locales sur $\mathscr{X} \otimes \mathfrak{o}_v$, ainsi que les champs de vecteurs locaux $D_1, \dots, D_d$. Si de plus la réduction modulo l'idéal premier $\mathfrak{p}_v$ est stable par puissance p-ième, on constate que pour tout i, en réduction modulo $\mathfrak{p}_v$,

$$\widehat{\alpha}_*(D_i^p) = \widehat{\alpha}_*(D_i)^p = \frac{\partial^p}{\partial x_i^p} = 0.$$

Comme la réduction modulo $\mathfrak{p}_v$ de F est supposée stable par puissance p-ième, il en résulte que $D_i^p = 0$ modulo $\mathfrak{p}_v$. Si de plus p ne divise pas le discriminant de K, on a alors $v(p) = 1$ et

$$v(e_1^{n_1} \dots e_d^{n_d} \cdot x_i) \geqslant \lfloor n_1/p \rfloor + \dots + \lfloor n_d/p \rfloor$$

et

$$v(P_{n,i}(0)) \geqslant -\sum_{j=1}^{d} (v(n_j!) - \lfloor n_j/p \rfloor) \geqslant -\frac{n_1 + \dots + n_d}{p(p-1)}$$

d'où l'on déduit le lemme.

De ces estimées découle facilement (lemme de Schwarz v-adique) une majoration, valable pour toute place v finie,

$$h_v(\varphi_D^{(n)}) \leqslant nC_v \tag{7.6.1}$$

et de plus,

$$\sum_{v \in \Sigma_{K,f}} C_v < +\infty. \tag{7.6.2}$$

Pour tout plongement complexe $\sigma \colon K \hookrightarrow \mathbf{C}$, soit $M_\sigma = B(0, R_\sigma)^d$ le polydisque ouvert de centre O et de rayon $R_\sigma \in \mathbf{R}_+^* \cup \{+\infty\}$ et soit $\psi_\sigma \colon M_\sigma \to \mathscr{Y}_\sigma(\mathbf{C})$ une application holomorphe induisant un isomorphisme d'un voisinage de O dans M_σ avec un voisinage de P dans la feuille holomorphe passant par P du feuilletage défini par F. Par hypothèse, de telles applications existent pour tout σ, et pour la place σ_0, on a $R_{\sigma_0} = +\infty$.

Fixons une section globale sans zéro ε_σ de $\psi_\sigma^* L$. Si $s \in E_D^n$, on écrit $\psi_\sigma^* s = f \varepsilon_\sigma^D$ où f est une fonction holomorphe sur M_σ s'annulant à l'ordre n en l'origine.

Soit pour tout σ un réel R'_σ tel que $0 < R'_\sigma < R_\sigma$. Soit $j^n f$ le jet d'ordre n de f en l'origine : c'est l'application polynomiale homogène de degré n :

$$\mathbf{C}^d \to \mathbf{C}, \qquad (a_1, \dots, a_d) \mapsto \sum_{n_1 + \dots + n_d = n} \frac{a_1^{n_1}}{n_1!} \cdots \frac{a_d^{n_d}}{n_d!} \frac{\partial^{n_1}}{\partial z_1^{n_1}} \cdots \frac{\partial^{n_d}}{\partial z_d^{n_d}} f(0).$$

D'après le lemme de Schwarz usuel, on a pour tout $(a_1, \dots, a_d) \in \mathbf{C}^d$ l'inégalité

$$|j^n f(a_1, \dots, a_d)| \leqslant \max(|a_i|)^n \, \|f\|_{R'_\sigma} (R'_\sigma)^{-n},$$

$\|f\|_{R'_\sigma}$ désignant le sup de $|f|$ sur le polydisque $\overline{B}(0, R'_\sigma)^d$ et la norme du jet de s est majorée par

$$\|j^n s\| \leqslant \left\|\mathrm{d}\psi_\sigma^{-1}\right\|^n (R'_\sigma)^{-n} \, \|\psi^* s\|_{R'_\sigma} \left\|\varepsilon_\sigma^{-1}\right\|_{R'_\sigma}^D .$$

Finalement, compte tenu de l'inégalité (5.4), il existe deux constantes A et $B(R'_\sigma)$ telles que

$$\|j^n s\| \leqslant (R'_\sigma/A)^{-n} B(R'_\sigma)^D$$

et

$$h_\sigma(\varphi_D^{(n)}) \leqslant D \log B(R'_\sigma) - n \log(R'_\sigma/A). \tag{7.6.3}$$

L'inégalité (7.3.1) découle alors immédiatement des inégalités (7.6.1), (7.6.2) et (7.6.3) et du fait que R'_{σ_0} puisse être pris arbitrairement grand.

