AST

Séminaire sur les pinceaux de courbes elliptiques (à la recherche de «Mordell effectif») - Pages préliminaires

Astérisque, tome 183 (1990), p. 1-6

<http://www.numdam.org/item?id=AST_1990__183__1_0>

183 ASTÉRISQUE

1990

SÉMINAIRE SUR LES PINCEAUX DE COURBES ELLIPTIQUES

(à la recherche de «Mordell effectif»)

Lucien SZPIRO

Avec la participation de :
Daniel BERTRAND, Jean-Benoît BOST, Renée ELKIK
Marguerite FLEXOR, David W. MASSER, Jean-François MESTRE
Laurent MORET-BAILLY, Joseph OESTERLÉ, Christophe SOULÉ
Lucien SZPIRO

SOCIÉTÉ MATHÉMATIQUE DE FRANCE
Publié avec le concours du CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

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

INTRODUCTION

Ce séminaire s'est tenu en 1988 à l'Institut Henri Poincaré à Paris. Il est centré sur la "conjecture du discriminant" énoncée dans l'exposé 1 : Sur un corps de nombres donné le "discriminant minimal d'une courbe elliptique doit avoir une borne supérieure polynomiale en le "conducteur" de cette courbe.

Les raisons géométriques et la difficulté arithmétique de cette conjecture sont montrées dans l'exposé 1. On y note aussi que le "grand théorème" de Fermat s'en déduit. L'exposé 2 de D.W. Masser (qui a été donné oralement par M. Hindry) montre qu'on ne peut guère avoir mieux qu'un polynôme de degré "$6+\varepsilon$" dans la "conjecture du discriminant". L'exposé 3 de M. Flexor et J. Oesterlé indique une conséquence, due essentiellement à G. Frey sur les points de torsion des courbes elliptiques. Notons qu'une autre conséquence, sur les points d'ordre infini des courbes elliptiques : la conjecture de S. Lang, est montrée dans un article récent de Hindry et Silverman.

Les exposés 4, 5, 6 s'occupent de l'amont de la conjecture : quelles autres conjectures l'impliqueraient ? On pourrait craindre que cet exercice (conjecture implique conjecture) est aurorétique. Nous espérons qu'il n'en est rien. L'exposé 4 de L. Moret-Bailly explique une idée fameuse de Parshin : Une inégalité analogue au théorème de Bogomolov-Miyaoka "$C_1^2 \leq 3\, C_2$" implique un "Mordell effectif" très fort. On montre ensuite qu'un tel "Mordell effectif" très fort pour <u>une</u> courbe modulaire implique la conjecture du discriminant. Notons que récemment L.Moret-Bailly et moi-même avons réussi à montrer qu'un"Mordell effectif" très fort pour <u>une</u> courbe (i.e. non forcément modulaire) implique le même résultat (à paraître).

L'exposé 5, de R. Elkik, démontre le théorème de Manin-Drinfeld par la méthode inédite de P. Deligue. Ce théorème est utilisé dans l'exposé 4. Il s'énonce : la différence entre deux pointes d'une courbe modulaire, est de torsion. L'exposé 6 de J.B. Bost, J.F. Mestre, L. Moret-Bailly explicite les "classes de Chern" de certaines surfaces arithmétiques de genre 2. Une des conséquences des résultats exposé est la prudence requise dans la conjecture analogue à $C_1^2 \leq 3\ C_2$ en arithmétique !

Les exposés 7 et 8 ne sont ni en amont, ni en aval mais rive gauche et rive droite du courant. L'exposé 7 de D. Bertand établit une constante bornant le degré d'isogénies entre courbes elliptiques sur un corps donné (comparer à l'exposé 3). Ce thème a été traité précédemment (et ailleurs) par Faltings, Masser, Wüstholz. L'exposé 8 de C. Soulé compare les théories de Nevanlinna et Arakelov sur l'espace projectif.

L. SZPIRO.

TABLE DES MATIÈRES

SÉMINAIRE SUR LES PINCEAUX DE COURBES ELLIPTIQUES

(à la recherche de "Mordell effectif")

L. Szpiro

Page

RÉSUMÉS DES EXPOSÉS

SZPIRO (L.) *Discriminant et conducteur des courbes elliptiques.*

Cet article présente une conjecture naturelle sur le discriminant des courbes elliptiques. On démontre d'abord cette conjecture sur le corps de fonctions, par une preuve jamais publiée. On explicite ensuite la conjecture pour les courbes de Frey et pour les courbes de Weil. On termine enfin par un exemple du à A. DOUADY qui montre la difficulté d'ordre arithmétique des problèmes qui se posent.

MASSER (D. W.) *Note on a Conjecture of Szpiro.*

A conjecture of Szpiro states that $|D| \leq C(\varepsilon)N^{6+\varepsilon}$ for every elliptic curve defined over the rationals with minimal discriminant D and conductor N. We show that this inequality, if true, cannot be much improved ; for example, it would be false with N^{ε} replaced by any fixed power of $\log N$.

FLEXOR (M.), OESTERLÉ (J.) *Sur les points de torsion des courbes elliptiques.*

Soit K un corps de nombres. On conjecture que le nombres de points de torsion, rationnels sur K, d'une courbe elliptique définie sur K est majoré par une constante qui ne dépend que de K. (Pour $K = \mathbb{Q}$, cet énoncé a été démontré par Mazur, et la constante peut être prise égale à 16). G. Frey, le premier, a vu que la conjecture précédente est impliquée par une autre conjecture, énoncée par Szpiro en 1982, reliant discriminants et conducteurs des courbes elliptiques sur K. Nous présentons ici une démonstration de ce fait, en explicitant les liens entre les constantes qui interviennent dans les deux conjectures.

MORET-BAILLY (L.) *Hauteurs et classes de Chern sur les surfaces arithmétiques.*

Parshin a montré qu'un analogue arithmétique de l'inégalité de Bogomolov-Miyaoka pour les surfaces complexes impliquerait, via une version effective de la conjecture de Mordell, la conjecture du discriminant de Szpiro (et par suite la "conjecture *abc*" et le grand théorème de Fermat en degré assez grand). On donne une démonstration complète de ces résultats, en partant d'une version affaiblie de l'inégalité de Bogomolov-Miyaoka.

ELKIK (R.) *Le théorème de Manin-Drinfeld.*

Si Γ est un sous-groupe de congruence de $S\ell(2,\mathbb{Z})$ et X_Γ la compactification de la courbe $\mathfrak{h}|_\Gamma$, le Théorème de Manin Drinfeld affirme que tout diviseur de degré 0 de X_Γ à support dans les pointes, définit un élément de torsion du groupe de Picard. Cet énoncé est réinterprété par Deligne comme un énoncé de scindage de la structure de Hodge-mixte sur $H^1(\mathfrak{h}|_\Gamma,\mathbb{Q})$, qui est établi en séparant les valeurs propres d'une correspondance de Hecke sur la composante de poids 0 et sur la composante de poids 1 de ce groupe de cohomologie.

BOST (J.B.), MESTRE (J.F.), MORET-BAILLY (L.) *Sur le calcul explicite des "classes de Chern" des surfaces arithmétiques de genre 2.*

Dans cet exposé, nous décrivons comment calculer explicitement les invariants deg $f_* \omega_{X/B}$ et $(\omega_{X/B} . \omega_{X/B})$ définis à la Arakelov, attachés à une courbe semi-stable $f : X \to B = \mathrm{Spec}\, O_K$ de fibre générique lisse et de genre 2 sur l'anneau des entiers d'un corps de nombres K .

Nous calculons ensuite numériquement ces invariants sur deux exemples, à savoir une courbe ayant réduction semi-stable sur $\mathbb{Q}$ (nous présentons une construction de telles courbes), puis la courbe dont la fibre générique admet comme équation affine $y^2 + y = x^5$.

BERTRAND (D.) *Hauteurs et isogénies.*

Soit d un entier > 0 . Dans un récent travail [MW2], Masser et Wüstholz ont établi l'existence d'une constante effectivement calculable $c(d)$ telle que si k désigne un corps de nombres de degré d et E une courbe elliptique définie sur k , de hauteur de Faltings $h(E/k)$, toutes les courbes elliptiques définies sur k et isogènes à E sont liées à E par une isogénie de degré $\leq c(d)h(E/k)^4$. On donne ici une autre démonstration de ce résultat (sous une forme d'ailleurs un peu plus faible). L'outil nouveau est formé par les modèles de Néron, qui permettent d'éviter le recours à des calculs explicites sur les invariants de Weierstrass.

SOULÉ (C.) *Théorie de Nevanlinna et théorie d'Arakelov .*

On exhibe dans ce texte un parallélisme entre les théories de Nevanlinna et d'Arakelov dans le cas de l'espace projectif $\mathbb{P}^n$. La forme de Levine est un courant sur $\mathbb{P}^n(\mathbb{C})$ qui joue un rôle central dans la théorie de Nevanlinna à valeurs dans $\mathbb{P}^n(\mathbb{C})$. On montre que c'est aussi le courant de Green associé à une classe de Chern arithmétique, au sens de la théorie d'Arakelov en dimension supérieure développée par H. Gillet et l'auteur.

L. Szpiro

Discriminant et conducteur des courbes elliptiques

Astérisque, tome 183 (1990), p. 7-18
<http://www.numdam.org/item?id=AST_1990__183__7_0>

Société Mathématique de France
Astérisque 183 (1990)

DISCRIMINANT ET CONDUCTEUR DES COURBES ELLIPTIQUES

L. Szpiro

Cet exposé présente une conjecture sur le discriminant des courbes elliptiques (conjecture 1 dans le texte). Ce sujet a été traité par de nombreux auteurs depuis que je m'en suis préoccupé. (Citons : [V], [O] [H]). Je n'ai donc pas voulu trop alourdir le contenu de ce court exposé et me suis contenté,en tentant de garder l'intelligibilité du texte, de n'y inclure que des faits non écrits ailleurs.

Le premier paragraphe expose la conjecture et en donne la preuve pour le corps de fonctions via la classe de Kodaira-Spencer.

Le deuxième paragraphe explique les exemples de Frey, qui donnent de mirifiques conséquences de la conjecture 1. D'autres conséquences seront expliquées dans le reste du séminaire. Au paragraphe 3 nous étudions le discriminant des courbes de Weil et nous donnons des exemples, dus à A. Douady, qui montrent la difficulté des problèmes qui se posent.

Les notations et conventions adoptées dans cet article sont celles de [Sz 1] et de [D]. En particulier une courbe elliptique sera toujours munie d'une section unité ([D]) , si elle a un modèle semi-stable celui-ci sera régulier ([Sz 1]) (compactification relative du modèle de Néron). Je remercie le référée de la revue Astérisque pour le travail minutieux effectué sur ce court article.

L'exposé oral du séminaire sur ce sujet a été fait par M. Hindry. Je me suis inspiré de ses notes [H] dans le § 2 .

1. UNE CONJECTURE SUR LE DISCRIMINANT DES COURBES ELLIPTIQUES.

En 1978 j'ai démontré le théorème qui suit,reliant le "discriminant" et le "conducteur" d'une courbe elliptique sur un corps de fonctions. La démonstration de cet énoncé est essentiellement contenue dans [Sz 1]. Mais, bien des mathématiciens s'en sont plaints,car les énoncés de loc. cit. semblent ne concerner que les courbes de genre au moins deux.

THÉORÈME 1. Soit $f : E \to C$ un morphisme propre et plat d'une surface E, lisse sur un corps k, dans une courbe C, projective, lisse de genre q et géométriquement connexe sur e.
Supposons que la fibre générique de f soit une courbe elliptique lisse et géométriquement connexe sur le corps de fonctions de C. Supposons de plus que f ne soit pas isotrivial et que ses fibres dégénérées soient semi-stables. Alors, si Δ_E est le diviseur discriminant de f et si s est le nombre de points géométriques de C dont la fibre n'est pas lisse on a :

$$\deg \Delta_E \leq p^e\, 6(2q - 2 + s)$$

où p est la caractéristique de k, et p^e le degré d'inséparabilité du morphisme de C dans la droite des "j", déduit de f. (Si la caractéristique de k est nulle on convient que $p^e = 1$).

Démonstration. On a deux suites exactes fondamentales :

(1) $0 \to f^* \Omega^1_{C/k} \to \Omega^1_{E/k} \to \Omega^1_{E/C} \to 0$

(II) $0 \to \Omega^1_{E/C} \to \omega_{X/C} \to \bigoplus\limits_{\substack{P \text{ singulier} \\ \text{dans sa fibre}}} k(P) \to 0$

où $\Omega^1_{Y/Z}$ est le faisceau des différentielles de Y sur Z, et $\omega_{Y/Z}$ est le faisceau dualisant relatif si $Y \to Z$ est localement d'intersection complète.

Notons S le diviseur réduit de C tel que $E \to C$ soit lisse sur $C - S$. En appliquant le fonteur f_* aux deux suites on obtient :

a) un morphisme

$$f_* \Omega^1_{E/C} \to R^1 f_* f^* \Omega^1_{C/k} = \Omega^1_{C/k} \otimes \omega_E^{-1}$$

où $\omega_E = f_* \omega_{E/C}$ (notons que $\omega_{E/C} = f^* \omega_E$). Ce morphisme coïncide avec l'application de Kodaira-Spencer sur $C - S$ (qui ici n'est autre que la dérivée de l'application j).

b) $0 \to f_* \Omega^1_{E/C} \to \omega_E \to \bigoplus_{P \text{ singulier}\ldots} k(P)$

On déduit de cette suite exacte que

$$f_* \Omega^1_{E/C} \simeq \omega_E(-S) \qquad \text{(S est réduit !!)}$$

On a donc, par a) et b) un morphisme

$$\omega_E^{\otimes 2} \to \Omega^1_{C/k}(S)$$

qui est non nul quand la dérivée de l'application j ne s'annulle pas. En caractéristique zéro c'est le cas si j n'est pas constant, en caractéristique $p > 0$ c'est le cas si f n'est pas un "pull-back" par le morphisme de Frobénius de C.

En prenant les degrés de ces deux faisceaux inversibles, et en notant qu'on a $\deg \Delta_E = 12 \deg \omega_E$ on obtient le théorème 1. □

Notons qu'il est apparu, plus tard, de nombreuses démonstrations différentes (Frey [F1], Hindry-Silverman [H,S] par la formule d'Hurwitz quand $k = \mathbb{C}$ et encore plus tard par "a,b,c" [0] en toute caractéristique).

L'analogie entre les corps de nombres et les corps de fonctions d'une variable pousse à conjecturer un énoncé analogue pour les courbes elliptiques sur un corps de nombres. Cette analogie est renforcée par la théorie d'Arakelov, qui en mettant des métriques, dites permises, aux places à l'infini donne un degré "naturel" $\deg_{Ar}(\omega_E)$ au faisceau ω_E défini plus haut.

Ces idées se trouvent confortées par le théorème suivant dont j'ai publié une démonstration dans [Sz 2] :

<u>THÉORÈME</u>. Soit E une courbe elliptique semi-stable sur un corps de nombres K alors on a :

$$12 \deg_{Ar}(\omega_E) = \log \text{Norme}_{K/\mathbb{Q}} (\Delta_{\min}(E)) .$$

J'ai donc soumis, notamment à l'occasion de l'école d'été de Hanovre en septembre 82, la conjecture suivante :

<u>CONJECTURE 1.</u> Soit K un corps de nombres, il existe une constante $\sigma(K)$ ne dépendant que de K telle que, pour toute courbe elliptique E sur K, de conducteur N_E et de discriminant minimal Δ_E on ait :

$$\text{Norme}_{K/\mathbb{Q}} (\Delta_E) \leq (\text{Norme}_{K/\mathbb{Q}}(N_E))^{\sigma(K)} .$$

On peut énoncer une conjecture plus optimiste :

<u>CONJECTURE 1 forme forte</u>. Soit K un corps de nombres. Alors pour tout nombre réel positif ε, il existe une constante $C(K,\varepsilon)$ telle que :

pour toute courbe elliptique E sur K de discriminant minimal Δ_E et de conducteur N_E on ait

$$\mathrm{Norme}_{K/\mathbb{Q}}\,(\Delta_E) \leq C(K,\varepsilon)\,(\mathrm{Norme}_{K/\mathbb{Q}}(N_E))^{6+\varepsilon}$$

Notons que Masser ([M]) a montré qu'on ne peut espérer un exposant plus petit que $6+\varepsilon$.

2. LES COURBES DE FREY.

G. Frey [Fr 1] a donné de très brillants exemples de courbes elliptiques semi-stables. Rappelons brièvement sa construction.

Soient a,b,c des entiers sans facteurs communs tels que $a+b = c$. Considérons la courbe elliptique $E_{a,b,c}$ d'équation (non minimale)

$$y^2 = x(x+a)\,(x-b)$$

Frey montre les faits suivants :

a) Si $2^4/a$ et $b \equiv -1\ (4)$ alors $E_{a,b,c}$ est semi-stable.

b) Dans ce cas son équation minimale est donnée par

$$y^2 + xy = x^3 + \frac{a-b-1}{4}\,x^2 - \frac{abx}{16}$$

c) Toujours sous les hypothèses de a) le discriminant minimal de $E_{a,b,c}$ est égal à $2^{-8}\,a^2\,b^2\,c^2$.

Si on applique la conjecture 1 a une courbe de Frey on obtient :

$$\text{Si}\quad a+b = c \qquad (a,b) = 1 \qquad \text{alors}$$

$$|abc| \leq 2^8 \Big(\prod_{p|abc} p\Big)^{\sigma/2} \qquad \text{où}\ \sigma = \sigma(\mathbb{Q})$$

Je ne résiste pas à appliquer cette conjecture à une solution hypothétique de l'équation de Fermat : $x^p + y^p = z^p \qquad (xyz) \neq 0)$

la conjecture 1 impliquerait que :

$$p \leq \frac{8 \log 2}{\log xyz} + \frac{\sigma}{2}$$

ce qui prouverait, au moins, "Fermat asymptotique".

Notons aussi que si l'on regarde les solutions entières d'une équation de la forme

$$a_1 X^{n_1} + a_2 X^{n_2} = a_3 X^{n_3}$$

où les a_i sont premiers entre eux, la conjecture 1 implique qu'il existe une constante $C(a_1,a_2,a_3)$ telle que : l'équation ci-dessus n'ait pas de solutions toutes non nulles et premières entre elles pour $\inf(n_i) \geq C(a_1,a_2,a_3)$.

J. Oesterlé dans [O] a donné les exemples suivants qui montrent que dans la conjecture 1 forte on ne peut prendre $\varepsilon = 0$:

Partant de trois nombres premiers entre eux a_0,b_0,c_0 tels que $a_0 + b_0 = c_0$ définissons la suite (a_n,b_n,c_n) par :

$$c_{n+1} = c_n^2 \qquad b_{n+1} = (a_n - b_n)^2 \qquad a_{n+1} = 4\, a_n\, b_n$$

on voit facilement que $a_n + b_n = c_n$ et que ces trois nombres n'ont pas de facteur commun.

Pour tout nombre entier n notons $R(n)$ (pour radical de n) le produit sans facteurs carrés des nombres premiers divisant n . Le lecteur vérifiera facilement qu'on a :

$$\frac{a_{n+1}\, b_{n+1}\, c_{n+1}}{R(a_{n+1}\, b_{n+1}\, c_{n+1})^3} \cdot \frac{R(a_n\, b_n\, c_n)^3}{a_n\, b_n\, c_n} \geq 4$$

et donc que $\Delta(E_{a_n,b_n,c_n}) \Big/ N\left(E_{a_n,b_n,c_n}\right)^6$ n'est pas borné.

Remarque : Le processus de récurrence définissant la suite a_n, b_n, c_n peut s'interpréter de la façon suivante : c'est la multiplication par 2 dans le groupe multiplicatif $\mathbb{C}_m$ réalisé comme le cercle de rayon 1 dans $\mathbb{C}$. En effet, un triplet tel que $a+b = c$ conne sur une extension quadratique de $\mathbb{Q}$ un point $\left(\sqrt{\frac{a}{b}}, \sqrt{\frac{b}{c}}\right)$ du cercle $x^2 + y^2 = 1$, il est alors facile de voir que les formules pour $\sin 2\theta$ et $\cos 2\theta$ expliquent la récurrence. Il serait intéressant de voir ce que donne la multiplication par deux sur une courbe elliptique ayant des points d'ordre infini et une équation en trois monomes (e.g. $Y^3 = X^3 + 6$) .

On a vu plus haut, en utilisant les courbes de Frey que la conjecture 1 prend la forme "lycéenne" suivante : Il existe une constante k telle que si a,b,c sont des entiers sans facteurs communs satisfaisant à $a+b = c$ alors $|abc| \leq \left(\prod_{p|abc} p\right)^k$

(sous la forme forte : pour tout $\varepsilon > 0$ il existe une constante $C(\varepsilon)$ telle que

$$|abc| \leq C(\varepsilon) \left(\prod_{p|abc}\right)^{3+\varepsilon}$$

Masser et Oesterlé ont proposé, alors, la conjecture suivante : $a+b = c$, mêmes hypothèses alors

$$\sup(|a|,|b|,|c|) \leq \left(\prod_{p|abc} p\right)^{\ell}$$

(ℓ une constante). Il est clair que la conjecture 1 implique celle-ci si on ne dit rien sur ℓ . La forme forte de la conjecture de Masser Oesterlé est : Pour tout $\varepsilon > 0$ il existe une constante $C(\varepsilon)$ telle que si $a+b = c$ (a,b,c sans facteur communs) alors

$$\sup(|a|,|b|,|c|) \leq C(\varepsilon) \left(\prod_{p|abc} p\right)^{1+\varepsilon}$$

Cette forme forte ne semble pas être conséquence de la conjecture 1 forte. Par contre elle implique clairement la conjecture forte sur $|abc|$ et même la forme forte de la conjecture 1 (cf. par exemple Vojta) en raisonnant sur l'équation :

$$c_4^3 - c_6^2 = 1728\, \Delta .$$

Notons qu'en étudiant le discriminant d'une courbe de Frey quotientée par un point d'ordre 2 comme dans [Sz 2] on voit que

$|\Delta_{min}(E)| \leq C(\varepsilon)\, N(E)^{6+\varepsilon}$

implique $\sup(|a|,|b|,|c|) \leq C'(\varepsilon) \left(\prod_{p|abc} p\right)^{6/5+\varepsilon}$.

En effet la valeur absolue du discriminant d'un tel quotient bien choisi d'une courbe de Frey est égal à

$$2^{-4}\, abc^4 \qquad (2^4 | a \text{ , et } a,b,c \text{ sont positifs }) .$$

Remarquons enfin une autre conséquence - conjecturale donc - de la conjecture 1 : Il existe une constante σ telle que pour tout nombre entier a

$$a \leq \left(\prod_{p|a(a+1)} p\right)^{\sigma}$$

3. <u>LES COURBES DE WEIL</u>.

Une courbe elliptique E sur $\mathbb{Q}$ est dite de Weil si elle est dominée par une courbe modulaire $X_0(N)$, le morphisme $\varphi : X_0(N) \to E$ étant défini sur $\mathbb{Q}$. On dit de plus que E est une courbe de Weil forte si $H_1(\varphi,\mathbb{Z})$ (ou $\pi_1(\varphi)$) est surjectif. Shimura [Sh] a montré qu'il y a correspondance bianivoque entre les courbes de Weil fortes images de $X_0(N)$ et les nouvelles formes modulaires de poids deux, et de niveau N . Carayol, [C], a montré que pour une courbe de Weil forte E , image de $X_0(N)$, N est égal au conducteur de E . Taniyama a conjecturé que toute courbe elliptique sur $\mathbb{Q}$ est de Weil. A. Weil [W] a montré que si une courbe elliptique E sur $\mathbb{Q}$, ainsi que ses différentes "tordues", ont une fonction L satisfaisant une equation fonctionnelle attendue quand on change s en 2-s , alors la transformée de Mellin de la fonction L de E est une forme modulaire de poids 2 . Par le résultat de Shimura cité plus haut et le théorème de Faltings (conjecture de Tate) on en déduit qu'une telle courbe elliptique est de Weil.

On voit ainsi, bien qu'à l'heure actuelle la conjecture de Taniyama ne soit pas démontrée, qu'il est crucial de tester une conjecture sur les courbes elliptiques,sur les courbes de Weil. Un effort dans ce sens a été entrepris par Golfeld ([G] et Mestre-Oesterlé [M-O]. Il est raisonnable de dire que c'est G. Frey qui a eu le premier l'intuition que la conjecture de Taniyama entrainait "Fermat" via la conjecture 1. On ne sait pas, au moment où j'écris ces lignes que la conjecture 1 est vraie pour les courbes de Weil.

Notons cependant que Ribet [R] a montré que "Taniyama" implique "Fermat" mais sans passer par la conjecture 1 .

PROPOSITION 1. Soit E une courbe de Weil forte f la nouvelle forme modulaire de poids 2 et de niveau N , normalisée, correspondant à E . Si α est une différentielle de Néron sur E on à $\varphi^* \alpha = c\, f\, dz$ où c (constante de Manin) est un entier.

On conjecture que $|c| = 1$ et on sait, par Raynaud, que si N est sans facteur carré, $|c|$ est borné absolument. Si $\| f \|$ est la norme de Peterson de f et $h_F(E)$ la hauteur modulaire de E (introduite par Faltings-Arakelov) on a :

$$\frac{1}{2} \log \deg \varphi = h_F(E) + \log \| f_E \| + \log |c| + \log 2\pi$$

(cf. par exemple [Si]).

D'autre part Faltings a démontré [Fa 1] au moins quand E est semi-stable sur $\mathbb{Q}$ (ici N sans facteurs carrés), qu'on a :

$$12\, h_F(E) = \log |\Delta_{min}(E)| - \log |\Delta(\tau)\ \mathrm{Im}(\tau)^6|$$

On voit ainsi qu'une borne polynomiale

$$\deg \varphi \leq N^\rho \qquad (\rho \text{ indépendant de } N \text{ et } E)$$

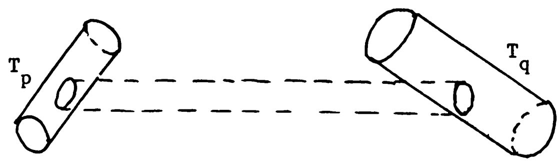
implique la conjecture 1 car on sait minorer polynomialement le carré scalaire de Peterson (cf. [G]).

On peut naturellement se demander si on peut borner le degré d'un morphisme φ , non constant, d'une courbe X de genre $g \geq 2$ dans une courbe elliptique E sur $\mathbb{C}$, en fonction de g . (Notons que le genre de $X_0(N)$ est polynomial en N). On voit, comme le genre de E vaut un, que la formule de Hurwitz ne donne rien ! D'autre part, il faut imposer $H_1(\varphi)$ surjectif sinon les isogénies de E retirent tout espoir. Même dans ce cas là, A. Douady nous a fourni les exemples simples suivants qui, pour nous, signifient que le problème de borner le degré de φ est de nature arithmétique.

Exemples de A. Douady. Soient p et q deux entiers premiers entre eux nous allons construire un morphisme algébrique sur $\mathbb{C}$, d'une courbe de genre 2 , X , dans une courbe elliptique E , surjectif sur les H_1 et de degré $p+q$.

Soient trois tores T_1, T_p, T_q que nous considérons comme des cylindres dont les extrémités sont identifiées. De plus T_i sera de longueur i ($i = 1, p, q$) et de même base. On envoie les tores T_p et T_q sur T_1 par les morphismes φ_p et φ_q correspondants aux identifications : T_p est l'empilement de p tores identiques à T_1 et T_q est l'empilement de q tores identiques à T_1 .

Soit α_1 , un "segment de droite" assez petit dans T_1 et soient α_p et α_q deux "segments de droites" s'envoyant bijectivement sur α_1 . Remplaçant les α_i , $i = p,q$ par des "cercles" C_i on peut recoller T_p et T_q selon C_p et C_q



on obtient ainsi une surface **topologique** compacte X de genre 2, avec un morphisme continu de degré $p+q$, $\varphi : X \to T_1 = E$, ramifié seulement en deux points (les extrémités de α_1) .

On a les deux faits suivants :

a) $H_1(X) \to H_1(T_1)$ est surjectif: si σ et τ sont les générateurs de $H_1(T_1)$ (cf. le dessin) σ , $p\tau$ et $q\tau$ sont dans l'image de φ . p et q étant premiers entre eux, σ et τ sont dans l'image de φ $H_1(\varphi)$.

b) Fixant une structure algébrique (analytique) sur T_1 , c'est un théorème de Riemann qu'il existe une structure algébrique sur X qui rende φ un morphisme algébrique.

U.R.A. 0213 du C.N.R.S.
"Analyse complexe et Géométrie"
Université de Paris VI
I.H.P.
11, rue Pierre et Marie Curie
75005 - PARIS CEDEX 05

BIBLIOGRAPHIE

[C] CARAYOL H. "Sur les représentations ℓ-adiques associées aux formes modulaires de Hilbert". Ann. Sc. ENS 19 (1986), 409-468.

[F 1] FALTINGS G. "Calculus on arithmétic surfaces". Annals of Maths. vol. 119 (1984) 387-424.

[F 2] FALTINGS G. "Endlichkeitssätze fur abelshe varietäten über Zalhenkörpern". Inventiones Math. vol. 73, Fasc. 3 (1983), 349-366.

[Fr] FREY G. "Links between elliptic curves and certain dioplantine equations". Annales universitatis Saraviensis, series mathematicae I., 1986.

[G] GOLFELD D. "Modular elliptic curves and dioplantine problems" à paraître.

[H.S.] HINDRY M. et SILVERMAN J.H. "The cannonical height and integral points on elliptic curves". Inv. Math. 93, 419-450 (1988).

[H] HINDRY M. "a,b,c , conducteur, discriminant". Preprint PARIS VI, 1988.

[M] MASSER. "On a conjecture of Szpiro". Ce volume.

[M.S] MAZUR B. et SWINNERTON-DYER H.P.F. "Arithmetic of Weil curves". Inv. Math. 25 (1974) 1-61.

[O] OESTERLE J. "Nouvelles approches du << théorème >> de Fermat". Séminaire Bourbaki n° 694, 1988.

[Sh] SHIMURA G. "Arithmetic theory of arithmetic functions". Publications of the mathematical society of Japan, Iwanami Shoten Publishers and Princeton University press 1971.

[Si] SILVERMAN J.H. "Heights and elliptic curves" in Arithmetic Geometry, Springer-Verlag New York 1986.

[Sz 1] SZPIRO L. "Propriétés numériques du faisceau dualisant relatif" dans "Séminaire sur les pinceaux de courbes de genre au moins deux" Astérisque n° 89.

[Sz 2] SZPIRO L. "Sur les propriétés numériques du dualisant relatif d'une surface arithmétique" à paraître volume Grothendieck.

[V] VOJTA P. "Diophantine approximations and value distribution theory". Lecture notes in math., 1239, Springer-Verlag 1987.

[W] WEIL A. "Zeta function and Mellin transform". Algebraic geometry Bombay 1968, TIFR 1969, 400-402.

D. W. MASSER

Note on a conjecture of Szpiro

Astérisque, tome 183 (1990), p. 19-23
<http://www.numdam.org/item?id=AST_1990__183__19_0>

Société Mathématique de France
Astérisque 183 (1990)

NOTE ON A CONJECTURE OF SZPIRO

D. W. MASSER

1. Elliptic Curves.

L. Szpiro has put forward the

Conjecture. For each $\varepsilon > 0$ there is a constant $C(\varepsilon)$ with the following property. Let E be any elliptic curve defined over the rationals with minimal discriminant D and conductor N. Then $|D| \leq C(\varepsilon)N^{6+\varepsilon}$.

This has a number of remarkable consequences (see for example [V] and [HS]), and so a proof would be of considerable interest. Perhaps also a disproof would have some significance. In the present note we show at least that the inequality of the conjecture cannot be much improved; in particular, it would be false in the form $|D| \leq CN^6(\log N)^k$ for any absolute constants C and k. This research was supported in part by the National Science Foundation.

Theorem. For any $\delta > 0$ and N_0 there is an elliptic curve E defined over the rationals whose minimal discriminant D and conductor $N \geq N_0$ satisfy

$$|D| \geq N^6 \exp\{(24-\delta)(\log N)^{1/2}(\log\log N)^{-1}\} .$$

The proof of this result will be reduced to number theory using the following observation. First for a non-zero rational integer n we write $S(n)$ for the square-free kernel of n; that is, the product of all distinct positive primes dividing n.

Lemma 1. Suppose a,b,c are coprime rational integers with

$$a+b+c = 0 , \quad a \equiv 1 \pmod 4), \quad c \equiv 0 \pmod{32} .$$

Then the equation

$$y^2 = x(x-a)(x+b) \tag{1}$$

defines an elliptic curve E whose minimal discriminant D and conductor N satisfy

$$|D| = 2^{-8}(abc)^2 , \quad N = S(abc) .$$

Proof. In the standard notation ([S] p. 46) the equation (1) gives

$$c_4 = 16(a^2 + ab + b^2) , \quad \Delta = 16(abc)^2 .$$

Let p be an odd prime. It is easy to verify that if p divides Δ then p cannot divide c_4. It follows (see [S] p. 172) that the equation (1) is minimal for all $p \neq 2$.

This is not so for $p = 2$. Indeed, the change of variables

$$x = 4x' + a \ , \quad y = 8y' + 4x'$$

leads to the equation

$$y'^2 + x'y' = x'^3 + (\alpha + 8\beta)x'^2 + 2a\beta x' \ , \tag{2}$$

where the integers α and β are defined by

$$a = 4\alpha + 1 \ , \quad c = -32\beta \ .$$

For this new equation we have

$$c_4' = a^2 + ab + b^2 \ , \quad \Delta' = 2^{-8}(abc)^2 \ ;$$

and since c_4' is odd, we see now that (2) is minimal for $p = 2$.

The formula for D follows at once. The formula for N follows from the definition ([S] p. 361). For if p does not divide abc (in particular $p \neq 2$) then E has good reduction at p. If p divides abc and $p \neq 2$ then (1) is minimal and p does not divide c_4, so E has multiplicative reduction ([S] p. 180). Finally if $p = 2$ then (2) is minimal, c_4' is odd, and again E has multiplicative reduction. This completes the proof of Lemma 1.

It is clear that our Theorem is a consequence of Lemma 1 together with the following

Proposition. <u>For any</u> $\delta > 0$ <u>and</u> S_0 <u>there are coprime rational integers</u> a,b,c <u>with</u>

$$a + b + c = 0 \ , \quad a \equiv 1 \pmod 4 \ , \quad c \equiv 0 \pmod{32}$$

<u>and</u> $S = S(abc) \geq S_0$ <u>satisfying</u>

$$|abc| \geq S^3 \exp\{(12-\delta)(\log S)^{1/2}(\log\log S)^{-1}\} \ . \tag{3}$$

A similar result with the weaker inequality

$$\max(|a|,|b|,|c|) \geq S \exp\{(4-\delta)(\log S)^{1/2}(\log\log S)^{-1}\}$$

was established recently by C. Stewart and R. Tijdeman [ST]. In the next section we shall prove our Proposition by means of a small modification in their proof.

2. Number Theory. We require a preliminary lemma. For $y \geq 0$ write $\theta(y) = \sum_{p \leq y} \log p$ as usual, and for $x \geq 0$ let $\Psi_o(x,y)$ be the number of positive odd integers not exceeding x that are divisible only by primes not exceeding y.

Lemma 2. For any $\delta > 0$ and all sufficiently large x we have

$$e^{-\theta(y)}\Psi_o(x,y) \geq \exp\{(4-\delta)(\log x)^{1/2}(\log\log x)^{-1}\},$$

where $y = (\log x)^{1/2}$.

Proof. Let $\Psi(x,y)$ denote the usual number of positive integers not exceeding x that are divisible only by primes not exceeding y. Good estimates when $y = (\log x)^{1/2}$ were obtained by V. Ennola [E]; we use the version

$$\Psi(x,y) = \exp\{\pi(y)\log\log x - y + O(y(\log y)^{-2})\}$$

given by K.K. Norton ([N] p. 25). Here

$$\pi(y) = y(\log y)^{-1} + y(\log y)^{-2} + O(y(\log y)^{-3})$$

is the usual prime counting function, and we deduce that

$$\Psi(x,y) = \exp\{y + 2y(\log y)^{-1} + O(y(\log y)^{-2})\}. \tag{4}$$

Clearly also

$$\Psi(x,y) = \sum_{h=o}^{\infty} \Psi_o(2^{-h}x,y) = \sum_{h=o}^{H} \Psi_o(2^{-h}x,y) \leq (H+1)\Psi_o(x,y) \tag{5}$$

for $H = [(\log x)/(\log 2)]$. Finally

$$\theta(y) = y + O(y(\log y)^{-2}), \tag{6}$$

and this together with (4) and (5) leads to the inequality of Lemma 2.

Proof of Proposition. Select x large, put $y = (\log x)^{1/2}$, and let p be the least prime greater than y. Write $T = \Psi_0(x,y)$ and define the positive integer t by

$$x \leq 2^t < 2x .$$

From Lemma 2 we see that $T/pt \to \infty$ as $x \to \infty$. Define the positive integer n by

$$\frac{1}{2}T \leq 2^n pt < T ,$$

and assume x is so large that $n \geq 5$. Since $T > 2^n pt$, a simple application of the Box Principle enables us to find $t+1$ odd integers $x_0, \ldots, x_t$, divisible only by primes not exceeding y, satisfying

$$1 \leq x_0 < x_1 < \ldots < x_t \leq x ,$$

and in the same residue class modulo $2^n p$. Since $2^t \geq x$, we can find i with $1 \leq i \leq t$ and

$$x_i \leq 2x_{i-1} . \tag{7}$$

Let d be the highest common factor of x_i and x_{i-1}, and write

$$a = \pm x_i/d , \quad b = \mp x_{i-1}/d , \quad c = \mp(x_i - x_{i-1})/d ,$$

where the sign is chosen such that $a \equiv 1 \pmod 4$. Since d is odd and $n \geq 5$, we also have $c \equiv 0 \pmod{32}$; and clearly $a+b+c = 0$. Further $p > y$ and so p does not divide x_i; thus p does not divide d. Because p divides $x_i - x_{i-1}$, it must divide c, so that

$$S = S(abc) \geq p .$$

Therefore by assuming x sufficiently large we may suppose $S \geq S_0$ as required.

It remains to check (3). Now clearly $S(ab) \leq \frac{1}{2}e^{\theta(y)}$, and since 2^n divides c we have $S(c) \leq 2^{-(n-1)}|c|$. Thus

$$S \leq S(ab)S(c) \leq 2^{-n}e^{\theta(y)}|c| . \tag{8}$$

Also $|a| \geq |c|$, and (7) gives $|b| \geq \frac{1}{2}|a| \geq \frac{1}{2}|c|$, so that

$$|abc| \geq \frac{1}{2}|c|^3 \geq \frac{1}{2}S^3(2^n e^{-\theta(y)})^3 .$$

Further $p \leq 2y$ and so

$$2^n \geq T/(2pt) \geq T/(4yt) \geq (1/8)T(\log x)^{-3/2} .$$

Therefore

$$|abc| \geq 2^{-10}S^3(\log x)^{-9/2}(e^{-\theta(y)}T)^3 .$$

Hence by Lemma 2, if x is sufficiently large we have

$$|abc| \geq S^3\exp\{(12-\delta)(\log x)^{1/2}(\log\log x)^{-1}\} .$$

The Proposition follows on noting from (6) and (8) that if x is sufficiently large then

$$S \leq e^{\theta(y)}|c| \leq e^{2y}x \leq x^{1+\delta} .$$

References

[E] V. Ennola, On numbers with small prime divisors, Ann. Acad. Sci. Fenn. (Series AI) 440 (1969), 1-16.

[HS] M. Hindry and J.H. Silverman, The canonical height and integral points on elliptic curves, Invent. Math. 93 (1988), 419-450.

[N] K.K. Norton, Numbers with small prime factors, and the least k-th power non-residue, Memoirs A.M.S. Vol. 106 (1971).

[S] J.H. Silverman, The arithmetic of elliptic curves, Graduate Texts in Math. Vol. 106, Springer-Verlag, New York - Berlin - Heidelberg - Tokyo 1985.

[ST] C.L. Stewart and R. Tijdeman, On the Oesterlé-Masser conjecture, Monats. Math. 102 (1986), 251-257.

[V] P. Vojta, Dicphantine approximations and value distribution theory, Lectures Notes in Math. Vol. 1239, Springer-Verlag, Berlin - Heidelberg - New York - London - Paris - Tokyo 1987.

D.W.MASSER
University of Michigan
Ann Arbor, USA

M. FLEXOR
J. OESTERLÉ

Sur les points de torsion des courbes elliptiques

Astérisque, tome 183 (1990), p. 25-36
<http://www.numdam.org/item?id=AST_1990__183__25_0>

Société Mathématique de France
Astérisque 183 (1990)

Sur les points de torsion des courbes elliptiques

par M. Flexor et J. Oesterlé [1]

1. Énoncé des résultats

Soit K un corps de nombres. Une courbe elliptique définie sur K ne possède qu'un nombre fini de points de torsion rationnels sur K. On a la conjecture classique suivante (dont une démonstration, qui malheureusement semble incomplète, a été publiée dans [1]) :

CONJECTURE 1. - *Il existe une constante* A(K) *telle que, pour toute courbe elliptique* E *définie sur* K, *on ait*

(1) $$\mathrm{Card}(E(K)_{\mathrm{tors}}) \leq A(K).$$

Lorsque K est égal à $\mathbb{Q}$, la conjecture 1 est une conséquence du résultat plus précis suivant de Mazur ([5], th.8) : si E est une courbe elliptique définie sur $\mathbb{Q}$, le groupe $E(\mathbb{Q})_{\mathrm{tors}}$ est isomorphe à l'un des groupes

$$\mathbb{Z}/n\mathbb{Z} \qquad \text{avec } 1 \leq n \leq 10 \text{ ou } n = 12,$$

$$\text{ou} \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} \qquad \text{avec } 1 \leq n \leq 4\,,$$

et par suite est d'ordre au plus 16.

