Astérisque

MARC HINDRY

Sur les conjectures de Mordell et Lang (d'après Vojta, Faltings et Bombieri)

Astérisque, tome 209 (1992), p. 39-56

<http://www.numdam.org/item?id=AST_1992__209__39_0>

SUR LES CONJECTURES DE MORDELL ET LANG (d'après VOJTA, FALTINGS et BOMBIERI).

Marc HINDRY

1 Introduction

Dans tout le texte, k désigne un corps de nombres, O_k son anneau d'entiers, C une courbe algébrique projective lisse définie sur k et g le genre de C. L'ensemble des points de C rationnels sur k est noté C(k).

On sait que:

si g=0 alors C(k) est ou bien vide ou bien en bijection avec $\mathbf{P}^1(k)$;
si g=1 alors ou bien C(k) est vide ou bien est un groupe de type fini (théorème de Mordell-Weil); la loi de groupe est par ailleurs algébrique;
si g≥2 alors C(k) est fini (Conjecture de Mordell=théorème de Faltings [F1]).
Si U est un ouvert affine de C on peut s'intéresser aux points entiers que je noterai (un peu abusivement) $U(O_k)$; on dispose alors du théorème de Siegel [Si]: $U(O_k)$ est fini sauf (peut-être) si g=0 et C–U possède au plus deux éléments. La preuve de Siegel utilise essentiellement deux ingrédients que j'explicite plus loin: a) la théorie des approximations diophantiennes (Thue-Siegel-Dyson-Gelfond-Roth-Schmidt) et b) le théorème de Mordell-Weil appliqué à la jacobienne de C.
Ces ingrédients n'apparaissent pas dans la preuve de la conjecture de Mordell par Faltings [F1] (Voir aussi les séminaires [Sz1] et [Co-Si]) même si les jacobiennes et les variétés abéliennes y jouent un rôle prépondérant. Vojta a donné une nouvelle preuve de la conjecture de Mordell dans la lignée de Siegel [V1]. Faltings , en développant les idées de Vojta a ensuite prouvé la généralisation suivante, conjecturée par Lang:

THÉORÈME 1(Faltings [F2];voir aussi [Sz2]): *Soit* X *une sous-variété d'une variété abélienne* A *définies sur* k; *on suppose que* X *ne contient aucun translaté de sous-variété abélienne non nulle, alors* X(k) *est fini.*

La preuve de Vojta [V1] utilise des idées et des techniques sophistiquées de géométrie arithmétique "à la Arakelov", notamment [G-S3]; Bombieri [B] a

simplifié cette preuve et donné une version très jolie et "presque élémentaire" du travail de Vojta; c'est un article que tout mathématicien souhaitera lire.
Les liens entre la géométrie et l'approximation diophantienne "à la Siegel" ont été développés dans plusieurs directions: Vojta a annoncé dans [V4] une inégalité plus fine que celle que nous donnons et valable sur toutes les courbes; cette inégalité contient la conjecture de Mordell et le théorème de Roth. Dans [F2] Faltings prouve une généralisation du théorème de Siegel également conjecturée par Serge Lang: un ouvert affine d'une variété abélienne ne contient qu'un nombre fini de points entiers définis sur un corps de nombres donné.
J'explicite dans cette introduction les deux ingrédients fondamentaux mentionnés ci-devant; le paragraphe suivant introduit l'outil de base de la géométrie diophantienne: les hauteurs; je donne dans les paragraphes 3 et 4 une esquisse des preuves respectivement de la conjecture de Mordell selon Vojta et du théorème 1 selon Faltings, il ne saurait donc être question d'originalité ici mais j'espère que cette présentation facilitera à certains la lecture des articles originaux décrivant ces beaux résultats. Le paragraphe 5 complète sur certains points le paragraphe 4 et décrit la conjecture générale de Serge Lang [La1] (maintenant un théorème); le dernier paragraphe raconte une application de ces résultats à l'étude des points algébriques de degré donné sur une courbe.

a)Approximations diophantiennes.
L'idée de Siegel est qu' une suite infinie de points entiers sur une courbe affine doit tendre vers l'un de ses points à l'infini (se rapprocher d'une asymptote) et donc en fournir de très bonnes approximations. Remarquons que cette remarque si simple est en défaut (au moins littéralement) si l'on travaille avec des points rationnels; on a donc longtemps cru qu'elle était inutilisable quand les points ne sont pas entiers, Vojta a montré qu'il n'en était rien.
Je donne un schéma de preuve d'inégalités de ce type (une bonne référence générale est [Sch1]):

THÉORÈME DE ROTH: *Soit α un nombre algébrique irrationnel et $\kappa>2$, alors il existe un nombre fini de solutions rationnelles à l'inégalité:*

$$(*) \qquad |\alpha - \frac{p}{q}| < q^{-\kappa}.$$

Premier pas: on fixe m assez grand, et $d_1,\ldots,d_m$ entiers et on construit un polynôme $P \in \mathbf{Z}[X_1\ldots,X_m]$ de degré au plus d_i en X_i, s'annulant beaucoup en $(\alpha,\ldots,\alpha)$ et dont les coefficients sont de taille controlée (Lemme de Siegel ou principe des boites).
Deuxième pas: On suppose qu'il existe $p_1/q_1,..,p_m/q_m$ vérifiant (*); alors on prouve que P et un certain nombre de ses dérivées sont petits en

$\beta=(p_1/q_1,...,p_m/q_m)$ par une simple application de la formule de Taylor.

Troisième pas (difficile): On emploie un théorème de non-annulation, dont je donne ci-après un enoncé ("lemme de Roth à deux variables"). On doit prouver qu'une dérivée d'ordre assez petit est non nulle i.e.:

$$\eta := \partial_i P(\beta)\neq 0 \quad \text{avec } \partial_i=\frac{1}{i_1!..i_m!}(\partial/\partial X_1)^{i_1}..(\partial/\partial X_m)^{i_m}.$$

Quatrième pas: comme η est rationnel et non nul on écrit :

$$(\text{Dénominateur}(\eta))^{-1}<|\eta|$$

C'est l''inégalité de Liouville"; elle fournit une contradiction si m est assez grand et si les q_i sont très échelonnés (Cf remarques ci-dessous)

Remarques:

i)Il est vital pour les estimations arithmétiques de diviser par les factorielles.