7.7. Remarque. — La majoration (7.6.2) est un analogue de la condition $\tau = 0$ du chapitre 6. Ce n'est d'ailleurs pas surprenant : dans le contexte de la conjecture de Grothendieck, la condition $\tau = 0$ provient justement de l'hypothèse d'annulation des p-courbures, de même que l'inégalité (7.6.2) a été établie en utilisant la p-intégrabilité du feuilletage.

Références

[1] A. Abbes & T. Bouche – « Théorème de Hilbert–Samuel "arithmétique" », *Ann. Inst. Fourier (Grenoble)* **45** (1995), no. 2, p. 375–401.

[2] Y. Amice – *Les nombres p-adiques*, Collection SUP : Le Mathématicien, vol. 14, Presses Universitaires de France, Paris, 1975.

[3] Y. André – *G-functions and geometry*, Vieweg, Braunschweig, 1989.

[4] ______, « Sur la conjecture des p-courbures de Grothendieck et Katz », Prépublication 134, Institut de mathématiques de Jussieu, 1997.

[5] ______, « Séries Gevrey de type arithmétique, I. Théorèmes de pureté et de dualité », *Ann. of Math.* **151** (2000), p. 705–740.

[6] ______, « Séries Gevrey de type arithmétique, II. Transcendance sans transcendance », *Ann. of Math.* **151** (2000), p. 741–756.

[7] Y. André & F. Baldassarri – « Geometric theory of G-functions », in *Arithmetic geometry (Cortona, 1994)*, Cambridge Univ. Press, Cambridge, 1997, p. 1–22.

[8] D. Bertrand, M. Emsalem, F. Gramain, M. Huttner, M. Langevin, M. Laurent, M. Mignotte, J.-C. Moreau, P. Philippon, É. Reyssat & M. Waldschmidt – « Les nombres transcendants », *Mém. Soc. Math. France (N.S.)*, vol. 13, 1984.

[9] D. Bertrand – « Groupes algébriques et équations différentielles linéaires », in *Séminaire Bourbaki, 1991/92*, Exp. 750, Astérisque, vol. 206, 1992, p. 183–204.

[10] J.-P. Bézivin & P. Robba – « A new p-adic method for proving irrationality and transcendence results », *Ann. of Math.* **129** (1989), no. 1, p. 151–160.

[11] ______, « Rational solutions of linear differential equations », *J. Austral. Math. Soc. Ser. A* **46** (1989), no. 2, p. 184–196.

[12] F. A. Bogomolov & M. L. McQuillan – « Rational curves on foliated varieties », prépublication M/01/07, I.H.É.S., 2001.

[13] E. Bombieri – « On G-functions », in *Recent progress in analytic number theory, Vol. 2 (Durham, 1979)*, Academic Press, London, 1981, p. 1–67.

[14] A. Borel – *Linear algebraic groups*, second éd., Springer-Verlag, New York, 1991.

[15] É. Borel – « Sur une application d'un théorème de M. Hadamard », *Bulletin des sciences mathématiques* (1894).

[16] J.-B. Bost – « Périodes et isogénies des variétés abéliennes sur les corps de nombres (d'après D. Masser et G. Wüstholz) », in *Séminaire Bourbaki, 1994/95*, Exp. 795, Astérisque, vol. 237, 1996, p. 115–161.

[17] ______, « Algebraic leaves of algebraic foliations over number fields », *Publ. Math. Inst. Hautes Études Sci.* **93** (2001), p. 161–221.

[18] D. V. Chudnovsky & G. V. Chudnovsky – « Applications of Padé approximations to the Grothendieck conjecture on linear differential equations », in *Number theory* (New York, 1983–84), Lect. Notes Math., vol. 1135, 1985, p. 52–100.

[19] C. Deninger & E. Nart – « Formal groups and L-series », *Comment. Math. Helv.* **65** (1990), no. 2, p. 318–333.

[20] L. Di Vizio – « Sur la théorie géométrique des G-fonctions. Le théorème de Chudnovsky à plusieurs variables », *Math. Ann.* **319** (2001), p. 181–213.

[21] B. Dwork – « On the rationality of the zeta function of an algebraic variety », *Amer. J. Math.* **82** (1960), p. 631–648.

[22] B. Dwork, G. Gerotto & F. J. Sullivan – *An introduction to G-functions*, Annals of Math. Studies, no. 133, Princeton Univ. Press, 1994.

[23] G. Eisenstein – « Über eine allgemeine Eigenschaft der Reihen-Entwicklungen aller algebraischen Functionen (1852) », in *Mathematische Gesammelte Werke, Band II*, Chelsea Publishing Co., New York, 1975, p. 765–767.