Revenons au cas où K est un corps de nombres quelconque. Manin ([4]) démontre en 1969 que si p est un nombre premier, la courbe modulaire $X_0(p^n)$ n'a , pour n assez grand, qu'un nombre fini de points rationnels sur K (un cas particulier de la conjecture de Mordell, démontrée par Faltings en 1983) ; il en déduit que l'ordre de la composante p-primaire de $E(K)_{\mathrm{tors}}$ est majoré par une constante ne dépendant que de p et de K.

---

(1) Le second auteur remercie le Tata Institute of Fundamental Research pour un séjour à Bombay durant lequel a été rédigé cet article.

Étant donnée une courbe elliptique E définie sur K, nous noterons Δ_E l'idéal discrimant minimal de E et N_E l'idéal conducteur de E ; lorsque E est semi-stable (i.e. a en toute place finie de K bonne réduction ou réduction de type multiplicatif), N_E est le produit des idéaux premiers de l'anneau des entiers de K qui divisent Δ_E. Posons

(2) $$\beta_E = \frac{\log(N_{K/\mathbb{Q}}(\Delta_E))}{\log(N_{K/\mathbb{Q}}(N_E))}$$

(avec par convention $\beta_E = 1$ lorsque $N_{K/\mathbb{Q}}(N_E)$ est égal à 1, c'est-à-dire lorsque E a partout bonne réduction).

Szpiro formule en 1982 la conjecture suivante (cf. [7], conj. 1) :

CONJECTURE 2. - *Il existe une constante* B(K) *telle que, pour toute courbe elliptique semi-stable* E *définie sur* K, *on ait*

(3) $$\beta_E \leq B(K).$$

(Une forme optimiste de la conjecture 2 affirme que pour tout $\varepsilon > 0$ il n'existe, à K-isomorphisme près, qu'un nombre fini de courbes elliptiques définies sur K, semi-stables ou non, pour lesquelles on a $\beta_E \geq 6 + \varepsilon$).

Frey ([2]), le premier, a remarqué que la conjecture 2 implique la conjecture 1. Dans cette direction, il convient de citer la majoration, obtenue par voie analytique par Hindry et Silverman ([3], th.7.1) :

(4) $$\mathrm{Card}(E(K)_{tors}) \leq (20\, \beta_E)^{8[K:\mathbb{Q}]}\, 10^{\beta_E}.$$

Dans cet article, nous établissons par voie algébrique, en suivant les idées de Frey, d'autres majorations de l'ordre de $E(K)_{tors}$, qui montrent que la conjecture 2 implique la conjecture 1.

Lorsque la courbe elliptique E (définie sur K) n'est pas semi-stable, ou bien lorsqu'elle a partout bonne réduction, l'ordre de $E(K)_{tors}$ est majoré par une constante qui ne dépend que de K, comme il résulte des trois théorèmes suivants :

THÉORÈME 1. - *Soit* E *une courbe elliptique définie sur* K, *qui a mauvaise réduction de type additif en au moins deux places finies de* K, *de caractéristiques résiduelles distinctes. On a*

(5) $$\mathrm{Card}(E(K)_{tors}) \leq 12.$$

Remarque 1. - L'inégalité (5) est optimale : ainsi par exemple la courbe elliptique E d'équation $y^2 - 2y = x^3$ a mauvaise réduction de type additif aux places de $K = \mathbb{Q}(\sqrt{-3})$ de caractéristiques résiduelles 2 et 3, et le groupe $E(K)_{tors}$ est d'ordre 12.

THÉORÈME 2. - *Soit* E *une courbe elliptique définie sur* K, *qui a mauvaise réduction de type additif en au moins une place finie de* K. *On a*

(6) $$\mathrm{Card}(E(K)_{tors}) \leq 48[K:\mathbb{Q}].$$

Remarque 2. - Soient p un nombre premier et L une extension finie de $\mathbb{Q}_p$. Nous démontrerons que si une courbe elliptique E définie sur L a mauvaise réduction de type additif, on a $\mathrm{Card}(E(L)_{tors}) \leq 48e$, où e est l'indice de ramification de L sur $\mathbb{Q}_p$. Le théorème 2 s'en déduit aussitôt en prenant pour L le complété de K en une place finie en laquelle la courbe elliptique a mauvaise réduction de type additif.

THÉORÈME 3. - *Soit* E *une courbe elliptique définie sur* K *qui a partout bonne réduction. On a*

(7) $$\mathrm{Card}(E(K)_{tors}) \leq 5.2^{[K:\mathbb{Q}]}.$$

Remarque 3. - Seule l'hypothèse que E a bonne réduction en une place de K de caractéristique résiduelle 2 est utilisée dans la démonstration de l'inégalité (7). Il serait intéressant de savoir si, sous les hypothèses du théorème 3, le cardinal de $E(K)_{tors}$ est majoré par une fonction polynomiale de $[K:\mathbb{Q}]$.

Si E est une courbe elliptique définie sur K, posons

(8) $$\beta'_E = \sup_F \beta_F ,$$

où F parcourt l'ensemble des courbes elliptiques K-isogènes à E. (À K-isomorphisme près, il n'y a qu'un nombre fini de telles courbes, d'après les résultats de Serre exposés dans [6]). La conjecture 2 de Szpiro entraîne la conjecture 1 d'après les théorèmes 1, 2, 3 précédents et le théorème suivant :

THÉORÈME 4 (Frey). - *Soit* E *une courbe elliptique semi-stable définie sur* K, *qui a mauvaise réduction en au moins une place finie de* K. *On a*

(9) $$\mathrm{Card}(E(K)_{\mathrm{tors}}) \leq \beta_E'^2.$$

2. Points de torsion des groupes formels

Soit L un corps complet pour une valuation discrète v, que l'on suppose normée : on a $v(L^{\times}) = \mathbb{Z}$. Notons A l'anneau de valuation de v et $\mathfrak{m}$ l'idéal maximal de A. Supposons que L soit de caractéristique 0 et que le corps résiduel $A/\mathfrak{m}$ soit de caractéristique $p > 0$. Enfin soit $e = v(p)$ l'indice de ramification absolu de L.

Rappelons qu'une loi de groupe formel (commutative à un paramètre) sur A est une série formelle $G \in A[[X,Y]]$ telle que :

a) $G(X,0) = X$ et $G(0,Y) = Y$;

b) $G(X,Y) = G(Y,X)$;

c) $G(X,G(Y,Z)) = G(G(X,Y),Z)$.

Soit G une telle loi de groupe formel. Pour chaque entier $r \geq 1$, l'ensemble $\mathfrak{m}^r$ muni de la loi de composition $(x,y) \longmapsto G(x,y)$ est un groupe commutatif, que l'on note $G(\mathfrak{m}^r)$. La multiplication par un entier $n \geq 0$ dans ce groupe est donnée par $x \longmapsto [n]_G(x)$, où $[n]_G = nX + \ldots$ est une série formelle dans $A[[X]]$ que l'on définit par récurrence par

$$[0]_G = 0 \qquad [n+1]_G = G(X,[n]_G).$$

PROPOSITION 1. - *Soit* G *une loi de groupe formel (commutative à un paramètre) sur* A. *Le sous-groupe de torsion de* $G(\mathfrak{m})$ *est un* p-*groupe fini d'ordre* $\leq \frac{p}{p-1}\,e$.

Pour tout entier $r \geq 1$, le groupe $G(\mathfrak{m}^r)/G(\mathfrak{m}^{r+1})$ est annulé par p. Par ailleurs, si r est assez grand, le logarithme et l'exponentielle du groupe formel induisent des isomorphismes de groupes réciproques l'un de l'autre entre $G(\mathfrak{m}^r)$ et le groupe additif $\mathfrak{m}^r$, de sorte que $G(\mathfrak{m}^r)$ est sans torsion. Il en résulte le sous-groupe de torsion $G(\mathfrak{m})_{\mathrm{tors}}$ de $G(\mathfrak{m})$ est annulé par une puissance de p.

Soit H un sous-groupe fini non nul de $G(\mathfrak{m})$. Notons n le plus petit entier naturel tel que p^n annule H, et H' le sous-groupe de H formé des éléments annulés par p^{n-1}. Le groupe H' est distinct de H ; son ordre est donc majoré par Card(H)/p. La série formelle $[p]_G$ s'écrit Xu(X), où $u \in A[[X]]$ est une série formelle telle que u(0) = p. Posons $w = u \circ [p^{n-1}]_G$. On a w(0) = p et

(10) $$[p^n]_G = [p]_G \circ [p^{n-1}]_G = [p^{n-1}]_G\, w\,.$$

LEMME 1. - *Soient* $f \in A[[X]]$ *une série formelle et* α *un élément de* $\mathfrak{m}$ *tel que* $f(\alpha) = 0$. *Il existe une série formelle* $g \in A[[X]]$ *telle que* $f(X) = (X-\alpha)g(X)$.

Ecrivons $f = \sum_{i=0}^{\infty} a_i X^i$. La série $\sum_{i=1}^{\infty} a_i (X^{i-1}+\alpha X^{i-2}+\ldots+\alpha^{i-2}X + \alpha^{i-1})$ converge alors dans l'anneau A[[X]], muni de la topologie J-adique, où J est l'idéal engendré par X et $\mathfrak{m}$. Soit g sa somme. On a $(X-\alpha)g(X) = \sum_{i=1}^{\infty} a_i (X^i - \alpha^i) = f(X) - f(\alpha) = f(X)$, d'où le lemme.

Pour tout $x \in H-H'$, on a $[p^n]_G(x) = 0$ et $[p^{n-1}]_G(x) \neq 0$, d'où w(x) = 0 en vertu de la formule (10). On déduit alors du lemme 1 que la série formelle w est multiple de $\prod_{x \in H-H'} (X-x)$ dans A[[X]]. En particulier le terme constant w(0) = p est multiple de $\prod_{x \in H-H'} x$ dans A, et l'on a $e = v(p) \geq \mathrm{Card}(H-H') \geq (1-\frac{1}{p})\,\mathrm{Card}(H)$. Nous avons ainsi prouvé que l'on a $\mathrm{Card}(H) \leq \frac{p}{p-1}\,e$ pour tout sous-groupe fini H de $G(\mathfrak{m})$. La proposition 1 en résulte, puisque $G(\mathfrak{m})_{tors}$ est réunion filtrante de tels sous-groupes.

3. Points de torsion d'une courbe elliptique définie sur un corps local

Soient L, A, v, $\mathfrak{m}$, p et e comme au n°2. Notons $\tilde{L}$ le corps résiduel $A/\mathfrak{m}$ et supposons-le parfait.

Soit E une courbe elliptique définie sur L. Notons $\tilde{E}$ la fibre spéciale du modèle de Néron de E sur A, et $\tilde{E}^{\circ}$ la composante neutre de $\tilde{E}$. On dispose d'un homomorphisme de réduction $E(L) \to \tilde{E}(\tilde{L})$. Il est surjectif parce que le modèle Néron de E est lisse sur A et que l'anneau A est complet par hypothèse. Notons $E_1(L)$ le noyau de l'homomorphisme de réduction et $E_0(L)$ le groupe des points de $E(L)$ dont la réduction appartient à $\widetilde{E}^{\circ}(\widetilde{L})$. On a ainsi une filtration $0 \subset E_1(L) \subset E_0(L) \subset E(L)$ de $E(L)$ et le groupe quotient $E_0(L)/E_1(L)$ est isomorphe à $\widetilde{E}^{\circ}(\widetilde{L})$.

PROPOSITION 2. - a) *Le sous-groupe de torsion de* $E_1(L)$ *est un* p-*groupe fini d'ordre* $\leq \frac{p}{p-1}$ e.

b) *Lorsque* E *a mauvaise réduction de type additif, l'indice* $[E(L) : E_0(L)]$ *est majoré par* 4.

De la loi de groupe sur le modèle de Néron de E, on déduit par complétion formelle le long de la section nulle une loi de groupe formel G (commutative à un paramètre) sur A, et le groupe $E_1(L)$ est canoniquement isomorphe au groupe $G(\mathfrak{m})$. L'assertion a) résulte ainsi de la proposition 1. L'indice $[E(L) : E_0(L)]$ est majoré par le nombre de composantes connexes géométriques de $\widetilde{E}$, et, d'après la classification de Néron, ce nombre est au plus 4 lorsque E a mauvaise réduction de type additif. Cela prouve b).

COROLLAIRE. - *Supposons que le corps* $\widetilde{L}$ *soit fini et soit* q *son cardinal. Si la courbe elliptique* E *a bonne réduction , on a*

$$\mathrm{Card}(E(L)_{tors}) \leq \frac{p}{p-1}\, e\, (q+1+[2\sqrt{q}]).$$

Si E a bonne réduction, $\widetilde{E}$ est une courbe elliptique sur $\widetilde{L}$. On a alors

$$[E(L) : E_1(L)] = \mathrm{Card}(\widetilde{E}(\widetilde{L})) \leq q + 1 + [2\sqrt{q}]$$

d'après les majorations de Hasse. Par ailleurs le groupe $E_1(L)_{tors}$ est d'ordre inférieur à $\frac{p}{p-1}$ e d'après la proposition 2, a), d'où le corollaire.

PROPOSITION 3. - *Supposons que la courbe elliptique* E *ait mauvaise réduction de type additif. Le groupe* $E(L)_{tors}$ *est alors fini. Son ordre est de la forme* $p^n m$ *avec* $n \geq 0$ *et* $m \leq 4$. *Il est majoré par* 48e.

Quitte à remplacer L par la complétion d'une de ses extensions algébriques non ramifiées maximales, on se ramène au cas où le corps $\tilde{L}$ est algébriquement clos. Il existe alors une plus petite extension finie L' de L sur laquelle E acquiert réduction semi-stable ([6], 5.6). C'est une extension galoisienne de L ; notons Φ son groupe de Galois. Soient A' la fermeture intégrale de A dans L'. Notons E' la courbe elliptique sur L' déduite de E par extension des scalaires, $\underline{E}$ et $\underline{E'}$ les modèles de Néron de E et de E' sur A et A' respectivement, $\tilde{E}$ et $\tilde{E}'$ leurs fibres spéciales. Remarquons que le corps résiduel $\tilde{L}$ de A s'identifie canoniquement à celui de A'. En vertu de la propriété universelle des modèles de Néron, il existe un unique A'-morphisme $u : \underline{E} \otimes_A A' \to \underline{E'}$ qui induit l'identité $E \otimes_K K' \to E'$ sur les fibres génériques. Soit $\tilde{u} : \tilde{E} \to \tilde{E}'$ le morphisme déduit de u par passage aux fibres spéciales. La restriction de $\tilde{u}$ à la composante neutre $\tilde{E}^\circ$ de $\tilde{E}$ est nulle, car le groupe algébrique $\tilde{E}^\circ$ est isormorphe au groupe additif, alors que $\tilde{E}'^\circ$ est isomorphe au groupe multiplicatif ou est une courbe elliptique. Il en résulte que $E_0(L)$ est contenu dans $E'_1(L')$. D'après la prop. 2, a), $E'_1(L')_{tors}$ est un p-groupe fini et l'on a

(11) $$\mathrm{Card}(E'_1(L')_{tors}) \leq \frac{p}{p-1}\, e\, \mathrm{Card}(\Phi).$$

(Noter que l'indice de ramification absolu de L' est $e\mathrm{Card}(\Phi)$.) Grâce à la prop. 2, b), on en déduit que le groupe $E(L)_{tors}$ est fini, que son ordre s'écrit $p^n m$ avec $n \geq 0$, $m \leq 4$, et que l'on a

(12) $$\mathrm{Card}(E(L)_{tors}) \leq \frac{4p}{p-1}\, e\, \mathrm{Card}(\Phi) \leq 8e\mathrm{Card}(\Phi).$$

Lorsque l'ordre de Φ est majoré par 6, cela achève la démonstration.

Avant de traiter les autres cas, remarquons que Φ opère par transport de structure sur le schéma $\underline{E'}$; cette opération n'est pas A'-linéaire, mais seulement semi-linéaire relativement à l'opération de Φ sur A'. On en déduit, parce que Φ opère trivialement sur le corps résiduel de A', une opération de Φ sur le $\tilde{L}$-schéma $\tilde{E}'$, c'est-à-dire un homomorphisme $\Phi \to \mathrm{Aut}_{\tilde{L}}(\tilde{E}')$. Cet homomorphisme est injectif ([6],5.6). Supposons maintenant que l'ordre de Φ

soit strictement supérieur à 6 ; il en est alors de même de celui de $\mathrm{Aut}_{\tilde{L}}(\tilde{E}')$, et l'on est dans l'un des deux cas suivants (*loc. cit.*) :

a) On a p = 2, E' a bonne réduction, l'invariant modulaire de la courbe elliptique $\tilde{E}'$ est 0, le groupe $\mathrm{Aut}_{\tilde{L}}(\tilde{E}')$ est d'ordre 24 et le groupe Φ est d'ordre 8 ou 24. Dans ce cas $\tilde{E}'$ est isomorphe à la courbe elliptique d'équation $y^2-y = x^3$ et l'image de Φ dans $\mathrm{Aut}_{\tilde{L}}(\tilde{E}')$ contient l'automorphisme $(x,y) \longmapsto (x,y+1)$ de $\tilde{E}'$.

b) On a p = 3, E' a bonne réduction, l'invariant modulaire de la courbe elliptique $\tilde{E}'$ est 0, le groupe $\mathrm{Aut}_{\tilde{L}}(\tilde{E}')$ est d'ordre 12 et le groupe Φ également. Dans ce cas $\tilde{E}'$ est isomorphe à la courbe elliptique d'équation $y^2 = x^3-x$, l'homomorphisme $\Phi \to \mathrm{Aut}_{\tilde{L}}(\tilde{E}')$ est bijectif et $(x,y) \longmapsto (x+1,y)$ est un automorphisme de $\tilde{E}'$.

Dans chacun des deux cas ci-dessus, on constate que le seul point de $\tilde{E}'(\tilde{L})$ fixé par Φ est 0. Comme on a $\sigma \circ \tilde{u} = \tilde{u}$ pour tout $\sigma \in \Phi$, le morphisme $\tilde{u} : \tilde{E} \to \tilde{E}'$ est nul et le groupe E(L) est contenu dans $E'_1(L')$. De (11), on déduit alors

$$\mathrm{Card}(E(L)_{\mathrm{tors}}) \leq \frac{p}{p-1}\, e \;\; \mathrm{Card}(\Phi) \leq 48e.$$

Cela termine la démonstration de la prop. 3.

PROPOSITION 4. - *Supposons que* E *ait mauvaise réduction de type multiplicatif. Soit* P *un point de torsion de* E(L). *Notons n son ordre et* m *le plus petit entier* ≥ 1 *tel que* mP *appartienne à* $E_0(L)$. *Soit* E' *la courbe elliptique quotient de* E *par le sous-groupe engendré par* P. *Notons* Δ *et* Δ' *les discriminants de modèles minimaux de* E *et* E' *respectivement. Alors* m *divise* $v(\Delta)$ *et l'on a* $v(\Delta') = nv(\Delta)/m^2$.

Quitte à effectuer une extension finie non ramifiée du corps de base, on se ramène au cas où E' est une courbe de Tate $\mathbb{G}_m/q^{\mathbb{Z}}$, avec $q \in \mathfrak{m}$. On a

$v(\Delta) = v(q)$, $E(L) = L^{\times}/q^{\mathbb{Z}}$ et $E_0(L) = A^{\times}q^{\mathbb{Z}}/q^{\mathbb{Z}}$. Soit x un élément de $L^{\times}$ dont la classe modulo $q^{\mathbb{Z}}$ soit le point P. Par définition, m est le plus petit entier ≥ 1 tel que x^m appartienne à $A^{\times}q^{\mathbb{Z}}$, c'est-à-dire tel que $mv(x)$ soit multiple de $v(q) = v(\Delta)$. L'entier m divise n et $v(\Delta)$, et l'on a $x^m = \zeta q^r$, avec $\zeta \in A^{\times}$ et r un entier premier à m. Par définition de n, ζ est une racine primitive (n/m)-ième de l'unité. Choisissons des entiers a et b tels que $ar + bm = 1$ et posons $q' = (x^a q^b)^{n/m}$. On a les relations

(13) $$q'^m = (\zeta^a q^{ar} q^{bm})^{n/m} = q^{n/m}$$

(14) $$q'^r = (x^{ar} \zeta^{-b} x^{bm})^{n/m} = x^{n/m}.$$

Les morphismes $\lambda \longmapsto \lambda^{n/m}$ et $\lambda \longmapsto \lambda$ de $\mathbb{G}_m$ dans $\mathbb{G}_m$ définissent des isogénies

$$u : \mathbb{G}_m/q^{\mathbb{Z}} \to \mathbb{G}_m/q^{(n/m)\mathbb{Z}} = \mathbb{G}_m/q'^{m\mathbb{Z}}$$

et $$v : \mathbb{G}_m/q'^{m\mathbb{Z}} \to \mathbb{G}_m/q'^{\mathbb{Z}}$$

de degrés n/m et m respectivement. L'isogénie $v \circ u$ est de degré n. On a $u(P) = u(xq^{\mathbb{Z}}) = x^{n/m} q'^{m\mathbb{Z}} = q'^r q'^{m\mathbb{Z}}$ d'après (14), d'où $(v \circ u)(P) = 0$. Le noyau de $v \circ u$ est donc le sous-groupe cyclique d'ordre n de E engendré par P, et la courbe elliptique E' est isomorphe à la courbe de Tate $\mathbb{G}_m/q'^{\mathbb{Z}}$. On a alors

$$v(\Delta') = v(q') = nv(q)/m^2 = nv(\Delta)/m^2$$

d'après (13), d'où la proposition.

COROLLAIRE. - *Supposons que* E *ait mauvaise réduction de type multiplicatif et soit* H *un sous-groupe fini de* E(L). *Il existe des entiers naturels* a *et* b *tels que* b *divise* a *et que* H *soit isomorphe au groupe* $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$. *Notons* E' *la courbe elliptique* E/bH, *et* Δ *et* Δ' *les discriminants de modèles minimaux de* E *et* E'. *On a*

(15) $$v(\Delta) + v(\Delta') \geq 2\sqrt{\mathrm{Card}(H)}.$$

Le groupe des points de torsion de $E(\overline{L})$, où $\overline{L}$ est une clôture algébrique de L, est isomorphe à $(\mathbb{Q}/\mathbb{Z})^2$. D'après le théorème des diviseurs élémentaires, tout sous-groupe de $(\mathbb{Q}/\mathbb{Z})^2$ est isomorphe à un groupe de la forme

$\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$, où a, b sont des entiers naturels tels que b divise a. Cela prouve la première assertion. Pour démontrer la seconde, on se ramène, comme dans la démonstration de la prop. 4, au cas où E est une courbe de Tate $\mathbb{G}_m/q^{\mathbb{Z}}$. Tous les points d'ordre b de $E(\overline{L})$ appartiennent à H, donc sont rationnels sur L. Il en résulte que q est une puissance b-ième dans L ; sa valuation $v(q) = v(\Delta)$ est multiple de b. Soit Q un point d'ordre a de H. Le groupe bH est le groupe cyclique d'ordre a/b engendré par le point P = bQ. Soit m le plus petit entier ≥ 1 tel que mP appartienne à $E_0(L)$. Comme $E_0(L)$ est d'indice $v(\Delta)$ dans E(L), le point $(v(\Delta)/b)P = v(\Delta)Q$ appartient à $E_0(L)$, et m divise $v(\Delta)/b$. D'après la prop.4, on a $v(\Delta') = av(\Delta)/bm^2$, d'où

$$v(\Delta)+v(\Delta') = \frac{v(\Delta)}{bm}\left(bm + \frac{a}{m}\right) \geq bm + \frac{a}{m} \geq 2\sqrt{ab}.$$

Cela démontre le corollaire.

4. Démonstration des théorèmes 1 à 4

Dans ce numéro, K désigne un corps de nombres et E une courbe elliptique définie sur K.

a) *Démonstration du théorème* 1

Supposons que E ait mauvaise réduction de type additif en au moins deux places finies de K de caractéritiques résiduelles p et p' distinctes. Soient n et n' les plus grands diviseurs de l'ordre de $E(K)_{tors}$ premiers à p et à p' respectivement. Les entiers n et n' sont majorés par 4 d'après la prop.3 du n°3. Comme l'ordre de $E(K)_{tors}$ divise ppcm(n,n'), il divise 12. Cela démontre le théorème 1.

Remarque 4. - Si l'on a $p \geq 5$ ou $p' \geq 5$, il résulte de la démonstration précédente que l'on a $\mathrm{Card}(E(K)_{tors}) \leq 4$.

b) *Démonstration du théorème* 2

D'après la remarque 2 du n°1, le théorème 2 résulte de la prop.3 du n°3.

c) *Démonstration du théorème* 3

Supposons que la courbe elliptique E ait bonne réduction en une place finie v de K de caractéristique résiduelle 2. Notons e l'indice de ramification et f le degré résiduel de cette place. On a ef $\leq$ [K:$\mathbb{Q}$], et d'après le corollaire de la prop.2 du n°3, appliqué en prenant pour L le complété de K en v, on a

$$\mathrm{Card}(E(K)_{\mathrm{tors}}) \leq 2e\left(2^f+1+[2^{1+(f/2)}]\right).$$

On a $1 \leq 2^{f-1}$ et $[2^{1+(f/2)}] \leq 2^f$, d'où

$$\mathrm{Card}(E(K)_{\mathrm{tors}}) \leq 5e2^f \leq 5[K:\mathbb{Q}]2^f/f.$$

Comme la suite $(2^n/n)_{n\geq 1}$ est croissante, $2^f/f$ est majoré par $2^{[K:\mathbb{Q}]}/[K:\mathbb{Q}]$ et $\mathrm{Card}(E(K)_{\mathrm{tors}})$ par $5.2^{[K:\mathbb{Q}]}$, d'où le théorème 3.

d) *Démonstration du théorème* 4

Supposons que la courbe elliptique E soit semi-stable et n'ait pas partout bonne réduction. On voit comme dans la preuve du cor. de la prop.4 que le groupe fini $E(K)_{\mathrm{tors}}$ est isomorphe à un groupe de la forme $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$, où a, b sont des entiers naturels tels que b divise a.Notons E' la courbe elliptique quotient de E par le sous-groupe fini $bE(K)_{\mathrm{tors}}$. Elle est K-isogène à E, donc a même conducteur N_E que E. Par définition de la constante β'_E (cf. formules (2) et (8) du n°1), on a

$$\log(N_{K/\mathbb{Q}}(\Delta_E)) \leq \beta'_E \log(N_{K/\mathbb{Q}}(N_E))$$

$$\log(N_{K/\mathbb{Q}}(\Delta_{E'})) \leq \beta'_E \log(N_{K/\mathbb{Q}}(N_E)).$$

Notons q_v le cardinal du corps résiduel d'une place finie v de K. En sommant les deux inégalités précédentes, on obtient

$$(16) \qquad \sum_v (v(\Delta_E) + v(\Delta_{E'}))\log q_v \leq 2\, \beta'_E \sum_v \log q_v,$$

où les sommes sont étendues à l'ensemble des places finies de K en lesquelles E a mauvaise réduction. Pour une telle place, on a

$v(\Delta_E) + v(\Delta_{E'}) \geq 2\sqrt{\mathrm{Card}(E(K)_{tors})}$ d'après le corollaire de la prop.4 du n°3. La somme $\sum_v \log q_v$ étant non nulle par hypothèse, on déduit de (16) que l'on a $\sqrt{\mathrm{Card}(E(K)_{tors})} \leq \beta'_E$, d'où le théorème 4.

BIBLIOGRAPHIE

[1] V.A. DEMIANENKO, *Sur la torsion des courbes elliptiques*, Izv. Akad. N. CCCP 35 (1971), 280-307.

[2] G. FREY, *Links between elliptic curves and solutions of* A–B = C, Proceedings of the Journées Arithmétiques ULM, 1987.

[3] M.HINDRY et J.H. SILVERMAN, *The canonical height and integral points on elliptic curves*, Invent. Math. 93 (1988), 419-450.

[4] Ju. I. MANIN, *The* p-*torsion of elliptic curves is uniformly bounded*, Math. USSR Izvestija, vol.3 (1969).

[5] B. MAZUR, *Modular curves and the Eisenstein ideal*, Publ. math. IHES 47 (1977), 33-186.

[6] J.-P. SERRE, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques,* Invent. Math. 15 (1972), 259-331.

[7] L. SZPIRO, *Discriminant et conducteur des courbes elliptiques*, dans ce volume.

M. FLEXOR
Département de mathématiques
Bâtiment 425
Université de Paris Sud
91405 Orsay

J. OESTERLÉ
Université de Paris VI
Tour 45-46, 5ème étage
4, Place Jussieu
75005 Paris 5ème

LAURENT MORET-BAILLY

Hauteurs et classes de Chern sur les surfaces arithmétiques

Astérisque, tome 183 (1990), p. 37-58
<http://www.numdam.org/item?id=AST_1990__183__37_0>

Société Mathématique de France
Astérisque 183 (1990)

Hauteurs et classes de Chern sur les surfaces arithmétiques

Laurent Moret-Bailly

0. Introduction.

On présente dans cet exposé les idées de Parshin [P] sur le thème : "un analogue arithmétique de l'inégalité de Bogomolov-Miyaoka $c_1^2 \leq 3\,c_2$ pour les surfaces complexes impliquerait, entre autres, la conjecture de Szpiro sur le discriminant des courbes elliptiques sur $\mathbb{Q}$".

Après le rappel de l'inégalité de Bogomolov-Miyaoka au § 1, puis des généralités sur les familles de courbes au § 2, notamment sur la "mesure de la mauvaise réduction", on énonce au § 3 l'"hypothèse BM", qui est un analogue arithmétique de Bogomolov-Miyaoka, assez affaibli par rapport à [P] ; on montre ensuite que BM équivaut à une variante de la "conjecture des petits points" de Szpiro.

Au § 4 on introduit l'hypothèse ME ("Mordell effectif") qui est une majoration de la hauteur d'un point d'une courbe de genre ≥2 sur un corps de nombres, en termes du corps de rationalité de ce point : à degré (sur $\mathbb{Q}$) fixé, la borne est *linéaire* par rapport au logarithme du discriminant. Pour plus de commodité, on étend cette hypothèse à des variétés (propres) arbitraires munies d'une hauteur quelconque, de sorte qu'elle est évidemment fausse avec cette généralité ; toutefois, on montre au § 5 que BM implique une telle généralisation de ME, valable pour des variétés qui paramètrent une famille de courbes lisses de genre ≥2. La "construction de Kodaira" montre que les courbes de genre ≥2 tombent elles-mêmes sous le coup de cet énoncé.

Le § 6 est consacré à la conjecture du discriminant de Szpiro pour les courbes elliptiques sur $\mathbb{Q}$; on montre que celle-ci est conséquence de ME appliquée à une courbe modulaire. De même, au § 7, on déduit de ME une version de la "conjecture *abc*", en appliquant ME à un revêtement ramifié convenable de $\mathbb{P}^1$. Enfin, on fait au § 8 quelques commentaires sur l'effectivité des méthodes et des résultats.

1. Inégalité de Bogomolov-Miyaoka.

1.1. Soit X une surface projective irréductible lisse complexe de type général. On a alors l'inégalité ([M], [Y])

$$c_1^2(X) \leq 3\, c_2(X) \tag{1.1.1}$$

entre les classes de Chern de X ; des inégalités plus faibles avaient été obtenues auparavant par Bogomolov ([B], avec 4 au lieu de 3) et Van de Ven ([V], avec 8).

1.2. On énoncera au § 3 un analogue de (1.1.1) pour les "surfaces arithmétiques". Celles-ci sont des courbes sur des anneaux d'entiers algébriques, il faut donc d'abord reformuler (1.1.1) en termes de fibrations en courbes. Soit $f: X \to B$ un morphisme surjectif de la surface X sur une courbe B lisse de genre q. On suppose que f fait de X une B-courbe semi-stable (voir les rappels au § 2) ; la fibre générique est alors de genre $g \geq 2$ puisque X est de type général.

La première classe de Chern $c_1(X)$ est la classe dans Pic(X) du faisceau dualisant

$$\omega_X = \omega_{X/B} \otimes f^* \omega_B \tag{1.2.1}$$

de sorte que

$$c_1^2(X) = (\omega_{X/B} \cdot \omega_{X/B}) + 2(2g-2)(2q-2). \tag{1.2.2}$$

On sait par ailleurs que

$$c_2(X) = \sum_{b \in B} \delta_b(X) \; + \; (2g-2)(2q-2) \tag{1.2.3}$$

où $\delta_b(X)$ désigne le nombre de points singuliers de la fibre $f^{-1}(b) = X_b$. Il en résulte que l'avatar relatif de (1.1.1) est

$$(\omega_{X/B} \cdot \omega_{X/B}) \leq \; (2g-2)(2q-2) + 3 \sum_{b \in B} \delta_b(X). \tag{1.2.4}$$

Plus généralement, $c_1^2(X) \leq \lambda\, c_2(X)$ $(\lambda \in \mathbb{R})$ équivaut à

$$(\omega_{X/B} \cdot \omega_{X/B}) \leq \lambda \sum_{b \in B} \delta_b(X) + (\lambda-2)(2g-2)(2q-2). \tag{1.2.5}$$

1.3. Le lecteur pourra consulter [P] pour des variantes de ces inégalités, notamment sans hypothèse sur le genre des fibres ou celui de B. Mentionnons celle-ci : l'inégalité (1.2.4) reste vraie si l'on remplace X par son *modèle stable* X_0 sur B ; ceci ne change pas le membre de gauche et diminue les δ_b . En fait on a, pour tout $b \in B$, $\delta_b(X_0) \leq 3g-3$, de sorte que l'on obtient une majoration de $(\omega_{X/B} \cdot \omega_{X/B})$ uniquement en termes des genres et du nombre de fibres singulières.

2. Familles de courbes à singularités ordinaires.

2.1. Soit B un schéma. On appelle *B-courbe nodale* un morphisme $f : X \to B$ propre, surjectif et plat, dont les fibres géométriques sont des courbes n'ayant comme singularités que des points doubles ordinaires. Le $\mathcal{O}_X$-module cohérent $\Omega_{X/B}$ des différentielles relatives de f admet alors une stratification de Fitting du type

$$\mathrm{Sing}(X/B) \subset X$$

où $\mathrm{Sing}(X/B)$ est le plus grand sous-schéma fermé Y de X tel que $\Omega_{X/B} \otimes_{\mathcal{O}_X} \mathcal{O}_Y$ soit localement libre de rang 2 sur Y.

2.2. *Description locale.* Avec les notations de 2.1, si $B = \mathrm{Spec}\, R$ où R est local complet de corps résiduel k, et si $x \in X$ est un point singulier k-rationnel de la fibre fermée de f, le complété $A = \widehat{\mathcal{O}}_{X,x}$ de $\mathcal{O}_{X,x}$ est R-isomorphe à $R[[u,v]]/(uv-t)$ où $t \in R$, d'où une présentation

$$A \xrightarrow{\binom{v}{u}} A \times A \xrightarrow{(du,dv)} \Omega_{X/B} \otimes_{\mathcal{O}_X} A \longrightarrow 0$$

qui montre que $\mathrm{Sing}(X/B) \times_X \mathrm{Spec}\, A$ est défini par l'idéal (u,v) donc isomorphe comme R-schéma à $\mathrm{Spec}(R/tR)$.

2.3. On déduit de 2.2 que $\mathrm{Sing}(X/B)$ (dont la formation, par construction, commute à tout changement de base) est *fini et non ramifié* sur B ; si l'on pose

$$\Sigma(X/B) = f_* \mathcal{O}_{\mathrm{Sing}(X/B)} \tag{2.3.1}$$

alors $\Sigma(X/B)$ est un $\mathcal{O}_B$-module cohérent, isomorphe localement pour la topologie étale sur B à $\bigoplus_{i=1}^{s} \mathcal{O}_B/t_i\mathcal{O}_B$ pour $s \in \mathbb{N}$ et $t_i \in \mathcal{O}_B$ convenables. En particulier on a pour tout $b \in B$

$$\mathrm{rg}_b\, \Sigma(X/B) = \delta_b(X) \tag{2.3.2}$$

où, par définition $\mathrm{rg}_b\,\Sigma(X/B) = \dim_{\kappa(b)}(\Sigma(X/B)\otimes_{\mathcal{O}_B}\kappa(b))$, et où $\delta_b(X)$ désigne le nombre géométrique sur $\kappa(b)$ de points singuliers de la fibre X_b.

Enfin, comme $\mathrm{Sing}(X/B)$ est fini sur B, la formation de $\Sigma(X/B)$ commute à tout changement de base.

Proposition 2.4. *Soit $f : X \to B$ une B-courbe nodale. On suppose que $B = \mathrm{Spec}\,\Lambda$ est un trait de point fermé b et de point générique η, et que $f_\eta : X_\eta \to \eta$ est lisse, de sorte que $\Sigma(X/B)$ est un Λ-module de longueur finie.*

Soit $p : X' \to X$ une résolution minimale des singularités de X. Alors la longueur du Λ-module $\Sigma(X/B)$ est égale au nombre géométrique $\delta_b(X')$ de points singuliers de X'_b.

Preuve. On obtient X' à partir de X en éclatant le sous-schéma *réduit* $\mathrm{Sing}\,X$ formé des points singuliers de X, et en répétant le processus jusqu'à obtenir un schéma régulier. Or il résulte de la non-ramification de $\mathrm{Sing}(X/B)$ (qui contient $\mathrm{Sing}\,X$) que les corps résiduels des points de $\mathrm{Sing}\,X$ sont des extensions séparables de $\kappa(b)$, de sorte que la formation du sous-schéma $\mathrm{Sing}\,X$ commute au changement de base $\Lambda \to \Lambda'$ où Λ' est un anneau de valuation discrète complet, non ramifié sur Λ et de corps résiduel une clôture algébrique de $\kappa(b)$. On peut donc supposer Λ complet à corps résiduel algébriquement clos (on rappelle que l'éclatement commute au changement de base plat).

Soient $x_1,\dots,x_s$ les points singuliers de X_b : on a pour $1 \le i \le s$

$$\widehat{\mathcal{O}}_{X,x_i} \simeq \Lambda[[x,y]]\,/\,(xy-t_i)$$

avec $t_i = \pi^{e_i}$ où π est une uniformisante de Λ, et dans ces conditions

$$\Sigma(X/B) \simeq \bigoplus_{i=1}^{s} \Lambda / t_i\,\Lambda$$

de sorte que la longueur de $\Sigma(X/B)$ est la somme des e_i. L'assertion de la proposition est donc claire si X est régulier : dans ce cas les e_i sont égaux à 1, et $s = \delta_b(X) = \delta_b(X')$. Il suffit donc de voir que la somme des e_i ne change pas par éclatement d'un point singulier (i.e. d'un point x_i tel que $e_i \ge 2$). Le calcul est fait notamment dans [SPC], I, proposition 2.2 : si $e_i \ge 2$ et si $p_i : X_i \to X$ est l'éclaté de x_i dans X, alors $(X_i)_b$ contient, au-dessus de x_i, deux points doubles réguliers dans X_i, et de plus, si $e_i \ge 2$, un point double du type $\Lambda[[x,y]]\,/(xy-\pi^{e_i-2})$. ■

2.5. On suppose maintenant que B est un schéma régulier de dimension 1, et que pour tout point maximal η de B la fibre X_η de $f : X \to B$ est lisse. On peut alors mesurer la "mauvaise réduction" de f par le diviseur effectif $\underline{\delta}(X/B)$ sur B, défini par

$$(2.5.1) \qquad \begin{aligned} \underline{\delta}(X/B) &= \sum \mathrm{lg}_b \ \Sigma(X/B)_b \,[b] \\ &= \sum \ \delta_b(X')\,[b] \end{aligned}$$

où la somme est prise sur les points fermés b de B, X' est une résolution minimale des singularités de X, et lg_b est la longueur comme $\mathcal{O}_{B,b}$-module. L'équivalence des deux formules résulte évidemment de 2.4. La connaissance de $\underline{\delta}(X/B)$ équivaut à celle de la classe de $\Sigma(X/B)$ dans le groupe de Grothendieck des $\mathcal{O}_B$-modules cohérents de longueur finie. Bien entendu on peut considérer $\underline{\delta}(X/B)$ comme un idéal inversible de $\mathcal{O}_B$; sa formation commute à tout changement de base $B' \to B$ où B' est un schéma régulier de dimension 1, plat sur B.

Remarque 2.5.2. Supposons de plus que X soit une B-courbe stable de genre $g \geq 2$ (voir rappels ci-dessous). Alors X s'interprète comme un 1-morphisme φ_X de B vers le champ $\overline{\mathcal{M}}_g$ des courbes stables de genre g [D-M]. Celui-ci est un champ algébrique lisse sur Spec $\mathbb{Z}$ et contient un diviseur à croisements normaux E paramétrant les courbes singulières. Dans ces conditions on peut vérifier, en utilisant la description locale de $\overline{\mathcal{M}}_g$ et E donnée dans [D-M], que $\underline{\delta}(X/B) = \varphi_X^*(E)$.

2.6. *Rappels sur les courbes stables et semi-stables.* Si k est un corps algébriquement clos, on appelle *courbe semi-stable* (resp. *stable*) sur k une k-courbe nodale et connexe C, de genre arithmétique ≥ 1 (resp. ≥ 2), telle que toute composante irréductible de C isomorphe à $\mathbb{P}^1_k$ contienne au moins deux (resp. trois) points singuliers de C. Il revient au même d'exiger que le faisceau dualisant $\omega_{C/k}$ soit de degré ≥ 0 (resp. > 0) sur chaque composante de C.

Si B est un schéma, une B-courbe *semi-stable* (resp. *stable*) est par définition une B-courbe nodale dont les fibres géométriques sont semi-stables (resp. stables).