ii)Les théorèmes d'annulation (Dyson, Roth [Ro], Viola [Vi], Esnault-Viehweg [E–V]) utilisent la notion d'indice, ou ordre d'annulation pondéré; on définit l'indice d'un polynôme P en un point β par rapport aux poids $(d_1,...,d_m)$ par:

$$\text{Indice}_{(d_1,...,d_m)(\beta)}(P):=\min\{\frac{i_1}{d_1}+..+\frac{i_m}{d_m} / \partial_i P(\beta)\neq 0\}.$$

Dans la pratique les d_i sont effectivement les degrés de P par rapport à X_i. Donnons l'énoncé promis:

LEMME DE ROTH ("À DEUX VARIABLES"): *soit* $\varepsilon>0$, α_1,α_2 *deux nombres algébriques et* $P\in Q[X,Y]$ *non nul de degré au plus* d_1,d_2 *et supposons que*

1) $d_2/d_1<\varepsilon$

2) $h(P)+4d_1<\varepsilon^2\min(d_1h(\alpha_1),d_2h(\alpha_2))$

alors on a :

$$\text{Indice}_{(d_1,d_2)(\alpha_1,\alpha_2)}(P)<4\varepsilon.$$

Ici, h désigne la hauteur logarithmique usuelle (Cf paragraphe suivant). On pourra lire la preuve dans l'article original de Roth [Ro] ou dans celui de Bombieri [B]; il faut penser pour que le lemme soit utile que ε est petit et donc que d_1 est beaucoup plus grand que d_2 d'après (1) et donc pour majorer efficacement les dérivées de P (deuxième étape) et vérifier l'hypothèse (2) on aura besoin que $d_1h(\alpha_1)$ soit du

même ordre de grandeur que $d_2h(\alpha_2)$ et il faudra supposer:

(**) $h(\alpha_1)/h(\alpha_2) < \varepsilon$ ou encore $\log q_i/\log q_{i+1} < \varepsilon$

(avec les notations de la construction précédente) .

Ceci est la raison de l'ineffectivité congénitale de la méthode: on doit supposer l'existence de bonnes approximations avec des dénominateurs croissant exponentiellement pour montrer que de telles approximations n'existent pas. La preuve de Vojta souffre du même défaut et -tout comme la preuve de Faltings mais pour d'autres raisons- n'est pas effective. Par contre la méthode est très bonne pour borner le nombre des solutions (Cf théorème 2).

b) Jacobienne d'une courbe algébrique.

On définit un plongement de C dans une variété abélienne A=Jac(C) en choisissant un point origine $O \in C$. Sur $\mathbf{C}$ on procède ainsi: on choisit une base $\omega_1,..,\omega_g$ des 1–formes holomorphes sur C et on définit:

$j: C \longrightarrow A=Jac(C)=\mathbf{C}^g/\Omega$

$x \longrightarrow (\int_o^x \omega_1,..,\int_o^x \omega_g)$ modulo périodes.

Cette construction peut se faire algébriquement d'après Weil [W] (voir aussi l'article de Milne dans [Co-Si]). Dans ce cas A est une variété abélienne définie sur k et A(k) est un groupe de type fini. En particulier $A(k)\otimes\mathbf{R}=\mathbf{R}^r$ avec r=rangA(k) et l'application de C(k) dans cet espace est à fibres finies ("finite-to-one"). Ainsi pour prouver que C(k) est fini il suffit de prouver que son image dans $A(k)\otimes\mathbf{R}$ est finie.

Remarque: la description analytique donnée ci-dessus se transcrit mot pour mot à une variété X de dimension quelconque; on obtient ainsi une variété abélienne: sa variété d'Albanese (voir [La2]), mais bien sûr l'application obtenue n'est pas injective en général; en fait cela donne un caractérisation différentielle des sous-variétés de variétés abéliennes: ce sont celles qui ont "suffisamment" de 1-formes régulières.

2 Hauteurs associées à un diviseur.

C'est l'outil de base pour ces questions, des références générales sont [La1], [Se] et [Sz1]; en voici deux définitions donnant des éclairages différents:

1ère définition (Weil):

Si $P=(x_0,...,x_n)\in \mathbf{P}^n(\mathbf{Q})$, on peut supposer $x_i\in \mathbf{Z}$ et $pgcd(x_i)=1$; on pose alors $h(P)=\log\max|x_i|=\Sigma_v \log\max|x_i|_v$

La deuxième somme est prise sur toutes les places de $\mathbf{Q}$ et d'après la formule du produit est indépendante des coordonnées; de plus sous cette forme la définition se généralise immédiatement aux corps de nombres.

Si D est un diviseur très ample sur une variété X, il correspond à un plongement $\phi_D: X\longrightarrow \mathbf{P}^n$ et on pose $h_D(P):=h(\phi_D(P))$; en général un diviseur est la différence de deux diviseurs très amples D=A–B et on pose $h_D:=h_A-h_B$. La notation est abusive car la hauteur définie ainsi dépend du plongement et en tant que fonction du diviseur n'est définie qu'à une fonction bornée près; il est coutumier d'appeler hauteur de Weil associée à D tout représentant de la classe de h_D modulo les fonctions bornées.

2ème définition (Arakelov):

On étend X en un schéma $\mathfrak{X}$ projectif sur $spec(O_k)$; on pose $\mathfrak{D}$=clôture de Zariski de D dans $\mathfrak{X}$ et on note $\mathfrak{L}$ le fibré en droites associé. On choisit une métrique $\|\ \|_v$ sur $O(D)$ pour chaque place archimédienne. Un point de X(k) correspond dans ce langage à une section du morphisme $\mathfrak{X}\longrightarrow spec(O_k)$ et $P^*\mathfrak{L}$ est alors un fibré en droites (métrisé) sur O_k et si f est un élément non nul (une"section ne s'annulant pas en P") on pose:

$Deg_{Arakelov}(P^*\mathfrak{L})=\log Card(P^*\mathfrak{L}/fO_k)-\Sigma_v \log\|f\|_v$, où la somme est prise sur les places archimédiennes. La définition de la hauteur d'Arakelov est alors:

$[k:Q]h_{\mathfrak{X},\mathfrak{L},\|\ \|}(P)=Deg_{Arakelov}(P^*\mathfrak{L})$

On observe que $h_{\mathfrak{X},\mathfrak{L},\|\ \|}$ est bien une hauteur de Weil pour D, en particulier si $\mathfrak{X}',\mathfrak{L}',\|\ \|'$ désignent un autre modèle de X, un autre prolongement de O(D) et d'autres métriques alors la différence entre $h_{\mathfrak{X},\mathfrak{L},\|\ \|}$ et $h_{\mathfrak{X}',\mathfrak{L}',\|\ \|'}$ est bornée; les propriétés fondamentales sont les suivantes:

H1) h_D ne dépend que de la classe de D (mod O(1))

H2) $h_{D+D'}=h_D+h_{D'}$ mod O(1)

H3) $h_{f^*D}=h_D\circ f$ mod O(1) lorsque f est un morphisme entre deux variétés projectives X et Y.