[24] T. Ekedahl & N. Shepherd-Barron – « A conjecture on the existence of compact leaves of algebraic foliations », prépublication, 1999, disponible sur *http ://www.dpmms.cam.ac.uk/ nisb/*.

[25] G. Faltings – « Endlichkeitsätze für abelsche Varietäten über Zahlkörpern », *Invent. Math.* **73** (1983), no. 3, p. 349–366.

[26] H. Gillet & C. Soulé – « Amplitude arithmétique », *C. R. Acad. Sci. Paris Sér. I Math.* **307** (1988), p. 887–890.

[27] P. Graftieaux – « Formal groups and the isogeny theorem », *Duke Math. J.* **106** (2001), no. 1, p. 81–121.

[28] ______, « Formal subgroups of abelian varieties », *Invent. Math.* **145** (2001), no. 1, p. 1–17.

[29] D. R. Grayson – « Reduction theory using semistability », *Comment. Math. Helv.* **59** (1984), p. 600–634.

[30] T. Honda – « On the theory of commutative formal groups », *J. Math. Soc. Japan* **22** (1970), p. 213–246.

[31] N. Jacobson – *Lie algebras*, Dover Publications Inc., New York, 1979, republication of the 1962 original.

[32] N. M. Katz – « Nilpotent connections and the monodromy theorem : applications of a result of Turrittin », *Publ. Math. Inst. Hautes Études Sci.* **39** (1970), p. 175–232.

[33] ______, « Algebraic solutions of differential equations (p-curvature and the Hodge filtration) », *Invent. Math.* **18** (1972), p. 1–118.

[34] ______, « A conjecture in the arithmetic theory of differential equations », *Bull. Soc. Math. France* **110** (1982), no. 2, p. 203–239, Erratum, p. 347–348.

[35] L. Kronecker – « Über die Irreductibilität von Gleichungen », *Monatsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin* (1880).

[36] M. Laurent – « Sur quelques résultats récents de transcendance », in *Journées Arithmétiques, 1989 (Luminy, 1989)*, Astérisque, vol. 198-200, 1991, p. 209–230.

[37] O. Mathieu – « Classification des algèbres de Lie simples », in *Séminaire Bourbaki, 1998/99*, Exp. 858, Astérisque, vol. 266, 2000, p. 245–286.

[38] Y. Miyaoka – « Deformations of a morphism along a foliation and applications », in *Algebraic geometry, Bowdoin, 1985 (Brunswick, Maine, 1985)*, Amer. Math. Soc., Providence, RI, 1987, p. 245–268.

[39] A. Ogus – « Hodge cycles and crystalline cohomology », ch. 6 in *Hodge cycles, motives, and Shimura varieties*, Lect. Notes Math., vol. 900, Springer Verlag, 1982, p. 357–414.

[40] R. Rumely, C. F. Lau & R. Varley – « Existence of the sectional capacity », *Mem. Amer. Math. Soc.*, vol. 145 no. 690, 2000.

[41] H. A. Schwarz – « Ueber diejenigen Fälle in welchen die Gaussische hypergeometrische Reihe eine algebraische Funktion ihres vierten Elementes darstellt », *J. Reine Angew. Math.* **75** (1873), p. 292–335.

[42] J.-P. Serre – *Abelian ℓ-adic representations and elliptic curves*, W. A. Benjamin, Inc., New York-Amsterdam, 1968.

[43] C. L. Siegel – « Über einige Anwendungen diophantischer Approximationen (1929) », in *Gesammelte Abhandlungen, Band I*, 1966, p. 209–266.

[44] C. Soulé – « Hermitian vector bundles on arithmetic varieties », in *Algebraic Geometry (Santa Cruz, 1995)*, vol. 62, Part 1, 1997, p. 383–419.

[45] C. Soulé, D. Abramovich, J.-F. Burnol & J. Kramer – *Lectures on Arakelov geometry*, Cambridge studies in advanced mathematics, vol. 33, Cambridge University Press, 1992.

[46] U. Stuhler – « Eine Bemerkung zur Reduktionstheorie quadratischer Formen », *Arch. Math.* **27** (1976), p. 604–610.

[47] L. Szpiro – « Degrés, intersections, hauteurs », in *Séminaire sur les pinceaux arithmétiques : la conjecture de Mordell* (L. Szpiro, éd.), Astérisque, vol. 127, Soc. Math. France, 1985, p. 11–28.

[48] S.-W. Zhang – « Positive line bundles on arithmetic varieties », *J. Amer. Math. Soc.* **8** (1995), p. 187–221.

A. Chambert-Loir

Centre de Mathématiques
École polytechnique
F-91128 Palaiseau Cedex
E-mail : chambert@math.polytechnique.fr