Soit B un schéma noethérien régulier intègre de dimension 1, de point générique $\eta = \operatorname{Spec} K$, et soit X_η une courbe sur K. On dit que X_η a *réduction semi-stable* sur B s'il existe un modèle semi-stable de X_η sur B, c'est-à-dire une B-courbe semi-stable de fibre générique X_η. Le *théorème de réduction semi-stable* de Grothendieck affirme que si X_η est propre, lisse, géométriquement connexe de genre ≥ 1 sur K, alors il existe une extension finie K' de K telle que $X_\eta \otimes_K K'$ ait réduction semi-stable sur le normalisé de B dans K'. Plus précisément ([SPC], I, cor. 5.18) si n est un entier ≥ 3, inversible sur B, tel que les points d'ordre n de la jacobienne $J = \underline{\mathrm{Pic}}^0_{X_K/K}$ soient rationnels sur K, alors X_η a réduction semi-stable sur B. En particulier (sans restriction sur les caractéristiques) X_η a réduction semi-stable dès que les points d'ordre 12 de J sont K-rationnels.

Soit X un modèle semi-stable de X_η (supposée lisse de genre $g \geq 1$). Par résolution des singularités de X on obtient le *modèle régulier minimal* X_1 de X_η, qui est encore semi-stable. Si de plus $g \geq 2$, on peut contracter dans X (ou dans X_1) les $\mathbb{P}^1$ de self-intersection -2 contenus dans les fibres, pour obtenir l'unique *modèle stable* X_0 de X_η (contrairement au modèle stable, le modèle régulier minimal ne "commute" pas en général au changement de base $B' \to B$ où B' est ramifié sur B). Il résulte de 2.4 que le diviseur $\underline{\delta}(X/B)$ de (2.5.1) *ne dépend que de* X_η (supposée à réduction semi-stable) et non du modèle semi-stable X choisi.

2.7. On suppose maintenant que $B = \mathrm{Spec}\, R$ où R est l'anneau des entiers d'un corps de nombres K. Si X est une B-courbe semi-stable (avec X_K lisse de genre $g \geq 1$), on "compactifie" $\underline{\delta}(X/B)$, au sens d'Arakelov, en posant

$$\underline{\delta}_c(X/B) = \underline{\delta}(X/B) + \sum_{\sigma : K \to \mathbb{C}} \delta_\sigma(X)[\sigma] \tag{2.7.1}$$

où $\delta_\sigma(X)$ est défini comme suit : on pose $X_\sigma = X_K \otimes_K \mathbb{C}$ (où K est plongé dans $\mathbb{C}$ au moyen de σ) et $\delta_\sigma(X) = \delta(X_\sigma)$ où δ est l'invariant de Faltings [F] ; il nous suffira ici de savoir que δ est une fonction continue à valeurs réelles sur $\mathcal{M}_g(\mathbb{C})$ où $\mathcal{M}_g$ est l'espace des modules des courbes de genre g.

(On aurait pu, comme le font certains auteurs, sommer sur les places archimédiennes de K plutôt que sur les plongements complexes, la fonction $\sigma \longmapsto \delta_\sigma(X)$ étant invariante par conjugaison ; dans ce cas, il faut modifier, dans la suite, les définitions de $\underline{\Delta}(X_K)$ et du degré d'un diviseur en affectant les places complexes du poids 2).

Le diviseur $\underline{\delta}_c(X/B)$ commute (en un sens évident) au changement de corps de base, et ne dépend que de X_K. Notons cependant que si $\underline{\delta}(X/B)$ est ≥ 0 par construction, il n'en est pas de même a priori des $\delta_\sigma(X)$. Pour "borner la mauvaise réduction" de X, nous utiliserons plutôt

$$|\underline{\delta}_c(X/B)| = \underline{\delta}(X/B) + \sum_{\sigma} |\delta_\sigma(X)|\, [\sigma] \tag{2.7.2}$$

$$\underline{\Delta}(X_K) = \underline{\Delta}(X/B) = N_{R/\mathbb{Z}}\, |\underline{\delta}_c(X/B)|$$

de sorte que $\underline{\Delta}(X_K)$ est un élément du monoïde $\mathrm{Div}_{c+}(\mathbb{Z})$ décrit comme suit : $\mathbb{P}$ désigne l'ensemble des nombres premiers, $\overline{\mathbb{P}} = \mathbb{P} \cup \{\infty\}$, $\mathrm{Div}_c(\mathbb{Z})$ est le groupe des applications $v \to n_v : \overline{\mathbb{P}} \to \mathbb{R}$, à support fini, telles que $n_v \in \mathbb{Z}$ si $v \in \mathbb{P}$, et $\mathrm{Div}_{c+}(\mathbb{Z}) \subset \mathrm{Div}_c(\mathbb{Z})$ est l'ensemble des applications à valeurs ≥ 0. La norme intervenant dans la formule est définie par linéarité à partir des cas suivants : si $b \in B$ est un point fermé de caractéristique p, la norme de $[b]$ est $[\kappa(b) : \mathbb{F}_p][p]$, et si σ est un plongement complexe de K, la norme de $[\sigma]$ est $[\infty]$.

Si K' est une extension finie de K, et $X = X \otimes_K K'$, on a

$$\underline{\Delta}(X_{K'}) = [K' : K]\, \underline{\Delta}(X_K)\,. \tag{2.7.3}$$

3. Hypothèse BM et petits points.

3.1. Soit R l'anneau des entiers d'un corps de nombres K, et soit $B = \mathrm{Spec}\, R$. Soit

$$f : X \longrightarrow B$$

une B–courbe semi-stable à fibre générique lisse de genre $g \geq 2$. On suppose de plus que X est un schéma régulier.

Arakelov [A] a défini une théorie des intersections (à valeurs réelles) pour les faisceaux inversibles sur X munis de métriques aux places archimédiennes de B, vérifiant certaines conditions. En particulier le faisceau dualisant relatif $\omega_{X/B}$ est muni de telles "métriques à l'infini" canoniques, et le membre de gauche de (1.2.5) a donc un sens (cf. [A], [SPA]). D'autre part le substitut le plus naturel du terme $2q-2$ est $\log |D_K|$, où D_K désigne le discriminant de K sur $\mathbb{Q}$ (le lecteur peut préférer par exemple $\log(2^{-2r_2} |D_K|)$ où r_2 est le nombre de places complexes de K; ceci n'a guère d'importance pour la suite).

L'analogue non archimédien de la somme au membre de droite de (1.2.5) est alors

$$\sum_{\substack{b \text{ point} \\ \text{fermé de } B}} \delta_b(X) \log \mathbf{N}(b)$$

où $\mathbf{N}(b) = \mathrm{Card}\, \kappa(b)$ est la norme de b. Il suffit bien entendu de restreindre cette somme à $b \in S = \{$places de mauvaise réduction de $f\}$.

Il est vraisemblable que l'on doive aussi introduire une contribution archimédienne, comme expliqué en 2.7, de sorte que le terme en question de (1.2.5) "doit" être remplacé par

$$\deg_R \underline{\delta}_c(X/B) = \sum_{b\in B} \delta_b(X) \log \mathbf{N}(b) + \sum_{\sigma : K\to \mathbf{C}} \delta_\sigma(X) .$$

On dispose donc d'un analogue arithmétique de l'inégalité (1.2.5), à savoir

$$(\omega_{X/B} \cdot \omega_{X/B}) \leq \lambda \deg_B \underline{\delta}_c(X/B) + (\lambda-2)(2g-2) \log |D_K| \tag{3.1.1}$$

où λ serait une constante absolue, disons ≥ 3. A propos de la valeur de λ, remarquons que si l'on étend le corps de base de K à K', les deux premiers termes de (3.1.1) sont multipliés par $[K':K]$; comme on peut trouver K' avec $\log |D_{K'}|/[K':K]$ arbitrairement grand, la moindre des choses est que le coefficient de $\log |D_K|$ dans (3.1.1) soit ≥ 0.

Des calculs de Bost, Mestre et l'auteur, pour certaines courbes de genre 2 sur $\mathbf{Q}$, mettent cependant en défaut une telle formule, cf. 3.2.3 ci-dessous et l'exposé 6 de ce séminaire. On sera donc plus prudent dans la formulation de l'hypothèse ci-dessous :

Hypothèse BM. *Il existe des applications*

$$\begin{aligned} A_{\mathrm{BM}}, B_{\mathrm{BM}} : \mathbb{N}_{\geq 2} \times \mathrm{Div}_{c+}(\mathbb{Z}) \times \mathbb{N}_{\geq 1} &\longrightarrow \mathbb{R} \\ (g, \underline{\Delta}, d) &\longmapsto A_{\mathrm{BM}}(g, \underline{\Delta}, d), B_{\mathrm{BM}}(g, \underline{\Delta}, d) \end{aligned}$$

telles que pour K, R, X comme en 3.1 *avec* $[K:\mathbf{Q}] \leq d$ *et* $\underline{\Delta}(X/B) \leq \underline{\Delta}$ *, on ait* :

$$(\omega_{X/B} \cdot \omega_{X/B}) \leq A_{\mathrm{BM}}(g, \underline{\Delta}, d) \log|D_K| + B_{\mathrm{BM}}(g, \underline{\Delta}, d) . \tag{3.1.2}$$

(voir (2.7.2) pour la définition de $\underline{\Delta}(X/B)$).

Remarque 3.2.1. L'inégalité (3.1.1) implique (3.1.2) avec

$$\begin{aligned} A_{\mathrm{BM}}(g, \underline{\Delta}, d) &= (\lambda-2)(2g-2) \\ B_{\mathrm{BM}}(g, \underline{\Delta}, d) &= \lambda \deg_{\mathbb{Z}} \underline{\Delta} = \lambda \, (\sum_{p\in \mathbb{P}} \underline{\Delta}(p) \log p + \underline{\Delta}(\infty)) ; \end{aligned}$$

on passe de (3.1.1) à (3.1.2) en majorant δ_σ par $|\delta_\sigma|$ pour $\sigma : K \to \mathbf{C}$.

Remarque 3.2.2. Soit X_0 le modèle stable de X sur B ; on obtient une variante plus forte de BM en remplaçant, pour $b \in B$, $\delta_b(X)$ par $\delta_b(X_0)$, cf. remarque 1.3. Compte tenu de la majoration uniforme $\delta_b(X_0) \leq 3g-3$, la partie non archimédienne de $\underline{\delta}_c(X/B)$ n'intervient plus alors que par son support S (ensemble des places de mauvaise réduction). Si l'on pousse jusqu'au bout l'analogie entre places archimédiennes et non archimédiennes, il n'y a alors pas lieu d'introduire les termes archimédiens $\delta_\sigma(X)$, et la variante envisagée revient simplement à postuler (3.1.2) où A_{BM} et B_{BM} ne dépendent que de g, d et S.

Remarque 3.2.3. L'inégalité (3.1.1) peut se reformuler sans faire intervenir $\underline{\delta}_c(X/B)$. Le R-module localement libre $f_*\omega_{X/B}$ est muni de métriques naturelles aux places archimédiennes de K (cf. par exemple l'exposé 6 de ce séminaire, formule (1)) de sorte qu'il a un degré. La formule de Noether, démontrée dans [MB], donne :

(3.2.3.1) $$12 \deg_B f_*\omega_{X/B} = (\omega_{X/B}\cdot\omega_{X/B}) + \deg_B \underline{\delta}_c(X/B) - 4g\,[K:\mathbb{Q}] \log 2\pi$$

de sorte que (3.1.1) est équivalente à

(3.2.3.2)
$$(\lambda+1)\,(\omega_{X/B}\cdot\omega_{X/B}) \leq 12\lambda \deg_B f_*\omega_{X/B} + 4\lambda g\,[K:\mathbb{Q}] \log 2\pi + (\lambda-2)(2g-2) \log |D_K|.$$

C'est sous cette forme que (3.1.1) sera invalidée dans l'exposé 6 (pour une courbe particulière de genre 2 sur $\mathbb{Q}$, et tout $\lambda>0$).

3.3. Nous allons, dans le reste de ce §, expliquer le lien entre BM et la "conjecture des petits points" de Szpiro ([SPA], XI, 3.1).

Pour X comme en 3.1, on définit la hauteur

(3.3.1) $$h_\omega :\ X(\overline{K}) \to \mathbb{R}$$

où $\overline{K}$ désigne une clôture algébrique de K, comme la hauteur associée au $\mathcal{O}_X$-module $\omega_{X/B}$ muni de ses métriques d'Arakelov. Ainsi, si K' est une extension finie de K, d'anneau des entiers R', et si $P\in X(K')$ se prolonge en $\widetilde{P}\in X(R')$ par propreté, on a par définition

(3.3.2) $$[K':\mathbb{Q}]\ h_\omega(P) = \deg_{R'} \widetilde{P}^*\,\omega_{X/B}.$$

Si X' désigne le modèle régulier minimal de $X\otimes_R R'$, alors $\widetilde{P}$ définit une section de X' sur Spec R' ; si E désigne l'image de cette section, vue comme diviseur sur X', alors on a la *formule d'adjonction* ([SPA], II, théorème 6.11)

(3.3.3) $$[K':\mathbb{Q}]\ h_\omega(P) = -(E.E)$$

que nous n'utiliserons pas mais que nous rappelons pour faire le lien avec [SPA], XI, §3.

Comme $\omega_{X/B}$ est ample sur la fibre générique X_K, $h_\omega(P)$ est minoré (en fait par 0, voir plus bas) indépendamment de P. On peut donc poser

$$\text{(3.3.4)} \qquad \mathrm{hmin}(X) = \inf_{P\in X(\overline{K})} h_\omega(P).$$

On pose d'autre part

$$\text{(3.3.5)} \qquad e(X) = (\omega_{X/B}.\, \omega_{X/B})/[K:\mathbf{Q}].$$

Si K' et X' sont comme ci-dessus, alors $e(X')=e(X)$; ceci résulte par exemple de (5.4.2) plus bas.

La proposition ci-dessous et son corollaire sont, sauf la première inégalité, dus à Szpiro :

Proposition 3.4. *Avec les hypothèses et notations de* 3.3, *on a les inégalités*

$$0 \le e(X) \le 2g(2g-2)\,\mathrm{hmin}(X) \le g\,e(X).$$

Preuve. L'inégalité $e(X)\geq 0$ est un théorème de Faltings ([F], ou [SPA], III, théorème 5, *a)*). La seconde inégalité est prouvée dans [SPA], III, théorème 5, *b)* (ou II, 6.17) comme conséquence du théorème de l'indice.

Prouvons la troisième, c'est-à-dire $\mathrm{hmin}(X) \le e(X)/(4g-4)$. Posons $\omega = \omega_{X/B}$, et pour tout réel α notons $\omega(\alpha)$ le faisceau ω où l'on a multiplié les métriques par $e^{-\alpha}$; en d'autres termes $\omega(\alpha) = \omega\otimes\mathcal{O}_X(\alpha X_\infty)$ où X_∞ est le diviseur d'Arakelov somme des fibres archimédiennes. Le degré de $\omega(\alpha)$ est $2g-2>0$ et sa self-intersection est $(\omega.\omega)+2\alpha(2g-2)[K:\mathbf{Q}]$; choisissons α tel que $(\omega(\alpha).\omega(\alpha))>0$, c'est-à-dire

$$\text{(3.4.1)} \qquad \alpha > -e(X)/(4g-4).$$

On peut alors appliquer à $\omega(\alpha)$ le théorème d'existence de Faltings ([SPA], III, théorème 4) : il existe un entier $n>0$ et un diviseur d'Arakelov *effectif* D tels que $\mathcal{O}_X(D) \simeq \omega(\alpha)^{\otimes n}$. Quitte à changer le corps de base et à remplacer X par le modèle minimal idoine (ce qui ne change pas $\mathrm{hmin}(X)$ ni $e(X)$) on peut supposer que D est de la forme

$$\text{(3.4.2)} \qquad D = V + \textstyle\sum_{i=1}^{N} E_i$$

où les E_i sont des sections de $X \to B$ (donc $N=n(2g-2)$) et où V est *vertical*. Intersectant avec ω, on a d'une part, par définition de $\omega(\alpha)$:

$$(3.4.3) \qquad (\omega(\alpha).\omega) = (\omega.\omega) + \alpha(2g-2)[K:\mathbb{Q}]$$

et d'autre part, d'après (3.4.2) :

$$(3.4.4) \qquad n\,(\omega(\alpha).\omega) = (\,(V + \textstyle\sum_{i=1}^{N} E_i).\,\omega) \geq \sum_{i=1}^{N} (E_i.\,\omega) = [K:\mathbb{Q}] \sum_{i=1}^{N} h_\omega(P_i)$$

où P_i est le point générique de E_i : l'inégalité du milieu provient du fait que V est effectif et que ω est de degré ≥ 0 sur chaque composante d'une fibre. D'où

$$\inf_{i=1,\dots,N} h_\omega(P_i) \leq \frac{1}{N} \sum_{i=1}^{N} h_\omega(P_i) \leq (\omega(\alpha).\omega)/(2g-2)[K:\mathbb{Q}] = \alpha + (e(X)/(2g-2))$$

où la première inégalité est triviale, la seconde résulte de (3.4.4), et l'égalité de (3.4.3) (on rappelle que $N=n(2g-2)$).

A fortiori, on a $\mathrm{hmin}(X) \leq \alpha + (e(X)/(2g-2))$ pour tout α vérifiant (3.4.1), d'où le résultat. ■

Corollaire 3.5 *L'hypothèse* BM *équivaut à la variante suivante de la "conjecture des petits points"* ([SPA], XI, 3.1) *: il existe des applications*

$$\begin{array}{rl} A_{\mathrm{PP}}, B_{\mathrm{PP}}: & \mathbb{N}_{\geq 2} \times \mathrm{Div}_{c+}(\mathbb{Z}) \times \mathbb{N}_{\geq 1} \longrightarrow \mathbb{R} \\ & (g, \underline{\Delta}, d) \longmapsto A_{\mathrm{PP}}(g, \underline{\Delta}, d)\,,\ B_{\mathrm{PP}}(g, \underline{\Delta}, d) \end{array}$$

telles que pour K, R, X comme en 3.1 *avec* $[K:\mathbb{Q}] \leq d$ *et* $\underline{\Delta}(X/B) \leq \underline{\Delta}$ *, il existe un point* $P \in X(\overline{K})$ *vérifiant*

$$h_\omega(P) \leq A_{\mathrm{PP}}(g, \underline{\Delta}, d) \log|D_K| + B_{\mathrm{PP}}(g, \underline{\Delta}, d)\ . \ ■$$

4. Variations sur Mordell effectif.

4.1. L'hypothèse ME qui va suivre (voir 4.4) est un raffinement de la conjecture de Mordell; on va commencer par la formuler de manière plus générale. Soient K un corps de nombres, X un K-schéma propre (que l'on peut sans dommage supposer réduit). Soit L un faisceau inversible sur X. On fixe une clôture algébrique $\overline{K}$ de K, et on se donne une hauteur (logarithmique) $h : X(\overline{K}) \to \mathbb{R}$ associée à L.

Hypothèse ME(X,L). *Pour tout entier $d \geq 1$ il existe des réels $A_{\mathrm{ME}}(X,h,d)$ et $B_{\mathrm{ME}}(X,h,d)$ tels que, pour toute extension finie K' de K avec* $[K':\mathbb{Q}] \leq d$ *et tout*

$P \in X(K')$, on ait

(4.1.1) $$h(P) \le \frac{1}{d}\ A_{\mathrm{ME}}(X,h,d)\ \log|D_{K'}| + B_{\mathrm{ME}}(X,h,d).$$

Remarques.

4.1.2. Une variante optimiste de ME consisterait à imposer à A_{ME} et B_{ME} d'être *indépendants* de d.

4.1.3. La validité de $\mathrm{ME}(X,L)$ ne dépend pas du choix de h (d'où la notation), car si h' est une autre hauteur associée à L la différence $h-h'$ est bornée sur $X(\overline{K})$. Pour la même raison la "constante" A_{ME} de (4.1..1) (mais non B_{ME}) ne dépend, elle aussi, que de X et L: on la notera souvent $A_{\mathrm{ME}}(X,L,d)$.

4.1.4. Si L' est un autre faisceau inversible sur X, alors "$\mathrm{ME}(X,L)$ et $\mathrm{ME}(X,L')$" implique $\mathrm{ME}(X,L\otimes L')$ avec

$$A_{\mathrm{ME}}(X,L\otimes L',d) = A_{\mathrm{ME}}(X,L,d) + A_{\mathrm{ME}}(X,L',d)$$
$$B_{\mathrm{ME}}(X,h+h',d) = B_{\mathrm{ME}}(X,h,d) + B_{\mathrm{ME}}(X,h',d)$$

où h' est une hauteur associée à L'. En particulier $\mathrm{ME}(X,L)$ implique $\mathrm{ME}(X,L^{\otimes n})$ pour tout $n>0$.

4.1.5. Si L^{-1} est engendré par ses sections globales sur X, alors h est majorée et par suite $\mathrm{ME}(X,L)$ est vraie avec $A_{\mathrm{ME}} = 0$.

4.1.6. La validité de $\mathrm{ME}(X,L)$ ne dépend que du schéma X et non de K, en ce sens que si K_0 est un sous-corps de K et si X_0 désigne X vu comme K_0-schéma, alors $\mathrm{ME}(X,L)$ équivaut à $\mathrm{ME}(X_0,L)$ avec les mêmes fonctions A_{ME} et B_{ME} (autrement dit, on peut toujours supposer que $K = \mathbb{Q}$).

Proposition 4.2. *Soient $\pi : X_1 \to X$ un K-morphisme propre, $L_1 = \pi^*L$. Soit h_1 la hauteur $h\circ\pi$ sur $X_1(\overline{K})$* (qui est associée à L_1).

(i) *Si* $\mathrm{ME}(X,L)$ *est vérifiée, alors* $\mathrm{ME}(X_1,L_1)$ *est vérifiée avec* $A_{\mathrm{ME}}(X_1,h_1,d) = A_{\mathrm{ME}}(X,h,d)$, *et de même pour* B_{ME}.

(ii) *Si* $\mathrm{ME}(X_1,L_1)$ *est vérifiée et si π est* surjectif et non ramifié *(donc* fini*), alors* $\mathrm{ME}(X,L)$ *est vérifiée avec* $A_{\mathrm{ME}}(X,h,d) = A_{\mathrm{ME}}(X_1,h_1,md)$ *pour un choix convenable de* $B_{\mathrm{ME}}(X,h,d)$, *où l'on a posé*

$$m = \max_{x\in X_1}\,[\kappa(x) : \kappa(\pi(x))].$$

Preuve. L'assertion (i) est immédiate puisque π envoie $X_1(K')$ dans $X(K')$ pour toute extension K' de K. Prouvons (ii). Il existe un ensemble fini S de places de K tel que si U est le spectre de l'anneau des S-entiers de K , π se prolonge en un morphisme fini, surjectif et non ramifié $\pi_U : X_{1,U} \to X_U$ de U-schémas propres. Si K' est une extension finie de K, tout $P \in X(K')$ se relève en $P_1 \in X_1(K'')$, où K'' est une extension de K' de degré $\leq m$, et *non ramifiée en-dehors de* S. Il résulte alors de [S], 1.3, proposition 4, que, posant $d' = [K':\mathbb{Q}]$ et $d'' = [K'':\mathbb{Q}]$:

(4.2.1) $$\frac{d''}{d'} \log |D_{K''/K'}| \leq C := \sum_{p \in S_0} \log p + (\mathrm{Card}\, S) \log m$$

où S_0 désigne l'ensemble des caractéristiques résiduelles des places de S, d'où

(4.2.2) $$\frac{1}{d''} \log |D_{K''}| \leq \frac{1}{d'} \log |D_{K'}| + \frac{C}{d'} \cdot$$

D'autre part, $\mathrm{ME}(X_1, L_1)$ donne puisque $d'' \leq md'$:

(4.2.3) $$h(P) = h_1(P_1) \leq \frac{1}{d''} A_{\mathrm{ME}}(X_1, h_1, md') \log |D_{K''}| + B_{\mathrm{ME}}(X_1, h_1, md')$$

d'où le résultat en reportant (4.2.2). ■

Corollaire 4.3. (i) $\mathrm{ME}(X,L)$ *est vérifiée si et seulement si* $\mathrm{ME}(Y, L_{|Y})$ *est vérifiée pour toute composante irréductible* Y *de* X.

(ii) *Si* K_1 *est une extension finie de* K, *alors* $\mathrm{ME}(X,L)$ *équivaut à* $\mathrm{ME}(X_1, L_1)$ *où* (X_1, L_1) *est déduit de* (X,L) *par extension des scalaires de* K *à* K_1.

Il suffit en effet d'appliquer 4.2 à la projection naturelle $X_1 \to X$ où, dans la partie (i), X_1 désigne le schéma somme des composantes irréductibles de X. ■

Remarque 4.3.1. Le corollaire ci-dessus permet de se ramener, pour prouver $\mathrm{ME}(X,L)$, au cas où X est *géométriquement irréductible* sur K.

4.4. On notera $\mathrm{ME}(X)$ la propriété "$\mathrm{ME}(X,L)$ est vraie pour tout L". Si X est projectif sur K et L *ample* sur X , alors $\mathrm{ME}(X,L)$ équivaut à $\mathrm{ME}(X)$.

$\mathrm{ME}(X)$ implique que $X(K')$ est fini pour toute extension finie K' de K. En particulier $\mathrm{ME}(X)$ est trivialement fausse si X est une courbe de genre ≤ 1. On s'intéressera surtout dans la suite à l'hypothèse suivante :

Hypothèse ME. $\mathrm{ME}(X)$ *est vérifiée pour toute courbe* X *propre et lisse sur* $\mathbb{Q}$ (ou sur un corps de nombres quelconque, cf. 4.1.6) *à composantes géométriques de genre* ≥ 2.

Observer que ME équivaut à "ME(X, ω_X) est vérifiée pour toute courbe X propre et lisse sur un corps de nombres", le cas du genre 0 ou 1 étant trivial d'après 4.1.5. On pourrait donc se demander si, en dimension quelconque, ME(X, ω_X) serait toujours vraie pour X propre et lisse sur K (avec $\omega_X = \Omega^d_{X/K}$, $d = \dim X$). Il n'en est rien, comme me l'a fait remarquer E. Viehweg : on peut en effet construire une surface lisse X contenant une courbe de genre ≤ 1 et telle que ω_X soit ample (par exemple une surface lisse de degré 5 dans $\mathbb{P}^3$ contenant une droite).

5. De Bogomolov-Miyaoka à Mordell effectif.

Théorème 5.1. *Soit X un schéma propre sur $\mathbb{Q}$, et soit $f: Y \to X$ une X-courbe propre et lisse, à fibres géométriquement connexes de genre $\gamma \geq 2$. Soit L le faisceau inversible $\langle \omega_{Y/X}, \omega_{Y/X} \rangle$ sur X, où $\langle\, ,\rangle$ désigne l'accouplement de Deligne* (cf. rappels en 4.1).

Alors BM *implique* ME(X,L) *avec*

$$A_{\mathrm{ME}}(X, L, d) = A_{\mathrm{BM}}(\gamma, Nd\underline{v}, Nd)$$

pour $\underline{v} \in \mathrm{Div}_{c+}(\mathbb{Z})$ *convenable et* $N = 4\,\mathrm{Card}\ \mathrm{Sp}_{2\gamma}(\mathbb{Z}/12\mathbb{Z})$.

Théorème 5.2. BM *implique* ME.

5.3. Montrons que 5.2 est une conséquence facile de 5.1, grâce à la "construction de Kodaira". Supposant BM, il suffit de prouver ME(X), où X est une courbe projective, lisse et géométriquement connexe de genre $g \geq 2$ sur un corps de nombres K. On peut de plus étendre K, et remplacer X par un revêtement fini étale (4.2). Ceci permet de supposer ([K] ; [SPA], exposé X) qu'il existe une X-courbe projective et lisse $f: Y \to X$, à fibres géométriquement connexes de genre $\gamma \geq 2$, et *non isotriviale* (i.e. "à modules variables"). Le degré, sur la courbe X, de $L = \langle \omega_{Y/X}, \omega_{Y/X} \rangle$ est la self-intersection de $\omega_{Y/X}$ sur la surface Y donc est >0 : c'est un théorème général d'Arakelov mais dans le cas de la construction de Kodaira on peut calculer ce degré directement. Donc L est *ample* sur X , de sorte que, d'après 4.4, ME(X) équivaut à ME(X,L), elle-même conséquence de BM si l'on en croit le théorème 5.1. ■

Remarque 5.3.1. Dans l'argument ci-dessus on peut en fait calculer explicitement

L en termes de ω_X (du moins à torsion près dans Pic(X)) de sorte que l'on obtient $A_{\mathrm{ME}}(X, \omega_X, d)$ de façon effective en termes de A_{BM} .

Le reste du § 5 est consacré à la preuve du théorème 5.1.

5.4. *Rappels sur l'accouplement de Deligne* ([SGA 4], exposé XVIII ; [SPA], exposé II ; [D]). Si $f : X \to B$ est une courbe propre et plate sur un schéma B, à fibres de Cohen-Macaulay, et L, M deux faisceaux inversibles sur X, on construit un faisceau inversible $<L,M>_f$ sur B, bilinéaire en L et M et commutant à tout changement de base $B' \to B$; on le notera aussi $<L,M>_{X/B}$, ou simplement $<L,M>$ si aucune confusion n'est à craindre. On le calcule ainsi : si $D \subset X$ est un diviseur de Cartier effectif et plat sur B, on a un isomorphisme canonique de $\mathcal{O}_B$-modules inversibles

(5.4.1) $$<L, \mathcal{O}_X(D)> \simeq N_{D/B}(L_{|D}) .$$

De plus ([D], § 6) si B est un $\mathbb{C}$-schéma lisse avec X lisse sur B, et si L et M sont munis de métriques hermitiennes C^∞ (ou même parfois de "métriques singulières") on définit de façon naturelle une métrique hermitienne sur $<L,M>$; voir aussi [SPA], exposé II pour le cas particulier des métriques permises au sens d'Arakelov.

Si $L = M$ on notera $<L,L> = L^2_{X/B}$ ou L^2 ; c'est donc un $\mathcal{O}_B$-module inversible que l'on ne confondra pas avec le $\mathcal{O}_X$-module $L^{\otimes 2}$. Si les fibres de f sont de Gorenstein (par exemple nodales) et si $L = M = \omega_{X/B}$ on obtient un $\mathcal{O}_B$-module $\omega^2_{X/B}$.

Si B est le spectre de l'anneau des entiers d'un corps de nombres K, avec X_K lisse géométriquement connexe sur K de genre ≥ 1, et si L et M sont munis de métriques d'Arakelov aux places archimédiennes, alors $<L,M>$ a un degré (puisqu'il est muni de normes aux places archimédiennes) ; ce degré, lorsque X est régulier et f semi-stable, n'est autre que l'intersection d'Arakelov $(L.M)$ [SPA]. Si f est semi-stable et si $\pi : X' \to X$ est l'éclaté d'un point singulier de X, on a un isomorphisme canonique

(5.4.2) $$<L,M>_{X/B} \simeq <\pi^*L, \pi^*M>_{X'/B}$$

(représenter M par un diviseur ne passant pas par le point éclaté, et appliquer (5.4.1)) et un isomorphisme non moins canonique $\pi^*\omega_{X/B} \simeq \omega_{X'/B}$ (comme le diviseur exceptionnel E est un $\mathbb{P}^1$ de self-intersection -2, le faisceau $\omega_{X'/B}$ est trivial sur E), de sorte que $\omega^2_{X/B}$ ne dépend que de X_K (supposée lisse) et non du choix du modèle semi-stable X ; de plus son degré, dans la situation de 3.1 (où X est supposé régulier) est égal à $(\omega_{X/B}.\ \omega_{X/B})$.

5.5. Plaçons-nous maintenant dans la situation du théorème 5.1 : X est un schéma propre sur $\mathbb{Q}$ et $f: Y \to X$ une X-courbe lisse à fibres géométriquement connexes de genre $\gamma \geq 2$. On veut montrer que $\mathrm{ME}(X, \omega^2_{X/B})$ est conséquence de BM. *Pour cela nous supposerons d'abord que* :

(5.5.1) le noyau de la multiplication par 12 dans $\underline{\mathrm{Pic}}^0_{Y/X}$ est constant, i.e. X-isomorphe à $(\mathbb{Z}/12\mathbb{Z})^{2\gamma}_X$.

Dans ces conditions, soit K une extension finie de $\mathbb{Q}$, d'anneau des entiers R, et soit $P \in X(K)$. Vu l'hypothèse (5.5.1), le modèle régulier minimal $\mathcal{Y}_P \to \operatorname{Spec} R$ de la fibre Y_P de f en P est semi-stable (cf. 2.6). Posons alors $d = [K:\mathbb{Q}]$ et

(5.5.2)
$$h(P) = \frac{1}{d}\ \deg_R \omega^2_{\mathcal{Y}_P/R} = e(\mathcal{Y}_P) \in \mathbb{R} \qquad \text{(cf. (3.3.5))}$$
$$\underline{v}(P) = \frac{1}{d}\ \underline{\Delta}(\mathcal{Y}_P) \in \mathrm{Div}_{c+}(\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Q}\ .$$

Dans la première formule $\omega^2_{\mathcal{Y}_P/R}$ est bien entendu muni de sa structure hermitienne canonique. Notons que $h(P)$ et $\underline{v}(P)$ ne dépendent que de l'image de P dans $X(\overline{\mathbb{Q}})$, et non de K. De plus ils se calculent par les mêmes formules si l'on remplace $\mathcal{Y}_P$ par le modèle *stable* de Y_P sur R : ceci résulte de 2.4 pour $\underline{v}(P)$, et de 5.4 pour $h(P)$.

Les lemmes 5.6 et 5.7 qui suivent n'utilisent pas l'hypothèse BM et seront démontrés un peu plus loin (5.10).

Lemme 5.6. $h : X(\overline{\mathbb{Q}}) \to \mathbb{R}$ *est une hauteur associée au faisceau* $\omega^2_{Y/X}$.

Lemme 5.7. *Il existe* $\underline{v} \in \mathrm{Div}_{c+}(\mathbb{Z})$ *tel que pour tout* $P \in X(\overline{\mathbb{Q}})$ *on ait* $\underline{v}(P) \leq \underline{v}$.

Corollaire 5.8. *Sous l'hypothèse* (5.5.1), BM *implique* $\mathrm{ME}\,(X, \omega^2_{Y/X})$ *avec* $A_{\mathrm{ME}}\,(X, \omega^2_{Y/X}, d) = A_{\mathrm{BM}}\,(\gamma, d\underline{v}, d)$ *où* $\underline{v}$ *est comme en* 5.7.

Preuve du corollaire : gardant les notations K, P, d ci-dessus, le lemme 5.7 donne $\underline{\delta}(\mathcal{Y}_P) \leq d\underline{v}$; appliquant BM à $\mathcal{Y}_P$, on trouve l'inégalité

$$h(P) \leq \frac{1}{d}\ A_{\mathrm{BM}}\,(\gamma,\ d\underline{v}\ , d) \log|D_K| + B_{\mathrm{BM}}(\gamma,\ d\underline{v}\ , d)\ .$$

On obtient bien ME $(X, \omega^2_{Y/X})$ compte tenu du lemme 5.6. ■

5.9. *Preuve du théorème* 5.1. Ne supposant plus (5.5.1), soit K_1 l'extension de $\mathbb{Q}$ (de degré 4) engendrée par les racines douzièmes de l'unité ; posons $X_1 = X \otimes_{\mathbb{Q}} K_1$, et $Y_1 = Y \times_X X_1$. Le X_1-schéma en groupes noyau de la multiplication par 12 dans $\underline{\mathrm{Pic}}_{Y_1/X_1}$ est alors muni d'une dualité alternée à valeurs dans $(\mu_{12})_{X_1} \simeq (\mathbb{Z}/12\mathbb{Z})_{X_1}$, et à ce titre il est trivialisé par un revêtement étale X_2 de X_1, de groupe $\mathrm{Sp}_{2\gamma}(\mathbb{Z}/12\mathbb{Z})$ et donc de degré N sur X. On applique alors 5.8 sur X_2, puis 4.2 pour redescendre à X. ■

5.10. Il reste à démontrer 5.6 et 5.7. On peut pour cela remplacer X par X_1 et Y par $Y_1 = Y \times_X X_1$, où $\pi : X_1 \to X$ est *propre et surjectif* : en effet, pour $P \in X(\overline{\mathbb{Q}})$, $h(P)$ et $\underline{v}(P)$ ne dépendent que de la courbe Y_P sur $\overline{\mathbb{Q}}$. Or il existe un tel X_1 et un diagramme

(5.10.1) $$\mathcal{Y} \to \mathcal{X} \to B = \mathrm{Spec}\, \mathbb{Z}$$

induisant sur $\mathbb{Q}$ le diagramme $Y_1 \to X_1 \to \mathrm{Spec}\, \mathbb{Q}$, et où $\mathcal{Y}$ et $\mathcal{X}$ sont propres et plats sur B et $\mathcal{Y}$ une $\mathcal{X}$-courbe *stable* : en effet on commence par prolonger X et Y au-dessus d'un ouvert de Spec $\mathbb{Z}$, et l'on applique alors [SPA], V, lemme 1.6 (conséquence de la propreté sur $\mathbb{Z}$ du champ des courbes stables de genre γ).

Pour prouver 5.6 et 5.7 nous supposerons donc (remplaçant X par X_1) l'existence d'un diagramme (5.10.1) induisant $Y \to X \to \mathrm{Spec}\, \mathbb{Q}$ sur la fibre générique.

Dans ces conditions, et avec les notations de 4.2, si $\widetilde{P}: \mathrm{Spec}\, R \to \mathcal{X}$ prolonge P (puisque $\mathcal{X}$ est propre sur $\mathbb{Z}$) alors la surface arithmétique $\mathcal{Y}_{\widetilde{P}}$ déduite de $\mathcal{Y}$ par le changement de base $\widetilde{P}$ n'est autre que le modèle stable de Y_P sur Spec R. Il est alors clair par définition que h est la hauteur sur $X(\overline{\mathbb{Q}})$ déduite du modèle propre $\mathcal{X} \to B$ de X muni du faisceau inversible $\omega^2_{\mathcal{Y}/\mathcal{X}}$, lui-même équipé de ses métriques canoniques aux places archimédiennes. Ceci prouve le lemme 5.6.

Montrons 5.7 en commençant par la partie archimédienne $\underline{v}(P)(\infty)$. Si $P \in X(K)$ avec $[K:\mathbb{Q}] = d < \infty$, et si l'on note σ_i $(i=1,\dots,d)$ les plongements de K dans $\mathbb{C}$, on a par définition (cf. 2.7) $\underline{v}(P)(\infty) = \frac{1}{d} \sum_{i=1}^{d} |\delta(Y_{\sigma_i P})|$ où δ est l'invariant de Faltings. Comme $X(\mathbb{C})$ est une variété compacte, l'application $x \in X(\mathbb{C}) \longmapsto \delta(Y_x)$ est bornée. La formule ci-dessus implique que $\underline{v}(P)(\infty)$ est bornée par la même constante.

Pour borner la "partie finie" de $\underline{v}(P)$, on considère comme il se doit le

$\mathcal{O}_{\mathcal{X}}$-module cohérent $\Sigma(\mathcal{Y}/\mathcal{X})$ défini en 2.3. Comme $\mathcal{Y}_{\mathbb{Q}} \to \mathcal{X}_{\mathbb{Q}}$ est lisse, ce faisceau est nul sur $\mathcal{X}_{\mathbb{Q}}$ donc à support dans un nombre fini de fibres de $\mathcal{X} \to \operatorname{Spec} \mathbb{Z}$. Il est en particulier annulé par un entier non nul n ; d'autre part son rang en chaque point de $\mathcal{X}$ est borné par un entier r indépendant du point (par exemple $r = 3\gamma-3$, comme on l'a dit en 1.3). Si $P \in X(K)$ avec $[K:\mathbb{Q}] = d$, et si on prolonge P en $\tilde{P} \in \mathcal{X}(R)$ où R est l'anneau des entiers de K, alors $\Sigma(\mathcal{Y}_{\tilde{P}} / \operatorname{Spec} R)$ est donc un R-module de longueur finie, annulé par n et partout de rang $\leq 3\gamma-3$, de sorte que le diviseur $\underline{\delta}(\mathcal{Y}_{\tilde{P}} / \operatorname{Spec} R)$ de (2.5.1) est $\leq (3\gamma-3)\operatorname{div}_R(n)$ d'où

$$\underline{\Delta}(Y_P) = N_{\operatorname{Spec} R/\operatorname{Spec} \mathbb{Z}}\ \underline{\delta}(\mathcal{Y}_{\tilde{P}} / \operatorname{Spec} R) \leq [K:\mathbb{Q}]\,(3\gamma-3)\operatorname{div}(n)$$

et enfin $\underline{v}(P) \leq (3\gamma-3)\operatorname{div}(n)$ d'où le lemme. ■

Remarque 5.11. Si l'on admet la version renforcée de BM mentionnée en 3.2.2, le lemme 5.7 devient inutile : on remarque simplement que les courbes $\mathcal{Y}_P$ ont toutes bonne réduction en-dehors d'un ensemble fini, indépendant de P, de nombres premiers. On retrouve essentiellement l'argument utilisé dans [SPA], XI, §3 pour déduire un "Mordell effectif" de la conjecture des petits points.

6. De Mordell effectif à la conjecture du discriminant.

6.1. L'hypothèse CD ci-dessous implique, comme on sait (ce séminaire, exposé 1), le "grand théorème de Fermat en degré assez grand" (effectif en fonction des constantes A_{CD} et B_{CD}) :

Hypothèse CD (conjecture de Szpiro). *Il existe des constantes A_{CD} et B_{CD} telles que pour toute courbe elliptique E sur $\mathbb{Q}$, à réduction semi-stable sur $\mathbb{Z}$, on ait*

$$\log|\Delta_{\min}(E)| \leq A_{\mathrm{CD}} \log N(E) + B_{\mathrm{CD}}$$

où $\Delta_{\min}(E)$ (resp. $N(E)$) désigne le discriminant minimal (resp. le conducteur) de E.

Théorème 6.2. ME *implique* CD.

6.3. Fixons une fois pour toutes une courbe modulaire X sur $\mathbb{Q}$, de genre ≥ 2. L'invariant modulaire j se prolonge en un morphisme fini, encore noté j : $X \to \mathbb{P}^1_{\mathbb{Q}}$; notons n son degré.