H4) Si D est effectif, si $P\notin D$, alors $h_D(P)\geq -C^{te}$ ("inégalité de Liouville")

La notation O(1) désigne comme d'habitude la classe des fonctions bornées.

Commentaires: La définition de Weil a bien sûr le mérite d'être naturelle, on a envie de dire incontournable; elle rend clair aussi le fait qu'il n'y ait qu'un nombre fini de points de hauteur bornée (le théorème de Northcott, voir [La1], donne un énoncé un peu plus fort). La définition d'Arakelov enrichit la palette des analogies entre corps de nombres et corps de fonctions (entre géométrie et arithmétique); elle permet aussi en enrichissant la structure de "supprimer les O(1)" ou au moins de leur donner une valeur. En effet les propriétés H1,2,3,4 sont transparentes sur cette définition:

H1) h_D est définie à partir du fibré associé O(D).

H2) Si l'on munit $O(D+D')\equiv O(D)\otimes O(D')$ de la métrique produit tensoriel de celles de O(D) et O(D') on obtient une égalité.

H3) Si l'on choisit des modèles tels que f s'étende en $f:\mathfrak{X}\longrightarrow\mathfrak{Y}$ et si l'on muni O(f*D) de la métrique pullback de celle de O(D) on obtient une égalité.

H4) Si f est une section de O(D) dont le support est D posons $\|f\|_\infty=\sup_v\sup_P\|f(P)\|_v$, alors avec les notations d'Arakelov:

$$h_{\mathfrak{X},\mathfrak{L},\|\ \|}(P)\geq -\log\|f\|_\infty \qquad \text{(il suffit d'écrire } \mathrm{Card}(P^*\mathfrak{L}/f\mathcal{O}_k)\geq 1)$$

De plus si X est une variété abélienne et D est ample symétrique alors $h_D(P)=q_D(P)+O(1)$ avec q_D quadratique et même définie positive sur $X(k)\otimes\mathbf{R}$; cette forme quadratique s'appelle la hauteur de Néron-Tate associée à D. On se trouve donc dans une situation "à la Minkovski": on a un réseau (l'image de X(k)) dans un espace vectoriel euclidien $X(k)\otimes\mathbf{R}$.

3 La "conjecture" de Mordell.

On reprend le plongement associé à un point rationnel O fixé:

$j: C\longrightarrow A=Jac(C)$

On dispose du diviseur ample sur A

$\Theta=j(C)+...+j(C)$ (somme g–1 fois)

Je supposerai pour simplifier que Θ est symétrique (cela est toujours vrai pour un translaté de Θ et même dans certains cas on peut choisir O de sorte que cela soit

vrai).
On a donc une norme euclidienne || || sur $A(k)\otimes\mathbf{R}$ telle que:
$q_{\Theta}(x)=\frac{1}{2}\|x\|^2$. On notera <,> le produit scalaire associé.
On démontre alors les deux inégalités suivantes pour les points de C(k):

INEGALITÉ DE MUMFORD [M1]:*Soit* $\lambda>1/g$, *alors il existe* C_1 *telle que si* $x\neq y\in C(k)$ *et si* $C_1\leq\|x\|\leq\|y\|\leq 2\|x\|$ *alors*

$$\cos(x,y):=\langle x,y\rangle/\|x\|\|y\|\leq\lambda .$$

INEGALITÉ DE VOJTA [V1]:*Soit* $\lambda>1/\sqrt{g}$, *alors il existe* C_2,C_3 *telles que si* $x,y\in C(k)$ *et* $C_2\leq\|x\|\leq C_3\|y\|$ *alors*

$$\cos(x,y):=\langle x,y\rangle/\|x\|\|y\|\leq\lambda .$$

C'est un exercice de géométrie euclidienne de prouver que (en choisissant le même λ dans les deux inégalités, voir [V1] et [B]) on obtient:

THÉORÈME 2(Vojta):*notons* r *le rang du groupe de Mordell-Weil de la jacobienne de* C *et* C_1, C_2, C_3 *les constantes associées à* C *et* λ. *Alors:*

$$\mathrm{Card}\{x\in C(k)/\|x\|\geq\max(C_1,C_2)\}\leq(1+\frac{\log C_3}{\log 2})(1+\frac{1}{\sin(\frac{1}{4}\mathrm{Arcos}(1))})^r$$

Remarque: l'inégalité de Vojta suffit à prouver la conjecture de Mordell mais le résultat obtenu est plus précis .

Preuve de l'inégalité de Mumford [M1]:
On démontre les relations de classes de diviseurs (voir [M1] et [M2]); rappelons que Θ est supposé symétrique:

$j^*(\Theta)=g(O)$

$(jxj)^*(add^*(\Theta)-p_1^*(\Theta)-p_2^*(\Theta))=-\Delta'$

où add, p_1, p_2 sont respectivement l'addition et les projections de AxA vers A et $\Delta':=\Delta-Cx(O)-(O)xC$ et Δ est la diagonale de CxC.
Grâce aux propriétés H1,H2,H3 on obtient:

$$h_{(O)}(x)=\frac{1}{2g}\|j(x)\|^2+O(1)$$

$h_{\Delta'}(x,y)=-<j(x),j(y)>+O(1)$

$h_{\Delta}(x,y)=\frac{1}{2g}\|j(x)\|^2+\frac{1}{2g}\|j(y)\|^2-<j(x),j(y)>+O(1)$

On observe que la forme quadratique du membre de droite n'est pas définie positive (si $g\geq 2$!!) alors que, d'après la propriété H4 on a $h_{\Delta}(x,y)\geq O(1)$ si $(x,y)\notin\Delta$ i.e. si $x\neq y$. On en tire aisément l'inégalité de Mumford.

Preuve de l'inégalité de Vojta [V1]:

Le point de départ de Vojta est de considérer des diviseurs plus généraux de la forme:

$D=d_1Cx(O)+d_2(O)xC+d_3\Delta'$

(Remarque: si $d_1=d_2=d_3=1$ on retrouve $D=\Delta$)

Ayant fixé une hauteur $h_{(O)}$ associée à (O) sur C et une hauteur $h_{\Delta'}$ associée à Δ' sur $C\times C$ on a une hauteur associée à D définie par $h_D(x,y)=d_1h_{(O)}(x)+d_2h_{(O)}(y)+d_3h_{\Delta'}(x,y)$ et l'on obtient comme précédemment:

$h_D(x,y)=\frac{d_1}{2g}\|x\|^2+\frac{d_2}{2g}\|y\|^2-d_3<x,y>+O(d_1+d_2+d_3)$

La forme quadratique qui apparaît n'est pas définie positive dès que:

$$d_1d_2<g^2d_3^2$$

Toute la difficulté réside maintenant dans l'obtention d'une minoration $h_D(x,y)\geq -c(d_1,d_2,d_3)$

Vojta résoud ce problème avec des techniques très similaires à celles de l'approximation diophantienne.

Une première idée est de construire une section f de O(D) de taille controlée et si (par chance!) $f(x,y)\neq 0$ alors l'inégalité de Liouville donnera $h_D(x,y)\geq -\log\|f\|_\infty$.

Vojta construit f en montrant que D est très ample (sous des conditions explicitées ci-dessous) et en utilisant un théorème de Riemann-Roch arithmétique dû à Gillet-Soulé [G-S1] (voir [G-S2] pour une construction semblable). Bombieri remarque que le théorème de Riemann-Roch classique sur la surface CxC (l'inégalité, déjà connue des géomètres italiens, suffit) donne l'existence de beaucoup de sections, sous la condition:

$$gd_3<d_1d_2$$

on obtient un espace vectoriel de dimension proportionnelle à d_1d_2 et le lemme de Siegel permet de choisir une section de norme petite.

La deuxième idée est de dériver la section obtenue et de montrer qu'elle ne peut s'annuler avec un ordre trop élevé en (x,y); en effet on ne peut pas garantir $f(x,y)\neq 0$. Plus précisément on définit l'indice de la section f au point (x,y) comme

au paragraphe 1:

Indice$_{(d_1,d_2)(x,y)}(f):=\min\{\frac{i_1}{d_1}+\frac{i_2}{d_2}/\partial_i f(x,y)\neq 0\}$

Ici $\partial_i=\partial_{i_1,i_2}=\frac{1}{i_1!i_2!}(\frac{\partial}{\partial x_1})^{i_1}(\frac{\partial}{\partial x_2})^{i_2}$ où x_1 et x_2 sont des paramètres locaux en x et y sur la courbe C.

Remarque: dire qu'une dérivée de f s'annule n'a pas vraiment de sens (cela dépend de la trivialisation choisie) mais l'ordre d'annulation est bien défini.

Sous la condition:

$$d_2/d_1 \text{ très petit} \qquad (*)$$

on obtient une bonne borne pour Indice$_{(d_1,d_2)(x,y)}(f)$; Vojta utilise le "lemme de Dyson" sur CxC qu'il a prouvé pour cela [V2] et Bombieri utilise le lemme de Roth que j'ai enoncé (on commence par projeter CxC sur $\mathbf{P}^1x\mathbf{P}^1$).

Les contraintes explicitées de la preuve forcent pratiquement à choisir des paramètres proportionnels à:

$d_1:=[d/\|x\|^2]$ $d_2:=[d/\|y\|^2]$ et $d_3:=[d/\|x\|\|y\|(\sqrt{g}+\varepsilon)]$

où d est un paramètre qui tendra vers l'infini et ε est suffisament petit pour que $g<(\sqrt{g}+\varepsilon)^2<g^2$. Alors $d_1\|x\|^2$ est presque égal à $d_2\|y\|^2$ et la condition (*) équivaut à $\|x\|/\|y\|$ très petit, ce qui est précisément une des hypothèses. En joignant ces idées à de délicates estimations de la taille des derivées on obtient l'inegalité de Vojta.

4 Les sous-variétés de variétés abéliennes.

Je donne dans ce paragraphe l'esquisse de la preuve du théorème 1: l'extension par Faltings des idées du paragraphe précédent aux variétés de dimension >1, en essayant de faire ressortir le parallélisme des idées.

On considère donc $j:X\longrightarrow A$ une sous-variété d'une variété abélienne A et on appelle encore Θ un diviseur symétrique et ample sur A et $\|.\|$ la norme euclidienne associée à Θ sur $A(k)\otimes\mathbf{R}$. Comme dans la preuve du théorème de Roth on choisit un entier m et un réel ε petit (voir paragraphe suivant pour la "valeur" de m; si dimX=1 alors m=2); on dispose alors sur $A^m=AxA...xA$ des diviseurs suivants:

$\Theta_i=p_i^*(\Theta)$ (diviseur 'fibre")

$P_{ij}=(p_i+p_j)^*(\Theta)-p_i^*(\Theta)-p_j^*(\Theta)$ (diviseur de Poincaré)
On travaille maintenant avec les diviseurs:
$D':=d_1\Theta_1+\ldots+d_m\Theta_m-e_1P_{12}-\ldots e_{m-1}P_{m-1,m}$ sur $A^m=A\times\ldots\times A$ et $D:=(j\times\ldots\times j)^*(D')$ sur $X^m=X\times\ldots\times X$. On calcule de la même façon $h_D(x_1,..,x_m)$ à partir de $\|x_i\|$ et $\langle x_i,x_j\rangle$; en effet $q_{\Theta_i}(x)=\frac{1}{2}\|x_i\|^2$ et $q_{P_{ij}}(x_1,..,x_m)=\langle x_i,x_j\rangle$ donc :

$$h_D(x_1,..,x_m)=\frac{1}{2}\sum d_i\|x_i\|^2-\sum e_i\langle x_i,x_{i+1}\rangle+O(\sum d_i+e_i)$$

La partie nouvelle et réellement difficile est la minoration de $h_D(x_1,..,x_m)$. Faltings montre que, sous les conditions suivantes:
A1) X ne contient pas de sous-variété abélienne translatée;
A2) m a été choisi assez grand (en fonction de dimX) et ε assez petit (en fonction de m);
A3) $d_i/d_{i+1}>r=r(\varepsilon,m)$ et $d_id_{i+1}=(2-\varepsilon)^2e_i^2$;
on a D ample sur X^m.
Remarques: D' n'est jamais ample sur A^m. La façon dont les deux premières hypothèses sont utilisées ainsi que leur nécessité est discutée au paragraphe suivant. La troisième hypothèse permet l'utilisation d'un outil nouveau qui remplace le lemme de Dyson ou Roth: le théorème du produit, très jolie découverte de Faltings:

THÉORÈME DU PRODUIT (Faltings [F2]).