On notera h la hauteur naïve sur $\mathbb{P}^1(\overline{\mathbb{Q}})$ (de sorte que si $a,b \in \mathbb{Z}$ sont premiers entre eux, $h(a/b) = \log \max \{|a|, |b|\}$). Si E désigne une courbe elliptique sur $\mathbf{Q}$, on utilisera les faits suivants :

(6.3.1) (a) $j(E)$ se relève en un point $\tilde{j} \in X(K)$ où K est un corps de nombres de degré $[K:\mathbf{Q}] \leq n$, non ramifié en dehors des places divisant $vN(E)$ où v est le "niveau" de X (indépendant de E) ;
(b) si E a réduction semi-stable sur $\mathbb{Z}$ alors $|\Delta_{\min}(E)|$ est le dénominateur de $j(E)$ (écrit sous forme irréductible). En particulier $\log|\Delta_{\min}(E)| \leq h(j(E))$.

Notons enfin h_1 la hauteur $h \circ j$ sur $X(\overline{\mathbf{Q}})$. Dans ces conditions on a une version plus précise du théorème 6.2 :

Théorème 6.4. *On suppose vérifiée* ME(X,h_1). *Alors* CD *est vérifiée avec les constantes*

$$A_{\mathrm{CD}} = (1+\log n)\, A_{\mathrm{ME}}(X,h_1,n)$$
$$B_{\mathrm{CD}} = B_{\mathrm{ME}}(X,h_1,n) + (\log n + \log n \log v_0 + \log v_0)\, A_{\mathrm{ME}}(X,h_1,n)$$

où v_0 est le produit des nombres premiers divisant v.

Preuve. Soit E une courbe elliptique sur $\mathbf{Q}$, à réduction semi-stable sur $\mathbb{Z}$. Il suffit d'après (6.3.1) (b) de majorer $h(j(E)) = h_1(\tilde{j})$ où $\tilde{j}$ est comme en (6.3.1) (a). Appliquant ME, on a, puisque $[K:\mathbf{Q}] \leq n$:

(6.4.1) $$\log|\Delta_{\min}(E)| \leq h_1(\tilde{j}) \leq \frac{1}{n} A_{\mathrm{ME}}(X,h_1,n) \log|D_{K/\mathbf{Q}}| + B_{\mathrm{ME}}(X,h_1,n).$$

D'après [S], proposition 6, on a (compte tenu de (6.3.1) (a)) :

$$\frac{1}{n}\log|D_K| \leq \log(v_0 N(E)) + (1+\log(v_0 N(E)))\log n$$
$$= (1+\log n)\log N(E) + (1+\log n)\log v_0 + \log n$$

où l'on a majoré le nombre de nombres premiers divisant $vN(E)$ par $1+\log(v_0 N(E))$. Reportant dans (6.4.1) on en déduit le théorème. ■

7. De Mordell effectif à la "conjecture *abc*".

7.1. Soit X le modèle projectif lisse sur $\mathbf{Q}$ de la courbe d'équation affine $y^2+y=x^5$. C'est une courbe de genre 2, et la fonction y définit un revêtement $\pi\colon X \to \mathbb{P}^1$ de degré 5, totalement ramifié aux points 0, -1 et ∞. Soit $y=b/a$ un point de $\mathbb{P}^1(\mathbf{Q})$, avec a et b entiers premiers entre eux. Posons $c=a+b$, $m=y^2+y=bc/a^2$, et $K=\mathbf{Q}(\sqrt[5]{m})$. Alors les coordonnées y et $x=\sqrt[5]{m}$ définissent un point $P\in X(K)$ tel que $\pi(P)=y$. Si l'on note h la hauteur naïve sur $\mathbb{P}^1_{\mathbf{Q}}$ et $h_1=h\circ\pi$, l'hypothèse ME appliquée à P donne

$$\log\max(|a|,|b|)\leq \frac{1}{5}A_{\mathrm{ME}}(X,h_1,5)\log|D_{K/\mathbf{Q}}| + B_{\mathrm{ME}}(X,h_1,5).$$

Les nombres premiers ramifiés dans K sont parmi ceux qui divisent abc, dont le produit sera noté rad(abc). Pour un tel nombre premier p, la p-composante de $D_{K/\mathbf{Q}}$ est au plus p^4 si $p\neq 5$, et au plus 5^5 si $p=5$, d'où $|D_{K/\mathbf{Q}}|\leq 5\ \mathrm{rad}(abc)^4$ et finalement

Théorème 7.2. *On suppose vérifiée* ME(X), *où X est la courbe définie ci-dessus. Alors, si a et b sont deux entiers premiers entre eux et $c=a+b$, on a*

$$\log\max(|a|,|b|)\leq \frac{4}{5}A_{\mathrm{ME}}(X,h_1,5)\log\mathrm{rad}(abc) + B_{\mathrm{ME}}(X,h_1,5)+\frac{1}{5}\log 5. \blacksquare$$

Les liens directs entre la conjecture du discriminant et la "conjecture *abc*" sont étudiés notamment dans l'exposé 1 de ce séminaire.

8. Questions d'effectivité.

8.1. Chacune des hypothèses envisagées dans ce qui précède fait intervenir une "constante A" et une "constante B". Le lecteur aura remarqué que, dans les énoncés du type "l'hypothèse X implique l'hypothèse Y", il est possible de calculer A_{Y} en fonction de A_{X} mais qu'il n'en va pas de même en général pour les constantes B. La résistance de ces dernières provient toujours de la contribution des mauvaises places lorsque l'on passe d'un objet défini sur un corps de nombres (morphisme non ramifié dans 4.2 (ii), famille de courbes dans 5.10) à un modèle entier. Bien entendu ces mauvaises places comprennent les places archimédiennes, lorsqu'il s'agit de comparer des métriques sur des fibrés ; un des points les plus difficiles semble être la majoration de la fonction δ de Faltings, obtenue en 5.9 par un argument de compacité.

8.2. Disons quelques mots du passage de BM à CD. Soit X la courbe modulaire utilisée au § 6 (celle-ci est d'ailleurs à peu près quelconque; le "bon" cadre pour ME serait plutôt celui des champs algébriques, en l'occurrence le champ sur Spec ($\mathbb{Z}$) des courbes elliptiques, convenablement compactifié). Lorsque l'on déduit

ME(X) de BM (supposé effectif), nous avons vu en 5.3.1 que l'on obtient une valeur effective pour $A_{\mathrm{ME}}(X, \omega_X)$; or, le théorème 6.4 donne A_{CD} en termes de $A_{\mathrm{ME}}(X, h_1)$, où h_1 est déduite via le morphisme j de la hauteur naïve sur $\mathbb{P}^1$, donc est associée à $\mathcal{O}_X(D)$ où D est le diviseur des pointes sur X. Calculer A_{CD} revient donc à comparer, à $O(1)$ près, les hauteurs h_ω et h_1 associées respectivement à ω_X et $\mathcal{O}_X(D)$. Or on déduit sans peine du théorème de Manin-Drinfeld (ce séminaire, exposé 7) que, pour M et $N>0$ convenables, on a $\omega_X^{\otimes M} \simeq \mathcal{O}_X(ND)$, et par conséquent la différence $(\deg D)h_\omega - (\deg \omega_X)h_1$ est bornée.

Références.

[A] S. Ju. ARAKELOV, *Intersection theory of divisors on an arithmetic surface,* Math. USSR. Izv. 8 (1974) n° 6, 1167-1180.

[B] F.A. BOGOMOLOV, *Holomorphic tensors and vector bundles on projective varieties,* Izvestija AN SSSR, ser. math., 42 (1978), 1227-1287 ; trad. anglaise Math. USSR Izv. vol. 13 n° 3 (1979), 499-555.

[D] P. DELIGNE, *Le déterminant de la cohomologie*, Contemporary Math. 67 (1987), 93-177.

[D-M] P. DELIGNE et D. MUMFORD, *The irreducibility of the space of curves of given genus,* Pub. Math. IHES vol. 36.

[F] G. FALTINGS, *Calculus on arithmetic surfaces,* Ann. of Math. 119 (1984), 387-424.

[K] K. KODAIRA, *A certain type of irregular algebraic surface,* Journal d'Analyse Mathématique, 19 (1967).

[M] Y. MIYAOKA, *On the Chern numbers of surfaces of general type,* Invent. Math. 42 (1977), 225-237.

[MB] L. MORET-BAILLY, *La formule de Noether pour les surfaces arithmétiques,* preprint.

[P] A.N. PARSHIN, *The Bogomolov-Miyaoka-Yau inequality for arithmetical surfaces and its applications*, Séminaire de théorie des nombres de Paris 1986-87, Progress in Math. (Birkhäuser) vol. 75.

[S] J.-P. SERRE, *Quelques applications du théorème de densité de Chebotarev,* Pub. Math. IHES vol. 54, 123-201.

[SGA 4] M. ARTIN, A.GROTHENDIECK, J.-L. VERDIER et al., *Séminaire de Géométrie Algébrique du Bois Marie* 1963/64, tome 3, Springer LNM 305.

[SPA] L. SZPIRO et al., *Séminaire sur les pinceaux arithmétiques : la conjecture de Mordell,* Astérisque vol. 127.

[SPC] L. SZPIRO et al., *Séminaire sur les pinceaux de courbes de genre au moins deux*, Astérisque vol. 86.

[V] A. VAN DE VEN, *On the Chern numbers of certain complex and almost-complex manifolds*, Proc. Nat. Acad. Sci. USA, 55 (1966), 1624-1627.

[Y] S.-T. YAU, *Calabi's conjecture and some new results in algebraic geometry,* Proc. Nat. Acad. Sci. USA, 74 (1977), 1789-1799.

Laurent Moret-Bailly
IRMAR, Université de Rennes-I
Campus de Beaulieu
F-35042 Rennes Cedex
EARN : moret@FRCICB81

Astérisque

RENÉE ELKIK

Le théorème de Manin-Drinfeld

Astérisque, tome 183 (1990), p. 59-67
<http://www.numdam.org/item?id=AST_1990__183__59_0>

Société Mathématique de France
Astérisque 183 (1990)

Le Théorème de Manin–Drinfeld

R. ELKIK

Si N est un entier positif on désigne par $\Gamma(N)$ le sous–groupe de $SL(2,\mathbb{Z})$ formé des matrices congrues à l'identité modulo N. Un sous–groupe Γ de $SL(2,\mathbb{Z})$ est appelé sous–groupe de congruence s'il existe N tel que $\Gamma \supset \Gamma(N)$. On désigne alors par X_Γ^o (resp. X_Γ) la surface de Riemann quotient du demi–plan de Poincaré par Γ (resp. sa complétion projective lisse). On appelle "pointes" les points de $X_\Gamma - X_\Gamma^o$. Le théorème de Manin–Drinfeld s'énonce ainsi :

THÉORÈME. ***Si*** Γ ***est un sous-groupe de congruence, la classe de tout diviseur de degré*** 0 ***de*** X_Γ ***à support dans les pointes, est un élément de torsion de*** $\mathrm{Pic}^o(X_\Gamma)$.

La démonstration originelle de ce théorème est due à Manin [Ma] complétée par Drinfeld [Dr].

Dans le cas du groupe $\Gamma_o(p)$, p premier, la courbe modulaire correspondante n'a que deux pointes P_o et P_∞. Si l'on pose

$$\Delta(2) = q \prod_{n=1}^{\infty} (1-q^n)^{24} \quad , \text{où} \quad q = e^{2i\pi\tau}$$

et $\Delta_p(\tau) = \Delta(p\tau)$ le quotient Δ/Δ_p définit une fonction rationnelle sur $X_{\Gamma_o(p)}$ dont le diviseur est $(p-1)(P_o-P_\infty)$. On peut montrer que pour $p>3$ la classe de (P_o-P_∞) est d'ordre exactement $\frac{p-1}{d}$, où $d = \frac{12}{(p-1,12)}$.
[pour plus de détails voir Ogg [0]).

Nous avons choisi d'exposer en détail la démonstration proposée par Deligne [De 1]. Le principe est le suivant :

a) Le théorème de Manin–Drinfeld est équivalent à l'énoncé suivant :
La structure de Hodge–mixte sur $H^1(X^o_\Gamma,\mathbb{Q})$ est scindée.

La démonstration de cette équivalence est l'objet du §1.

b) Il suffit d'établir le théorème pour les groupes $\Gamma(N)$: c'est clair.

c) L'entier N étant fixé on considère une correspondance de Hecke sur la courbe $X_{\Gamma(\mathrm{N})}$ qui définit un endomorphisme de $H^1(X^o_{\Gamma(\mathrm{N})},\mathbb{Z})$ muni de sa structure de Hodge mixte. L'ensemble des valeurs propres de cet opérateur agissant sur la composante de poids 1, c'est–à–dire essentiellement sur les formes modulaires cuspidales est disjoint de l'ensemble des valeurs propres pour l'action sur la partie de poids 2, qui correspond aux formes non cuspidales. Ceci permet de scinder la structure de Hodge sur $\mathbb{Q}$.

I – THÉORÈME.

***Soient** X **une courbe projective lisse sur** $\mathbb{C}$, S **un ensemble fini de points de** X **et** $j: X^o = X-S \hookrightarrow X$ **l'inclusion du complémentaire de** S **dans** X. **Les conditions suivantes sont équivalentes** :*

a) ***la classe de tout diviseur de degré** 0 **à support dans** S **est un élément de torsion de*** $\mathrm{Pic}^o(X)$.

b) ***La structure de Hodge mixte sur** $H^1(X^o,\mathbb{Q})$ **est scindée** (i.e. **somme directe de structures pures**).*

Cet énoncé résulte aisément de [De 3 §10–3] auquel réfère [De 1]. Le principe de la démonstration est alors le suivant : on considère le 1–motif formé de :

– la variété abélienne $\mathrm{Pic}^o(X)$
– le groupe D^o_S des diviseurs de degré 0 sur X portés par S
– l'homomorphisme classe de D^o_S dans $\mathrm{Pic}^o(X)$.

Il est clair sur sa définition que le H^1 de Hodge mixte de ce motif se scinde sur $\mathbb{Q}$ ssi la condition a) est remplie. On montre que ce H^1 motivique et $H^1(X^o,\mathbb{Z})$ sont isomorphes (comme structure de Hodge) à torsion par $\mathbb{Z}(1)$ près.

Lors de l'exposé oral nous avons suivi [De 3]. Nous donnons ici une démonstration un peu différente.

Rappelons d'abord la description de $H^1(X^o,\mathbb{Z})$. Si $\varphi: A \longrightarrow B$ est un homomorphisme de faisceaux abéliens sur un espace topologique on note $[A \xrightarrow{\varphi} B]$ le complexe dont les seuls termes non nuls sont A en degré 0, B en degré 1 et qui a φ pour différentielle.

On a les isomorphismes suivants [De 2] :

$$\begin{aligned} H^1(X^\circ,\mathbb{C}) &\xrightarrow{\sim} \mathbb{H}^1(X^\circ_{\circ},[0_{X^\circ} \xrightarrow{d} \Omega^1_{X^\circ}]) \\ &\xleftarrow{\sim} \mathbb{H}^1(X,[j_*0_{X^\circ} \xrightarrow{d} j_*\Omega^1_{X^\circ}) \\ &\xleftarrow{\sim} \mathbb{H}^1(X,0_X \xrightarrow{d} \Omega^1_X<S>) \end{aligned}$$

où $\Omega^1_X<S>$ désigne le faisceau des formes différentielles méromorphes sur X, holomorphes en restriction à X° et admettant des pôles d'ordre ≤ 1, aux points de S. La filtration par le poids sur $H^1(X^\circ,\mathbb{Z})$ est définie par : $W_{0,\mathbb{Z}} = 0$, $W_{1,\mathbb{Z}} = j^*H^1(X,\mathbb{Z})$ $(= H^1(X,\mathbb{Z}))$, $W_{2,\mathbb{Z}} = H^1(X^\circ,\mathbb{Z})$.

Si A désigne $\mathbb{Q}$, $\mathbb{R}$, ou $\mathbb{C}$ on note $W_{i,A}$, le sous-module $W_{i,\mathbb{Z}} \otimes A$ de $H^1(X^\circ,A)$. On a $W_{1,\mathbb{C}} = \mathrm{Im}(\mathbb{H}^1(X,O_X \xrightarrow{d} \Omega^1_X) \longrightarrow \mathbb{H}^1(X,O_X \xrightarrow{d} \Omega^1_X<S>))$.

Si s est un point de X on note $\mathbb{C}_s$ le faisceau sur X de fibre $\mathbb{C}$ en s et nul ailleurs. On a alors une suite exacte :

$$(\Sigma) \qquad 0 \longrightarrow \Omega^1_X \longrightarrow \Omega^1_X<S> \xrightarrow{r} \bigoplus_{s\in\mathbb{C}} \mathbb{C}_s \longrightarrow 0$$

$$w \longrightarrow r(w) = \oplus\, 2i\pi\, \mathrm{res}_s(w).$$

Notons encore $\bigoplus_{s\in S} \mathbb{C}_s$, l'espace des sections globales de ce faisceau et $\mathcal{U}$ le noyau de la forme linéaire sur $\bigoplus_{s\in S} \mathbb{C}_s : \bigoplus_s a_s \longrightarrow \sum_s a_s$. L'ensemble des points entiers de $\mathcal{U}$ s'identifie naturellement au groupe $D^\circ_S : \sum_s n_s.s \longrightarrow \bigoplus_s n_s$.

On vérifie aisément qu'on a le diagramme commutatif suivant dont les lignes sont exactes :

$$\begin{array}{ccccccc} 0 \longrightarrow & H^1(X,\mathbb{C}) & \longrightarrow & H^1(X^\circ,\mathbb{C}) & \longrightarrow & Gr^W_2(H^1(X^\circ,\mathbb{C})) & \longrightarrow 0 \\ & \uparrow \varphi_1 & & \uparrow \varphi & & \varphi_2 \uparrow & \\ 0 \longrightarrow & H^0(X,\Omega^1_X) & \longrightarrow & H^0(X,\Omega^1_X<S>) & \longrightarrow & U & \longrightarrow 0\,. \end{array}$$

La 1ère (resp. 2ème) ligne est déduite de la suite de cohomologie associée à l'inclusion $[O_X \to \Omega^1_X] \longrightarrow [O_X \to \Omega^1_X<S>]$ (resp. à Σ). Les flèches verticales sont induites par l'inclusion $\Omega^1_X<S>[-1] \longrightarrow [O_X \xrightarrow{d} \Omega^1_X<S>]$. En outre la flèche r a été définie de sorte que φ_2 soit compatible aux structures entières et identifie donc $\mathrm{Gr}^W_2(H^1(X^\circ,\mathbb{Z}))$ à D°_S.

La filtration de Hodge sur $H^1(X^\circ,\mathbb{C})$ est définie par $F^0 = H^1(X^\circ,\mathbb{C})$, $F^1 = \mathrm{Im}\,\varphi$, $F^2 = 0$. Comme l'application $F^1 \longrightarrow \mathrm{Gr}^W_2$ est surjective celui–ci est muni d'une structure pure de type (1,1). En outre $\mathrm{Gr}^{W}_{1} = H^{1}(X,\mathbb{C})$ est muni de sa structure pure "usuelle" de type ((0,1)(1,0)).

Une structure de Hodge mixte, extension de 2 structures pures de poids consécutifs est toujours scindée sur $\mathbb{R}$ [G,S]. Et il facile d'exhiber ici le scindage de cette structure sur $\mathbb{R}$: en effet $F_1^{\,1} \cap \overline{F^1}$ est un supplémentaire de $H^1(X,\mathbb{C})$ dans $H^1(X^o,\mathbb{C})$. Le supplémentaire cherché de $H^1(X,\mathbb{R})$ dans $H^1(X^o,\mathbb{R})$ est donc $F_1^{\,1} \cap H^1(X^o, \mathbb{R})$.

La démonstration du théorème repose sur le lemme suivant :

LEMME. ***Pour qu'une forme*** $w \in H^0(X,\Omega^1_X\langle S\rangle)$ ***définisse une classe de cohomologie entière de*** X^o ***il faut et il suffit qu'il existe une fonction méromorphe*** f ***sur*** X ***(automatiquement holomorphe non nulle sur*** X^o***) telle que*** $w = \frac{1}{2i\pi}\frac{df}{f}$.

La condition est clairement suffisante. Montrons qu'elle est nécessaire. Soient $\pi : \tilde{X}^o \longrightarrow X^o$ le revêtement universel de X^o et Γ son groupe d'automorphismes. Il existe une fonction holomorphe h sur $\tilde{X}^o$ telle que $\pi^*w = dh$. L'hypothèse faite sur w signifie que pour tout γ dans Γ, on a $h\circ\gamma - h \in \mathbb{Z}$. Il existe donc une fonction holomorphe f sur X^o telle que $f\circ\pi = e^{2\pi i h}$, et l'on a sur X^o $\frac{df}{f} = 2\pi i w$. La méromorphie de f sur X résulte de l'hypothèse $w \in H^0(X,\Omega^1_X\langle S\rangle)$.

Considérons donc $w = \frac{1}{2\pi i}\frac{df}{f} \in H^0(X,\Omega^1_X\langle S\rangle)$.

On a alors $\sum_S \mathrm{res}_s(w)s = \mathrm{Div}(f)$.

Le lemme signifie donc que pour qu'un élément de D^o_S se relève dans $F^1 \cap H^o(X^o,\mathbb{Z})$, il faut et il suffit qu'il soit principal, ce qui est un énoncé légèrement plus précis que celui du théorème.

II – ACTION DES CORRESPONDANCES SUR LA COHOMOLOGIE.

Considérons un diagramme cartésien

$$\begin{array}{ccc} Y^o & \hookrightarrow & Y \\ {\scriptstyle p^o}\downarrow & & \downarrow{\scriptstyle p} \\ X^o & \hookrightarrow & X \end{array}$$

dans lequel p^o est un morphisme fini de courbes lisses sur $\mathbb{C}$, étendu en p entre leurs complétions projectives lisses. On désigne par S (resp. $\tilde{S}$) l'ensemble des points de $X-X^o$ (resp. $Y-Y^o$).

On peut définir des homomorphismes $p^{o*} : H^1(X^o,\mathbb{Z}) \longrightarrow H^1(Y^o,\mathbb{Z})$ et $p^o_* : H^1(Y^o,\mathbb{Z}) \longrightarrow H^1(X^o,\mathbb{Z})$, le premier par contravariance de la cohomologie, le second grâce à la dualité de Poincaré et la covariance de l'homologie localement finie pour les morphismes propres. On vérifie que ce sont des homomorphismes de structure de Hodge.

Notons d'abord que l'injection $p^*\,\Omega^1_X \longrightarrow \Omega^1_Y$ se prolonge en un isomorphisme de faisceaux sur Y : $p^*\,\Omega^1_X\langle S\rangle \xrightarrow{\sim} \Omega^1_Y\langle \tilde{S}\rangle$ (car $\frac{dz^n}{z^n} = n\,\frac{dz}{z}$).

a) <u>La montée</u> : on en déduit des homomorphismes de faisceaux sur X : $\Omega^1_X \longrightarrow p_*\,\Omega^1_Y$, $\Omega^1_X\langle S\rangle \xrightarrow{\sim} p_*\,\Omega^1_Y\langle\tilde{S}\rangle$, et un diagramme commutatif de complexes

$$\text{(D)}\qquad \begin{array}{ccc} [O_X \xrightarrow{d} \Omega^1_X] & \longrightarrow & [O_X \xrightarrow{d} \Omega^1_X\langle S\rangle] \\ \downarrow\varphi & & \downarrow\varphi^o \\ [p_*O_Y \xrightarrow{d} p_*\Omega^1_Y] & \longrightarrow & [p_*O_Y \xrightarrow{d} p_*\Omega^1_Y\langle\tilde{S}\rangle]\,. \end{array}$$

L'homomorphisme p^{o*} est le composé de $H^o(\varphi^o)$ avec l'isomorphisme :
$\mathbb{H}^o(X,[p_*O_Y \xrightarrow{d} p_*\Omega^1_Y\langle\tilde{S}\rangle]) \xrightarrow{\sim} \mathbb{H}^o(Y,[O_Y \xrightarrow{d} \Omega^1_Y\langle\tilde{S}\rangle])$.
La compatibilité de φ^{o*} à la filtration par le poids se lit sur (D) dont la colonne de gauche correspond à W_1. Le morphisme de complexes φ^o induit des morphismes entre les tronqués bêtes et ceci fournit la compatibilité à F.

b) <u>La descente</u> : on dispose d'un morphisme trace : $p_*O_Y \xrightarrow{\mathrm{Tr}} O_X$ et d'un morphisme Trace $p_*\Omega^1_Y \xrightarrow{\mathrm{Tr}} \Omega^1_X$ qui prolonge

$$p_*p^*\Omega^1_X \xrightarrow{\sim} \Omega^1_X \otimes_{O_X} p_*O_Y \xrightarrow{1\otimes\mathrm{Tr}} \Omega^1_X$$

et s'étend en $\mathrm{Tr} : p_*\Omega^1_Y\langle\tilde{S}\rangle \longrightarrow \Omega^1_X\langle S\rangle$. De plus $\mathrm{Tr}\circ d = d\circ\mathrm{Tr}$.

On a donc un diagramme commutatif de complexes sur X :

$$\begin{array}{ccc} [p_*O_Y \xrightarrow{d} p_*\Omega^1_Y] & \longrightarrow & [p_*O_Y \xrightarrow{d} p_*\Omega^1_Y\langle\tilde{S}\rangle] \\ \downarrow\mathrm{Tr} & & \downarrow\mathrm{Tr}^o \\ [O_X \xrightarrow{d} \Omega^1_X] & \longrightarrow & [O_X \xrightarrow{d} \Omega^1_X\langle S\rangle]\,. \end{array}$$

On définit p^o_* comme le composé de

$$\mathbb{H}^{o}(Y,[O_Y \longrightarrow \Omega^1_Y<\tilde{S}>] \xrightarrow{\sim} \mathbb{H}^{o}(X,[p_*O_Y \xrightarrow{d} p_*\Omega^1_Y<\tilde{S}>])$$

avec $\mathbb{H}^o(\mathrm{Tr}^o)$ et on vérifie que c'est un endomorphisme de structures de Hodge comme en a).

III – LE SCINDAGE DE LA COHOMOLOGIE DE $X^o_{\Gamma(N)}$.

On rappelle que si f est une forme modulaire de poids 2 pour un sous–groupe d'indice fini Γ de $\mathrm{Sl}_2(\mathbb{Z})$ et $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ est une matrice à coefficients entiers de déterminant > 0 , on définit $f/[\alpha]$ par

$$f/_{[\alpha]}(z) = \mathrm{Det}(\alpha).(cz+d)^{-2}f(\frac{az+b}{cz+d}) .$$

En outre si f et g sont modulaires cuspidales pour Γ leur produit scalaire de Peterson est défini ainsi

$$<f,g> = \frac{1}{\mu}\int_{D} f(z)\overline{g(z)}\,\frac{dx dy}{y^2}$$

où μ est le degré du revêtement $X_\Gamma \longrightarrow X_{\mathrm{SL}(2,\mathbb{Z})}$ et D un domaine fondamental pour Γ .

On pose $\|f\| = <f,f>^{\frac{1}{2}}$. On a alors pour tout α comme plus haut

(1) $$\|f\| = \|f/[\alpha]\|$$

(cf. par exemple [L] chap. III ou [Sh] chap.III).

On fixe dans la suite un entier N et on écrit X (resp. X^o, resp. S) pour $X_{\Gamma(N)}$ (resp. $X^o_{\Gamma(N)}$, resp. l'ensemble des pointes). On désigne par $\mathcal{S}$ (resp. $\mathcal{S}^o$) l'espace des formes modulaires (resp. cuspidales) de poids 2 pour $\Gamma(N)$. On rappelle que $\mathcal{S}$ (resp. $\mathcal{S}^o$) s'identifie à $H^o(X,\Omega^1_X<S>)$ (resp. $H^o(X,\Omega^1_X)$).

On choisit maintenant un nombre premier p congru à 1 modulo N . Posons $\alpha_p = \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)$ et $\Gamma' = \Gamma(N) \cap \alpha_p^{-1}\Gamma(N)\alpha_p = \left\{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma(N)\ ,\ c \equiv 0(p)\right\}$. La double classe $M = \Gamma(N)\alpha_p\Gamma(N)$ est égale à l'ensemble des matrices entières congrues à Id mod N et de déterminant p . Si on pose $\alpha_j = \left(\begin{smallmatrix} 1 & Nj \\ 0 & p \end{smallmatrix}\right)$, $\forall j\,[0,p-1]$ on a une décomposition de M en classes à gauche sous $\Gamma(N)$

$M = \bigcup\limits_{j=0}^{p} \Gamma(N)\alpha_j$, d'où on déduit une décomposition de $\Gamma(N)$ en classes sous Γ' : $\Gamma(N) = \bigcup\limits_{j=0}^{p} \Gamma'\beta_j$, $\beta_j = \alpha_p^{-1}.\alpha_j$.

On dispose en outre de 2 morphismes finis $p^{o}, q^{o} : X^{o}_{\Gamma'} \longrightarrow X^{o}$ définis ainsi. Si pour tout $\Gamma \in SL(2,\mathbb{Z})$ on note p_{Γ} l'application quotient : $\mathfrak{h} \longrightarrow X^{o}_{\Gamma}$ on a

$p \circ p_{\Gamma'} = p_{\Gamma(N)}$; $q \circ p_{\Gamma'} = p_{\Gamma(N)} \circ \alpha_p$. Le diagramme :

$$\begin{tikzcd} & X^{o}_{\Gamma'} \arrow[dl, "q"'] \arrow[dr, "p"] & \\ X^{o} & & X^{o} \end{tikzcd}$$

définit un endomorphisme $T = p_* \circ q^*$ de la cohomologie de X^{o} . Si on identifie $H^{o}(X, \Omega^1_X\langle S\rangle)$ à f l'action de T se décrit ainsi :

$$T(f) = \sum_{j=0}^{p} f/[\alpha_p][\beta_j] = \sum_{j=0}^{p} f/[\alpha_j]$$

[pour plus de détails cf. [Sh] §7.3).

Pour $f \in \mathscr{S}$ nous écrirons son développement de Fourier en $i\infty$: $f = \sum\limits_{n=0}^{\infty} f_n\, q^n$, $q = e^{2i\pi z/N}$. On a alors :

$$f/[\alpha_p] = p \sum_{n=0}^{\infty} f_n\, q^{np} .$$

En particulier :

(2)
$$(f/[\alpha_p])_o = pf_o$$

(3)
$$\forall f \in \mathscr{S}, \lambda \in \mathbb{C} , f/_{[\alpha_p]} = \lambda f \Rightarrow f = 0 .$$

On vérifie d'autre part aisément que

(4)
$$(f/_{[\alpha_j]})_o = \frac{1}{p} f_o \qquad \forall j \in [0, p-1]$$

et donc

(5) $$T(f)_o = (p+1)f_o\ .$$

Comme $\Gamma(N)$ et M sont stables sous l'action de $\mathrm{SL}(2,\mathbb{Z})$ par conjugaison on étend (5) à toutes les pointes.

(6) Pour toute pointe s on a $T(f)(s) = (p+1)f(s)$.

Il résulte de (6) que la seule valeur propre de T agissant sur $\mathscr{S}/\mathscr{S}^o$, donc sur $\mathrm{Gr}^2_W(H^1(X^o_0,\mathbb{Z}))$ est $p+1$.

Soient maintenant $\lambda \in \mathbb{C}$ et $f \in \mathscr{S}^o-\{0\}$ tels que $T(f) = \lambda.f$. On a d'après (1) :

$$|\lambda|\,\|f\| \leq \sum_j \|f/[\alpha_j]\| \leq (p+1)\|f\|$$

avec égalité ssi tous les $f/[\alpha_j]$ sont égaux entre eux et colinéaires à f, ce qui est interdit par (3) et donc $|\lambda| < p+1$.

Cette majoration des valeurs propres de T agissant sur $\mathscr{S}^o$ est mauvaise, mais suffisante pour notre propos.

Soit $P(\Lambda) \in \mathbb{Z}[\Lambda]$ le polynôme caractéristique de T agissant sur $H^1(X,\mathbb{Z})$.

L'endomorphisme $P(T)$ de $H^1(X^o,\mathbb{Q})$ a pour image un supplémentaire de $H^1(X,\mathbb{Q})$ contenu dans F^1, ce qui montre que la structure de Hodge sur $H^1(X^o,\mathbb{Q})$ est scindée.

Bibliographie

[De 1] P. DELIGNE. *Valeurs de fonctions L et périodes d'intégrales.* Proc. Symp. Pure Math., Vol. 33 (1979), AMS, 313–346.

[De 2] P. DELIGNE. *Théorie de Hodge* 2. Inst. Hautes Etudes Sci. Publ. Math. (1972) 5–57.

[De 3] P. DELIGNE. *Théorie de Hodge* 3. Inst. Hautes Etudes Sci. Publ. Math. 44 (1974) 5–77.

[G.S] P. GRIFFITHS and W. SCHMID. *Recent Developments in Hodge Theory.* Proceedings of the International colloquium on Discrete Subgroups, Bombay (1973) 31–127.

[Dr] V.G. DRINFEL'D. *Two Theorems on Modular curves.* Functional analysis and its application, Vol. 7 n° 2, Translated from Russian 1973, 155–156.

[L] S. LANG. *Introduction to Modular forms.* Springer–Verlag (1976).

[Ma] J. MANIN. *Parabolic Points and Zeta functions of Modular curves.* Izv. Akad. Nauk SSSR., Vol. 6 n° 1 (1972) AMS Translation 19–64.

[O] A. OGG. *Rational Points on certain elliptic curves.* Proc. Symp. Pure Maths, Vol. 24, (1973), AMS, 221–231.

ELKIK Renée
Université de Paris–Sud
Mathématique, bât. 425
91405 ORSAY (France)

Astérisque

JEAN-BENOÎT BOST
JEAN-FRANÇOIS MESTRE
LAURENT MORET-BAILLY

Sur le calcul explicite des « classes de Chern » des surfaces arithmétiques de genre 2

Astérisque, tome 183 (1990), p. 69-105
<http://www.numdam.org/item?id=AST_1990__183__69_0>

Société Mathématique de France
Astérisque 183 (1990)

Sur le calcul explicite des "classes de Chern" des surfaces arithmétiques de genre 2.

Jean-Benoît BOST, Jean-François MESTRE, Laurent MORET-BAILLY.

Introduction

Soient K un corps de nombres, A l'anneau des entiers de K et $B = \operatorname{Spec} A$. Dans cet article, nous expliquons comment calculer les invariants $\deg f_*\omega_{X/B}$ et

$$(\omega_{X/B}.\omega_{X/B}) := \deg \langle \omega_{X/B}, \omega_{X/B} \rangle,$$

définis à la Arakelov, attachés à une courbe semi-stable $f : X \to B$, de fibre générique lisse et de genre 2.

Rappelons que ces deux nombres jouent un rôle analogue, en géométrie arithmétique, à celui des invariants c_1^2 et c_2 d'une surface projective irréductible lisse sur un corps (*cf.* [7]). En effet, si $f : X \to B$ est un morphisme surjectif d'une telle surface vers une courbe lisse de genre q, qui fait de X une B-courbe semi-stable de genre g, alors $c_1^2(X)$ et $c_2(X)$ s'expriment simplement en fonction de g, q et des entiers $\deg f_*\omega_{X/B}$ et $(\omega_{X/B}.\omega_{X/B})$ (définis au moyen de la théorie classique de l'intersection). Explicitement, il vient d'après [7] (1.2.1 – 1.2.2) et les formules de Riemann-Roch et de Noether:

$$c_1^2(X) = (\omega_{X/B}.\omega_{X/B}) + 2(2g-2)(2q-2)$$
$$c_2(X) = 12\deg f_*\omega_{X/B} - (\omega_{X/B}.\omega_{X/B}) + (2g-2)(2q-2).$$

En géométrie arithmétique, l'auto-intersection $(\omega_{X/B}.\omega_{X/B})$ est, de loin, le plus difficile à évaluer des deux nombres réels $\deg f_*\omega_{X/B}$ et $(\omega_{X/B}.\omega_{X/B})$. Pour le calculer, lorsque X est de genre 2, nous procédons en deux étapes:

- Au §1, nous exprimons $(\omega_{X/B}.\omega_{X/B})$ au moyen de l'intersection d'Arakelov $(P.Q)$ de deux points de Weierstrass P et Q de X.

- Au §2, nous évaluons la "composante archimédienne" de $(P.Q)$: si σ est un plongement archimédien de K et si X_σ désigne la surface de Riemann $X \otimes_\sigma \mathbf{C}$, la valeur $G_\sigma(P,Q)$ de la fonction de Green-Arakelov de X_σ peut s'exprimer au moyen des valeurs en des points de 2-torsion de la fonction de Néron $\|\theta\|$ sur la jacobienne $\operatorname{Pic} X_\sigma$ et de l'intégrale sur $\operatorname{Pic} X_\sigma$ de $\log \|\theta\|$ (*cf.* [2]).

Indiquons que l'on aurait pu calculer l'invariant $(\omega_{X/B}.\omega_{X/B})$ en utilisant la formule pour l'invariant δ de Faltings donnée dans [2] et la formule de Noether pour une surface arithmétique (*cf.* [5]) sous la forme précisée figurant dans [8]. La méthode suivie dans cet article évite de recourir à ce dernier résultat.

Dans les §3 et §4, nous effectuons le calcul numérique de $\deg f_*\omega_{X/B}$ et $(\omega_{X/B}.\omega_{X/B})$ dans des cas particuliers explicites. Nous considérons ainsi la courbe sur $\mathbf{Q}$, lisse, admettant comme modèle plan

$$y^2 = x(x-1)(4x^3 + 13x^2 - 17x + 4).$$

Cette courbe a réduction semi-stable sur $\mathbf{Q}$ et a bonne réduction en dehors de 21737. Son modèle stable $X \to B = \operatorname{Spec} \mathbf{Z}$ est régulier, de fibre en 21737 une courbe nodale irréductible possédant un unique point singulier. On trouve:

$$\deg f_*\omega_{X/B} = -1{,}466599\ldots, \quad (\omega_{X/B}.\omega_{X/B}) = 2{,}32\ldots.$$

Nous considérons ensuite la courbe sur $\mathbf{Q}$, lisse, admettant comme modèle

$$y^2 + y = x^5.$$

Cette courbe, dont la jacobienne est à multiplications complexes par $\mathbf{Z}[\zeta_5]$, où ζ_5 désigne une racine primitive cinquième de 1, a bonne réduction potentielle partout. Sur l'anneau des entiers B' du corps $K' = \mathbf{Q}(\sqrt{1-\zeta_5}, \sqrt[5]{2})$, elle admet un modèle X' ayant bonne réduction partout. Le calcul donne:

$$\begin{aligned}
\frac{1}{[K':\mathbf{Q}]}\deg f_*\omega_{X'/B'} &= \log 4\pi - \frac{1}{2}\log \Gamma(1/5)^5\Gamma(2/5)^3\Gamma(3/5)\Gamma(4/5)^{-1} \\
&= -2{,}597239125\ldots \\
\frac{1}{[K':\mathbf{Q}]}(\omega_{X'/B'}.\omega_{X'/B'}) &= 0{,}2162\ldots.
\end{aligned}$$

Au moyen de ces valeurs, on vérifie que X' fournit un contre-exemple à certaines conjectures sur les "classes de Chern" des surfaces arithmétiques, du moins dans leur version la plus naïve (*cf.* §4.5). Le lecteur pourra d'ailleurs constater qu'il en est de même de l'exemple précédent.

Signalons que les invariants des surfaces arithmétiques $\deg f_*\omega_{X/B}$ et $\deg \langle\omega_{X/B}, \omega_{X/B}\rangle$ considérés dans cet exposé sont en fait des invariants de courbes sur $\overline{\mathbf{Q}}$. Plus précisément, pour toute courbe C lisse, irréductible et complète sur $\overline{\mathbf{Q}}$, de genre ≥ 1, on peut trouver un corps de nombres K

sur lequel C est définie et a réduction semi-stable. Considérons alors un modèle semi-stable $X \to B$ de C sur l'anneau des entiers de K et posons

$$e(X) = [K : \mathbf{Q}]^{-1} \deg \langle \omega_{X/B}, \omega_{X/B} \rangle.$$

On peut montrer que le nombre réel $e(X)$ est indépendant du choix du corps K et du modèle X ([7], §5.4). Il en va de même du quotient

$$h(X) = [K : \mathbf{Q}]^{-1} \deg f_* \omega_{X/B},$$

qui n'est autre que la hauteur géométrique (ou hauteur de Faltings stable) de la jacobienne de X.

Nous utilisons dans cet exposé les définitions et notations introduites dans [9], auquel nous renvoyons pour tout ce qui concerne la géométrie d'Arakelov sur les surfaces arithmétiques. En fait, nous ne faisons appel qu'à la théorie de l'intersection d'Arakelov (*cf.* [1] et [5], §2) dans la version que permet d'en donner l'accouplement de Deligne (*cf.* [9] et [4]).