Soit $x\in\mathbf{P}=\mathbf{P}^{n_1}\times..\times\mathbf{P}^{n_m}$, *et* f *une section de* $L=O(d_1,..,d_m)$ (*i.e. un polynôme multihomogène de degré* $d_1,..,d_m$)
On pose:

$$\text{Indice}_{x,(d_1,\ldots,d_m)}(f):=\max\{\ \frac{i_1}{d_1}+..+\frac{i_m}{d_m}\ \textit{/pour tout opérateur différentiel}\ \partial_k\ \textit{d'ordre}\ \le i_k\ \textit{sur}\ \mathbf{P}^{n_k}\ \textit{on a}\ \partial_1\cdots\partial_m f(x)=0\}$$

On note:

$$Z_\sigma:=\{x\in\mathbf{P}/\text{Ind}_{x,d}(f)>\sigma\}$$

Soit $\varepsilon>0$. *Il existe r (dépendant de* ε*) tel que si* $d_i/d_{i+1}>r$ *alors toute composante irréductible* Z *de* $Z_{\sigma+\varepsilon}$ *qui est aussi une composante de* Z_σ *est de la forme* $Z=Z_1\times..\times Z_m$ *avec* Z_i *sous-variété de* $\mathbf{P}^{n_i}$ *de degré borné par une constante dépendant seulement de* ε.

Ce théorème est énoncé sur un corps algébriquement clos; la seule difficulté sur un corps non algébriquement clos provient du fait qu'une composante irréductible peut ne pas être géométriquement irréductible.
Faltings a d'ailleurs montré [F4] comment on pouvait retrouver le théorème de Roth et la généralisation de Schmidt (le "théorème du sous-espace" [Sch2]) en utilisant ce théorème du produit.
Comme pour le théorème de Roth pour montrer qu'il n'existe pas de suite infinie de points rationnels dans X, on choisit m un grand entier et ε un réel petit; il suffit de montrer qu'il n'existe pas de suite $(x_1,..,x_m)$ de points de X(k) vérifiant:

a) $<x_i,x_{i+1}>\geq(1-\varepsilon/4)\|x_i\|\|x_{i+1}\|$ (i.e. les points sont dans un même cône)

b) $\|x_{i+1}\|/\|x_i\|>r=r(\varepsilon)$ et enfin

c) $\|x_1\|$ grand en fonction de ε.

On choisit alors s_i des nombres rationnels très proches de $\|x_i\|^{-1}$ et les paramètres $d_i=s_i^2(2-\varepsilon)$ et $e_i=s_is_{i+1}$ de sorte que les conditions A3) soient remplies; le calcul de la hauteur fournit:

$h_D(x_1,..,x_m)<\frac{1}{2}\sum s_i^2(2-\varepsilon)\|x_i\|^2-\sum s_is_{i+1}\|x_i\|\|x_{i+1}\|(1-\varepsilon/4)+O(\sum s_i^2)$

$<-\varepsilon m/4+O(\|x_1\|^{-2})$

On choisit encore un réel σ disons plus petit que $\varepsilon/4$ et un entier d très grand et suffisamment divisible. L'amplitude et une version raffinée du lemme de Siegel utilisant le théorème des minima successifs de Minkovski permettent de construire une section f de O(dD) ayant un indice $<\sigma$ en x et une norme petite (c'est-à-dire telle que $\log\|f\|_\infty<C\sum ds_i^2$); l'indice est pris par rapport aux poids ds_i^2.

Remarquons que cela renverse un peu l'ordre habituel: le théorème de non annulation, ici le théorème du produit, est déjà inclus dans la construction de la fonction (section) auxiliaire.
On montre ensuite que la norme d'une dérivée de f (ne s'annulant pas en x) vérifie une inégalité du même type et on applique l'inégalité de Liouville pour obtenir $-Cmd/\|x_1\|<-\varepsilon md/2$; d'où une contradiction si $\|x_1\|$ est assez grand!

5 La conjecture générale de Serge Lang.

Lang avait conjecturé un enoncé plus général (voir [La1], [La3] et [La4]) qui peut maintenant être établi. Lang a aussi suggéré que l'énoncé analogue pour les variétés semi-abéliennes devait être vrai; une preuve de cela a été annoncé par Vojta; je me restreint ici à l'énoncé sur les variétés abéliennes:

THÉORÈME 3: *Soit* A *une variété abélienne complexe et* X *une sous variété analytique (fermée), soit* Γ *un sous-groupe de rang fini de* $A(\mathbf{C})$. *Alors il existe un nombre fini de points* t_i *de* Γ *et de sous-variétés abéliennes* B_i *(éventuellement nulles) telles que* t_i+B_i *soit contenu dans* X *et:*

$$X(\mathbf{C})\cap\Gamma=\cup t_i+(B_i(\mathbf{C})\cap\Gamma)$$

Cet énoncé contient bien sûr le théorème 1 (appliquer le théorème de Mordell-Weil) mais aussi la conjecture de Manin-Mumford (quand on prend $\Gamma=A_{torsion}$) prouvée auparavant par Raynaud [R1],[R2]. Cet énoncé général est conséquence du théorème suivant, comme cela est prouvé dans [R3] (quand il n'y a pas de sous-variétés abéliennes dans X) et dans [H1] (cas général); bien que l'énoncé semble analytique, on se ramène tout de suite à un corps de type fini sur $\mathbf{Q}$ et même, par des arguments de spécialisation non triviaux à un corps de nombres; la réduction d'un groupe de rang fini à un groupe de type fini utilise des arguments galoisiens.