Précisons que, si M est une surface de Riemann compacte de genre $g \geq 1$, nous munissons $\mathcal{O}_{M \times M}(\Delta_M)$ de la métrique bipermise normalisée comme en [9], (4.11.4.2), condition 4 — c'est-à-dire de la métrique définie par la fonction de Green-Arakelov sur $M \times M$ — et ω_M de la métrique qui s'en déduit (*cf.* [9], §4.11.3). Les "crochets de Deligne" considérés plus loin seront munis des métriques déduites de ces dernières. En outre, nous munissons $H^0(M, \omega_M)$ du produit scalaire $(.\mid.)$ défini par

$$(\alpha \mid \beta) = \frac{i}{2} \int_M \alpha \wedge \overline{\beta}, \tag{1}$$

et $\Lambda^g H^0(M, \omega_M)$ de la métrique $\|.\|$ qui s'en déduit:

$$\|\alpha_1 \wedge \ldots \wedge \alpha_g\|^2 = \det((\alpha_k \mid \alpha_l))_{1 \leq k,l \leq g} \tag{2}$$

(*cf.* [9], §4.12). Ce dernier choix de métrique intervient pour définir $\deg f_* \omega_{X/B}$. Il est malheureusement quelque peu arbitraire. La métrique $\|.\|'$ définie par

$$\|\alpha_1 \wedge \ldots \wedge \alpha_g\|'^2 = \det \left(\frac{i}{2\pi} \int_M \alpha_k \wedge \overline{\alpha_l} \right)_{1 \leq k,l \leq g}$$

est peut-être plus naturelle. Nous noterons $\deg' f_* \omega_{X/B}$ le degré d'Arakelov de $f_* \omega_{X/B}$ calculé en munissant $\Lambda^g f_* \omega_{X/B}$ de cette métrique aux places archimédiennes. Il vient

$$\deg' f_* \omega_{X/B} = \deg f_* \omega_{X/B} + \frac{g}{2} [K : \mathbf{Q}] \log \pi$$

et

$$h'(X) := [K : \mathbf{Q}]^{-1} deg' f_* \omega_{X/B} = h(X) + \frac{g}{2} \log \pi.$$

1. Faisceau canonique et points de Weierstrass des courbes de genre 2

1.1. Calcul du faisceau canonique

Dans ce paragraphe et le suivant, on se donne un schéma B et une B-courbe $f : X \to B$ projective lisse à fibres géométriquement connexes de genre 2.

Le $\mathcal{O}_B$-module $f_*\omega_{X/B}$ est localement libre de rang 2 et le morphisme "canonique"

$$\pi : X \longrightarrow \Gamma := \mathbf{P}(f_*\omega_{X/B})$$

est un revêtement double (génériquement séparable dans chaque fibre) de Γ, qui est une B-courbe localement isomorphe à $\mathbf{P}^1_B$ pour la topologie de Zariski sur B. Par définition de π, on a un isomorphisme canonique

$$\omega_{X/B} \xrightarrow{\sim} \pi^*\mathcal{O}_\Gamma(1). \tag{3}$$

On note σ l'involution hyperelliptique de X, *i.e.* l'involution associée à π.

Si L et M sont deux faisceaux inversibles sur X, on note $\langle L, M\rangle$ l'accouplement de Deligne de L et M: c'est un faisceau inversible sur B, défini à isomorphisme unique près. Si D est un diviseur de Cartier sur X, on notera $\langle D, M\rangle$ pour $\langle \mathcal{O}_X(D), M\rangle$.

Soit $P : B \to X$ une section de f: l'image de P est un diviseur relatif dans X, également noté P. Ainsi, si M est un faisceau inversible sur X, on a (par définition de $\langle\ ,\ \rangle$) un isomorphisme canonique $P^*M \xrightarrow{\sim} \langle P, M\rangle$.

Le diviseur $P + \sigma P$ est image réciproque par π du diviseur $\pi(P)$ sur Γ. Ce dernier est l'image d'une section de Γ sur B, de sorte que $\mathcal{O}_\Gamma(\pi(P))(-1)$ provient de B. Compte tenu de (3), on en déduit que $\omega_{X/B} \otimes \mathcal{O}_X(-P - \sigma P)$ est de la forme f^*L, où L est un faisceau sur B. On calcule L par restriction à la section P; on obtient ainsi

$$L = \langle P, \omega_{X/B}\rangle \otimes \langle P, -P - \sigma P\rangle.$$

La formule d'adjonction

$$\langle P, P\rangle \xrightarrow{\sim} \langle -P, \omega_{X/B}\rangle$$

donne alors

$$L = \langle P, -2P - \sigma P\rangle.$$

On dispose ainsi d'un isomorphisme canonique

$$\omega_{X/B} \xrightarrow{\sim} \mathcal{O}_X(P + \sigma P) \otimes f^*\langle P, -2P - \sigma P\rangle. \tag{4}$$

Le cas qui nous intéresse est celui où P est un point de Weierstrass de X, c'est-à-dire où $P = \sigma P$:

PROPOSITION 1 – *Pour toute section P σ-invariante de f, il existe un unique isomorphisme*

$$\omega_{X/B} \xrightarrow{\sim} \mathcal{O}_X(2P) \otimes f^*\langle P, P\rangle^{\otimes -3} \tag{5}$$

induisant par restriction à la section P l'isomorphisme d'adjonction

$$\langle P, \omega_{X/B}\rangle \xrightarrow{\sim} \langle P, P\rangle^{\otimes -1}.$$

De plus, lorsque $B = \operatorname{Spec} \mathbf{C}$, l'isomorphisme (5) *est une isométrie lorsque l'on munit les deux membres de leurs métriques hermitiennes canoniques d'Arakelov-Faltings.*

Démonstration. L'existence d'un isomorphisme (5) résulte des calculs qui précèdent; il est clair qu'on peut, en multipliant par une section de $\mathcal{O}_B^\times$, imposer la condition d'adjonction qui détermine alors (5) de manière unique. Enfin, si $B = \operatorname{Spec}\mathbf{C}$, l'isomorphisme (5) multiplie les métriques d'Arakelov par une constante, car ces métriques sont admissibles et ont donc même courbure. Comme l'isomorphisme d'adjonction est une isométrie, (5) est une isométrie au point P, donc partout. ∎

1.2. Auto-intersection du faisceau canonique

Conservons les notations du paragraphe précédent, et considérons deux sections σ-invariantes P et Q de f. Outre l'isomorphisme (5), on a aussi

$$\omega_{X/B} \xrightarrow{\sim} \mathcal{O}_X(2Q) \otimes f^*\langle Q, Q\rangle^{\otimes -3}. \tag{6}$$

On peut alors calculer $\langle \omega_{X/B}, \omega_{X/B}\rangle$ en utilisant respectivement (5) et (6) pour chacun des arguments, ce qui donne

$$\langle \omega_{X/B}, \omega_{X/B}\rangle \xrightarrow{\sim} \langle P, Q\rangle^{\otimes 4} \otimes \langle P, P\rangle^{\otimes -6} \otimes \langle Q, Q\rangle^{\otimes -6}. \tag{7}$$

Pour se débarrasser des auto-intersections au second membre, on remarque que le faisceau $\mathcal{O}_X(2P-2Q)$ provient d'un faisceau sur B, comme il résulte par exemple de (5) et (6). Donc $\langle 2P-2Q, P-Q\rangle$ est canoniquement trivial, ce qui donne

$$\langle P, Q\rangle^{\otimes 4} \xrightarrow{\sim} \langle P, P\rangle^{\otimes 2} \otimes \langle Q, Q\rangle^{\otimes 2}. \tag{8}$$

On obtient ainsi, en reportant dans (7):

PROPOSITION 2 – *Pour tout couple (P, Q) de sections σ-invariantes de f, il existe un isomorphisme canonique de faisceaux inversibles sur B*

$$\langle \omega_{X/B}, \omega_{X/B}\rangle \xrightarrow{\sim} \langle P, Q\rangle^{\otimes -8}. \tag{9}$$

De plus, lorsque $B = \mathrm{Spec}\,\mathbf{C}$, *l'isomorphisme ci-dessus est une isométrie lorsque l'on munit les deux membres de leurs normes hermitiennes canoniques.*

Démonstration. L'assertion sur les normes découle du fait que les isomorphismes (5), (6), (8) sont des isométries: cela résulte de la proposition 1 et, pour (8), du fait que la métrique d'Arakelov sur $\mathcal{O}_X(2P - 2Q)$ devient une métrique constante lorsque l'on trivialise $\mathcal{O}_X(2P - 2Q)$ (puisque (5) et (6) sont des isométries) et que, par conséquent, la métrique sur $\langle 2P - 2Q, P - Q\rangle$, canoniquement trivialisé, est la métrique triviale. ∎

1.3. Extension aux courbes singulières

On considère maintenant une B-courbe $f : X \to B$ projective et plate, à fibres géométriquement connexes de genre arithmétique 2 et de Gorenstein. Ainsi, l'on dispose encore d'un faisceau dualisant $\omega_{X/B}$ qui est un $\mathcal{O}_X$-module inversible. On suppose de plus que f est lisse au-dessus d'un ouvert schématiquement dense U de B.

Soit P une section de f contenue dans l'ouvert de lissité de X sur B (de sorte que son image est un diviseur de Cartier dans X), et telle que $P_{|U}$ soit invariante par l'involution canonique de X_U. La proposition 1, appliquée au-dessus de U, affirme l'existence d'une section partout non nulle sur U du faisceau $\omega_{X/B} \otimes \mathcal{O}_X(-2P) \otimes f^*\langle P, P\rangle^{\otimes 3}$ laquelle, d'après nos hypothèses, peut être vue comme une section méromorphe s_P de ce faisceau sur X. Notons V_P le diviseur de s_P. Son support est disjoint de X_U, et l'on dispose d'un isomorphisme canonique

$$\omega_{X/B} \xrightarrow{\sim} \mathcal{O}_X(2P) \otimes f^*\langle P, P\rangle^{\otimes -3} \otimes \mathcal{O}_X(V_P). \tag{10}$$

PROPOSITION 3 – *Conservons les hypothèses et les notations des deux derniers alinéas.*

i) La restriction du diviseur V_P *à la section* P *est le diviseur nul; en particulier le faisceau* $\langle P, V_P\rangle$ *est trivial.*

ii) Si B *est normal, ou si* X *est une* B*-courbe stable, alors le support de* V_P *est disjoint de* P.

iii) Si X *est normal ou est une* B*-courbe stable, et si de plus les fibres de* f *sont* irréductibles, *alors* $V_P = 0$.

Démonstration. i) Si l'on restreint s_P à la section P, on trouve une section méromorphe de $\langle P, \omega_{X/B}\rangle \otimes \langle P, P\rangle$ prolongeant la trivialisation sur U donnée par la formule d'adjonction. Or celle-ci se prolonge en une trivialisation sur B puisque f est lisse au voisinage de P, d'où l'assertion.

ii) Si B est normal, on le remplace par son localisé en un point maximal du fermé $P^{-1}(\mathrm{Supp}\, V_P)$, et X par son localisé au point correspondant de P. Alors B est de dimension 1 (le point fermé est support d'un diviseur de Cartier) et X est lisse sur B donc V_P est simplement un multiple de la fibre fermée. La conclusion résulte alors de i).

Le cas stable se déduit du précédent par réduction au cas "universel" où B est le champ des courbes stables de genre 2 (qui est lisse sur $\mathbf{Z}$ donc normal).

iii) résulte de ii) dans le cas normal: le support de V_P est de codimension 1 et disjoint de X_U donc est image réciproque d'un fermé de B, et ii) s'applique car B est automatiquement normal, X étant lisse sur B au voisinage de P. Le cas stable s'en déduit comme ci-dessus, la courbe stable de genre 2 universelle étant lisse sur $\mathbf{Z}$. ∎

PROPOSITION 4 – *On conserve les hypothèses de la proposition précédente, et on considère une section Q de f satisfaisant aux mêmes hypothèses que P. L'isomorphisme* (9) *sur U se prolonge en un isomorphisme*

$$\langle \omega_{X/B}, \omega_{X/B} \rangle \xrightarrow{\sim} \langle P, Q \rangle^{\otimes -8} \otimes \langle P, V_Q \rangle^{\otimes -1} \otimes \langle Q, V_P \rangle^{\otimes -1} \otimes \langle V_P, V_Q \rangle. \quad (11)$$

Démonstration. Il suffit de reprendre les calculs de 1.2. en utilisant (10). Les termes $\langle P, V_P \rangle$ et $\langle Q, V_Q \rangle$ disparaissent en vertu de la proposition 3 i), et l'on remarque que le faisceau $\mathcal{O}_X(2P - 2Q + V_P - V_Q)$ provient de la base, de sorte que son intersection avec $P - Q$ est triviale. ∎

Résumons les résultats obtenus dans les trois derniers paragraphes:

THÉORÈME 1 – *Soient B un schéma, et $f : X \to B$ une B-courbe projective et plate, à fibres géométriquement connexes de genre arithmétique* 2 *et de Gorenstein, tel que f soit lisse au-dessus d'un ouvert schématiquement dense U de B.*

Soient P et Q deux sections de f contenues dans l'ouvert de lissité de f, tels que $P_{|U}$ et $Q_{|U}$ soient invariantes par l'involution hyperelliptique de X_U.

Supposons X normal ou B-stable, et les fibres de f irréductibles.

1) On dispose d'un isomorphisme canonique

$$\langle \omega_{X/B}, \omega_{X/B} \rangle \xrightarrow{\sim} \langle P, Q \rangle^{\otimes -8}. \quad (12)$$

2) Supposons de plus que B soit le spectre de l'anneau des entiers d'un corps de nombres et notons (.) l'intersection d'Arakelov sur X. Alors on a l'égalité numérique

$$(\omega_{X/B} \cdot \omega_{X/B}) = -8(P.Q). \quad (13)$$

Démonstration. 1) résulte de (11) et de la proposition 3, iii), et 2) de ce que l'isomorphisme (12) est une isométrie aux places archimédiennes d'après la proposition 1. ∎

2. La fonction de Green-Arakelov d'une surface de Riemann de genre 2

2.1. Rappels sur la fonction $\|\theta\|$ et la fonction G

Rappelons quelques formules données dans [5].

Soit X une surface de Riemann compacte et connexe de genre $g > 0$.

La courbe X s'identifie à une sous-variété complexe de $\mathrm{Pic}^1 X$ grâce au plongement jacobien $j \ : \ X \longrightarrow \mathrm{Pic}^1 X$, qui associe à un point x de X la classe du fibré $\mathcal{O}(x)$ dans $\mathrm{Pic}\, X$. On désigne par Θ le sous-ensemble analytique de $\mathrm{Pic}^{g-1} X$, de codimension 1, constitué des sommes de $g-1$ éléments de X.

Soit $(\alpha_1, ..., \alpha_g)$ une base orthonormée de $H^0(X, \omega_X)$, muni du produit scalaire défini par la formule (1) (avec $M = X$). Notons α'_k l'unique forme différentielle de type $(1,0)$ sur $\mathrm{Pic}\, X$ invariante par translation et telle que $\alpha_k = j^* \alpha'_k$ et posons :

$$\nu = \frac{i}{2g} \sum_{k=1}^{g} \alpha_k \wedge \overline{\alpha}_k$$

$$\mu = \frac{i}{2} \sum_{k=1}^{g} \alpha'_k \wedge \overline{\alpha}'_k.$$

Ce sont des formes différentielles positives sur X et $\mathrm{Pic}\, X$, respectivement, indépendantes du choix de la base $(\alpha_1, ..., \alpha_g)$. On a :

$$\int_X \nu = 1 \quad \text{et} \quad \nu = \frac{1}{g} j^* \mu. \tag{14}$$

La $2g$-forme $\frac{1}{g!}\, \mu^g$ définit une mesure de Haar sur $\mathrm{Pic}\, X$, pour laquelle chacune des composantes $\mathrm{Pic}^k X$ de $\mathrm{Pic}\, X$ est de mesure 1.

Le fibré en droites $\mathcal{O}(\Theta)$ sur Pic^{g-1} possède une unique métrique $\| \,.\, \|_{\mathcal{O}(\Theta)}$ telle que :

1. la forme de courbure de $\mathcal{O}(\Theta)$ muni de cette métrique soit $-2\pi i \mu$;
2. si l'on pose $\| \, \theta \, \| = \| \, \mathbf{1} \, \|_{\mathcal{O}(\Theta)}$, où $\mathbf{1}$ désigne la section canonique, de diviseur Θ, du fibré $\mathcal{O}(\Theta)$, alors :

$$\int_{\mathrm{Pic}^{g-1} X} \| \, \theta \, \|^2 \, \frac{1}{g!} \, \mu^g = 2^{-g/2}.$$

Si Z est une matrice dans le demi-espace de Siegel $\mathcal{H}_g$, on pose pour tout $z \in \mathbf{C}^g$:

$$\theta(z;Z) = \sum_{n\in\mathbf{Z}^g} \exp(\pi i\, {}^t n.Z.n \, + \, 2\pi i\, {}^t n.z)$$
$$\|\theta\|_0(z;Z) = (\det Y)^{\frac{1}{4}} \exp(-\pi \; {}^t y.Y^{-1}.y) \mid \theta(z;Z) \mid,$$

où Y (resp. y) désigne la partie imaginaire de Z (resp. z).

On pose aussi, pour tout $(a,b) \in \mathbf{R}^g \times \mathbf{R}^g$:

$$\theta[{a \atop b}](0;Z) = \exp(\pi i\, {}^t a.Z.a \, + \, 2\pi i\, {}^t a.b)\theta(Za+b;Z).$$

Supposons maintenant le groupe $H_1(X,\mathbf{Z})$ muni d'une base symplectique, c'est-à-dire d'une base $\mathcal{B} = (a_1,...,a_g,b_1,...,b_g)$ telle que

$$a_i.a_j = 0, \quad b_i.b_j = 0, \quad a_i.b_j = \delta_{ij}.$$

Notons $(\omega_1,...,\omega_g)$ la base "canonique" de $H^0(X,\omega_X)$ et $\Omega = (\Omega_{ij})_{1\leq i,j\leq g}$ la matrice des périodes associées à $\mathcal{B}$. Elles sont définies par les relations :

$$\int_{a_i} \omega_j = \delta_{ij} \quad \text{et} \quad \int_{b_i} \omega_j = \Omega_{ij} \quad (1 \leq i,j \leq g).$$

La variété abélienne $\operatorname{Pic}^0 X$ s'identifie alors à $\mathbf{C}^g/\mathbf{Z}^g + \Omega\mathbf{Z}^g$. Compte tenu de cette identification, on a l'égalité de formes différentielles sur $\operatorname{Pic}^0 X$:

$$\mu = \frac{i}{2} \sum_{k,l=1}^{g} (Y^{-1})_{kl}\, dz_k \wedge d\bar{z}_l,$$

où Y désigne la partie imaginaire de Ω. Le diviseur des zéros de $\theta(.;\Omega)$ est $\mathbf{Z}^g + \Omega\mathbf{Z}^g$-périodique et définit donc un diviseur Θ_0 de $\operatorname{Pic}^0 X$. Il existe un unique élément $\Delta_{\mathcal{B}}$ de $\operatorname{Pic}^{g-1} X$ tel que $\Theta = \Theta_0 + \Delta_{\mathcal{B}}$, et l'on a pour tout $z \in \mathbf{C}^g$:

$$\| \theta \|([z] + \Delta_{\mathcal{B}}) = \|\theta\|_0(z;\Omega).$$

De plus, $2\Delta_{\mathcal{B}}$ est la classe de ω_X dans $\operatorname{Pic}^{2g-2} X$.

Rappelons aussi que la fonction de Green-Arakelov de X est l'unique fonction

$$G \; : \; X \times X \longrightarrow \mathbf{R}_+$$

non nulle en dehors de la diagonale telle que pour tout $x \in X$, $\log G(x,.)$ soit une fonction intégrable sur X et vérifie les conditions :

$$\int_X \log G(x,y)\, \nu(y) = 0 \tag{15}$$

$$d'\, d'' \log G(x,.) = \pi\, i(\nu - \delta_x), \tag{16}$$

où δ_x désigne la masse de Dirac en x.

Enfin, nous notons $\|.\|_A$ la métrique d'Arakelov sur ω_X. Sa 2-forme de courbure est égale à $-2\pi i\,(2g-2)\nu$.

2.2. Les invariants $\|\Delta_2\|(X)$ et $\|H\|(X)$ et la fonction $\|J\|$

Nous supposons dorénavant que le genre de X est égal à 2. La courbe X est donc hyperelliptique. Nous noterons σ l'involution hyperelliptique et $\mathcal{W}$ l'ensemble des six points de Weierstrass de X, c'est-à-dire des points fixes de σ (*cf.* §1.1).

La courbe X s'identifie au diviseur Θ par le plongement jacobien j. Nous pratiquons désormais cette identification. Nous considérons ainsi les points de X comme des éléments de $\operatorname{Pic}^1 X$.

Notons K la classe d'isomorphisme de ω_X dans $\operatorname{Pic}^2 X$. L'involution $t \mapsto K - t$ de $\operatorname{Pic}^1 X$ laisse invariants $\|\theta\|$, μ et Θ; sa restriction à Θ, identifié à X, coïncide avec σ. En particulier, pour tout point $W \in \mathcal{W}$, on a $2W = K$. De plus, $\sum_{W \in \mathcal{W}} W = 3K$.

Il est assez facile d'exprimer *à une constante additive près* la fonction $\log G$ au moyen de la fonction $\log \|\theta\|$ (*cf. infra*, identités (34) à (37)). La constante additive en question est déterminée par la condition (15) et son calcul exige donc *a priori* l'évaluation de l'intégrale sur X de $\log \|\theta\|$ composé avec le plongement jacobien, convenablement translaté. Heureusement, il est possible d'exprimer une telle intégrale au moyen de certaines valeurs de $\log \|\theta\|$ et de l'intégrale de $\log \|\theta\|$ sur $\operatorname{Pic}^1 X$. Cela permet de calculer $G(P,Q)$, lorsque $P, Q \in \mathcal{W}$, directement à partir d'une matrice des périodes de X, sans faire intervenir le plongement jacobien de X.

Il est commode, pour ce calcul, d'introduire deux invariants $\|\Delta_2\|(X)$ et $\|H\|(X)$ attachés à la courbe X, ainsi qu'une fonction $\|J\|$ sur $X \times X$ (*cf.* [2]).

Nous posons, pour toute matrice Z dans le demi-espace de Siegel $\mathcal{H}_2$:

$$\Delta_2(Z) = 2^{-12} \prod_{(a,b)\in\mathcal{P}} \theta[\begin{smallmatrix} a \\ b \end{smallmatrix}]\,(0; Z)^2,$$

où $\mathcal{P}$ désigne un ensemble de représentants, modulo $\mathbf{Z}^2 \times \mathbf{Z}^2$, des couples $(a, b) \in (\frac{1}{2}\mathbf{Z})^2 \times (\frac{1}{2}\mathbf{Z})^2$ tels que $4\,{}^t a.b$ soit pair. Comme fonction de Z, Δ_2 est une forme $\mathrm{Sp}_4(\mathbf{Z})$-modulaire, de poids 10 et non nulle sur le complémentaire de l'orbite sous $\mathrm{Sp}_4(\mathbf{Z})$ des matrices diagonales dans $\mathcal{H}_2$. Nous définissons alors une fonction $\|\Delta_2\|$ sur $\mathcal{H}_2$, invariante sous $\mathrm{Sp}_4(\mathbf{Z})$, en posant :

$$\| \Delta_2 \|(Z) = (\det \operatorname{Im} Z)^5 \mid \Delta_2(Z) \mid .$$

Soit Ω la matrice des périodes de X associée à une base symplectique $\mathcal{B}$ de $H_1(X, \mathbf{Z})$. Le nombre réel strictement positif $\|\Delta_2\|(\Omega)$ ne dépend que de X; nous le noterons $\|\Delta_2\|(X)$. Soit $\mathbf{P}$ l'ensemble des 10 points P de $\operatorname{Pic}^1 X \setminus \Theta$ tels que $2P = K$; c'est aussi l'ensemble des points de $\operatorname{Pic}^1 X$ de la forme $P+Q+R-K$, où P, Q et R sont trois points de Weierstrass de X distincts. Il vient :

$$\| \Delta_2 \|(X) = 2^{-12} \prod_{M \in \mathbf{P}} \| \theta \|^2(M).$$

Par ailleurs, nous posons

$$\log \|H\|(X) = \int_{\mathrm{Pic}^1 X} \log \|\theta\| \frac{\mu^2}{2}.$$

Nous posons, pour tout $(z, z') \in \mathbf{C}^2 \times \mathbf{C}^2$:

$$J(z,z') = \begin{vmatrix} \frac{\partial \theta}{\partial z_1}(z,\Omega) & \frac{\partial \theta}{\partial z_1}(z',\Omega) \\ \frac{\partial \theta}{\partial z_2}(z,\Omega) & \frac{\partial \theta}{\partial z_2}(z',\Omega) \end{vmatrix}.$$

Nous définissons alors une fonction $\|J\|$ sur $X \times X$, indépendante du choix de $\mathcal{B}$, en posant pour tout couple $(x, x') \in X \times X$:

$$\|J\|(x,x') = (\det Y) \exp[-\pi\, {}^t y.Y^{-1}.y - \pi\, {}^t y'.Y^{-1}.y'] \, |J(z,z')|,$$

où z (resp. z') désigne un point de $\mathbf{C}^2$ tel que $x - \Delta = [z]$ (resp. $x' - \Delta = [z']$) dans $\mathrm{Pic}^0(X) = \mathbf{C}^2/\mathbf{Z}^2 + \Omega\mathbf{Z}^2$, et où y (resp. y') désigne la partie imaginaire de z (resp. z').

Pour tout couple (P, Q) de points de Weierstrass de X distincts, on dispose de la relation de Rosenhain (*cf.* [14], p. 433):

$$\|J\|(P,Q) = \pi^2 \prod_{W \in \mathcal{W} \setminus \{P,Q\}} \|\theta\|(P+Q+W-K). \tag{17}$$

2.3. Fonction de Green et points de Weierstrass

Pour évaluer les termes archimédiens dans l'intersection d'Arakelov de deux points de Weierstrass d'une surface arithmétique de genre 2, nous ferons appel au théorème suivant:

THÉORÈME 2 (*cf.* [2])- *Pour tout couple (P,Q) de points de Weierstrass de X distincts, on a*

$$G(P,Q)^2 = (2\pi)^{-2} \, \|\Delta_2\|(X)^{-1/4} \, \|H\|(X) \, \|J\|(P,Q).$$

En posant, pour tout $M \in \mathbf{P}$, $\varepsilon_{PQ}(M) = 1$ si M est de la forme $P + Q + W - K$ avec $W \in \mathcal{W} \setminus \{P,Q\}$, et $\varepsilon_{PQ}(M) = -1$ sinon, on peut réécrire cette formule comme suit:

$$G(P,Q)^4 = 4 \prod_{M \in \mathbf{P}} \|\theta\|(M)^{\varepsilon_{PQ}(M)} \, \|H\|(X)^2.$$

On en déduit:

COROLLAIRE – *Pour tout point de Weierstrass P de X, on a*

$$\prod_{Q\in\mathcal{W}\setminus\{P\}} G(P,Q)^2 = 4\|\Delta_2\|(X)^{-1/4}\|H\|(X)^5.$$

La démonstration du théorème 2 figure en appendice, à la fin de l'article.

3. Une famille de courbes de genre 2

3.1. La courbe C_F d'équation $y^2 + y = F(x)/x(x-1)$.

Dans ce paragraphe et les suivants, on considère un polynôme unitaire de degré 3

$$F(X) = X^3 + aX^2 + bX + c$$

à coefficients dans un anneau intègre A, tel que $F(0)$ et $F(1)$ soient *inversibles* dans A. On s'intéressera notamment au cas *universel* où a, b, c sont des indéterminées et où A est l'anneau $\mathbf{Z}[a, b, c, c^{-1}, (1+a+b+c)^{-1}]$.

Posons $B = \operatorname{Spec} A$ et notons $\bar{F}$ l'homogénéisé de F:

$$\bar{F}(X,T) = T^3F(X/T).$$

Vu l'hypothèse sur F, la fonction rationnelle $F(x)/x(x-1)$ sur $\mathbf{P}^1_B$ détermine un B-morphisme

$$\begin{array}{rcl} \beta : \mathbf{P}^1_B & \longrightarrow & \mathbf{P}^1_B \\ (X:T) & \longmapsto & (\bar{F}(X,T) : XT(X-T)). \end{array}$$

De même la fonction $y^2 + y$ détermine un B-morphisme

$$\begin{array}{rcl} \alpha : \mathbf{P}^1_B & \longrightarrow & \mathbf{P}^1_B \\ (Y:Z) & \longmapsto & (Y^2 + YZ : Z^2) \end{array}$$

(par convention on identifie $\lambda \in \mathbf{A}^1$ à $(\lambda : 1) \in \mathbf{P}^1$, et on pose $\infty = (1:0)$). On définit alors la courbe C_F "d'équation $y^2+y = F(x)/x(x-1)$" comme le B-schéma produit fibré au-dessus de $\mathbf{P}^1_B$ de $\alpha :\ \mathbf{P}^1_B \to \mathbf{P}^1_B$ et $\beta :\ \mathbf{P}^1_B \to \mathbf{P}^1_B$. On dispose ainsi d'un diagramme cartésien

$$\begin{array}{ccc} C_F & \xrightarrow{\beta'} & \mathbf{P}^1_B \\ \pi \downarrow & & \downarrow \alpha \\ \mathbf{P}^1_B & \xrightarrow{\beta} & \mathbf{P}^1_B. \end{array}$$

PROPOSITION 5 –

i) Le morphisme structural $f : C_F \to B$ est plat et localement d'intersection complète; ses fibres géométriques sont intègres, de genre arithmétique 2 et ont au plus un point singulier.

ii) Le morphisme f admet trois sections W_0, W_1 et W_∞, contenues dans le lieu de lissité de f et se projetant respectivement par π sur les sections 0, 1, ∞ de $\mathbf{P}^1_B$ et par β' sur la section ∞ de $\mathbf{P}^1_B$; le revêtement double π est ramifié le long de W_0, W_1 et W_∞, tandis que β' y est étale.

iii) Si $2 = 0$ dans l'anneau A, π est étale hors de W_0, W_1 et W_∞, et C est lisse sur B.

iv) Supposons que A soit un corps de caractéristique $\neq 2$. Notons $R(X)$ le polynôme (de degré 3) $X(X-1)+4F(X)$ et désignons par C'_F la courbe dans $(\mathbf{P}^1 \times \mathbf{P}^1)_B$ d'équation affine

$$z^2 = \frac{R(x)}{x(x-1)}.$$

On dispose d'un diagramme commutatif, dont la première ligne est un isomorphisme:

$$\begin{array}{ccc} C_F & \xrightarrow[\sim]{\iota} & C'_F \\ \pi \downarrow & & \downarrow \pi' \\ \mathbf{P}^1_B & = & \mathbf{P}^1_B \end{array}$$

où π' et ι sont donnés en coordonnées affines par

$$\pi'(x,z) = x \quad \text{et} \quad \iota(x,y) = (x, 2y+1).$$

Par conséquent, π est ramifié exactement aux points 0, 1, ∞ et au-dessus des zéros de R. De plus, un point de C est singulier (resp. singulier ordinaire) si et seulement si son image par β dans $\mathbf{P}^1_B$ est à distance finie et est racine multiple (resp. double) de $R(x)$. En particulier, la courbe C_F admet au plus un point singulier.

Démonstration. Par définition, C_F est définie dans $(\mathbf{P}^1 \times \mathbf{P}^1)_B$ par le polynôme bihomogène $Z^2\bar{F}(X,T) - XT(X-T)(Y^2+YZ)$. Ainsi C_F est un diviseur relatif dans $(\mathbf{P}^1 \times \mathbf{P}^1)_B$; il est donc plat et localement d'intersection complète sur B.

Montrons ii). L'existence de W_0, W_1 et W_∞ est immédiate. De plus la réunion (disjointe) de ces trois sections est l'image réciproque par β' de la section à l'infini de $\mathbf{P}^1_B$. Cela implique que β' est étale, et donc que C est lisse sur B, le long de W_0, W_1 et W_∞. Enfin α est ramifié à l'infini, d'où l'assertion sur π.

Si $2 = 0$ dans A, α est étale en-dehors de la section à l'infini de $\mathbf{P}^1_B$. L'assertion sur π dans iii) en résulte par changement de base, ainsi que la lissité de C compte tenu de ii).

Supposons maintenant 2 inversible dans A. Les assertions de iv) sont évidentes. De plus, lorsque A est un corps de caractéristique $\neq 2$, C_F est irréductible: sinon, comme elle est revêtement double de $\mathbf{P}^1_B$, elle serait réunion de deux composantes isomorphes à $\mathbf{P}^1_B$; cela est exclu, compte tenu par exemple de la ramification en W_0.

Reste à établir que les fibres géométriques de C_F sont de genre arithmétique 2. Il suffit pour cela de considérer le cas universel. L'assertion est alors claire au point générique de B et donc toujours vérifiée, puisque B est irréductible et f plat. ∎

REMARQUE. Si A est un corps algébriquement clos de caractéristique $\neq 2$, toute courbe sur A, complète, lisse et de genre 2 est isomorphe à une courbe C_F de la forme ci-dessus, avec R sans racine multiple.

3.2. Calcul[1] de $\langle \omega_{C_F/B}, \omega_{C_F/B} \rangle$

Conservons les notations de 3.1. et plaçons-nous dans le cas universel. Le schéma B est alors lisse sur $\mathbf{Z}$ et de dimension relative 3, de sorte que, d'après la proposition 5 i), C_F est un schéma de Cohen-Macaulay et de dimension 5. D'autre part, il résulte de la proposition 5, iii) et iv), que le lieu singulier relatif de f est fini sur B et se projette sur un fermé strict de B; il est donc de codimension ≥ 2 (égale à 2, en fait) dans C_F. On en conclut (critère de Serre) que C_F est un schéma normal et l'on peut donc appliquer le théorème 1 à $f : C_F \to B$, en prenant pour P et Q deux des sections W_0, W_1, W_∞. On obtient ainsi, pour $i, j \in \{0, 1, \infty\}$, un isomorphisme

$$\langle \omega_{C_F/B}, \omega_{C_F/B} \rangle \xrightarrow{\sim} \langle W_i, W_j \rangle^{\otimes -8}.$$

Si de plus $i \neq j$, alors W_i et W_j sont disjoints donc $\langle W_i, W_j \rangle$ est canoniquement trivialisé; il en est donc de même de $\langle \omega_{C_F/B}, \omega_{C_F/B} \rangle$, cette trivialisation dépendant *a priori* de i et j.

Par changement de base, cela s'étend immédiatement à une base B quelconque; d'où:

[1] Les résultats de cette section ne sont pas utilisés dans la suite de l'article.

PROPOSITION 6 - *Pour* $(i,j) \in \{0,1,\infty\}^2$, *on dispose d'un isomorphisme commutant à tout changement de base*

$$\langle \omega_{C_F/B}, \omega_{C_F/B} \rangle \xrightarrow{\sim} \langle W_i, W_j \rangle^{\otimes -8} \tag{18}$$

qui, lorsque C_F *est lisse sur* B, *coïncide avec l'isomorphisme* (9) *(pour* $X = C_F$, $P = W_i$, $Q = W_j$*). De plus il existe une trivialisation de* $\langle \omega_{C_F/B}, \omega_{C_F/B} \rangle$ *sur* B, *commutant à tout changement de base.* ∎

3.3. Calcul de $f_*\omega_{C_F/B}$

Sous les hypothèses de 3.1. notons x et y les fonctions rationnelles sur C_F définies respectivement par les morphismes π et β' et posons $z = 2y+1$. Supposons d'abord C_F lisse sur B. On laisse au lecteur le soin de vérifier que l'on a alors

$$\begin{aligned} \operatorname{div}(x) &= 2W_0 - 2W_\infty, \\ \operatorname{div}(z) &= \operatorname{div}(R(x)) - W_0 - W_1 + 2W_\infty, \\ \operatorname{div}(dx) &= \operatorname{div}(R(x)) + W_0 + W_1, \end{aligned}$$

de sorte que si l'on pose

$$\begin{aligned} \omega_1 &= \frac{z\,dx}{R(x)} = \frac{dx}{x(x-1)z} \\ \omega_2 &= \frac{xz\,dx}{R(x)} = \frac{dx}{(x-1)z}, \end{aligned} \tag{19}$$

alors le diviseur de ω_1 (resp. ω_2) est $2W_\infty$ (resp. $2W_0$). Ceci implique que (ω_1, ω_2) est une base du $\mathcal{O}_B$-module $f_*\omega_{C_F/B}$.

Sans hypothèse de lissité sur f, il est clair sur les formules (19) que ω_1 et ω_2 sont définies et non nulles au point générique de chaque fibre de f. En particulier, dans le cas universel, leurs diviseurs (lorsqu'elles sont vues comme sections rationnelles du $\mathcal{O}_{C_F}$-module inversible $\omega_{C_F/B}$) sont finis sur B et par suite, puisque C_F est normal, égaux respectivement à $2W_\infty$ et $2W_0$. On en déduit, pour B quelconque (puisque la formation de $f_*\omega_{C_F/B}$ commute à tout changement de base):

PROPOSITION 7 - *Les formes* ω_1 *et* ω_2 *de* (19) *forment une base du* $\mathcal{O}_B$-*module* $f_*\omega_{C_F/B}$.

On retrouve ainsi le fait que $\langle \omega_{C_F/B}, \omega_{C_F/B} \rangle$ est trivial puisque $\omega_{C_F/B}$ admet deux sections globales dont les diviseurs sont disjoints.

3.4. Construction de courbes de genre 2 sur un corps de nombres

Dans ce paragraphe et le suivant, on se donne un corps de nombres K. On note A l'anneau des entiers de K et $B = \operatorname{Spec} A$.

PROPOSITION 8 – *Soit $F \in A[X]$ un polynôme unitaire de degré 3 tel que $F(0)$ et $F(1)$ soient des unités de A et que le discriminant Δ de*

$$R(X) = X(X-1) + 4F(X)$$

soit non nul. La fibre générique $C_{F,K}$ de la B-courbe C_F d'équation $y^2+y = F(x)/x(x-1)$, définie en 3.1, est lisse, géométriquement connexe et de genre 2 sur K. La B-courbe C_F a bonne réduction en caractéristique 2, et mauvaise réduction en une place finie v de K de caractéristique $\neq 2$ si et seulement si $v(\Delta) > 0$. Dans ce cas, la fibre de C_F en v est une courbe intègre de genre géométrique 1 avec un unique point double Σ_v, à savoir le point de coordonnées $(x_0, 0)$, où x_0 est l'unique racine multiple de $R \bmod v$; ce point est ordinaire (resp. cuspidal) si x_0 est une racine double (resp. triple) de $R \bmod v$; lorsque x_0 est racine double de $R \bmod v$, Σ_v est un point régulier de C_F si et seulement si $v(\Delta) = 1$.

Cet énoncé est conséquence directe de la proposition 5, à l'exception de la dernière assertion, qui découle d'un calcul local facile.

On a vu (prop. 5, iv)) que la courbe $C_{F,K}$ admet comme modèle plan

$$z^2 = \frac{R(x)}{x(x-1)}.$$

On en déduit, en posant $t = x(x-1)z$, qu'elle admet aussi le modèle plan

$$t^2 = x(x-1)R(x).$$

La proposition suivante rassemble des conséquences directes des propositions 8, 5, 7, du théorème 1 et des définitions de $\deg f_*\omega_{C_F/B}$ et de l'intersection d'Arakelov.

PROPOSITION 9 – *Reprenons les notations de la proposition précédente, et supposons que, pour toute place finie v de K, les racines de $R \bmod v$ sont de multiplicité ≤ 2. Alors la courbe lisse $C_{F,K}$ sur K de modèle plan*

$$t^2 = x(x-1)R(x) \tag{20}$$

a réduction semi-stable sur K et a bonne réduction en dehors des places finies v de K telles que $v(\Delta) > 0$ et $\operatorname{Car} v \neq 2$. Son modèle stable sur B est C_F.

Les points W_0 *et* W_1 *de* $C_{F,K}$ *d'abscisse* [2] 0 *et* 1*, et le point à l'infini* W_∞ *(dans le modèle* (20)*) définissent des diviseurs disjoints dans* C_F.

Les formes différentielles

$$\omega_1 = \frac{dx}{t} \quad \text{et} \quad \omega_2 = \frac{xdx}{t}$$

forment une base de l'espace des formes différentielles de première espèce sur $C_{F,K}$*, qui est aussi une base du* $\mathcal{O}_B$*-module* $f_*\omega_{C_F/B}$.

Pour tout plongement σ *de* K *dans* $\mathbf{C}$*, notons* C_σ *la surface de Riemann déduite de* $C_{F,K}$ *par* σ *et* G_σ *la fonction de Green-Arakelov de* C_σ*, et posons*

$$A_\sigma = \frac{i}{2}\int_{C_\sigma} \omega_1 \wedge \overline{\omega_1}, \quad B_\sigma = \frac{i}{2}\int_{C_\sigma} \omega_1 \wedge \overline{\omega_2} \quad \text{et} \quad D_\sigma = \frac{i}{2}\int_{C_\sigma} \omega_2 \wedge \overline{\omega_2}.$$

Il vient alors

$$\deg f_*\omega_{C_F/B} = -\frac{1}{2} \sum_{\sigma:\, K \hookrightarrow \mathbf{C}} \log(A_\sigma D_\sigma - \mid B_\sigma \mid^2),$$

et, pour tout $(i,j) \in \{0,1,\infty\}^2$, $i \neq j$,

$$(\omega_{C_F/B} \cdot \omega_{C_F/B}) = 8 \sum_{\sigma: K \hookrightarrow \mathbf{C}} \log G_\sigma(W_i, W_j).$$

REMARQUE. La condition de la proposition précédente sur les multiplicités des racines de $R \bmod v$ est vérifiée dès que $v(\Delta) \leq 1$ pour toute place finie v de K telle que $\mathrm{Car}\, v \neq 2$. Dans ce cas, le modèle stable C_F est régulier.

3.5. Applications numériques

Au moyen de la proposition 9, on peut construire des surfaces arithmétiques $f : C_F \to B$ pour lesquelles le calcul des invariants $\deg f_*\omega_{C_F/B}$ et $(\omega_{C_F/B} \cdot \omega_{C_F/B})$ se ramène à des calculs "aux places infinies".

Pour évaluer numériquement ces invariants, on choisit, pour chaque plongement σ de K dans $\mathbf{C}$, une base symplectique

$$\mathcal{B}_\sigma = (a_{\sigma,1}, a_{\sigma,2}, b_{\sigma,1}, b_{\sigma,2})$$

de $H_1(C_\sigma, \mathbf{Z})$. Puis on calcule les périodes de ω_1 et ω_2 dans cette base. On forme ainsi les matrices

$$\Omega'_\sigma = \left(\int_{a_{\sigma,i}} \omega_j\right)_{1\leq i,j\leq 2} \quad \text{et} \quad \Omega''_\sigma = \left(\int_{b_{\sigma,i}} \omega_j\right)_{1\leq i,j\leq 2}.$$

[2] Par abscisse, nous entendons la coordonnée x.