THÉORÈME 4 (Faltings [F2]: *Soit* X *une sous-variété d'une variété abélienne* A *définies sur un corps de nombres* k; *il existe un nombre fini de points rationnels* t_i *et de sous-variétés abéliennes* B_i *telles que*

$$X(k)=\cup t_i+B_i(k).$$

Je ne présente pas la preuve assez semblable à la preuve du théorème 1 mais plus compliquée techniquement, toutefois j'explique où interviennent les sous-variétés abéliennes contenues (ou non) dans X et le début de la preuve de l'amplitude du diviseur D du paragraphe précédent. Notons $G_X:=\{a\in A/\ a+X=X\}$ le stabilisateur de X et Z_X l'adhérence de Zariski de l'union des translatés de sous-variétés abéliennes (non nulles, cette fois) contenus dans X; ainsi l'hypothèse du théorème 1 est que Z_X est vide et la conjecture de Lang dit que les points rationnels s'accumulent tous sur Z_X sauf pour un nombre fini d'entre eux.

LEMME 1: *Ou bien* G_X *est de dimension positive (et donc* $Z_X=X$), *ou bien* $Z_X\neq X$ et Z_X *est une union finie de sous-variétés stabilisées par une sous-variété abélienne de dimension positive.*

On peut bien sûr se ramener au cas numéro deux en quotientant par G_X Ce lemme est prouvé explicitement dans [R2] et [H1] et se trouve (caché) dans [Bg] (brièvement: il y a un nombre fini de sous-variété abéliennes maximales [Bg] dans X disons $B_1,..,B_s$ donc $Z_X=\cup(Z_i+B_i)$ où les Z_i sont des sous-variétés de X).

Revenons à la preuve de l'amplitude du diviseur D du paragraphe précédent. Un point essentiel est la considération du morphisme de X^m dans A^{m-1} défini par: $\alpha(x_1,..,x_m)=(t_1x_1-x_2,t_2x_2-x_3,..,t_{m-1}x_{m-1}-x_m)$ où les t_i sont entiers. Remarquons que si x_0+B est inclus dans X et si on pose $x_0 1=(x_0,..x_0)$ et $B(t_1,..,t_m)=\{(x,t_1x,t_1t_2x,..,t_1..t_{m-1}x)/x\in B\}$ alors $\alpha(x_0 1+B(t_1,..,t_m))$ est réduit à un point. Le lemme suivant est une petite généralisation du lemme 4.1 de Faltings [F2]:

LEMME 2: *Il existe* m *tel que si* $t_1\geq..\geq t_{m-1}\geq 2$ *alors le morphisme* α *de* X^m *dans* A^{m-1} *est génériquement fini; plus précisément les composantes de dimension positive des fibres sont de la forme* $x+B(t_1,..,t_m)$ *où* B *est une sous-variété abélienne maximale de* X.
De plus si $t_{m-1}\geq \deg X(2d)^{\dim X}$ *alors on peut choisir* $m=(\dim X+1)!$ (*où* deg X *et* d *désignent respectivement le degré projectif de* X *et le degré d'équations définissant* X *dans* A *dans un plongement projectif*).

Par définition de α l'image réciproque d'un point est formée des m–uplets $(x_1,..,x_m)$ tels que $x_{i+1}=t_ix_i-b'_i$ et donc de la forme $(x,t_1x-b_1,..,t_1..t_{m-1}x-b_{m-1})$ dans laquelle le point x vérifie : $x\in X\cap[t_1]^{-1}(X+b_1)\cap..\cap[t_1..t_{m-1}]^{-1}(X+b_{m-1})$; il faut donc prouver que les composantes de cet ensemble algébrique sont des translatés de sous-variétés abéliennes, si m est assez grand. Supposons prouvé que les composantes non abéliennes de tous les ensembles du type $(X+b_0)\cap[t_1]^{-1}(X+b_1)\cap..\cap[t_1..t_m]^{-1}(X+b_m)$ sont de dimension $\leq r$; soit alors $F:=X\cap[t_1]^{-1}(X+b_1)\cap..\cap[t_1..t_{m+k}]^{-1}(X+b_{m+k})$ contenant une composante Z non abélienne de dimension r, alors Z est aussi une composante de:
$F_1=(X+b_0)\cap[t_1]^{-1}(X+b_1)\cap..\cap[t_1..t_{m-1}]^{-1}(X+b_{m-1})$
et $[t_1..t_k](Z)$ est contenu dans:

$F_2=(X+b_k)\cap[t_{k+1}]^{-1}(X+b_{k+1})\cap..\cap[t_{k+1}..t_{m+k}]^{-1}(X+b_{m+k})$
et donc en est une composante. En utilisant la formule $\deg[t](Z)=\deg(Z)t^{2r}/|\mathrm{Ker}[t]\cap G_Z|$ et les autres lemmes de [H1] on obtient:

$$(t_{m+1}..t_k)^{2(r-\dim G_Z)}\leq(t_{k+1}..t_{m+k})^{2(\dim X-r)}\deg X(2d)^{\dim X}$$

ce qui borne visiblement k; on finit facilement la preuve du lemme par récurrence sur r en utilisant les hypothèses sur les t_i.

Considérons Θ'_i l'image réciproque de Θ par la i-ème projection sur A^{m-1}, soit $D_0=\alpha^*(\Sigma s_{i+1}{}^2\Theta'_i)=\Sigma(t_i s_{i+1} p_i - s_{i+1} p_{i+1})^*(\Theta)$; alors D_0 est ample si α est fini (et "génériquement ample" si α est génériquement fini). Si on s'arrange pour que $t_i s_{i+1}=s_i$ le diviseur D que nous souhaitons étudier s'écrit $D=D_0-\varepsilon\Sigma s_i{}^2\Theta_i$ et est donc certainement ample si ε est assez petit (mais dépendant des s_i). Il faut encore beaucoup travailler: Faltings utilise avec brio le théorème de Riemann-Roch, une variante du critère de Nakai-Moishezon (voir [Ha1] et [Ha2]) due à Kleiman et le théorème du produit pour rendre ε indépendant des paramètres.

5 Points algébriques sur les courbes

Le problème est le suivant: on considère une courbe lisse et projective C de genre g et l'on s'intéresse non pas à C(k) mais à l'union de tous les C(L) lorsque L décrit toutes les extensions de degré au plus d; notons cet ensemble $C_d(k)$; on veut savoir quand cet ensemble est fini et éventuellement le paramétrer si il est infini.
Le lien avec la conjecture de Lang est décrit dans [H1]: on commence par observer que les points algébriques de degré au plus d correspondent au points rationnels de $S^dC:=Cx...xC/\Sigma_d$, où Σ_d désigne le groupe symétrique avec son action évidente sur C^d. Plus précisément, à un point $x\in C(\bar{k})$ tel que $[k(x):k]=d$ on associe ses conjugués par Galois $x=x_1,..,x_d$ et le point $\varphi(x):=(x_1)+..+(x_d)\in S^dC(k)$; on identifie implicitement un élément de S^dC avec un diviseur effectif de degré d. Inversement, un point $D=(x_1)+..+(x_d)\in S^dC(k)$ est défini par des $x_i\in C(\bar{k})$ tels que l'ensemble $\{x_1,..,x_d\}$ soit stable par Galois et se décompose donc en orbites de points de degré $d_1,..d_r$ avec $d_1+..+d_r=d$; en particulier $[k(x_i):k]\leq d$. Ces considérations prouvent le lemme suivant:

LEMME 3:

a) $C_d(k)$ *est fini si et seulement si* $S^dC(k)$ *est fini.*

b) *Si* $C_{d-1}(k)$ *est fini alors* φ *définit une bijection entre* $C_d(k)$ *et* $S^dC(k)$ *à un nombre fini d'éléments près.*

Le lien avec la "conjecture" de Lang est établi grâce au théorème d'Abel-Jacobi: on

considère l'application:

ϕ_d: $S^dC \longrightarrow A=Jac(C)$

$(x_1)+..+(x_d) \longrightarrow x_1+..+x_d$ (la somme étant dans A bien sur)

On note classiquement $W_d=W_d(C)$ l'image; alors $\phi_d(D)=\phi_d(D')$ équivaut à $D=D'+(f)$ et si $D\neq D'$ on en déduit l'existence d'un morphisme

$f:C \longrightarrow \mathbf{P}^1$ non constant de degré au plus d; inversement l'existence d'un tel morphisme donne des diviseurs $f^*(x)$ (pour x dans $\mathbf{P}^1$) tous linéairement équivalents; en résumé ϕ_d contracte toutes les courbes rationnelles sur S^dC et celles-ci proviennent de morphismes de C sur $\mathbf{P}^1$.

La signification du lemme suivant est éclairée si l'on se souvient qu'une courbe de genre g admet un morphisme de degré d sur $\mathbf{P}^1$ si $d\geq 1+g/2$ (pour une preuve de ce fait, voir par exemple [K-L]).

LEMME 4: ϕ_d: $S^dC \longrightarrow W_d$ *est un isomorphisme si et seulement si il n'existe pas de morphisme non constant de degré*$\leq$d *de* C *sur* $\mathbf{P}^1$.

Le théorème suivant est une conséquence du théoreme 4 (Faltings [F2]) et était conjecturé dans [H1].

THÉORÈME 5: $C_d(k)$ *est fini pour tout corps de nombres si et seulement si* C *n'admet aucun morphisme de degré* $\leq$d *sur* $\mathbf{P}^1$ *et si* W_dC *ne contient aucun translaté de sous-variétés abéliennes.*

Remarquons que d'après des résultats généraux sur les diviseurs sur les courbes (voir par exemple [K-L]) la condition du théorème est vérifiée pour une courbe de genre g "générale" si $d<1+g/2$. On peut être plus précis par exemple dans le cas d=2; le théorème suivant est conséquence cette fois du théorème 4 (Faltings [F3]) comme cela est expliqué dans [H2].

THÉORÈME 6: $C_2(k)$ *est, à un nombre fini d'éléments près, l'union des points hyperelliptiques (i.e. images réciproques de* $\mathbf{P}^1(k)$ *par* $f:C\rightarrow\mathbf{P}^1$ *de degré* 2) *et surelliptiques ou bi-elliptiques (i.e. images réciproques de* E(k) *par* $f:C\rightarrow E$ *de degré* 2 *avec* E *courbe elliptique*)

Ce problème a été aussi considéré par Frey [Fr] sur les courbes modulaires et Silverman et Harris [Ha-Si]. Il est intéressant de remarquer que Vojta, en poussant

sa méthode obtient dans [V3] des résultats un peu moins précis mais en travaillant uniquement sur les courbes.
On peut donner l'exemple suivant d'une courbe de genre 3 hyperelliptique avec trois revêtements de degré 2 sur des courbes elliptiques:

$$y^2=(x^2-a^2)(x^2-a^{-2})(x^2-b^2)(x^2-b^{-2});$$

mais il est connu qu'une courbe hyperelliptique de genre >3 ne peut avoir un revêtement de degré 2 sur E (Preuve dans [F2] ou dans [A-C-G-H]); par contre la courbe $y^2-(x-a_1)(x-a_2)(x-a_3)=z^2-(x-a_4)...(x-a_{g+2})=0$ a pour genre g (si les a_i sont tous distincts) et est revêtement double de la courbe elliptique d'équation: $y^2=(x-a_1)(x-a_2)(x-a_3)$; en particulier si g>3 elle n'est pas hyperelliptique.

Harris et Abramovich ont poussé l'analyse plus loin en conjecturant:

CONJECTURE [A-H]
$C_d(k)$ *est fini pour tout corps de nombres* k *si et seulement si* C *ne possède aucun morphisme de degré au plus* d *de* C *sur* $\mathbf{P}^1$ *ou* E.

Il revient au même de conjecturer que si C n'est pas d-gonale, i.e. revêtement de $\mathbf{P}^1$ de degré d, et s'il existe une variété abélienne dans W_dC alors il existe une courbe elliptique dans W_dC et plus précisément C est "d-elliptique"; il s'agit donc d'une conjecture purement géométrique. Harris et Abramovic établissent dans le même article le résultat suivant:

THÉORÈME 7 [A-H]:
La conjecture est vraie si d<5 *sauf (peut-être) si* d=4 *et* g=7.

Ils donnent aussi un joli exemple d'une famille de courbes de genre 5 possédant une surface abélienne dans W_4 sans être un revêtement double d'une courbe de genre 2 (ni d'une courbe de genre 1).

(*ajouté sur épreuve, dernière minute*):
J'apprends que la conjecture de Abramovich et Harris est fausse: lorsque d≥10, Debarre et Fahlaoui ont construit des courbes de genre $g=1+d(d-1)/2$ n'admettant aucun morphisme de degré ≤d sur $\mathbf{P}^1$ ou une courbe elliptique mais telle que leurs W_d contiennent une courbe elliptique.
Dans une autre direction, Frey ("Curves with infinitely many points of fixed degree", à paraître dans Israel J.of Math.) a prouvé que si $C_d(k)$ est infini alors il existe un morphisme de C sur $\mathbf{P}^1$ de degré au plus 2d et défini sur k.