La matrice des périodes de C_σ associées à $\mathcal{B}_\sigma$ est alors

$$\Omega_\sigma = \Omega''_\sigma \Omega'^{-1}_\sigma.$$

Le calcul de ces périodes peut s'effectuer avec une grande précision, au moyen, par exemple, de l'algorithme quadratiquement convergent de Richelot (du moins lorsque C_σ est définie sur $\mathbf{R}$; *cf.* [13] ou [3]).

Grâce aux relations bilinéaires de Riemann

$$\int_{X_\sigma} \alpha \wedge \beta = \sum_{i=1}^{2} \left[\int_{a_{\sigma,i}} \alpha \cdot \int_{b_{\sigma,i}} \beta - \int_{b_{\sigma,i}} \alpha \cdot \int_{a_{\sigma,i}} \beta \right],$$

on déduit immédiatement des valeurs des matrices Ω'_σ et Ω''_σ celles des produits scalaires A_σ, B_σ et D_σ. On obtient finalement

$$A_\sigma D_\sigma - \mid B_\sigma \mid^2 = \det \operatorname{Im} \Omega_\sigma . \mid \det \Omega'_\sigma \mid^2 . \qquad (21)$$

Pour calculer $G_\sigma(W_i, W_j)$, on peut utiliser les formules des paragraphes 2.1 et 2.2 et le théorème 2. Le lecteur se reportera à [10], p. 3.82, pour la détermination du vecteur de Riemann $\Delta_{\mathcal{B}_\sigma}$.

Appliquons ce qui précède au cas où $K = \mathbf{Q}$. Les polynômes unitaires $F \in \mathbf{Z}[X]$ de degré 3 tels que $F(0)$ et $F(1)$ soient des unités s'écrivent soit

$$F(X) = X(X-1)(X-t) + \varepsilon,$$

soit

$$F(X) = X(X-1)(X-t) + \varepsilon(1-2X),$$

avec $t \in \mathbf{Z}$ et $\varepsilon = \pm 1$.

Considérons par exemple la famille

$$F_t(X) = X(X-1)(X-t) + 1.$$

Le discriminant de $R_t(X) = X(X-1) + 4F_t(X)$ vaut

$$256\,t^4 + 256\,t^3 - 1568\,t^2 - 816\,t - 5591.$$

Pour tout $t \in \mathbf{Z}$, $t \not\equiv 5 \mod 7$, on peut vérifier que F_t satisfait aux conditions de la proposition 9, *i.e.* que, pour tout nombre premier p impair, les racines de $R_t \bmod p$ sont de multiplicité au plus 2.

Prenons par exemple $t = -4$. Le discriminant de R_{-4} vaut 21737, qui est un nombre premier, et une équation de $C_{F_{-4}}$ sur $\mathbf{Q}$ est (*cf.* (20))

$$y^2 = x(x-1)(4x^3 + 13x^2 - 17x + 4).$$

On remarquera le caractère "particulièrement simple" de cette courbe parmi les courbes de genre 2 définies sur $\mathbf{Q}$: elle a réduction semi-stable sur $\mathbf{Q}$, son modèle stable sur $\mathbf{Z}$ est régulier et possède une seule fibre de mauvaise réduction, qui est irréductible et possède un unique point singulier [3]. En appliquant les méthodes expliquées plus haut, on obtient

$$\begin{array}{lll} h(C_{F_{-4}}) & = \deg f_* \omega_{C_{F_{-4}}/B} & = -1,466599\ldots \\ h'(C_{F_{-4}}) & = \deg' f_* \omega_{C_{F_{-4}}/B} & = -0,321869\ldots \\ e(C_{F_{-4}}) & = (\omega_{C_{F_{-4}}/B} \cdot \omega_{C_{F_{-4}}/B}) & = 2,32\ldots. \end{array}$$

Pour le calcul de l'intégrale quadruple $\log \|H\|$ nécessaire à l'obtention de l'invariant $(\omega_{C_{F_{-4}}/B} \cdot \omega_{C_{F_{-4}}/B})$, on a utilisé la méthode de quadrature de Gauss et, à titre de vérification, une méthode de quadrature de Monte-Carlo. Les calculs ont été effectués sur l'IBM 4341 de l'École normale supérieure. Les temps de calcul ont été négligeables, hormis celui de cette intégrale, qui a nécessité une dizaine de minutes de temps CPU.

4. La courbe $y^2 + y = x^5$

Nous calculons dans cette section les invariants e et h de la courbe sur $\overline{\mathbf{Q}}$ dont une équation affine est

$$y^2 + y = x^5$$

ou encore, grâce aux changements de variable $z = 2y + 1$ et $t = 2^{2/5}x$,

$$z^2 = 4x^5 + 1 \quad \text{ou} \quad z^2 = t^5 + 1.$$

C'est une courbe de genre 2 remarquable; elle est caractérisée par l'une quelconque des propriétés suivantes (*cf.* [6]):

- Son groupe d'automorphismes est le groupe $\mathbf{Z}/5\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$.
- Son groupe d'automorphismes n'est pas réduit à $\mathbf{Z}/2\mathbf{Z}$, et sa jacobienne est simple.
- Le point correspondant dans la variété de modules des courbes de genre 2 est singulier.

[3]Rappelons que, d'après Fontaine, la jacobienne d'une courbe C de genre 2 ayant réduction semi-stable sur $\mathbf{Q}$ ne peut avoir bonne réduction en toute place; il existe donc une place v de $\mathbf{Q}$ en laquelle la réduction du modèle stable de C, ou bien possède deux points singuliers, ou bien possède un unique point singulier et est irréductible.

4.1. Bonne réduction

Montrons que *la courbe X, propre et lisse sur $\mathbf{Q}$, d'équation affine*

$$y^2 + y = x^5$$

acquiert bonne réduction sur une extension convenable de $\mathbf{Q}$.

Le changement de variables

$$x' = \frac{1}{x} \qquad y' = \frac{x^2}{y}$$

établit un isomorphisme entre des ouverts des courbes affines lisses sur $\mathbf{Z}[1/5]$ d'équations $y^2 + y = x^5$ et $x' + x'^3 y' = y'^2$. Ainsi, X admet un modèle lisse sur Spec $\mathbf{Z}[1/5]$.

Vérifions que X a bonne réduction potentielle sur $\mathbf{Z}_5$. On a vu plus haut qu'elle admet comme équation $z^2 = t^5 + 1$ sur le corps $\mathbf{Q}(\sqrt[5]{2})$. Cette équation s'écrit encore [4]

$$z^2 = \prod_{i=0}^{4} (t + \zeta_5^i).$$

Sur le corps $\mathbf{Q}(\sqrt{1 - \zeta_5})$, elle devient

$$w^2 = u \prod_{i=1}^{4} (u - \alpha_i), \tag{22}$$

où α_i désigne l'unité cyclotomique $(1 - \zeta_5^i)/(1 - \zeta_5)$, grâce au changement de variables

$$t = (1 - \zeta_5)u - 1, \quad z = (1 - \zeta_5)^{5/2}\, w. \tag{23}$$

Si v est une place de caractéristique 5, alors $\alpha_i = \sum_{j=0}^{i-1} \zeta^j \equiv i \pmod{v}$ de sorte que les α_i sont distincts et non nuls mod v et que (22) définit une courbe lisse en v (de réduction $\bmod v$ $t^2 = u^5 - u$).

La démonstration qui précède montre aussi que X a bonne réduction sur le corps $K' = \mathbf{Q}(\sqrt{1 - \zeta_5}, \sqrt[5]{2})$.

4.2. Points de Weierstrass.

Notons R' l'anneau des entiers de K', $R_1 = R'[1/5]$, $B' = \operatorname{Spec} R'$ et $B_1 = \operatorname{Spec} R_1$. Notons W_∞ (resp. W_i, $i = 0, \ldots, 4$) le point de $X(K')$ au-dessus du point à l'infini de $\mathbf{P}^1$ (resp. du point d'abscisse $x = -\zeta_5^i/\sqrt[5]{4}$). Nous désignons encore par $W_\alpha (\alpha \in \{\infty, 0, \ldots, 4\})$ les sections correspondantes du modèle propre et lisse $\mathcal{X}'$ de X au-dessus de B'. Ce sont les points de Weierstrass de $\mathcal{X}' \to B'$ (*cf.* 1.1).

[4] Rappelons que ζ_5 désigne une racine primitive cinquième de l'unité.

PROPOSITION 10 - *Pour $\alpha \neq \beta \in \{\infty, 0, \ldots, 4\}$, le sous-schéma $W_\alpha \cap W_\beta$ de $\mathcal{X}'$ s'identifie à* $\operatorname{Spec} R'/(\sqrt[5]{2})$.

Démonstration. Il est clair sur l'équation (22) que W_α et W_β ne se rencontrent pas au-dessus d'une place de caractéristique 5 (en fait, au-dessus de toute place de caractéristique différente de 2). Soit $\mathcal{X}_1$ l'image inverse de B_1 dans $\mathcal{X}'$. Il suffit, pour démontrer la proposition, de prouver que le sous-schéma $W_\alpha \cap W_\beta \cap \mathcal{X}_1$ de $\mathcal{X}_1$ s'identifie à $\operatorname{Spec} R_1/(\sqrt[5]{2})$.

Les $W_\alpha \cap \mathcal{X}_1$ sont contenus dans l'ouvert affine de $\mathcal{X}_1$ d'équation $x' + x'^3 y' = y'^2$ considéré plus haut, et admettent comme équation

$$\begin{aligned} W_\infty : &\quad x' = y' = 0 \\ W_i : &\quad x' = -\zeta_5^{-i}\sqrt[5]{4},\ y' = -\zeta_5^{2i}\sqrt[5]{2} \ \ (0 \leq i \leq 4). \end{aligned}$$

Compte tenu du fait que $1 - \zeta_5^k$ est inversible dans R_1 si $k \not\equiv 0 \bmod 5$, on en déduit l'assertion annoncée. ∎

Notons $X_{\mathbf{C}}$ la surface de Riemann déduite de X (rappelons que X est définie sur $\mathbf{Q}$) et G la fonction de Green-Arakelov sur $X_{\mathbf{C}} \times X_{\mathbf{C}}$. Compte tenu de la définition de l'intersection d'Arakelov, on déduit immédiatement de la proposition précédente:

COROLLAIRE - *Pour $\alpha \neq \beta \in \{\infty, 0, \ldots, 4\}$, on a*

$$(W_\alpha . W_\beta)_{\mathcal{X}'} = \frac{1}{5}[K' : \mathbf{Q}] \log 2 - \sum_{\sigma : K' \hookrightarrow \mathbf{C}} \log G(\sigma W_\alpha, \sigma W_\beta). \tag{24}$$

Remarquons que le point σW_∞ de $X_{\mathbf{C}}$ est indépendant du plongement σ de K' dans $\mathbf{C}$: c'est toujours le point à l'infini de $X_{\mathbf{C}}$. Les autres points de Weierstrass de $X_{\mathbf{C}}$ sont permutés par l'automorphisme T de $X_{\mathbf{C}}$ défini par

$$T(x, y) = (\zeta_5^{-1} x, y),$$

qui admet le point à l'infini comme un point fixe. Par suite, $G(\sigma W_\infty, \sigma W_i)$ est *indépendant* de σ et de $i \in \{0, \ldots, 4\}$. Notons-le $G(W_\infty, W_0)$. Le corollaire du théorème 2 donne

$$G(W_\infty, W_0) = \left[\prod_{j=0}^{4} G(W_\infty, W_j)\right]^{1/5} = 2^{1/5} \|\Delta_2\|(X_{\mathbf{C}})^{-1/40} \|H\|(X_{\mathbf{C}})^{1/2}.$$

Il vient donc

PROPOSITION 11 - *Pour tout $i \in \{0, \ldots, 4\}$, on a*

$$\frac{1}{[K' : \mathbf{Q}]}(W_\infty . W_i)_{\mathcal{X}'} = \frac{1}{40} \log \|\Delta_2\|(X_{\mathbf{C}}) - \frac{1}{2} \log \|H\|(X_{\mathbf{C}}). \tag{25}$$

et les deux membres de (25) *sont indépendants de i.*

Le théorème 1 donne alors:

COROLLAIRE – *L'invariant $e(X)$ vaut*

$$\frac{1}{[K' : \mathbf{Q}]} (\omega_{\mathcal{X}'/B'} . \omega_{\mathcal{X}'/B'}) = -\frac{1}{5} \log \|\Delta_2\|(X_{\mathbf{C}}) + 4 \log \|H\|(X_{\mathbf{C}}). \tag{26}$$

4.3. Différentielles

Gardant les notations de 4.2., notons $f : \mathcal{X}' \to B'$ le morphisme structural, et considérons le R'-module localement libre de rang deux

$$E = f_* \omega_{\mathcal{X}'/B'}.$$

Pour calculer le degré d'Arakelov de E muni de ses métriques canoniques, considérons sur X les 1-formes

$$\begin{aligned} \omega_1 &= \frac{dx}{z} = \frac{dx}{2y+1} = \frac{dy}{5x^4} \\ \omega_2 &= x\, \omega_1. \end{aligned} \tag{27}$$

On constate sans peine que ω_1 et ω_2 définissent des 1-formes globales sur le modèle propre et lisse de X sur $\operatorname{Spec} \mathbf{Z}[1/5]$, à diviseurs disjoints. Considérant ω_1 et ω_2 comme des sections rationnelles de E, nous voyons donc qu'elles forment une base du $R'[1/5]$-module $E \otimes_{R'} R'[1/5]$. Pour voir ce qui se passe en une place v de caractéristique résiduelle 5, on utilise l'équation (22). Le changement de variables (23) donne

$$\begin{aligned} \omega_1 &= 2^{-2/5} (1-\zeta_5)^{-3/2} \frac{du}{w} \\ \omega_2 &= 2^{-4/5} (1-\zeta_5)^{-3/2} [(1-\zeta_5)u - 1] \frac{du}{w}. \end{aligned}$$

Or il est immédiat d'après l'équation (22) que du/w et $u\,du/w$ forment une base de $E \otimes_{R'} R'_v$, où R'_v est le complété de R' en v. Comme on a

$$\varepsilon := \omega_1 \wedge \omega_2 = 2^{-6/5} (1-\zeta_5)^{-2} \frac{du}{w} \wedge \frac{u\,du}{w}$$

dans $\Lambda^2_{R'}(E) \otimes_{\mathbf{Z}} \mathbf{Z}_5$, on en déduit que le diviseur de ε (vue comme section rationnelle de $\Lambda^2_{R'}(E)$) est celui de $(1-\zeta_5)^{-2}$. Si v est normalisée de sorte que $v(5) = 1$, on a donc $v(\varepsilon) = -1/2$ puisque $v(1-\zeta_5) = 1/4$.

Pour calculer le degré de E, il reste à déterminer la norme archimédienne de ε, qui est définie sur $\mathbf{Q}$. Il vient en effet, d'après ce qui précède,

$$\frac{1}{[K' : \mathbf{Q}]} \deg E = -\frac{1}{2} \log 5 - \log \|\varepsilon\|. \tag{28}$$

Rappelons que, par définition, on a

$$\|\varepsilon\|^2 = AD - B\bar{B}$$

où

$$A = \frac{i}{2}\int_{X_{\mathbf{C}}} \omega_1 \wedge \overline{\omega_1}, \quad B = \frac{i}{2}\int_{X_{\mathbf{C}}} \omega_1 \wedge \overline{\omega_2} \quad \text{et} \quad D = \frac{i}{2}\int_{X_{\mathbf{C}}} \omega_2 \wedge \overline{\omega_2}.$$

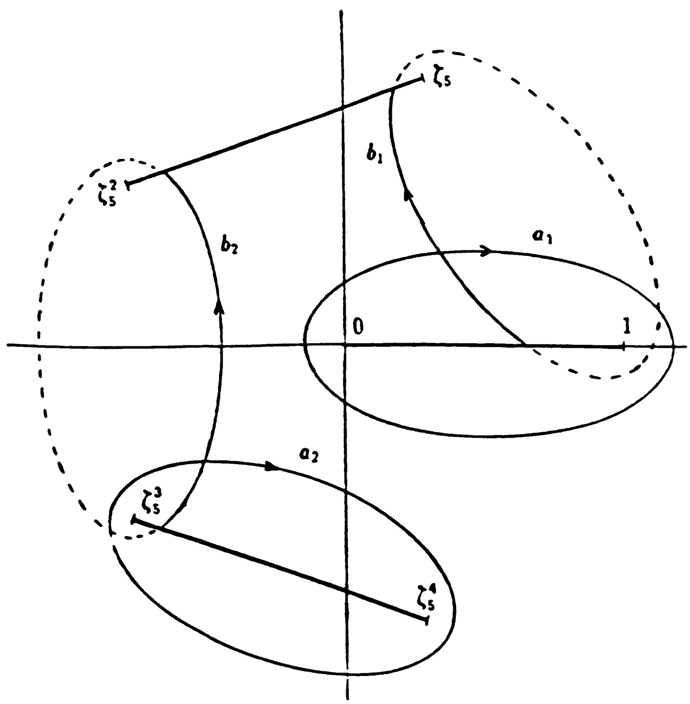
4.4. Calcul des périodes de X

Les valeurs des intégrales A, B et D se déduisent de celles des formes différentielles ω_1 et ω_2, grâce aux relations bilinéaires de Riemann.

Par le changement de variables $x = -2^{-2/5}U^{-1}$, $z = VU^{-3}$, l'équation $z^2 = 4x^5 + 1$ de X sur K' devient $V^2 = U^6 - U$. Dans ce nouveau modèle, les points de Weierstrass de X sont les points d'ordonnée nulle, et les différentielles ω_1 et ω_2 du paragraphe précédent s'écrivent

$$\omega_1 = 2^{-2/5}U dU/V \quad \text{et} \quad \omega_2 = -2^{-4/5}dU/V.$$

Pour calculer les périodes de la courbe $X_{\mathbf{C}}$, choisissons la base symplectique (a_1, a_2, b_1, b_2) de $H_1(X_{\mathbf{C}}, \mathbf{Z})$ représentée sur le dessin suivant, figurant $X_{\mathbf{C}}$ comme revêtement ramifié à 2 feuillets du "plan des U":



Posons, comme en 3.5,

$$\Omega' = \left(\int_{a_i} \omega_j\right)_{1\leq i,j\leq 2} \quad \text{et} \quad \Omega'' = \left(\int_{b_i} \omega_j\right)_{1\leq i,j\leq 2}.$$

Le calcul de ces matrices est facilité par l'existence de l'automorphisme T de X défini par $(U, V) \mapsto (\zeta_5 U, \zeta_5^3 V)$, déjà considéré en 4.2. L'action de T sur les différentielles de première espèce de X est donnée par les formules

$$T^*\omega_1 = \zeta_5^{-1}\omega_1, \quad T^*\omega_2 = \zeta_5^{-2}\omega_2, \tag{29}$$

et celle sur les cycles par [5]

$$\begin{array}{llll} T(a_1) = & -a_1 - b_1 & T(a_2) = & a_1 + b_1 - b_2 \\ T(b_1) = & a_1 + a_2 & T(b_2) = & a_2. \end{array}$$

On en déduit immédiatement que

$$b_1 = -a_1 - T(a_1), \quad a_2 = -a_1 - T(a_1) - T^2(a_1), \quad b_2 = T^2(a_1) + T^3(a_1). \tag{30}$$

Compte tenu du fait que, pour toute forme différentielle ω,

$$\int_{T^i a_1} \omega = \int_{a_1} (T^i)^* \omega,$$

les relations (29) et (30) permettent d'exprimer Ω' et Ω'' en fonction des périodes

$$B_1 = \int_{a_1} \omega_1 \quad \text{et} \quad B_2 = \int_{a_1} \omega_2.$$

On trouve ainsi

$$\begin{array}{l} \Omega' = \begin{pmatrix} 1 & 1 \\ -1-\zeta_5-\zeta_5^3 & -1-\zeta_5^3-\zeta_5^4 \end{pmatrix} \begin{pmatrix} B_1 & 0 \\ 0 & B_2 \end{pmatrix} \\ \Omega'' = \begin{pmatrix} -1-\zeta_5^3 & -1-\zeta_5^4 \\ \zeta_5+\zeta_5^4 & \zeta_5^2+\zeta_5^3 \end{pmatrix} \begin{pmatrix} B_1 & 0 \\ 0 & B_2 \end{pmatrix}. \end{array}$$

On en déduit la valeur de la matrice des périodes de $X_{\mathbf{C}}$ associée à la base (a_1, a_2, b_1, b_2):

$$\Omega = \Omega''\Omega'^{-1} = \begin{pmatrix} -\zeta_5^4 & \zeta_5^2+1 \\ \zeta_5^2+1 & \zeta_5^2-\zeta_5^3 \end{pmatrix},$$

puis, grâce à la formule (21) et aux relations

$$|\det \Omega'|^2 = 2 - \zeta_5^2 - \zeta_5^3 = \sqrt{5}\,\frac{1+\sqrt{5}}{2}$$

[5] Au signe près, on trouve ces formules dans [12].

$$\det \operatorname{Im} \Omega = \frac{5(\zeta_5 + \zeta_5^4)}{4} = \frac{5(-1+\sqrt{5})}{8},$$

on trouve

$$\|\varepsilon\|^2 = \frac{5\sqrt{5}}{4} \, |B_1 B_2|^2 \, . \tag{31}$$

Par ailleurs, les périodes B_1 et B_2 s'expriment simplement au moyen de la fonction B d'Euler, définie par

$$B(a,b) := \int_0^1 t^{a-1}(1-t)^{b-1} dt.$$

En effet, on a

$$|B_1| = 2^{3/5} \int_0^1 \frac{x\,dx}{\sqrt{x-x^6}} \quad \text{et} \quad |B_2| = 2^{1/5} \int_0^1 \frac{dx}{\sqrt{x-x^6}},$$

donc, grâce au changement de variable $t = x^5$,

$$|B_1| = \frac{2^{3/5}}{5} B(3/10, 1/2) \quad \text{et} \quad |B_2| = \frac{2^{1/5}}{5} B(1/10, 1/2). \tag{32}$$

La formule d'Euler $B(a,b) = \Gamma(a)\Gamma(b)/\Gamma(a+b)$ jointe à la formule de duplication $\sqrt{2\pi}\Gamma(2z) = 2^{2z-1/2}\Gamma(z)\Gamma(z+1/2)$ permet d'écrire, pour tout $x > 0$,

$$B(x, 1/2) = 2\pi \frac{\Gamma(2x)}{2^{2x}\Gamma(x+1/2)^2},$$

d'où

$$B_1 = \frac{2\pi}{5}\Gamma(3/5)\Gamma(4/5)^{-2}, \quad B_2 = \frac{2\pi}{5}\Gamma(1/5)\Gamma(3/5)^{-2}$$

et

$$\|\varepsilon\|^2 = \frac{5\sqrt{5}}{4}(4\pi^2\Gamma(1/5)\Gamma(3/5)^{-1}\Gamma(4/5)^{-2})^2.$$

En recourant à la formule

$$\sqrt{5}\Gamma(1/5)\Gamma(2/5)\Gamma(3/5)\Gamma(4/5) = 4\pi^2,$$

conséquence de la formule de multiplication de Gauss, on obtient finalement

PROPOSITION 12 - *La hauteur de Faltings stable $h(X)$ de la jacobienne de X vaut*

$$\frac{1}{[K':\mathbf{Q}]} \deg E = \log 4\pi - \frac{1}{2} \log \Gamma(1/5)^5\Gamma(2/5)^3\Gamma(3/5)\Gamma(4/5)^{-1}.$$

Observons que la hauteur $h'(X)$ admet l'expression suivante, peut-être plus élégante:

$$h'(X) = 2\log 2\pi - \frac{1}{2} \log \Gamma(1/5)^5\Gamma(2/5)^3\Gamma(3/5)\Gamma(4/5)^{-1}.$$

4.5. Résultats numériques et remarques

Après calculs sur ordinateur, on trouve

$$\begin{aligned}
&\|\Delta_2\|(X_{\mathbf{C}}) = 0,2070469497\ldots 10^{-4}\\
&\log\|\Delta_2\|(X_{\mathbf{C}}) = -10,78515008\ldots\\
&\log\|H\|(X_{\mathbf{C}}) = -0,4854\ldots\\
&e(X) = 0,2152\ldots\\
&h(X) = -2,597239125\ldots\\
&h'(X) = -1,452509239\ldots.
\end{aligned}$$

Observons que nous aurions pu calculer $e(X)$ à partir de $h(X)$ et de l'invariant de Faltings $\delta(X_{\mathbf{C}})$, grâce à la formule de Noether ([8]) qui s'écrit ici, puisque X a potentiellement partout bonne réduction,

$$12h(X) = e(X) + \delta(X_{\mathbf{C}}) - 8\log(2\pi),$$

et à la formule (*cf.* [2])

$$\delta(X_{\mathbf{C}}) = -16\log(2\pi) - \log\|\Delta_2\|(X_{\mathbf{C}}) - 4\log\|H\|.$$

Si l'on compare ces relations aux formules (26) et (28), on trouve

$$h(X) = -2\log(2\pi) - \frac{1}{10}\log\|\Delta_2\|(X_{\mathbf{C}})$$

puis

$$\|\varepsilon\| = (2\pi)^2\, 5^{-1/2}\, \|\Delta_2\|(X_{\mathbf{C}})^{1/10}.$$

En fait, cette dernière équation découle directement des formules de Thomae ([10], p. 3.121).

Montrons maintenant que X *contredit l'analogue arithmétique "naïf" de l'inégalité $c_1^2 \leq 3c_2$ de Bogomolov-Miyaoka*, et même, plus généralement, l'analogue de l'inégalité

$$c_1^2 \leq \lambda c_2, \tag{33}$$

pour tout $\lambda > 0$.

Rappelons que les classes de Chern d'une surface projective X fibrée sur une courbe B de genre q sont données par

$$c_1^2(X) = (\omega_{X/B}.\omega_{X/B}) + 2(2g-2)(2q-2)$$

$$c_2(X) = 12\deg f_*\omega_{X/B} - (\omega_{X/B}.\omega_{X/B}) + (2g-2)(2q-2),$$

tandis que l'analogue arithmétique de $2q-2$ est le logarithme de la valeur absolue du discriminant D_K du corps de base K. Ainsi, la traduction arithmétique de (33) affirmerait que, *si* X *est une courbe de genre* g *lisse sur* $\overline{\mathbf{Q}}$, *admettant un modèle stable sur un corps de nombres* K, *on a*

$$e(X) + \frac{2(2g-2)}{[K:\mathbf{Q}]} \log |D_K| \leq \lambda(12h(X) - e(X) + \frac{2g-2}{[K:\mathbf{Q}]} \log |D_K|)$$

(*cf.* Parshin [11] et [7], 3.2.3.2) c'est-à-dire, lorsque $g = 2$,

$$e(X) \leq \lambda(12h(X) - e(X) + \frac{2}{[K:\mathbf{Q}]} \log |D_K|) - \frac{4}{[K:\mathbf{Q}]} \log |D_K|.$$

Lorsque X est la courbe d'équation $y^2 + y = x^5$ et que K est le corps $\mathbf{Q}(\sqrt[5]{2}, \sqrt{1-\zeta_5})$, on a

$$[K:\mathbf{Q}] = 40, \quad D_K = 2^{72}\, 5^{85}, \quad \frac{1}{[K:\mathbf{Q}]} \log |D_K| = 4{,}667720\ldots,$$

et compte tenu des valeurs de $h(X)$ et $e(X)$ données plus haut, le membre de gauche de l'inégalité précédente est positif, alors que le coefficient de λ dans le membre de droite est strictement négatif.

On peut s'assurer qu'il en va toujours ainsi si l'on considère certaines variantes de cette inégalité, par exemple si l'on substitue $h'(X)$ à $h(X)$, ou $2^{-r_2} D_K$ à D_K, r_2 désignant le nombre de places complexes de K (ici $r_2 = 20$), ou encore en substituant à K le corps $K(\sqrt{-30030})$, et donc tous les corps apparaissant dans la tour de Golod-Shafarevich qui lui est classiquement associée.

Signalons enfin que ces vérifications n'exigent pas de connaître une valeur numérique de $e(X)$, mais seulement l'inégalité $e(X) \geq 0$, démontrée par Faltings dans [5] et la valeur de $h(X)$, exprimée plus haut au moyen de la fonction Γ.

Appendice: démonstration du théorème 2

A.1. Quelques formules relatives aux surfaces de Riemann de genre 2

La démonstration du théorème 2 va procéder en deux étapes. Tout d'abord, nous établirons les formules suivantes, qui relient les fonctions $\|\theta\|$ et G, mais font intervenir des constantes "inconnues" $\delta(X)$, $A(X)$ et $B(X)$.

i) Il existe $\delta(X) \in \mathbf{R}$ *tel que, quels que soient* $(x_1, x_2, y) \in X^3$, $x_1 \neq x_2$, *et* $(\omega_1, \omega_2) \in H^0(X, \omega_X)^2$,

$$\|\theta\|(x_1 + x_2 - y)\|\omega_1 \wedge \omega_2\| = e^{-\frac{\delta(X)}{8}} \left\| \begin{vmatrix} \omega_1(x_1) & \omega_2(x_1) \\ \omega_1(x_2) & \omega_2(x_2) \end{vmatrix} \right\|_A \frac{G(x_1, y)G(x_2, y)}{G(x_1, x_2)}. \tag{34}$$

ii) Il existe $A(X) \in \mathbf{R}$ *tel que, pour tout couple* (x, y) *de points de* X *distincts,*

$$\log G(x, y) = \frac{1}{2} \int_{\Theta + x - y} \log \|\theta\| \mu + A(X). \tag{35}$$

iii) Quel que soit $(x, y, z) \in X^3$*, on a*

$$G(x, \sigma(y))G(x, z)G(y, z) = e^{A(X)}\|\theta\|(x + y - z). \tag{36}$$

iv) Il existe $B(X) \in \mathbf{R}$ *tel que, quel que soit* $(x, y) \in X^2$,

$$G(x, y)G(x, \sigma(y)) = e^{B(X)} \|J\|(x, y). \tag{37}$$

Ensuite, nous établirons la proposition suivante, qui permet d'exprimer les constantes $\delta(X)$, $A(X)$ et $B(X)$ au moyen de $\|\Delta_2\|(X)$ et $\|H\|(X)$.

PROPOSITION 13 - *Pour tout couple* (P, Q) *de points de Weierstrass de* X *distincts, on a*

$$\log \|J\|(P, Q) - \int_{\Theta + P - Q} \log \|\theta_0\| \, \mu - 2 \log \|H\|(X) = 2 \log(2\pi). \tag{38}$$

Déduisons à présent le théorème 2 des formules (34) à (38).

D'après (37), il vient, pour tout couple (P, Q) de points de Weierstrass de X,

$$G(P, Q)^2 = e^{B(X)} \|J\|(P, Q). \tag*{$(39)_{PQ}$}$$

L'identité (36) montre que, pour tout triplet (P, Q, R) de points de Weierstrass de X, on a

$$G(P, Q) \, G(Q, R) \, G(R, P) = e^{A(X)} \|\theta\|(P + Q + R - K). \tag{40}$$

De plus, on déduit facilement de la définition de $\|\Delta_2\|(X)$ et des relations de Rosenhain

$$\|J\|(P, Q) \, \|J\|(Q, R) \, \|J\|(R, P) = (2\pi)^6 \, \|\theta\|(P + Q + R - K)^2 \, \|\Delta_2\|(X)^{1/2}. \tag{41}$$

En éliminant les valeurs de G, $\|J\|$ et $\|\theta\|$ entre les identités $(39)_{PQ}$, $(39)_{QR}$, $(39)_{RP}$ et (41), nous obtenons alors:

$$2A(X) - 3B(X) = 6\log(2\pi) + \frac{1}{2}\log\|\Delta_2\|(X). \tag{42}$$

Par ailleurs, les relations $(39)_{PQ}$ et (35) donnent, pour tout couple (P, Q) de points de Weierstrass de X distincts:

$$\log\|J\|(P,Q) - \int_{\Theta+P-Q} \log\|\theta\|\mu = 2A(X) - B(X). \tag{43}$$

La proposition 13 montre alors:

$$2A(X) - B(X) = 2\log(2\pi) + 2\log\|H\|(X). \tag{44}$$

On déduit immédiatement de (42) et (44) les valeurs de $A(X)$ et $B(X)$:

$$A(X) = -\frac{1}{8}\log\|\Delta_2\|(X) + \frac{3}{2}\log\|H\|(X)$$

$$B(X) = -2\log(2\pi) - \frac{1}{4}\log\|\Delta_2\|(X) + \log\|H\|(X), \tag{45}$$

puis on obtient le théorème 2 en reportant (45) dans $(39)_{PQ}$.

A.2. Démonstration des formules (34) à (37)

Démonstration de (34). Cette formule est établie dans [5], p. 402. On peut en donner une démonstration directe — qui n'est en fait qu'une variante de la démonstration de [5] — en montrant que, comme fonction de chacune des trois variables x, y et z décrivant X, les logarithmes des deux membres de (34) ont même image par $d'd''$: cela découle de (16) et des valeurs des courbures des métriques $\|.\|_{\mathcal{O}(\Theta)}$ et $\|.\|_A$. ∎

Démonstration de (35). En prenant le logarithme de l'identité (34), puis en l'intégrant par rapport à la mesure $\nu(x_1)$, on obtient, compte tenu des relations (15) et (14),

$$\frac{1}{2}\int_{\Theta+x_2-y} \log\|\theta\|\mu + \log\|\omega_1 \wedge \omega_2\|$$

$$= -\frac{\delta(X)}{8} + \int_X \log\left\| \begin{vmatrix} \omega_1(x_1) & \omega_2(x_1) \\ \omega_1(x_2) & \omega_2(x_2) \end{vmatrix} \right\|_A \nu(x_1) + \log G(x_2, y).$$

Par conséquent, il existe une fonction $\varphi : X \to \mathbf{R}$ telle que

$$\log G(x,y) - \frac{1}{2}\int_{\Theta+x-y} \log\|\theta\|\,\mu = \varphi(x). \tag{46}$$

Or on sait que

$$\log G(x,y) = \log G(y,x).$$

De plus, comme $\|\theta\|$, μ et Θ sont invariants par l'involution $t \mapsto K - t$ de $\mathrm{Pic}^1 X$, il vient

$$\int_{\Theta+y-x} \log \|\theta\|\mu = \int_{K-(\Theta+y-x)} \log \|\theta\|\mu = \int_{\Theta+x-y} \log \|\theta\|\mu.$$

Ainsi, le premier membre de (46) est symétrique en x et y, et φ est constante. ■

Démonstration de (36). Il suffit de démontrer (36) lorsque x est distinct de y et de $\sigma(y)$. Dans ce cas, $x+y$ est distinct de K et $x+y-\Theta$ rencontre transversalement Θ en x et y. De plus, d'après (34), il existe $C(x,y) \in \mathbf{R}$ tel que, pour tout $z \in X \setminus \{x,y\}$

$$\log \|\theta\|(x+y-z) - \log G(x,z) - \log G(y,z) = C(x,y). \tag{47}$$

Si l'on intègre cette égalité relativement à la mesure $\nu(z)$, on trouve, d'après (15) et (14),

$$C(x,y) = \frac{1}{2}\int_{x+y-\Theta} \log \|\theta\|\mu.$$

Comme $x+y-\Theta = K-(\Theta+\sigma(x)-y)$ et que $\log\|\theta\|$ et μ sont invariants par l'involution $t \mapsto K-t$ de $\mathrm{Pic}^1 X$, on en déduit

$$C(x,y) = \frac{1}{2}\int_{\Theta+\sigma(x)-y} \log \|\theta\|\mu. \tag{48}$$

L'identité (36) découle immédiatement de (35), (47) et (48). ■

Démonstration de (37). La fonction $\|J\|$ (sur $X \times X$) s'annule exactement sur les couples $(x,y) \in X^2$ tels que x et y aient même image par l'application de Gauss

$$X \simeq \Theta \to \check{\mathbf{P}}(T_0 \operatorname{Pic} X) \simeq \mathbf{P}(H^0(X,\omega_X)).$$

Or cette application n'est autre que le morphisme "canonique" et s'identifie à l'application évidente $X \to X/\sigma$. On prouve ainsi que le quotient

$$\frac{\|J\|(x,y)}{G(x,y)G(x,\sigma(y))}$$

se prolonge en une fonction continue non nulle sur $X \times X$. De plus, les relations (14) et (16) montrent que le logarithme de cette fonction est harmonique en chacune des variables. Elle est donc constante. ■

A.3. Démonstration de la proposition 13

A.3.1. Soit D l'hypersurface dans $\mathcal{H}_2$ orbite sous $\mathrm{Sp}_4(\mathbf{Z})$ des matrices diagonales dans $\mathcal{H}_2$.

Pour toute base symplectique $\mathcal{B}$ de $H_1(X, \mathbf{Z})$, la matrice des périodes Ω de X associée à $\mathcal{B}$ appartient à $\mathcal{H}_2$. De plus, les points de Weierstrass de X sont en bijection avec l'ensemble $\mathcal{I}$ des classes, modulo $\mathbf{Z}^2 \times \mathbf{Z}^2$, des couples $(a, b) \in (\frac{1}{2}\mathbf{Z})^2 \times (\frac{1}{2}\mathbf{Z})^2$ tels que $4 \cdot {}^t a.b$ soit impair, par l'application

$$\begin{aligned} \mathcal{I} &\to \mathrm{Pic}^1 X \\ [(a, b)] &\mapsto [a + \Omega b] + \Delta_{\mathcal{B}}, \end{aligned}$$

où $[a + \Omega b]$ désigne la classe dans $\mathbf{C}^2/(\mathbf{Z}^2 + \Omega\mathbf{Z}^2) \simeq \mathrm{Pic}^0 X$ de $a + \Omega b$.

Réciproquement, tout élément de $\mathcal{H}_2 \setminus D$ est la matrice des périodes d'une surface de Riemann de genre 2 dont l'homologie est munie d'une base symplectique. Cela se prouve facilement en considérant "l'application des périodes" $\mathcal{M}_2 \to \mathcal{A}_2$, qui est un morphisme dominant, et son prolongement de $\overline{\mathcal{M}_2}$ vers la compactification de Satake de $\mathcal{A}_2$.

Par suite, la proposition 13 peut s'exprimer comme une identité entre fonctions sur $\mathcal{H}_2 \setminus D$.

Il est commode, pour formuler et établir cette identité, d'introduire quelques notations.

Soit $\mathcal{T}$ le quotient de $\mathbf{C}^2 \times \mathcal{H}_2$ par l'action de $\mathbf{Z}^2 \times \mathbf{Z}^2$ définie par

$$(n_1, n_2).(z; Z) = (z + n_1 + Zn_2; Z),$$

où $(n_1, n_2) \in \mathbf{Z}^2 \times \mathbf{Z}^2$, $z \in \mathbf{C}^2$ et $Z \in \mathcal{H}_2$. L'application

$$\begin{array}{cccc} \pi : & \mathcal{T} & \to & \mathcal{H}_2 \\ & [(z; Z)] & \mapsto & Z \end{array}$$

est un morphisme lisse entre variétés $\mathbf{C}$-analytiques. Sa fibre en $Z \in \mathcal{H}_2$ est la surface abélienne $\mathbf{C}^2/(\mathbf{Z}^2 + Z\mathbf{Z}^2)$.

Pour tout $n = [(n_1, n_2)] \in (\mathbf{R}^2 \times \mathbf{R}^2)/(\mathbf{Z}^2 \times \mathbf{Z}^2)$, nous poserons

$$\begin{array}{cccc} s_n : & \mathcal{H}_2 & \to & \mathcal{T} \\ & Z & \mapsto & [(n_1 + Zn_2; Z)] \end{array}$$

$$\begin{array}{cccc} t_n : & \mathcal{T} & \to & \mathcal{T} \\ & [(z; Z)] & \mapsto & [(z + n_1 + Zn_2; Z)]. \end{array}$$

Il est clair que ce sont des applications $\mathbf{C}$-analytiques, que s_n est une section de π et que t_n est un automorphisme de $\mathcal{T}$ préservant les fibres de π.

La fonction $\|\theta\|_0$ sur $\mathbf{C}^2 \times \mathcal{H}_2$ est invariante sous l'action de $\mathbf{Z}^2 \times \mathbf{Z}^2$ et peut donc être considérée comme une fonction sur $\mathcal{T}$. Le lieu Θ_0 des zéros de $\|\theta\|_0$ est une hypersurface lisse dans $\mathcal{T}$ et le morphisme

$$\pi : \Theta_0 \setminus \pi^{-1}(D) \to \mathcal{H}_2 \setminus D$$

est lisse.