Bibliographie

[A-C-G-H] E. ARBARELLO, M. CORNALBA, P. GRIFFITHS and J. HARRIS. Geometry of curves, vol. I. *Springer* 1985.

[A-H] D. ABRAMOVICH and J. HARRIS. Abelian varieties and curves in W_dC. *Preprint.*

[Bg] F. BOGOMOLOV. Points of finite order on an abelian variety. *Izv. Akad. Nauk SSSR Ser. Mat.* **44** (1980); *AMS translation Math. USSR Izv.* **17** (1981), *55-72.*

[B] E. BOMBIERI. The Mordell conjecture revisited. *Ann. Scuola Norm. Sup. Pisa Ser. IV* **17** (1990), *615-640;* errata *ibid.* **18** (1991), *473.*

[Co-Si] G. CORNELL and J. SILVERMAN. Arithmetic geometry. *Springer* 1986.

[E-V] H. ESNAULT and E. VIEHWEG. Dyson's lemma for polynomials in several variables. *Inv. Math.* **78** (1984), *445-490.*

[F1] G. FALTINGS. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Inv. Math.* **73** (1983), *349-366.*

[F2] G. FALTINGS. Diophantine approximation on abelian varieties. *Annals of Math.* **133** (1991), *549-576.*

[F3] G. FALTINGS. The general case of Lang's conjecture. *Preprint.*

[F4] G. FALTINGS. *Preprint.*

[Fr] G. FREY. A remark on isogenies of elliptic curves over quadratic fields. *Compositio Math.* **58** (1986), *133-134.*

[G-S1] H. GILLET and G. SOULÉ. Un théorème de Riemann-Roch arithmétique. *C. R. Acad. Sci. Paris Sér. I Math.* **309** (1989), *929-932.*

[G-S2] H. GILLET and G. SOULÉ. Amplitude arithmétique. *C. R. Acad. Sci. Paris Sér. I Math.* **307** (1988), *887-890.*

[G-S3] H. GILLET and G. SOULÉ. Arithmetic intersection theory. *Publ. Math. IHES* **72** (1990), *93-174.*

[Ha1] R. HARTSHORNE. Algebraic geometry. *Springer* 1977.

[Ha2] R. HARTSHORNE. Ample subvarieties of algebraic varieties. *Springer Lecture Notes in Math.* **156** (1970).

[Ha-Si] J. HARRIS and J. SILVERMAN. Bielliptic curves and symmetric products. *Proc. Amer. Math. Soc.* **112** (1991), *347-356.*

[H1] M. HINDRY. Autour d'une conjecture de Serge Lang. *Inv. Math.* **94** (1988), *575-603.*

[H2] M. HINDRY. Points quadratiques sur les courbes. *C. R. Acad. Sci. Paris Sér. I Math.* **305** (1987), *219-221*

[K-L] S. KLEIMAN and D. LAKSOV. Another proof of the existence of special divisors. *Acta Math.* **132** (1974), *163-176.*

[La1] S. LANG. Fundamentals of diophantine geometry. *Springer* 1983.

[La2] S. LANG. Abelian varieties. *Interscience, New York* 1959.

[La3] S. LANG. Integral points on curves. *Publ. Math. IHES* **6** (1960), *27-43.*

[La4] S. LANG. Division points on curves. *Ann. Mat. Pura Appl. (4)* **70** (1965), *229-234.*

[M1] D. MUMFORD. A remark on Mordell's conjecture. *Amer. J. Math.* **87** (1965), *1007-1016.*

[M2] D. MUMFORD. Abelian varieties. *Oxford University Press* 1974.

[R1] M. RAYNAUD. Courbes sur une variété abélienne et points de torsion. *Inv. Math.* **71** (1983), *207-233.*

[R2] M. RAYNAUD. Sous-variétés d'une variété abélienne et points de torsion. *Arithmetic and geometry: papers dedicated to I.R. Shafarevich on the occasion of his sixtieth birthday, vol I, M. Artin and J. Tate ed., Birkhäuser* 1983, *327-352.*

[R3] M. RAYNAUD. Around the Mordell conjecture for function fields and a conjecture of Serge Lang. *Algebraic geometry, Springer Lecture Notes* **1016** (1983), *1-19.*

[Ro] F. ROTH Rational approximation to algebraic numbers. *Mathematika* **2** (1955), *1-20.*

[Sch1] W. SCHMIDT. Diophantine approximation. *Springer Lecture Notes* **785** (1980).

[Sch2] W. SCHMIDT. Approximation to algebraic numbers. *Enseign. Math.* **17** (1971), *187-253.*

[Se] J-P. SERRE. Lectures on the Mordell-Weil theorem (translated by M. Brown from notes by M. Waldschmidt). *Vieweg* 1989.

[Si] C. SIEGEL. Über einige Anwendungen diophantischer Approximationen. *Abh. Preuss. Akad. Wiss. Phys. Math. Kl.* (1929), *41-69.*

[Sz1] L. SZPIRO. Séminaire sur les pinceaux arithmétiques (la conjecture de Mordell). *Astérisque* **127** (1985).

[Sz2] L. SZPIRO. Sur les solutions d'un système d'équations polynomiales sur une variété abélienne (d'après Faltings et Vojta). *Séminaire Bourbaki, exposé 729, Astérisque* **189-190** (1990), *429-446.*

[Vi] C. VIOLA. On Dyson's lemma. *Ann. Scuola Norm. Sup. Pisa Ser. IV* **12** (1985), *105-135.*

[V1] P. VOJTA. Siegel's theorem in the compact case. *Annals of Math.* **133** (1991), *509-548.*

[V2] P. VOJTA. Dyson's lemma on the product of two curves. *Inv. Math.* **98** (1989), *107-113.*

[V3] P. VOJTA. Arithmetic discriminants and quadratic points on curves. *Arithmetic algebraic geometry, Texel '89, Birkhäuser "Progress in Mathematics"* **89** (1991), *356-376.*

[V4] P. VOJTA. A generalization of theorems of Faltings and Thue-Siegel-Roth-Wirsing. *J. Amer. Math. Soc.* **5** (1992), *763-804.*

[W] A. WEIL. Sur les courbes algébriques et les variétés qui s'en déduisent. *Hermann, Paris* 1948.

Marc HINDRY
UFR Mathématiques, Université Paris 7
2 Place Jussieu
75251 Paris cedex 05, FRANCE
et
Mathematics, Brown University
Providence RI 02912, U.S.A.