L'espace $\mathcal{H}_2$ est muni d'une forme de Kähler naturelle

$$\kappa = \frac{i}{16\pi} \operatorname{Tr}(Y^{-1}.dZ.Y^{-1}.d\overline{Z}), \quad (Y = \operatorname{Im} Z).$$

Par ailleurs, la forme de type $(1,1)$ sur $\mathbf{C}^2 \times \mathcal{H}_2$

$$\mu_1 = \frac{i}{2}\, {}^t(dz - dZ.Y^{-1}.y).Y^{-1}.(d\overline{z} - d\overline{Z}.Y^{-1}.y)$$

est invariante par l'action de $\mathbf{Z}^2 \times \mathbf{Z}^2$ et définit donc une forme de type $(1,1)$ sur $\mathcal{T}$, que nous noterons encore μ_1. De plus, pour tout $n \in (\mathbf{R}^2 \times \mathbf{R}^2)/(\mathbf{Z}^2 \times \mathbf{Z}^2)$, on a

$$s_n^* \mu_1 = 0 \quad \text{et} \quad t_n^* \mu_1 = \mu_1. \tag{49}$$

Nous poserons enfin

$$\mu_0 = \mu_1 + \pi^* \kappa. \tag{50}$$

On vérifie facilement l'égalité de courants [6] sur $\mathcal{T}$

$$\frac{1}{\pi i} d'd'' \log \|\theta\|_0 = \mu_0 - [\Theta_0]. \tag{51}$$

Notons $\int_\pi$ l'opération "d'intégration le long des fibres de π" des formes différentielles ou des courants sur $\mathcal{T}$. On établit aisément les identités

$$\int_\pi [\Theta_0]\mu_0 = \int_\pi \mu_0^2 = 2 \quad \text{et} \quad \int_\pi \mu_0^3 = 6\kappa. \tag{52}$$

A.3.2. Il découle des formules précédentes et des formules des paragraphes 2.1 et 2.2 que la proposition 13 peut se réécrire comme suit:

PROPOSITION 14 - *Pour tout couple (I_1, I_2) d'éléments de $\mathcal{I}$ distincts, l'identité suivante est satisfaite sur $\mathcal{H}_2 \setminus D$:*

$$\sum_{I \in \mathcal{I} \setminus \{I_1, I_2\}} s_{I+I_1+I_2}^* \log \|\theta\|_0 - \int_\pi [t_{I_1 - I_2}(\Theta_0)] \log \|\theta\|_0 \mu_0 - \int_\pi \log \|\theta\|_0 \mu_0^2 = 2\log 2. \tag{53}$$

[6] Si C est un cycle analytique dans une variété analytique, nous notons $[C]$ le courant d'intégration sur ce cycle.

On remarquera que chacune des sections $s_{I+I_1+I_2}$ ne rencontre pas Θ_0 au-dessus de l'ouvert $\mathcal{H}_2 \setminus D$. De plus le morphisme

$$\pi:\ t_{I_1-I_2}(\Theta_0) \setminus \pi^{-1}(D) \to \mathcal{H}_2 \setminus D$$

est lisse, et Θ_0 est transverse à $t_{I_1-I_2}(\Theta_0)$ dans chaque fibre $\pi^{-1}(Z)$, pour $Z \in \mathcal{H}_2 \setminus D$; par conséquent, la fonction généralisée

$$\int_\pi [t_{I_1-I_2}(\Theta_0)] \log \|\theta\|_0 \, \mu_0$$

est continue, et sa valeur en $Z \in \mathcal{H}_2 \setminus D$ coïncide bien avec

$$\int_{\pi^{-1}(Z)} [t_{I_1-I_2}(\Theta_0)] \log \|\theta\|_0 \, \mu_0.$$

Une remarque analogue s'applique à la fonction généralisée

$$\int_\pi \log \|\theta\|_0 \, \mu_0^2.$$

Notons φ la fonction sur $\mathcal{H}_2 \setminus D$ définie par le membre de gauche de (53). On sait déjà, d'après l'égalité (43) (démontrée plus haut à partir de (34-37) sans faire appel à la proposition 13), que cette fonction ne dépend pas de (I_1, I_2), mais que, pour tout $Z \in \mathcal{H}_2 \setminus D$, $\varphi(Z)$ ne dépend que de la classe d'isomorphie de la surface de Riemann $\Theta_0 \cap \pi^{-1}(Z)$. La fonction φ est donc invariante sous l'action de $\mathrm{Sp}_4(\mathbf{Z})$.

L'identité (53) résulte des énoncés suivants:

LEMME 1 – *Lorsque $Z' \in \mathcal{H}_2 \setminus D$ tend vers un point Z de D, $\varphi(Z')$ tend vers $2\log 2$.*

LEMME 2 – *La fonction φ est pluriharmonique sur $\mathcal{H}_2 \setminus D$.*

En effet, le lemme 1 montre que la fonction φ se prolonge en une fonction $\overline{\varphi}$ continue sur $\mathcal{H}_2$, qui, comme φ, est $\mathrm{Sp}_4(\mathbf{Z})$-invariante. De plus, d'après le lemme 2, $\overline{\varphi}$ est pluriharmonique sur le complémentaire de l'hypersurface D, donc pluriharmonique partout ("théorème de prolongement de Riemann"). Ces propriétés de $\overline{\varphi}$ entraînent qu'elle est constante, donc égale à $2\log 2$: toute fonction pluriharmonique sur l'espace analytique quotient $\mathcal{H}_2/\mathrm{Sp}_4(\mathbf{Z})$ est constante, car l'espace $\mathcal{H}_2/\mathrm{Sp}_4(\mathbf{Z})$ est le complémentaire d'un fermé analytique de codimension 2 dans sa compactification de Satake, qui est une variété projective normale.

A.3.3. Démonstration du lemme 1

Pour tout $\tau \in \mathbf{C}$ tel que $\mathrm{Im}\,\tau > 0$, on note E_τ la courbe elliptique $\mathbf{C}/(\mathbf{Z} + \tau\mathbf{Z})$, $e_2(\tau)$ la classe de $(1+\tau)/2$ dans E_τ et ν_τ la 2-forme sur E_τ

$$\nu_\tau = \frac{i}{2\,\mathrm{Im}\,\tau} dz \wedge d\overline{z}.$$

On rappelle que $\|\theta\|_0(z;\tau)$ définit une fonction sur E_τ dont l'unique zéro est $e_2(\tau)$.

Comme φ est $\mathrm{Sp}_4(\mathbf{Z})$-invariante, on peut supposer Z de la forme

$$\begin{pmatrix} \tau' & 0 \\ 0 & \tau'' \end{pmatrix}.$$

La fibre $\pi^{-1}(Z)$ s'identifie à $E_{\tau'} \times E_{\tau''}$; on notera p' et p'' ses projections sur $E_{\tau'}$ et $E_{\tau''}$.

Nous pouvons de plus choisir I_1 et I_2 de sorte que, en posant

$$P_i' = p' \circ s_{I_i}(Z) \quad \text{et} \quad P_i'' = p'' \circ s_{I_i}(Z), \quad i \in \{1,2\},$$

on ait

$$P_1' \neq P_2' \quad \text{et} \quad P_1'' \neq P_2''. \tag{54}$$

Il suffit par exemple de prendre

$$I_1 = \left(\begin{pmatrix} 1/2 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1/2 \end{pmatrix} \right) \quad \text{et} \quad I_2 = \left(\begin{pmatrix} 0 \\ 1/2 \end{pmatrix}, \begin{pmatrix} 1/2 \\ 0 \end{pmatrix} \right).$$

On vérifie alors que, pour tout $I \in \mathcal{I} \setminus \{I_1, I_2\}$, on a

$$p' \circ s_{I+I_1+I_2}(Z) \neq e_2(\tau') \quad \text{et} \quad p'' \circ s_{I+I_1+I_2}(Z) \neq e_2(\tau'').$$

Par suite, la fonction

$$\sum_{I \in \mathcal{I}\setminus\{I_1,I_2\}} s_{I+I_1+I_2}^* \log \|\theta\|_0$$

est définie et continue au voisinage de Z. De plus, comme

$$\Theta_0 \cap \pi^{-1}(Z) = p'^{-1}(e_2(\tau')) \cup p''^{-1}(e_2(\tau'')),$$

la condition (54) assure que Θ_0 et $t_{I_1-I_2}(\Theta_0)$ sont transverses dans $\pi^{-1}(Z)$. Cela entraîne que

$$\int_\pi [t_{I_1-I_2}(\Theta_0)] \log \|\theta\|_0 \, \mu_0$$

est elle aussi définie et continue au voisinage de Z. Il en va clairement de même de

$$\int_\pi \log \|\theta\|_0 \, \mu_0^2.$$

On obtient ainsi que φ admet une limite en Z, qui vaut

$$\sum_{I \in \mathcal{I}\setminus\{I_1,I_2\}} \log \|\theta\|_0(s_{I+I_1+I_2}(Z)) - \int_{E_{\tau'} \times E_{\tau''}} \log \|\theta\|_0(.;Z)\mu_0^2$$
$$- \int_{E_{\tau'} \times E_{\tau''}} [\{Q'\} \times E_{\tau''} \cup E_{\tau'} \times \{Q''\}] \log \|\theta\|_0(.;Z)\mu_0,$$

avec $Q' = e_2(\tau') + P_1' - P_2'$ et $Q'' = e_2(\tau'') + P_1'' - P_2''$. On vérifie sans difficulté que cette expression vaut $2\log 2$, au moyen des formules

$$\|\theta\|_0(z', z''; Z) = \|\theta\|_0(z'; \tau')\, \|\theta\|_0(z'', \tau''),$$

$$\mu_0 = p'^* \nu_{\tau'} + p''^* \nu_{\tau''} \quad \text{sur } \pi^{-1}(Z),$$

et du lemme suivant:

LEMME 3 – *Pour tout* $\tau \in \mathbf{C}$ *tel que* $\operatorname{Im} \tau > 0$, *on a*

$$\int_{E_\tau} \log \|\theta\|_0(z; \tau)\, \nu_\tau(z) = \frac{1}{3} \log \left[\frac{1}{2} \|\theta\|_0(0; \tau)\, \|\theta\|_0(\frac{1}{2}; \tau)\, \|\theta\|_0(\frac{\tau}{2}; \tau)\right].$$

Démonstration. Ce lemme se déduit immédiatement des formules de [5], p. 417, *lemma a)* et *proof a)*. On peut aussi le démontrer directement à partir du développement en produit infini de $\theta(z; \tau)$. ∎

A.3.4. Démonstration du lemme 2

Soient φ_1, φ_2 et φ_3 les fonctions sur $\mathcal{H}_2 \setminus D$

$$\varphi_1 = \sum_{I \in \mathcal{I} \setminus \{I_1, I_2\}} s^*_{I+I_1+I_2} \log \|\theta\|_0,$$

$$\varphi_2 = \int_\pi [t_{I_1 - I_2}(\Theta_0)] \log \|\theta\|_0\, \mu_0,$$

$$\varphi_3 = \int_\pi \log \|\theta\|_0\, \mu_0^2.$$

Il vient, d'après (49), (50) et (51),

$$\begin{aligned} \frac{1}{\pi i} d'd''\varphi_1 &= \textstyle\sum_{I \in \mathcal{I} \setminus \{I_1, I_2\}} s^*_{I+I_1+I_2} \mu_0 \\ &= 4\kappa. \end{aligned} \tag{55}$$

Le calcul de $d'd''\varphi_2$ fait intervenir des produits de courants. L'existence de ces produits et la validité des calculs qui suivent résultent de la transversalité des hypersurfaces Θ_0 et $t_{I_1 - I_2}(\Theta_0)$. De plus on a

$$\{\Theta_0 \cap t_{I_1 - I_2}(\Theta_0)\} \setminus \pi^{-1}(D) = s_{I_1}(\mathcal{H}_2 \setminus D) \cup s_{I_2}(\mathcal{H}_2 \setminus D). \tag{56}$$

Cela découle du fait que, si P et Q sont deux points distincts d'une surface de Riemann de genre 2, alors les diviseurs Θ et $\Theta + P - Q$ sont transverses dans $\operatorname{Pic}^1 X$ et l'on a

$$\Theta \cap (\Theta + P - Q) = \{P, Q\}.$$

Comme $[t_{I_1-I_2}(\Theta_0)]$ et μ_0 sont d' et d''-fermées, il vient

$$\frac{1}{\pi i}d'd''\varphi_2 = \int_\pi [t_{I_1-I_2}(\Theta_0)]\frac{1}{\pi i}d'd''\log\|\theta\|_0\,\mu_0,$$

puis, d'après (51),

$$\frac{1}{\pi i}d'd''\varphi_2 = \int_\pi [t_{I_1-I_2}(\Theta_0)](\mu_0 - [\Theta_0])\,\mu_0. \tag{57}$$

De plus, on tire de (56), (49) et (50)

$$\begin{aligned}\int_\pi [t_{I_1-I_2}(\Theta_0)].[\Theta_0].\mu_0 &= \int_\pi ([s_{I_1}(\mathcal{H}_2 \setminus D)] + [s_{I_2}(\mathcal{H}_2 \setminus D)]).\mu_0 \\ &= s_{I_1}^*\mu_0 + s_{I_2}^*\mu_0 \\ &= 2\kappa,\end{aligned} \tag{58}$$

tandis que, d'après (49),

$$\int_\pi [t_{I_1-I_2}(\Theta_0)]\mu_0^2 = \int_\pi [\Theta_0]\mu_0^2. \tag{59}$$

On trouve enfin, en utilisant le fait que μ_0^2 est d' et d''-fermée, puis les égalités (51) et (52):

$$\begin{aligned}\frac{1}{\pi i}d'd''\varphi_3 &= \int_\pi \frac{1}{\pi i}\log\|\theta\|_0\,\mu_0^2 \\ &= \int_\pi \mu_0^3 - \int_\pi [\Theta_0]\mu_0^2 \\ &= 6\kappa - \int_\pi [\Theta_0]\mu_0^2.\end{aligned} \tag{60}$$

Les identités (55), (57), (58), (59) et (60) montrent que $d'd''\varphi = 0$. ∎

Bibliographie

[1] S. JU. ARAKELOV. Intersection theory of divisors on an arithmetic surface, *Izv. Akad. Nauk. SSSR* 38. **6** (1974), 1167–1180.

[2] J.-B. BOST. Fonctions de Green-Arakelov, fonctions thêta et courbes de genre 2, *C. R. Acad. Sci. Paris.* **305, I** (1987), 643–646.

[3] J.-B. BOST et J.-F. MESTRE. Moyenne arithmético-géométrique et Périodes des Courbes de genre 1 et 2, *Gazette des Mathématiciens.* **38** (1988), 36–64.

[4] P. DELIGNE. Le déterminant de la cohomologie, *Contemporary Mathematics.* **67** (AMS 1987), 93–177.

[5] G. FALTINGS. Calculus on arithmetic surfaces, *Ann. of Math.* **119** (1984), 387–424.

[6] J. IGUSA. Arithmetic variety of moduli for genus two, *Ann. of Math.* **72** (1960), 612–649.

[7] L. MORET-BAILLY. Hauteurs et classes de Chern sur les surfaces arithmétiques, *ce volume.*

[8] L. MORET-BAILLY. La formule de Noether pour les surfaces arithmétiques, *Invent. Math.* **98** (1989), 491–498.

[9] L. MORET-BAILLY. Métriques permises, *in* Séminaire sur les pinceaux arithmétiques: la conjecture de Mordell, *édité par* L. Szpiro, *Astérisque.* **127** (1985), 29–87.

[10] D. MUMFORD. *Tata Lectures on Theta.* Volume II, Progress in Math. 43, Birkhäuser (1984).

[11] A.N. PARSHIN. The Bogomolov-Miyaoka-Yau inequality for arithmetical surfaces and its applications, *Sém. de théorie des nombres de Paris* 1986 – 87, *Progress in Math.* **75**.

[12] H.E. RAUCH. Theta constants on a Riemann surface with many automorphisms, *Symposia Mathematica.* **III** (1970), 305–323.

[13] F. RICHELOT. De transformatione integralium Abelianorum primi ordinis commentatio, *J. reine angew. Math.* **16** (1837), 221–341.

[14] G. ROSENHAIN. Mémoire sur les fonctions de deux variables et à quatre périodes qui sont les inverses des intégrales ultra-elliptiques de la première classe, *Mémoires des savants étrangers.* **XI** (1851), 362–468.

Jean-Benoît BOST – IHES, 35, route de Chartres, F-91440 BURES-SUR-YVETTE.

Jean-François MESTRE – ENS, 45, rue d'Ulm, F-75230 PARIS CEDEX 05 (EARN/BITNET: MESTRE@FRULM11).

Laurent MORET-BAILLY – IRMAR, Université de Rennes-I, Campus de Beaulieu, F-35042 RENNES CEDEX (EARN/BITNET: MORET@FRCICB81).

Astérisque

D. BERTRAND

Hauteurs et isogénies

Astérisque, tome 183 (1990), p. 107-125
<http://www.numdam.org/item?id=AST_1990__183__107_0>

Société Mathématique de France
Astérisque 183 (1990)

HAUTEURS ET ISOGÉNIES

par D. BERTRAND

Théorème (Masser-Wüstholz) : *soit* d *un entier* ≥ 1 . *Il existe un nombre réel* c(d) *effectivement calculable en fonction de* d *et une constante universelle effective* C *vérifiant la propriété suivante* . *Soient* E *une courbe elliptique définie sur un corps de nombres* k *de degré* d *sur* $\mathbf{Q}$, *et* γ *un majorant* ≥ 1 *des hauteurs logarithmiques des coefficients d'une équation de Weierstrass de* E *sur* k . *Pour toute courbe elliptique* E' *définie sur* k *et* k-*isogène à* E , *il existe une* k-*isogénie de* E' *vers* E *de degré majoré par* $c(d)\,\gamma^C$.

On trouvera une démonstration de cet énoncé dans [M-W2]. L'esquisse qu'en donne [Ma4] fournit 4 pour valeur de la constante C .

Nous donnons ici la preuve d'une version affaiblie de ce théorème: l'expression c(d) est remplacée par une fonction c(k) du corps k , effectivement calculable en termes de d et de la valeur absolue δ du *discriminant* de k sur $\mathbf{Q}$. Notre démarche suit celle de [Ma4], mais paraît, par certains aspects, mieux adaptée à d'éventuelles généralisations. Et on verra en fait (appendice A) qu'au prix d'une perte significative sur C , le théorème ci-dessus découle de la démonstration de sa version affaiblie : en d'autres termes, les données δ et γ sont intimement liées.

La démonstration comporte trois parties : la première, de nature essentiellement algébrique, consiste à décrire l'isogénie ϕ qui lie *a priori* E' à E dans un modèle de Weierstrass de E' dépendant de façon logarithmique de son degré N ; la dernière met en jeu la méthode de Baker qui, sous la forme rénovée que lui donnent les lemmes de zéros, fournit alors (modulo une réduction standard expliquée dans la deuxième partie) une isogénie de E' vers E de degré majoré par un monôme en Log N . Si on a pris soin de choisir ϕ de degré minimal , N est alors bien borné !

Le théorème fournit une version effective d'un classique théorème d'irréductibilité dû à Serre ([Se], IV, 2.1). Nous renvoyons à [Ma4] pour ses applications les plus marquantes, et à l'appendice C du présent texte pour son lien avec [Ra].

§1 Préparatifs

On reprend les hypothèses du théorème, et on considère une k-isogénie ϕ d'une courbe elliptique E'/k vers E, dont on note N le degré. On désigne par $C_1, C_2, \ldots$ des nombres réels > 0 effectivement calculables en fonction de d et de δ. Enfin, toutes <u>les hauteurs sont logarithmiques</u>.

Proposition 1: *il existe deux* k-*formes différentielles de 1ère espèce* ω (resp. ω')*sur* E (resp. E') *vérifiant les propriétés suivantes:*

i) $g_2(E,\omega)$ *et* $g_3(E,\omega)$ *sont des éléments de* k *de hauteurs majorées par* $C_1\gamma$;

ii) $\phi^*\omega = \beta\omega'$, *où* β *est un élément de* k *de hauteur* $\leq C_2 \operatorname{Log}N$;

iii) $g_2(E',\omega')$ *et* $g_3(E',\omega')$ *sont des éléments de* k *de hauteurs majorées par* $\gamma' = C_3(\gamma + \operatorname{Log}N)$.

Corollaire : *même énoncé avec* $\beta = 1$ (remplacer ω' par $\beta\omega'$).

<u>Démonstration</u> : Soient $\mathbf{E}$, $\mathbf{E'}$ les modèles de Néron de E , E' sur l'anneau O des entiers de k . Pour clarifier les idées, je décris tout d'abord la démonstration dans le cas où O est principal. Les O- modules $\omega_{\mathbf{E}}$ (image réciproque de $\Omega^1_{\mathbf{E}/O}$ par la section nulle) et $\omega'_{\mathbf{E'}}$ sont alors libres. J'en fixe des générateurs ω , ω' : ils ne sont définis qu'aux unités de k près, et c'est sur elles qu'on va jouer.

i) Sans perte de généralité, on peut supposer que l'équation de Weierstrass de E donnée par l'énoncé du théorème a des coefficients entiers (chasser les dénominateurs, qui sont majorés par $\exp(C_4\gamma)$).

Son discriminant est alors un élément de O de norme $\leq \exp(C_5\,\gamma)$, et il en est de même de $\Delta(E,\omega)$, qui le divise, et est bien entier en vertu des propriétés d'intégralité de la forme modulaire Δ (cf. [Ka], §1 , dont je rappelle d'ailleurs le principe plus loin). Il existe donc (Dirichlet) une unité ε de k telle que $\Delta\,(E,\,\omega/\varepsilon) = \varepsilon^{12}\,\Delta\,(E,\,\omega)$ soit de hauteur $\leq C_6\gamma$. La forme différentielle ω/ε (que nous convenons de rebaptiser ω) répond alors à la question.

ii) Les isogénies s'étendant aux modèles de Néron (voir [Ra]) , $\phi^*\omega$ est une section de $\omega_{E'}$, et il existe un élément β de O tel que $\phi^*\omega = \beta\omega'$. Le même raisonnement, appliqué à l'isogénie duale ϕ' de ϕ , fournit un élément β' de O tel que $\phi'^*\omega = \beta'\omega$. Mais alors, $\beta'\beta\omega = (\phi\phi')^*\omega = N\omega$, et l'entier rationnel $\mathrm{Norm}_{k/\mathbf{Q}}\beta$ divise N^d . Il existe donc une unité ε' de k telle que $\beta\varepsilon'$ soit de hauteur majorée par $C_7\mathrm{Log}N$, et la forme différentielle ω'/ε' (que nous rebaptiserons ω') vérifie ii).

iii) Montrons tout d'abord que $g_2(E',\,\omega')$ et $g_3(E',\,\omega')$ sont essentiellement des entiers de k . Il suffira alors, pour borner leurs hauteurs, de majorer leurs différentes valeurs absolues archimédiennes.

Si v est une place finie de k première à 6 , g_2 et g_3 , qui sont des formes modulaires entières sur O_v (cf. [Ka1, §1), prennent des valeurs dans O_v dès que ω' engendre $\omega_{E'}$ localement en v . Idem aux places divisant 6 , à des dénominateurs universellement bornés près. Les dénominateurs de $g_2(E',\,\omega')$ et $g_3(E',\,\omega')$ divisent donc un entier $C_8(k)$.

Passons aux places archimédiennes de k , que nous allons traiter suivant les techniques modulaires de [Ma1], §3 et [Ma3] . Soit v l'une d'elles. <u>Désignons, pour tout réseau Λ de $\mathbf{C}$, par $\varpi(\Lambda)$ le minimum des valeurs absolues de ses éléments non nuls</u>. Comme toute forme modulaire pour $SL_2(\mathbf{Z})$, soit f , de poids w(f) , est par définition bornée sur le domaine fondamental usuel, la fonction de réseaux $|f(\Lambda)|\,\varpi(\Lambda)^{w(f)}$

est bornée supérieurement. Les réseaux de périodes Λ_v, Λ'_v de ω et de ω' qui correspondent à v vérifiant $\beta^{-1}\Lambda'_v \subseteq \Lambda_v$, donc en particulier $\varpi(\Lambda'_v) \geq |\beta|_v\, \varpi(\Lambda_v)$, on en déduit :

$$\sup\{|g_2(\Lambda'_v)|_v^{1/2}, |g_3(\Lambda'_v)|_v^{1/3}\} \leq c\ |\beta|_v^{-2}\, \varpi(\Lambda_v)^{-2},$$

où c est une constante universelle, d'où, grâce à la majoration de la hauteur de β fournie par i) :

$$\mathrm{Log}\ \sup\{|g_2(E',\omega')|_v^{1/2}, |g_3(E',\omega')|_v^{1/3}\} \leq C_9(\mathrm{Log}N - \mathrm{Log}\ \varpi(\Lambda_v)).$$

Il reste à minorer $\varpi(\Lambda_v)$ en fonction de γ. Pour cela, complétons l'un des éléments ω_1 de Λ_v qui donne $\varpi(\Lambda_v)$ en une base directe $\{\omega_1, \omega_2 = \tau\omega_1\}$ de ce réseau, de sorte que (Hermite) $\mathrm{Im}\tau$ est $\geq \sqrt{3}/2$. La connaissance des zéros des fonctions $E_4(\tau)$ et $E_6(\tau)$ dans ce domaine entraîne que l'expression

$$\sup\{|g_2(\Lambda_v)|^{1/2}, |g_3(\Lambda_v)|^{1/3}\}\, \varpi(\Lambda_v)^2$$

est universellement minorée, et on déduit de l'inégalité de la taille la minoration : $\mathrm{Log}\ \varpi(\Lambda_v) \geq - C_{10}\,\gamma$. Предложение доказано (pour O principal).

Pour passer au cas général, il suffit de noter que tout O-module de rang 1 sans torsion admet un sous-O- module libre d'indice majoré par la racine carrée de la valeur absolue du discriminant de k. Grâce aux relations $g_\kappa(E, \lambda\omega) = \lambda^{-2\kappa} g_\kappa(E,\omega)$, les arguments précédents s'adaptent alors aisément en autorisant aux entiers de k qui y apparaissent d'avoir des dénominateurs divisant ces indices.

Remarque: **(i)** La démonstration (à la fois plus simple et plus précise !) que donne [Ma4] du corollaire à la Proposition 1 repose sur la formule suivante. Si Λ' est un sous-groupe d'indice N d'un réseau Λ, le réseau $N\Lambda$ est inclus dans Λ', et l'on a (d'après Eisenstein) :

$$g_\kappa(\Lambda') = g_\kappa(N\Lambda) + \varepsilon_\kappa \sum_x \wp^{(2\kappa-2)}(x, N\Lambda) \quad ,$$

où x parcourt un système de représentants de $\Lambda'/N\Lambda$, $\wp$ désigne la fonction de Weierstrass usuelle et ε_κ est une expression simple. Les propriétés arithmétiques standard des points de torsion conduisent alors aux estimations souhaitées, avec des constantes C_1, C_2, C_3 *ne dépendant maintenant plus que de* d .

Je me place désormais sous les hypothèses du corollaire à la proposition 1 . Dans la démonstration qui suit, on va privilégier une place archimédienne de k (choisie arbitrairement). Cela revient à considérer une fois pour toutes k comme un sous-corps de **C** , et , en particulier, E et E' comme des courbes elliptiques complexes. Nous désignerons par Λ , Λ' les réseaux de périodes de ω , ω' , par Ω_1 , Ω' des éléments non nuls de Λ , Λ' de valeurs absolues minimales, et par Ω_2 un élément de Λ tel que $\tau = \Omega_2/\Omega_1$ appartienne au domaine fondamental que l'on sait et représente la classe d'isomorphisme de E/**C** . Dans ces conditions, on peut énoncer, avec des constantes C_{11},... ne dépendant ici que de d :

Proposition 2 : (voir [Ma3]) *On a :* $|\mathrm{Log}\, \varpi(\Lambda_v)| \leq C_{11}(d)\, \gamma$. *En particulier,*
i) *le logarithme de la valeur absolue de* Ω' *est majoré par* $C_{11}\gamma'$;
ii) *le logarithme de la valeur absolue de* Ω_1 *(et donc de* Ω_2*) est minoré par* $- C_{11}\, \gamma$;
iii) *il existe deux entiers rationnels* b_1, b_2, *de valeurs absolues majorées par* $\exp(C_{12}(d)(\gamma + \gamma'))$, *tels que* $\Omega' = b_1 \Omega_1 + b_2 \Omega_2$.
Par ailleurs, $|\Omega_2/\Omega_1| \leq C_{13}(d)\gamma$.

<u>Démonstration</u>: la première assertion vient d'être démontrée (la minoration explicitement; reprendre l'argument sur $|f(\Lambda)|\, \varpi(\Lambda)^{w(f)}$ et y adjoindre l'inégalité de la taille pour la majoration). L'existence d'entiers b_1, b_2 vérifiant la relation de iii) étant claire ($\phi^*\omega = \omega'$!), leur majoration résulte alors de i) , de ii), et de la quasi-orthogonalité de la base $\{\Omega_1,\Omega_2\}$. Quant à la dernière assertion, on la lit directement sur le développement de Fourier de la fonction $j(\tau)$. (Noter, à ce propos, le changement d'échelle: le premier minimum de la norme sur Λ peut atteindre e^{γ} , mais le second ne dépassera pas γe^{γ} .)

§2 Passage à la transcendance

L'énoncé-fleuve qui suit sera démontré au §3. J'explique ici comment le théorème de l'introduction s'en déduit.

Proposition 3 : *Pour tout entier* $d \geq 1$, *il existe un nombre réel* $c'(d)$ *effectivement calculable en fonction de* d *et vérifiant la propriété suivante. Fixons un corps de nombres* k *de degré* d *sur* $\mathbf{Q}$, *des nombres réels* $g, g', r, r', B \geq 1$, *deux réseaux* Λ, Λ' *de* $\mathbf{C}$ *d'invariants dans* k *de hauteurs majorées par* g, g' *et un entier* n *égal à* 1 *ou* 2. *Supposons qu'il existe* n *éléments* $\Omega_1, \ldots, \Omega_n$ *de* Λ *linéairement indépendants sur* $\mathbf{Z}$ *et de valeurs absolues* $\leq \varpi(\Lambda)\, r$, *tels qu'une combinaison linéaire non triviale* $\Omega' = b_1 \Omega_1 + \ldots + b_n \Omega_n$ *à coefficients entiers de valeurs absolues* $\leq B$ *appartienne à* Λ' *et soit de valeur absolue* $\leq \varpi(\Lambda')\, r'$. *Posons enfin* : $h = g + g' + r^2 + r'^2 + \mathrm{Log}\, B$. *La propriété suivante est alors satisfaite* .

Plongeons de la façon usuelle les courbes elliptiques $E = \mathbf{C}/\Lambda$ *et* $E' = \mathbf{C}/\Lambda'$ *dans des plans projectifs, puis la variété abélienne* $G_n = E' \times E^n$ *dans un espace projectif par le biais d'un plongement de Segre . Repérons d'autre part l'espace tangent à l'origine de* G_n ,*qui s'identifie par construction à* $\mathbf{C} \times \mathbf{C}^n$, *au moyen des variables* $\{z', z_1, \ldots, z_n\}$, *et notons* V_n *son hyperplan d'équation :* $z' = b_1 z_1 + \ldots + b_n z_n$. *Il existe alors une sous-variété abélienne non triviale* H *de* G_n , *de degré projectif majoré par* $\delta_n = c'(d)\, h^{3n}$, *dont l'espace tangent à l'origine est contenu dans* V_n .

Corollaire : *sous les hypothèses de la proposition* 3 *où l'on peut toujours supposer que* n *vaut* 2 *), il existe une isogénie de* E' *vers* E *définie sur* k *et de degré majoré par* $c''(d)\, h^{24}$, *où* $c''(d)$ *est effectivement calculable en fonction de* d .

Vérifions qu'on a alors bien démontré le théorème principal, avec $C = 49$, et $c(d)$ remplacé par une constante effective $c(k) = c(d,\delta)$. Soient donc E' une courbe elliptique définie sur k et k-isogène à E , et N le minimum des degrés des k-isogénies liant E et E'. D'après les propositions 1 et 2, les hypothèses de la proposition 3 sont satisfaites avec $n = 2$, $g = \gamma$, $r = C_{13}\,\gamma$, $r' = 1$, $g' = \gamma' = C_3(\gamma + \mathrm{Log}\, N)$, et $\mathrm{Log}\, B = C_{12}(\gamma + \mathrm{Log}\, N)$, d'où : $h = C_{14}\,(\gamma^2 + \mathrm{Log}\, N)$. Le degré de l'isogénie que fournit son corollaire est, comme il se doit, minoré par le minimum N. Ainsi, $N \leq C_{15}\,(\gamma^2 + \mathrm{Log}\, N)^{24}$, donc : $N \leq c(k)\,\gamma^{49}$. (La remarque (i) permettrait bien entendu de supprimer ici la dépendence en δ.)

Remarques : **(ii)** L'unique hypothèse qualitative de la proposition 3 (à savoir que $\Lambda \cap \Lambda'$ n'est pas réduit à O) ne présuppose pas que les courbes elliptiques $\mathbf{C}/\Lambda$ et $\mathbf{C}/\Lambda'$ soient isogènes. Mais c'en est un corollaire, en vertu d'un vieux théorème de Schneider (il s'agit donc bien d'un énoncé de transcendance !).

(iii) Pour l'application qu'on a en vue, V_n n'est autre que l'espace tangent à l'origine du noyau de l'homomorphisme $\{P', P_1, \ldots, P_n\} \to \phi(P') - b_1P_1 - \ldots - b_nP_n$ de $E' \times E^n$ dans E (rappelons que $d\phi$ est représenté par la matrice 1). Le degré de la composante neutre H_n de ce sous-groupe algébrique croît polynômialement avec B, alors que le degré du sous-groupe H fourni par la conclusion de la proposition 3 est majoré par un polynôme en $\mathrm{Log} B$. Cette réduction au logarithme des estimations triviales est typique de la méthode de Baker (voir [Be2], Proposition 8).

(iv) Pour démontrer le corollaire à la proposition 3, point n'est besoin de préciser *le corps de définition de l'isogénie* ψ (de degré $\nu \leq c''\, h^{24}$) qu'il fournit. En effet, dans le cas général où le corps de base k contient le corps de définition de tous les endomorphismes de E, toute isogénie de E' vers E est automatiquement définie sur k (puisque sa duale, composée avec la k-isogénie donnée par hypothèse, est un endomomorphisme de E). Sinon, E admet des multiplications complexes par un ordre $\mathcal{R}$ d'un corps quadratique imaginaire non contenu dans k, et il suffit de noter que, dès qu'elle est non nulle, la somme de ψ et de sa conjuguée sous $\mathrm{Gal}(k.\mathcal{R}/k)$ est de degré $\leq 2\nu$. Si enfin ψ est de trace nulle, sa composée avec tout élément imaginaire pur α de $\mathcal{R}$ est une k-isogénie de E' vers E de degré $\leq v\ |\alpha|^2$; or il existe un tel élément α de norme sur **Q** majorée par la valeur absolue D du discriminant de R , et D est borné par c'''(d) (d'après Gross- Zagier...). Au risque d'abîmer un peu la constante C du théorème, mais de façon plus réaliste, on majorera D par $C_{18}(d)\, g^2 \leq C_{18}\, h^2$, grâce à la dernière assertion de la proposition 2 , appliquée au conjugué $j(R\ )$ de $j(\tau)$ (voir [F-P]).

Nous montrons maintenant comment la proposition 3 entraîne son corollaire. Retenons de sa conclusion que H est un sous-groupe connexe non trivial de G_n ne contenant pas E' et distinct de E^n (puisque Lie H est inclus dans V_n et que $b_1, \ldots, b_n$ ne sont pas tous nuls).

a) Supposons tout d'abord que les hypothèses de la proposition 3 soient satisfaites avec n = 1 . Le sous-groupe H de sa conclusion ne peut être qu'une courbe elliptique dans $E' \times E$, passant par l'origine et se projetant surjectivement sur chacun de ces deux facteurs . Ces projections sont donc des isogénies de H vers E et E' . Si d , d' désignent leurs degrés respectifs, le degré projectif H.(3E' + 3E) de H vaut 3(d + d') et en composant l'une avec la duale de l'autre, on obtient une isogénie de degré dd' $< \delta_1^{\,2} \ll h^6$ entre E et E' .

Si maintenant les hypothèses de la proposition 3 ne sont vérifiées qu'avec n = 2 , on distingue deux cas :

b) le sous-groupe connexe H de $E' \times E^2$ se projette surjectivement sur E' : si c'est une surface, la composante neutre de son intersection avec $E' \times E \times \{0\}$ -ou, si $b_1 = 0$, avec $E' \times \{0\} \times E$ - fournit une correspondance
du même type que supra (avec δ_1 remplacé par $3\delta_2$), d'où une isogénie entre E et E' de degré $\ll h^{12}$; si c'est une courbe, la composée de sa projection sur $E \times E$ avec la projection sur l'un des facteurs E est une isogénie de degré $\leq \delta_2$, et on aboutit à la même conclusion.

c) H est un sous-groupe connexe, et *propre* de $E \times E$. La considé- ration du quotient G_2/H va alors permettre de se ramener au cas n = 1 . Pour clarifier l'argument, je repousse à la remarque (vi) ci-dessous le cas de multiplications complexes (qu'on pouvait d'ailleurs traiter directement) et suppose que E n'en a pas. Le sous-groupe de $\mathrm{Hom}(E^2, E) \approx \mathbf{Z}^2$ formé des homomorphismes $u = (u_1, u_2)$ dont le noyau contient H est dans ce cas engendré par un élément (u_1, u_2) de $\mathbf{Z}^2$ vérifiant $|u_1|^2 + |u_2|^2 = \deg(H)/3$ (noter que u_1 et u_2 sont premiers entre eux - puisque H est connexe -, et appliquer à l'homomorphisme dual de u le lemme 3 de [Be3]; voir aussi [M-W1], III). Comme Lie(H) coïncide avec $V_2 \cap \mathrm{Lie}(E^2)$, ce sous-groupe contient (b_1, b_2) , et il existe un entier rationnel b tel que $(b_1, b_2) = b.(u_1, u_2)$. Mézalor, $\Omega = u_1\Omega_1 + u_2\Omega_2$ est un élément de Λ de valeur absolue $|\Omega| \leqslant \varpi(\Lambda)r^{\#}$, où $r^{\#} = 2r\sqrt{\delta_2}$, tel que :

$$\Omega' = b\Omega ,$$

où $|b| \leq B$. Bref, les hypothèses de la proposition 3 sont vérifiées avec h remplacé par $h^{\#} = g + g' + 4r^2\delta_2 + r'^2 + \mathrm{Log}\, B \leq C_{19}\, h^7$, et surtout, bien sûr, $n = 1$. D'après a), il existe donc une isogénie de E' vers E de degré $<< h^{\#3} << h^{21}$. QED (pour $\mathrm{End}\, E = \mathbf{Z}$).

Bien entendu, le point fondamental cette dernière réduction est qu'elle n'a guère augmenté la valeur absolue des périodes considérées : écrire $\Omega' = \Omega$, avec $\Omega = b_1\Omega_1 + b_2\Omega_2$ pour se placer dans le cas $n = 1$ transforme h en hB , ce qui serait rédhibitoire.

Remarques : (v) "v-*rang* " *d'une isogénie* : replaçons-nous dans la situation du §1. Le plus petit des entiers n vérifiant les hypothèses de la proposition 3 pour des valeurs de r' et Log B polynômiales en le *logarithme* du degré de l'isogénie ϕ est un analogue (lointain) du p-rang des isogénies, relativement à la place archimédienne v de k qu'on a privilégiée; Log B correspond alors au niveau des p-isogénies de [Ra], §4 . Dans cette optique, la preuve du corollaire peut se résumer ainsi: en général (cas b), le sous-groupe H de G_2 définit une "bonne" correspondance entre E et E' , et on a gagné; quand ce n'est pas le cas (cas c), ϕ est en fait de "v-rang" 1 , et (cas a) le sous- groupe H de G_1 que fournit la proposition 3 est encore une "bonne" correspondance entre E et E' . De façon plus sérieuse, les Chudnovsky ont remarqué qu'on peut toujours prendre $n = 1$ si v est une place réelle. Cela leur a donné la première démonstration transcendante du théorème de l'introduction, lorsque k admet un plongement réel ([Ch],§4). Voir [Be1] (corollaire au théorème 2) pour une autre apparition de cette notion de v-rang.

(vi) *Le cas de multiplications complexes.* Pour le traiter, le plus simple consiste à réécrire l'hypothèse de la proposition 3 sous la forme : $\Omega' = b\Omega$, où b est cette fois un élément de l'anneau R des endomorphismes de E (autrement dit, le v-rang sur R vaut toujours 1). La preuve du §3 s'étend sans difficulté, et on conclut comme en a) . On peut aussi (en remplaçant **Z** par R) reprendre l'argument précédent et ce, presque mot pour mot si R est principal (la rationnalité de b_1 et b_2 et la coprimalité de u_1 et u_2 entraînent que sans en changer les valeurs absolues, les éléments b , u_1 et u_2 de R peuvent être choisis rationnels). Si R n'est pas principal, le R -module $\mathrm{Hom}(E^2, E)$ contient un sous-R -module libre d'indice majoré, avec les notations de la remarque iv), par $\sqrt{D}$. On aboutit alors à une relation de la forme $\Omega'^* = b^*\Omega^*$, avec $|b^*| \leqslant \sqrt{D}B$, $r^* \leq \sqrt{D}r'$, $r^* \leq \sqrt{D}r^{\#}$, d'où une isogénie de degré $\ll h^{*3}$, où $h^* = \sqrt{D}h^7$. Les majorations de D données à la remarque (iv) permettent de conclure.

§3 La méthode de Baker

On reprend les notations de la proposition 3 , qu'on va maintenant démontrer. On désigne de plus par $\wp = \wp(z, \Lambda)$, $\wp' = \wp(z,\Lambda')$ les fonctions de Weierstrass associées aux réseaux Λ , Λ' (l'apostrophe n'est donc pas une dérivation). Les expressions $c_1, c_2, \ldots$ représentent désormais des nombres réels > O effectivement calculables en fonction du seul degré d de k sur **Q** .

Je regroupe tout d'abord les estimations, de nature analytique ou arithmétique, auxquelles on fera appel (la seconde, qui concerne le type de croissance de certaines fonctions thêta, est cruciale). J'exprime les résultats sur le réseau Λ , mais c'est leur analogue sur Λ' qui importe le plus dans les applications.

Proposition 4 (voir [Ma3]) : i) *pout tout couple* $\{t , \ell\}$ *d'entiers* ≥ 1, *la dérivée d'ordre* t *de* $\wp^{\ell}(z, \Lambda)$ *s'exprime comme un polynôme de degré* $\leq c_1(t+\ell)$ *en* $g_2(\Lambda)/2$, $\wp(z,\Lambda)$ *et sa dérivée première, à coefficients entiers de valeur absolue* $\leq c_1(t+\ell)\,\mathrm{Log}(t+\ell)$;

ii) *il existe une fonction thêta* $\theta = \theta(z,\Lambda)$ *associée au diviseur polaire de* $\wp$ *telle que, pour tout nombre complexe* z :

$$|\,\mathrm{Log}\max(|\theta(z)|, |\theta\wp(z)|)\,| \leq c_2\,(g + (|z|/\varpi(\Lambda))^2)$$

(noter les valeurs absolues au premier membre);

iii) *pour tout couple* $\{n,q\}$ *d'entiers* ≥ 1 , *et tout élément* Ω *de* Λ , *le nombre* $\wp(n\Omega/q)$, *s'il est défini, est algébrique sur* k , *de degré* $< q^2$, *et de hauteur (absolue)* $\leq c_3 g$;

iv) *pour tout couple* $\{n,q\}$ *d'entiers* ≥ 1 , *et tout élément* Ω *de* Λ *de valeur absolue* $\leq \varpi(\Lambda)\,t$, *le nombre* $\theta(n\Omega/q)$, *s'il est non nul, est de valeur absolue* $\geq \exp(-\,c_4\,(gq^2 + t^2(n/q)^2))$.

Démonstration: pour i), voir [Ba] , ou [Ma3] (ou encore [Da]); comme le covolume de Λ est minoré par $\varpi(\Lambda)^2/2$ (Hermite), ii) résulte immédiatement de [Co] ou de [F-P], dont on trouvera d'ailleurs des formes raffinées, et plus suggestives, dans [Ma3] et dans [Da]; iii) résulte de l'énoncé bien connu de Demjanenko-Zimmer (voir aussi [M-Z]); on en déduit que $|\wp(n\Omega/q)|$ est $\leq \exp(c_5 g q^2)$, et la minoration sous-jacente à ii) conduit à iv).

Remarque : (vii) Suivant une remarque de B. Mazur, la fonction thêta en question est un avatar archimédien de la fonction thêta p-adique canonique du cas ordinaire. En fait, le lemme 1.3.6 de [Ka 2] montre que la fonction $\theta(z)$ du lemme 3.1 de [Ma3] coïncide, à un facteur trivial près, avec le carré de la fonction $\Delta(\Lambda)^{1/12}\sigma(z,\Lambda)\exp(-s_2(\Lambda)z^2/2)$, où les notations σ et s_2 ont leur signification usuelle.

Passons à la démonstration de la proposition 3 . Je la détaille sous l'hypothèse (plus délicate, même si la conclusion en est moins précise) où n vaut 2 , et indique à la fin comment choisir les paramètres quand $n = 1$. J'omettrai l'indice 2 des notations G_2 , V_2 , δ_2 de la proposition.

1ère étape [Siegel: *construction d'un diviseur* Z *sur* $G = E' \times E^2$ *admettant* *un gros sous-schéma ponctuel supporté par l'origine*] Posons

$$L = 4\,d\,h^6 , \quad T = h^9 ,$$

toujours avec $h = g + g' + r^2 + \mathrm{Log}\,N$, et notons Ω le point $(\Omega', \Omega_1, \Omega_2)$ de $\mathbf{C}^3$. Il existe un polynôme $P(X, X_1, X_2)$ non nul de degrés partiels $\le L$, à coefficients entiers rationnels de hauteur $\eta \le c_6 h^{10}$, tel que la fonction

$$F(z', z_1, z_2) = P(\wp'(z'), \wp(z_1), \wp(z_2))$$

s'annule au point $(1/2)\Omega$ à un ordre de multiplicité $\ge T$ selon le champ de 2-directions défini par V .

Voici pourquoi : considérons la base

$$\{\partial_1 = b_1 \partial/\partial z' + \partial/\partial z_1 , \partial_2 = b_2 \partial/\partial z' + \partial/\partial z_2\}$$

de V . Par définition, on demande à F que toutes ses dérivées partielles d'ordre $< T$ en ∂_1 et ∂_2 s'annulent en $\Omega/2$. Il s'agit donc de résoudre un système linéaire d'ordre $< T^2$ en plus de L^3 variables, à coefficients dans un corps de nombres de degré $\le 9\,d$. D'après les assertions i) et iii) de la proposition 4 , le maximum de l'exponentielle des hauteurs (et d'un dénominateur commun) de ces coefficients est majoré par

$$B^T e^{c_7 (g + g')(L+T)} e^{c_8 (T+L)\mathrm{Log}(T+L)} ,$$

et le lemme de Siegel permet de conclure. Le diviseur effectif Z sur G correspondant au diviseur de la fonction analytique en $\mathbf{z} = (z', z_1, z_2)$:

$$\Theta(z) = (\theta'(z'+\Omega'/2)\theta(z_1+\Omega_1/2)\theta(z_2\Omega_2/2))^L F(z + \Omega/2) ,$$

passe alors par l'origine avec une multiplicité $\ge T$ le long de V .

<u>2ème étape</u> [extrapolation: *le diviseur* Z *passe en fait par un sous-groupe cyclique* Γ *pas trop petit de* G *, toujours avec forte multiplicité le long de* V (c'est, avec la définition même des coefficients de V , le seul passage analytique de la preuve)] . Soit q le plus petit entier impair tel que

$$q \ge h^{1/13} .$$

On va montrer que la fonction Θ s'annule en tous les multiples entiers de $(1/q)\Omega$ avec un multiplicité $\ge T/2$ le long de V . Soit donc $s\Omega/q$ un tel point, avec, sans perte de généralité, $|s| < q$.

Par périodicité, la fonction Θ s'annule en tous les multiples entiers de Ω avec une multiplicité $\geq T$ le long de V. Considérons alors la fonction d'une variable $f(z) = D\Theta(z\Omega)$, où D est un monôme différentiel d'ordre $\tau < T/2$ en les dérivations ∂_1, ∂_2 de V, tel que $D'\Theta(s\Omega/q)$ soit nul pour tout opérateur D' de ce type et d'ordre $< \tau$. La fonction f s'annule en tous les entiers à un ordre $\geq T - \tau \geq T/2$, et d'après les inégalités de Cauchy, la proposition 5, ii) et la majoration donnée des valeurs absolues des coefficients de Ω, son maximum sur un disque de rayon $R \geq 1$ vérifie :

$$|f|_R \leq (L+1)^3 e^{\eta}(BT)^T e^{c_2(2g+g'+4R^2(2r^2+r'^2))L}.$$

Le lemme de Schwarz, appliqué sur les disques de rayon $R = h^{3/2}$ et $3R$, entraîne alors que :

$$\operatorname{Log}|D\Theta(s\Omega/q)| \leq \operatorname{Log}|f|_1 \leq \operatorname{Log}|f|_R \leq -TR + \operatorname{Log}|f|_{3R} \leq -c_9 h^{10,5},$$

et on déduit de la formule de Leibniz, jointe à la définition de D et à la proposition 4, iv), que le nombre $\xi = DF(s\Omega/q + \Omega/2)$ vérifie :

$$\operatorname{Log}|\xi| \leq c_{10}((g+g')q^2 + r^2 + r'^2)L - c_9 h^{10,5} \leq -c_{11}h^{10,5}.$$

Mais d'après la proposition 4, iii), ce nombre est algébrique sur k, de degré $\leq 36\, q^6$, et de hauteur (absolue) majorée, à un facteur constant près, par

$$T \operatorname{Log} B + \operatorname{Log} H + \operatorname{Log} L + (T + L)(g + g' + \operatorname{Log}(L + T)) \leq c_{12}h^{10}.$$

Comme dq^6h^{10} est beaucoup plus petit que $h^{10,5}$ (pour $h > c_{13}$), la formule du produit impose à ξ d'être nul, et Θ s'annule bien en $s\Omega/q$ à un ordre $\geq T/2$ le long de V. En d'autres termes, le diviseur Z de G passe par le sous-groupe cyclique Γ engendré par $\exp_G(\Omega/q)$ avec une multiplicité $\geq T/2$ le long de V.

<u>3ème étape</u> [Le paradis des lemmes de zéros] On va faire appel au lemme de multiplicité de [Ph], dont je transcris maintenant l'énoncé dans notre contexte. La constante (effective) c qui y apparaît ne dépend que du plongement projectif de G.

Proposition 5 (Philippon) : *Soient* G *une variété abélienne plongée*

dans un espace projectif , λ *et* τ *deux entiers* ≥ 1 *,* Γ *un sous-groupe fini de* G *,* V *une sous espace de* Lie G *et* Z *un diviseur effectif sur* G *, de degré projectif* λ *. On suppose que* Z *passe par* Γ *avec un ordre de multiplicité* $\geq$ (dimG) τ *le long de* V *. Il existe alors une sous-variété abélienne* H *de* G *, distincte de* G *, telle que*

$$\tau^{\dim \pi_*(V)} \operatorname{card}(\pi(\Gamma)) \deg(H) \leq c\, \lambda^{\dim \pi(G)} ,$$

où π *désigne la projection de* G *sur* G/H .

D'après le 2ème pas, le diviseur Z construit au 1er pas vérifie les hypothèses de la proposition 5 avec $\tau = T/6$, $\lambda = c_{14} L$ et un sous-groupe Γ de cardinal q (on peut en effet supposer sans perte de généralité que $\boldsymbol{\Omega}$ est une période primitive du réseau $\Lambda' \times \Lambda^2$ de $\mathbf{C}^3$). Que peut-on alors dire de la sous-variété abélienne H de sa conclusion?

- elle ne peut être réduite à O , puisque $T^{\dim(V)} q = T^2 q$ est bien plus grand que $L^{\dim(G)} = L^3$;

- les sous-variétés abéliennes H dont l'algèbre de Lie n'est pas contenue dans V vérifient V + Lie H = Lie G , d'où $\dim \pi_*(V) = \dim \pi(G)$, et sont également exclues, en vertu de l'inégalité $T >> L$.

Ainsi, H est un sous-groupe algébrique connexe non trivial de G , d'algèbre de Lie contenue dans V , et de degré projectif

$$\deg H \leq c_{14}\, L\, (L/T)^{\dim(V/\mathrm{Lie}\ H)} \leq c'(d)\, h^6$$ (pour n = 2) .

Enfin, la démonstration précédente s'adapte facilement au cas n = 1 , où on pourra choisir comme paramètres :

$L = 4d\, h^3$, $T = h^6$, $\eta \approx h^7$, et R , q comme plus haut.

Remarques : (viii) Si les paramètres L et T de la construction du 1er pas expriment des conditions géométriques évidentes sur Z , c'est en *théorie d'Arakelov* que le paramètre η prend une signification naturelle : on peut en effet définir grâce à lui des métriques sur les fibrés $\mathcal{O}_G(L) \otimes k_v$ telles que le polynôme auxiliaire P s'interprète comme une section du fibré d'Arakelov correspondant. La référence au lemme de Siegel (c'est à dire au principe des tiroirs), plutôt qu'au théorème de

Minkowski, pour justifier l'existence d'une telle section, est standard en transcendence.

(ix) Dans le 2ème pas, le fait que ξ puisse être de degré élevé sur k joue contre nous. C'est pourtant bien ce qui se produit (d'après les théorèmes d'irréductibité de Serre). Il est cocasse que l'énoncé auquel on en a permette de raffiner une partie de ces théorèmes...

(x) Il n'est pas sans intérêt de noter que des énoncés similaires à la proposition 5 du 3ème pas (mais moins généraux) apparaissent également dans la démonstration "algébrique" des théorèmes de Faltings. Voir par exemple [MB], lemme 3.2.3 (contrairement à [Ph], la preuve de ce lemme de zéros ne fait d'ailleurs pas explicitement appel à la théorie de l'intersection).

(xi) La démarche de la démonstration ci-dessus, et de la réduction par passage au quotient du §2 , cas c , est inspirée de la preuve de la proposition 8 de [Be2] (voir [Wü] pour un analogue multiplicatif). Il est probable que la présentation donnée dans [P-W] de la méthode de Baker permette d'obtenir directement (i.e. sans hypothèse sur la valeur de n) la correspondance recherchée entre E et E' , et même d'éviter le recours aux points de division par q dans le lemme de zéros.

(xii) *Des courbes aux points* : La même méthode de transcendance permet d'établir le résultat suivant : si des points $P_1, \ldots, P_n$ de $E(k)$, de hauteurs de Néron-Tate $\leq \eta$, sont linéairement dépendants sur **Z** (on voudrait dire "isogènes entre eux dans leur ensemble"), ils sont nécessairement liés par une relation de dépendance linéaire à coefficients entiers de valeurs absolues (on voudrait dire, avec beaucoup de guillemets,"une isogénie de degré") $\leq c(E,n,k)\ \eta^{n-1}(\mathrm{Log}\ \eta)^{c(n)}$. Mais des méthodes purement algébriques - et tout aussi effectives - y conduisent également, sans même le terme en Log (cf. [Ma2] , [Be3]) . Il serait intéressant de traduire tout ceci en termes de 1-motifs.

Appendice

A) *Une chasse aux discriminants* : dans la version affaiblie que nous venons d'établir du théorème de [M-W2] , la dépendance de la "constante" c(k) en la valeur absolue δ du discriminant de k sur **Q** n'apparaît que par le biais de la constante C_3 de la proposition 3, et on vérifie aisément que c(k) est, à un facteur explicite en d près, de la forme $(\mathrm{Log}\ \delta)^{C'}$, où $C' = C-1$. Quitte à augmenter la constante C , on peut alors supprimer cette dépendance en δ . A titre de curiosité (puisqu'il est bien plus simple d'appliquer la remarque (i)), nous indiquons ici pourquoi.

Notons tout d'abord k_0 le corps de définition du modèle de Weierstrass de E donné dans l'énoncé du théorème, et N le degré de la k-isogénie dont on part. D'après l'inégalité de Hadamard (voir l'addendum de [Si]), le logarithme de la valeur absolue du discriminant de k_0 sur **Q** est $\ll \gamma$ (les constantes implicites de ce paragraphe ne dépendent que du degré d). Du corollaire 2.1.4 de [Ra] , joint au théorème de comparaison des hauteurs stable et modulaire de [MB], on déduit par ailleurs que la hauteur de l'invariant modulaire j(E') de E' est $\ll \gamma + \mathrm{Log}\ N$. Soient alors L_0 le sous-corps de k engendré sur k_0 par j(E') , et E" une courbe elliptique definie sur L_0 , isomorphe à E' sur la clôture algébrique $\overline{k}$ de L_0 , et munie d'un modèle de Weierstrass de hauteur $\ll h(j(E'))$. Il est clair qu'une telle courbe existe, et que l'extension L de L_0 engendrée par les points de 3-torsion de E et de E" est de degré $\leq$ 81d sur **Q** . Toujours d'après [Si], elle vérifie : $\mathrm{Log}|\mathrm{Disc}(L/\mathbf{Q})| \ll \gamma + \mathrm{Log}\ N$. Mais il existe par hypothèse une $\overline{k}$ -isogénie de E" vers E de degré N , et dès que E n'admet comme automorphismes que 1 et -1 (cas auquel on peut, sans perte de généralité, se ramener), un argument classique de cohomologie galoisienne et de rigidité impose à une telle isogénie d'être définie sur L . Le discriminant de L étant maintenant contrôlé, on peut appliquer au triplet (E, E", L) notre version affaiblie du théorème : il existe une L-isogénie de E" vers E de degré $\ll (\gamma + \mathrm{Log}\ N)^{C'} \gamma^{C}$. Idem, donc, avec une $\overline{k}$ -isogénie de E' vers E , donc encore, par l'argument de la remarque (iv), avec une k-isogénie de E' vers E . On conclut comme auparavant, en choisissant N minimal.

Noter que l'extension des scalaires obtenue par adjonction de points de torsion a rendu les courbes E et E" semi-stables. On aurait ainsi pu également contrôler le discriminant du corps de définition de l'isogénie en appliquant à la variété abélienne $E \times E''$ le théorème de lissité de Ribet [Ri].

B) *La constante* C : Tout d'abord, un point technique. On a ici choisi comme échelle de mesure des espaces tangents des tores complexes le minimum ϖ des valeurs absolues non nulles de leurs réseaux de périodes. Il aurait été plus rentable de prendre le covolume de ces réseaux (voir la preuve de la proposition 3, ii)). Cela permet, dans l'application du corollaire à la proposition 3, de prendre r de l'ordre de $\sqrt{\gamma}$, d'où une division de C par 2.

De façon plus fondamentale, on n'a fait appel, dans la formulation de la proposition 3, qu'à "la moitié" de l'information fournie par l'isogénie ϕ, alors que l'assertion iii) de la proposition 2 s'étend sans modification notoire au second minimum de Λ'. Pour en tirer parti, il convient d'étendre la proposition 3 en un énoncé de type "formes linéaires simultanées de logarithmes de points algébriques" (au sens de [P-W]).

En fait, tout porte à croire (voir [Ch], et [La], théorème 6, joint à la proposition 1 du présent texte) que du point de vue transcendant, la valeur optimale de C est 2. La tradition folklorique veut sans doute que C vaille 0 (au moins dans la version affaiblie du théorème), mais cela paraît sans espoir du côté transcendant

C) *Hauteurs* : Dans ce dernier paragraphe, les "constantes" dépendent de d et de δ, et nous nous restreignons pour simplifier aux courbes elliptiques E'/k munies d'une k-isogénie vers E et semi-stables (d'après le théorème de monodromie et le théorème d'Hermite, cette hypothèse est satisfaite sur une extension de k de degré et de discriminant effectivement contrôlés). Une fois le degré minimal N des k-isogénies entre E et E' borné, le corollaire 2.1.4 de [Ra] permet de majorer la valeur absolue m de la différence entre les hauteurs de Faltings $h(E) = h(E/k)$ et $h(E')$ de E et E'. On obtient : $m \ll \operatorname{Log} h(E)$. Au théorème 4.4.9 de [Ra], Raynaud donne une majoration de m *indépendante* du calcul de N, qui entraîne $m \ll (\operatorname{Log} B(E))^2$, où $B(E)$ désigne le maximum des normes des places de mauvaise réduction de E/k, mais est en fait beaucoup plus fine. Il serait intéressant de comparer ces majorations (à l'aide de l'inégalité de Stark, ou, comme dans [La], de la conjecture de Szpiro). De façon plus fondamentale, peut-on *déduire* des résultats de [Ra] une majoration du degré minimal N ?

Bibliographie

[Ba] A. BAKER : On the periods of the Weierstrass $\wp$-function; Symp. Math., 68-69, INDAM, IV, 155-174.

[Be1] D. BERTRAND : Galois orbits on abelian varieties; London M.S. L.N. 1O9, 1986, 21-35.

[Be2] D. BERTRAND : Lemmes de zéros et nombres transcendants; in Astérisque 145 -146 ,1987, 21-44. (Voir aussi: La théorie de Baker revisitée; Probl. Dioph. 84-85, n°2.)

[Be3] D. BERTRAND : Minimal heights and polarizations on abelian varieties; Prep. MSRI, Berkeley, Juin 1987 .

[Co] P. COHEN : Explicit calculation of some effective constants in transcendence theory; in Ph. D. Nottingham, 1985.

[Ch] D. & G. CHUDNOVSKY : Padé approximations and diophantine geometry; Proc. Nat.Ac. Sc. USA, 82, 1985, 2212-2216.

[Da] S. DAVID : Fonctions thêta et points de torsion des variétés abéliennes; CRAS Paris, 305, 1987, 211-214. (Voir aussi : Formes modulaires et dérivées de fonctions thêta; "Problèmes diophantiens" 86-87, n°4.)

[F-P] A. FAISANT- G. PHILIBERT: Approximations simultanées de τ et de $j(\tau)$; "Problèmes diophantiens" 83-84, t. 2, n°2.

[Ka1] N. KATZ : p-adic properties of modular forms and modular schemes ; in Modular Functions III, SLN 350, 1973, 69-190.

[Ka2] N. KATZ : p-adic interpolation of real analytic Eisenstein series; Ann. Math., 104, 1976, 459-571.

[La] M. LAURENT : Une nouvelle démonstration du théorème d'isogénie, d'après [Ch]; Birkhäuser Prog .Math., 71, 1987, 119-131.

[M-Z] Y. MANIN-Y. ZARHIN: Heights on families of abelian varieties; USSR Mat. Sb., 18, 1972, 169-179.

[Ma1] D. MASSER : Small values of heights on families of abelian varieties; SLN 1290, 1988, 109-148.

[Ma2] D. MASSER : Linear relations on algebraic groups; in "New advances in transcendence theory", ed. A. Baker, Cambridge U.P.,1988, 248-262.

[Ma3] D. MASSER : Counting points of small heights on elliptic curves; Bull. SMF, à paraître.

[Ma4] D. MASSER : Exposés en Bavière, été 1988.

[M-W1] D. MASSER-G. WUSTHOLZ : Fields of large transcendence degree generated by values of elliptic functions; Inv. mat. 72, 1983, 407-464.

[M-W2] D. MASSER-G. WUSTHOLZ : Estimating isogenies on elliptic curves ; Invent. math., à paraître.

[MB] L. MORET-BAILLY : Compactifications, hauteurs et finitude; in Astérisque 127, 1985, 113-129.

[Ph] P. PHILIPPON: Lemmes de zéros sur les groupes algébriques commutatifs; Bull. SMF, 114, 1986, 355-383, et 115, 1987, 397-399.

[P-W] P. PHILIPPON - M. WALDSCHMIDT : Formes linéaires de logarithmes simultanées sur les groupes algébriques; à paraître.

[Ra] M. RAYNAUD : Hauteurs et isogénies; Astérisque127, 1985, 199-234.

[Ri] K. RIBET : Endomorphisms of semi-stable abelian varieties over number fields; Ann. Maths 101, 1975, 555-562.

[Se] J-P. SERRE : Abelian ℓ -adic representations and elliptic curves; Benjamin, 1968.

[Si] J. SILVERMAN : The Thue equation and height functions; Birkhäuser Prog. Math., 31, 1983, 259-270.

[Wü] G. WUSTHOLZ: A new approach to Baker's theorem on linear forms in logarihms II; SLN 1290, 1988.

Daniel BERTRAND
Université de Paris VI
Mathématiques, T.46
75 251 Paris Cédex O5.

Astérisque

C. SOULÉ

Théorie de Nevanlinna et théorie d'Arakelov

Astérisque, tome 183 (1990), p. 127-135

<http://www.numdam.org/item?id=AST_1990__183__127_0>

Société Mathématique de France
Astérisque 183 (1990)

THÉORIE DE NEVANLINNA ET THÉORIE D'ARAKELOV

Par C. Soulé*

P. Vojta s'inspire dans [7] de l'analogie entre la théorie des hauteurs et celle de Nevanlinna pour proposer des conjectures très générales sur les équations diophantiennes en dimension arbitraire. Or on constate que l'extension en dimension supérieure de la théorie d'Arakelov ([1][2]) s'appuie sur les mêmes notions fondamentales que la théorie de Nevanlinna [5], en particulier celle de courants de Green (voir la définition au paragraphe 3.1 ci-dessous). Le but de cet exposé est d'illustrer ce fait dans le cas de l'espace projectif. La théorie de Nevanlinna pour la distribution des valeurs des applications holomorphes d'un espace affine dans un espace projectif utilise des courants appelés "formes de Levine" [4] dont on montre qu'ils donnent les classes de Chern du fibré quotient universel en théorie d'Arakelov. Les résultats exposés ici sont repris de [5] et [2].

1. Forme de Levine [4]

Soient $X = \mathbb{P}^n$ l'espace projectif complexe de dimension, n, $X_0,\dots,X_n$ des coordonnées homogènes sur X, $p \geq 1$ un entier, et Y la sous-variété de X d'équation

$$X_0 = X_1 = \dots = X_{p-1} = 0 .$$

On pose

$$\tau = \log\left(|X_0|^2 + |X_1|^2 + \dots + |X_n|^2\right)$$

et

$$\sigma = \log\left(|X_0|^2 + |X_1|^2 + \dots + |X_{p-1}|^2\right).$$

* IHES, 35 Route de Chartres, 91440 BURES sur YVETTE

Si $d = \partial + \bar{\partial}$ est la décomposition standard de la différentielle sur X, on note $d^c = \dfrac{\partial - \bar{\partial}}{4\pi i}$. La forme $\alpha = dd^c\tau$ est lisse sur X, et $\beta = dd^c\sigma$ est lisse sur X - Y.

On appelle <u>forme de Levine</u> la forme différentielle

(1) $$\Lambda = (\tau - \sigma)\left(\sum_{\nu=0}^{p-1} \alpha^{\nu}\beta^{p-1-\nu}\right)$$

sur X - Y. Si $Z = \sum_i n_i Z_i$ est un cycle sur X, on désigne par $\delta_Z = \sum_i n_i \delta_{Z_i}$ le courant d'intégration sur Z.

<u>THÉORÈME 1</u> [4]

La forme Λ *est intégrable sur* X. *Le courant associé* $[\Lambda]$ *vérifie l'équation*

(2) $$dd^c[\Lambda] = \alpha^p - \delta_Y .$$

<u>PREUVE</u> ([2], Prop. 5.1) :

L'éclaté X' de X le long de Y est la sous-variété de $\mathbb{P}^n \times \mathbb{P}^{p-1}$ formée des couples

$$(x\,;\,y) = (X_0,\ldots,X_n\,;\,Y_0,\ldots,Y_{p-1})$$

tels qu'il existe $t \in \mathbb{C}$ avec

(3) $$X_\alpha = t\,Y_\alpha \quad \text{pour tout } \alpha = 0,\ldots,p-1 .$$

Notons $f : X' \to X = \mathbb{P}^n$ et $g : X' \to Z = \mathbb{P}^{p-1}$ les projections évidentes. En dehors du diviseur $Y' = f^{-1}(Y)$ l'application f est un isomorphisme $X' - Y' \to X - Y$.

- Soit $\mathcal{L}_X$ (resp. $\mathcal{L}_Z$) le faisceau inversible canonique sur X (resp. Z). On peut définir sur X' un morphisme

$$\rho : f^*\mathcal{L}_X \to g^*\mathcal{L}_Z$$

de la façon suivante. Si s est une section de $f^*\mathcal{L}_X$ on a

$$s(x\,;\,y) = (X_0,\ldots,X_n) ,$$

où (X_i) est soit nul, soit un système de coordonées homogènes de x. On pose

$$\rho(s)(x\,;\,y) = (X_0,\ldots,X_{p-1}) .$$

L'équation (3) montre que $\rho(s)$ est une section de $g^*\mathcal{L}_Z$. On vérifie aisément que la section ρ du fibré inversible $g^*\mathcal{L}_Z \otimes f^*\mathcal{L}_X^{-1}$ a pour diviseur Y'.

Si on munit $\mathcal{O}_X$ et $\mathcal{O}_Z$ de leur métrique standard, la norme carrée de ρ est

$$\|\rho\|^2(x\,;y) = \left(|X_0|^2 + \ldots + |X_{p-1}|^2\right) / \left(|X_0|^2 + \ldots + |X_n|^2\right).$$

- Rappelons l'<u>équation de Poincaré-Lelong</u> [3].

Soit L un fibré holomorphe inversible sur une variété complexe X, h une métrique sur L et $s \neq 0$ une section méromorphe de L. Alors la fonction log h(s,s) est localement intégrable sur X et le courant associé [log h(s,s)] vérifie l'équation

(4) $$d\,d^c[\log h(s,s)] = \delta_{\mathrm{div}(s)} - \omega,$$

où $\omega = c_1(L,h)$ est la première forme de Chern de L associée au choix de la métrique h.

- On a donc

$$d\,d^c\left[\log\|\rho\|^2\right] = \delta_{Y'} + \beta' - \alpha',$$

où α' (resp.β') est la première forme de Chern de $f^*\mathcal{O}_X$ (resp. $g^*\mathcal{O}_Z$). Posons

$$\omega' = \sum_{v=0}^{p-1} (\alpha')^v (\beta')^{p-1-v}$$

et

$$\Lambda' = -\,\omega' \log\|\rho\|^2.$$

On a

$$\begin{aligned} -\,dd^c[\Lambda'] &= \delta_{Y'}.\ \omega' + (\beta' - \alpha')\,\omega' \\ &= \delta_{Y'}.\ \omega' + (\beta')^p - (\alpha')^p \\ &= \delta_{Y'}.\ \omega' - \alpha'^p \end{aligned}$$

puisque β' provient de Z et dim Z = p - 1.

Sur $X' - Y' = X - Y$ on a $\Lambda' = \Lambda$, donc Λ est intégrable et le courant $f_*[\Lambda']$ coincide avec $[\Lambda]$. De plus $\alpha' = f^*(\alpha)$ et $f_*(\alpha')^p = \alpha^p$. Donc $-\,dd^c\,[\Lambda] = f_*(\delta_{Y'}.\,\omega') - \alpha^p$

Comme $Y' = Y \times Z$ et

$$\int_Z \left(-\,c_1(\mathcal{O}_Z)\right)^k = \begin{cases} 1 \text{ si } k = p-1 \\ 0 \text{ sinon}, \end{cases}$$

on obtient

$$f_*(\delta_{Y'}.\,\omega') = \delta_Y$$

d'où l'équation (2) .

2. Théorie de Nevanlinna [5] :

2.1 Soit $m \geq 1$ un entier et

$$f : \mathbb{C}^m \to \mathbb{P}^n$$

une application holomorphe. On s'intéresse à la question suivante : $f(\mathbb{C}^m)$ rencontre-t-il Y ?

Si $z = (z_i) \in \mathbb{C}^m$ on pose

$$|z|^2 = \sum_{i=1}^{m} |z_i|^2$$

et, si $r > 0$ est un nombre réel,

$$B_r = \left\{ z \in \mathbb{C}^m \text{ tel que } |z| < r \right\}$$

et

$$S_r = \left\{ z \in \mathbb{C}^m \text{ tel que } |z| = r \right\}.$$

Soit $\omega = d\,d^c \log |z|^2$.

On fait l'hypothèse que $f(0)$ n'est pas dans Y et que $f^{-1}(Y)$ est soit vide, soit de codimension p dans $\mathbb{C}^m$. On introduit les fonctions suivantes :

$$T_f^k(r) = \int_0^r \frac{dt}{t} \int_{B_t} f^*(\alpha)^k\, \omega^{m-k}, \quad k \geq 0,$$

$$N_f(r) = \int_0^r \frac{dt}{t} \int_{f^{-1}(Y) \cap B_t} \omega^{m-p},$$

$$m_f(r) = \frac{1}{2} \int_{S_r} f^*(\Lambda)\, d^c \log |z|^2\, \omega^{m-p},$$

et

$$R_f(r) = \frac{1}{2} \int_{B_r} f^*(\Lambda)\, \omega^{m-p+1}.$$

On notera que $T_f^k(r)$ ne dépend pas de Y et que $R_f(r) = 0$ si $p = 1$ (car $\omega^m = 0$).

THÉORÈME 2 ("1er théorème principal") :

$$N_f(r) + m_f(r) = T_f^p(r) + R_f(r) + 0(1)$$

PREUVE [5] :

D'après le Théorème 1

$$d\,d^c [\Lambda] = \alpha^p - \delta_Y,$$

donc

$$\int_0^r \frac{dt}{t} \int_{B_t} d\,d^c f^*(\Lambda)\,\omega^{m-p} = T_f^p(r) - N_f(r).$$

Utilisant la formule de Stokes et l'égalité $\frac{dt}{t} = \frac{1}{2} d \log |z|^2$ sur S_t on trouve

$$\int_0^r \frac{dt}{t} \int_{B_t} d\,d^c f^*(\Lambda)\,\omega^{m-p}$$

$$= \frac{1}{2} \int_0^r d \log |z|^2 \int_{S_t} d^c f^*(\Lambda)\,\omega^{m-p}$$

$$= \frac{1}{2} \int_{B_r} d^c f^*(\Lambda)\, d \log |z|^2 \omega^{m-p} + 0(1)$$

(car $f(0) \notin Y$)

$$= m_f(r) - R_f(r) + 0(1).$$

COROLLAIRE :

$$N_f(r) \le T_f^p(r) + R_f(r) + 0(1)$$

PREUVE : La forme Λ est positive d'après (1), car α et β sont positives et $\tau - \sigma \ge 0$. Donc $m_f(r) \ge 0$ et le corollaire résulte du Théorème 2.

2.2. Soient G la grassmannienne des sous-espaces projectifs Y de codimension p de $\mathbb{P}^n$, et μ la mesure sur G qui est invariante par l'action du groupe unitaire $U(n + 1)$ et de masse totale $\mu(G) = 1$. Posons

$$t_f(r) = \int_{B_r} f^*(\alpha)^{p-1}\,\omega^{m-p+1}.$$

On fait l'hypothèse que, pour μ-presque tout Y, $f^{-1}(Y)$ est vide ou de codimension p.

THÉORÈME 3 : *Supposons que*

(H) $$\liminf_{r \to \infty} \left(t_f(r) \,/\, T_f^p(r)\right) = 0.$$

Alors, pour μ *-presque tout* Y, $f(\mathbb{C}^m) \cap Y$ *est non vide.*

N.B. : Si p = 1 l'hypothèse H) est toujours vérifiée.

PREUVE [5] :
- Notons $N_f(Y,r)$, $m_f(Y,r)$ et $R_f(Y,r)$ les fonctions associées à f et Y comme dans 2.1.

On a

(5) $$\int_G N_f(r)\, d\mu(Y) = T_f^p(r).$$

En effet les formes harmoniques sur $\mathbb{P}^n$ sont les formes $U(n+1)$-invariantes. Donc le courant

$$\int_G \delta_Y d\mu(Y)$$

est la projection harmonique de δ_Y, c'est à dire la forme α^p.

- Si l'on applique (5) et le Théorème 2 on obtient

(6) $$\int_G m_f(Y,r)\, d\mu(Y) = \int_G R_f(Y,r)\, d\mu(Y) + 0(1).$$

- Soit E l'ensemble des $Y \in G$ tels que $f(\mathbb{C}^m) \cap Y$ soit non vide. Supposons par l'absurde que $\mu(E) = 1-\varepsilon$, $\varepsilon > 0$. Si $Y \notin E$ on a $N_f(Y,r) = 0$ donc, d'après (5),

$$T_f^p(r) = \int_E N_f(Y,r)\, d\mu(Y)$$

Par le corollaire il vient

$$\begin{aligned} T_f^p(r) &\leq \int_E T_f^p(r)\, d\mu(Y) + \int_E R_f(Y,r)\, d\mu(Y) + 0(1) \\ &\leq (1-\varepsilon) T_f^p(r) + \int_G R_f(Y,r)\, d\mu(Y) + 0(1) \\ &= (1-\varepsilon) T_f^p(r) + \int_G m_f(Y,r)\, d\mu(Y) + 0(1) \end{aligned}$$

(grâce à (6)). Mais

$$\int_G m_f(Y,r)\, d\mu(Y) = \frac{1}{2}\int_{S_r} f^*\left(\int_G \Lambda(Y)\, d\mu(Y)\right) d^c \log|z|^2\, \omega^{m-p}$$

et la projection harmonique $\int_G \Lambda(Y)\, d\mu(Y)$ du courant Λ est nécessairement un multiple $c(n,p)\alpha^{p-1}$ de la forme α^{p-1}. On obtient ainsi

$$\int_G m_f(Y,r)\, d\mu(Y) = c(n,p)\, t_f(r)$$

et

$$T_f^p(r) \leq (1-\varepsilon) T_f^p(r) + c(n,p)\, t_f(r) + 0(1).$$

Ceci contredit l'hypothèse H).

2.3. La constante $c(n,p)$ qui apparaît dans la preuve ci-dessus a été calculée par W. Stoll.

THÉORÈME 4 [6] :

$$c(n,p) = \sum_{\nu=1}^{p} \sum_{\mu=0}^{n-p} \frac{1}{\mu+\nu}$$

3. Théorie d'Arakelov [1] [2] :

3.1. Soient X un schéma régulier, projectif et plat sur $\mathbf{Z}$, X^p l'ensemble des points de codimension p de X et $Z^p(X)$ le groupe libre engendré par X^p (les cycles de codimension p sur X). Si $Z \in Z^p(X)$, on note δ_Z le courant d'intégration sur $Z(\mathbb{C}) \subset X(\mathbb{C})$. On appelle courant de Green pour Z la donnée d'un courant g réel de type $(p-1, p-1)$ sur $X(\mathbb{C})$ tel que

$$d\, d^c g = \delta_Z - \omega,$$

où ω est une forme C^∞ (de type (p,p)).

Les équations (2) et (4) donnent des exemples de tels courants. Le groupe de Chov artithmétique $\widehat{CH}^p(X)$ est le groupe engendré par les couples (Z,g), où $Z \in Z^p(X)$ et g est un courant de Green pour Z, soumis aux relations suivantes :

a) $(\operatorname{div}(f), -\log |f|^2) = 0$

pour toute fonction rationnelle $f \neq 0$ sur une sous-variété fermée irréductible $Y \subset X$ de codimension $p-1$ (le courant $\log |f|^2$ sur $X(\mathbb{C})$ étant donné par l'intégration sur $Y(\mathbb{C})$ contre la fonction intégrable $\log |f|^2$).

b) $(0, \partial u + \bar{\partial} v) = 0$

pour tous les courants u et v de type $(p-2, p-1)$ et $(p-1, p-2)$.

3.2. Si E est un fibré algébrique sur X, h une métrique hermitienne sur le fibré holomorphe sur $X(\mathbb{C})$ associé à E, et $p \geq 0$ un entier, on définit dans [2] une classe de Chern $\hat{c}_p(E,h) \in \widehat{CH}^p(X)$ caractérisée par les propriétés suivantes :

i) $\hat{c}_0 = 1$

ii) Si L est un fibré inversible, $\hat{c}_1(L, h)$ est la classe du couple $(\operatorname{div}(s), -\log h(s,s))$ pour toute section rationnelle non nulle de L (voir (4)).

iii) Si $E = L_1 \oplus \ldots \oplus L_n$ est une somme directe de fibrés inversibles, h_i une métrique sur L_i, $1 \leq i \leq n$, et h la somme directe orthogonale des h_i, on a

$$\hat{c}_p(E, h) = \sigma_p\left(\hat{c}_1(L_i, h_i)\right),$$

où σ_p est la p-ième fonction symétrique élémentaire.

iv) Si E (resp.L) est un fibré de rang n (resp.1) sur X et h (resp.h') une métrique hermitienne sur E (resp. L) on a

$$\hat{c}_p(E \otimes L,\ h \otimes h') = \sum_{i=0}^{p} \binom{n-i}{p-i} \hat{c}_i(E)\, \hat{c}_1(L)^{p-i} .$$

v) Si $f : Y \to X$ est un morphisme algébrique on a

$$\hat{c}_p(f^*E, f^*h) = f^*\hat{c}_p(E, h).$$

On trouvera dans [1] la définition de

$$f^* : \widehat{CH}^p(X) \to \widehat{CH}^p(Y)$$

et celle du produit

$$\widehat{CH}^p(X) \otimes \widehat{CH}^1(X) \to \widehat{CH}^{p+1}(X).$$

3.3. Sur l'espace projectif $X = \mathbb{P}^n$ sur $\mathbb{Z}$ on désigne par Q le fibré canonique de rang n (quotient de $\mathcal{O}_X^{n+1}$ par $\mathcal{O}(1)$) et h la métrique induite sur Q par la métrique standard sur $\mathbb{C}^{n+1}$. Soit $Y \subset X$ la sous-variété d'équation

$$X_0 = X_1 = \ldots = X_{p-1} = 0$$

et Λ la forme de Levine.

THÉORÈME 5 ([2], Thm. 5.2.) :
La classe du couple (Y, Λ) *dans* $\widehat{CH}^p(\mathbb{P}^n)$ *est la p-ième classe de Chern* $\hat{c}_p(Q, h)$.

PREUVE : Notons $\delta_{n,p}$ la différence de ces deux éléments de $\widehat{CH}^p(\mathbb{P}^n)$. Du Théorème 1 et des propriétés i) à v) de $\hat{c}_p$ on déduit que l'image $\delta_{n,p}$ dans le groupe de Chow usuel CH^p et dans le groupe $A^{pp}(X)$ des formes de type (p,p) sur $X(\mathbb{C})$ (par l'application qui à (Z,g) associe $\omega = \delta_Z + dd^c g$) est nulle. Or le groupe

$$\mathrm{Ker}\left(\widehat{CH}^p(X) \to CH^p(X) \oplus A^{pp}(X)\right)$$

s'identifie au groupe de cohomologie

$$H^{p-1,p-1}\left(\mathbb{P}^n(\mathbb{C}), \mathbb{R}\right) = \mathbb{R}$$

([1] et [2] loc-cit.). Si $\mathbb{P}^{p-1} \subset \mathbb{P}^n$ est le sous-espace défini par les équations $X_p = X_{p+1} = \ldots = X_n = 0$, on constate que le morphisme de corestriction

$$H^{p-1,p-1}\left(\mathbb{P}^n(\mathbb{C}), \mathbb{R}\right) \to H^{p-1,p-1}\left(\mathbb{P}^{p-1}(\mathbb{C}), \mathbb{R}\right)$$

est un isomorphisme envoyant $\delta_{n,p}$ sur $\delta_{p-1,p-1}$. Mais si $n = p - 1$ la variété Y est vide et $\sigma = \tau$, donc $\Lambda = 0$. Par conséquent $\delta_{p-1,p-1} = 0$ et $\delta_{n,p} = 0$.

APPLICATION : Du Théorème 5 on déduit dans [2], Prop. 5.4, une nouvelle preuve du Théorème 4.

Références

[1] H. Gillet, C. Soulé : Arithmetic Intersection Theory (1988), Preprint IHES.

[2] H. Gillet, C. Soulé : Characteristic classes for algebraic vector bundles with hermitian metric (1988), à paraître dans Annals of Maths.

[3] P. Griffiths, J. Harris : Principles of Algebraic Geometry (1978), John Wiley and Sons.

[4] H. Levine : A theorem on holomorphic mappings into complex projective space, Annals of Maths. 71, n° 2 (1960), 529-535.

[5] B.V. Shabat : Distribution of values of holomorphic mappings, Translation AMS 61 (1985)

[6] W. Stoll : About the value distribution of holomorphic maps into projective space, Acta Math. 123 (1969), 83-114.

[7] P. Vojta : Diophantine Approximations and Value Distribution Theory, Lec Notes in Maths 1239 (1987), Springer-Verlag.