LUCIEN SZPIRO

La conjecture de Mordell

Séminaire N. Bourbaki, 1983-1984, exp. nº 619, p. 83-103.
<http://www.numdam.org/item?id=SB_1983-1984__26__83_0>

Séminaire BOURBAKI
36e année, 1983/84, n° 619 Novembre 1983

LA CONJECTURE DE MORDELL
[d'après G. Faltings]

par Lucien SZPIRO

0. PLAN DE L'EXPOSÉ

1. INTRODUCTION : LES ÉQUATIONS DIOPHANTIENNES

On appelle équations diophantiennes les systèmes finis d'équations :

$$F_1(X_1,\dots,X_n) = 0 \ , \ F_2(X_1,\dots,X_n) = 0 \ , \ F_t(X_1,\dots,X_n) = 0$$

où les F_i sont des polynômes en les variables $(X_1,\dots,X_n)$, à coefficients rationnels - ou par extension à coefficients dans un corps de nombres. On s'intéresse aux solutions rationnelles - ou par extension aux solutions dans un corps de nombres - de ces équations.

Soit K un corps de nombres contenant tous les coefficients des F_i, et soit $\sigma : K \to \mathbb{C}$ un plongement de K dans le corps des nombres complexes. Il est naturel de considérer la variété fermée V dans l'espace affine $\mathbb{A}^n_{\mathbb{C}}$ définie par les F_i .

(Si les F_i sont homogènes on regardera plutôt la sous-variété fermée de $\mathbb{P}^{n-1}_{\mathbb{C}}$ définie par les F_i.) Le premier cas intéressant est celui où la variété V est irréductible de dimension 1 sur $\mathbb{C}$ et sera essentiellement le seul cas étudié dans cet exposé. Soit $V = C$ une courbe algébrique sur le corps des complexes $\mathbb{C}$. On associe à C un entier g, appelé son genre, défini de la façon suivante : Soit $\overline{C}$ la fermeture projective de C et $\tilde{C}$ la normalisée (désingularisée) de $\overline{C}$. On sait que $\tilde{C}$ comme variété différentielle est une surface de Riemann compacte sans bord. Le nombre de trous de $\tilde{C}$ est le genre g. $(H^1(\tilde{C},\mathbb{Z}) \simeq \mathbb{Z}^{2g})$. Les solutions des équations $(F_i = 0)$ dans un corps K correspondent bijectivement à l'ensemble des points rationnels de C sur K, noté $C(K)$.

Prenons par exemple une seule équation $F(X,Y,Z)$ homogène de degré n à coefficients entiers. F définit une courbe plane C dans $\mathbb{P}^2$. Supposons que C n'ait pour singularités, sur $\mathbb{C}$, que des *points doubles à tangentes distinctes* et soit r le nombre de ces points doubles. Alors le genre de $\tilde{C}$ est égal à :

$$\frac{(n-1)(n-2)}{2} - r .$$

Comme F est homogène si (a,b,c) sont des rationnels tels que $F(a,b,c) = 0$ et si $\lambda \in \mathbb{Q}$, $F(\lambda a,\lambda b,\lambda c) = 0$ aussi. On ne s'intéressera donc qu'aux solutions entières (a,b,c) sans facteur commun. L'ensemble de telles solutions est en bijection avec $C(\mathbb{Q})$.

L'importance de cet exemple vient de ce qu'on peut montrer que toute courbe lisse et projective sur K a un modèle dans $\mathbb{P}^2$ dont les singularités sont celles décrites ci-dessus. L'importance du genre vient de ce qu'il permet de définir trois cas ($g = 0$, $g = 1$, $g \geq 2$) où l'ensemble des solutions est de différente nature.

THÉORÈME 1.— *Soit* K *un corps de nombres et* C *une courbe lisse, géométriquement connexe, projective sur* K *et de genre* g. *Alors pour tout corps de nombres* K' *on a*

a) *Si* $g = 0$ *et si* $C(K') \neq \emptyset$, $C \underset{K'}{\simeq} \mathbb{P}^1_{K'}$ *(infinité de solutions).*

b) *Si* $g = 1$, $C(K')$ *est vide ou est un espace principal homogène sous un groupe commutatif de type fini (théorème de Mordell* [Mo]*).*

c) *Si* $g \geq 2$, $C(K')$ *est fini (conjecturé par Mordell* [Mo], *démontré par Faltings* [F2]*).*

La partie b) a été généralisée par A. Weil dans sa thèse : soit A une variété abélienne définie sur un corps de nombres K ; alors $A(K)$ est un groupe commutatif de type fini (théorème de Mordell-Weil).

Notons tout de suite que, sauf dans des cas particuliers, la description des solutions pour $g \geq 1$ n'est *pas effective*. Par exemple si C est plongée dans un espace projectif $\mathbb{P}^n_{\mathbb{Q}}$, $C(\mathbb{Q})$ est en bijection avec les points de coordonnées homogènes $(x_0,\ldots,x_n)$, $x_i \in \mathbb{Z}$, $\mathrm{pgcd}(x_i) = 1$ qui sont dans C . Un résultat effectif dirait "quelque chose" sur le $\sup_i |x_i|$ (et donc sur le nombre de points de $C(K)$ quand $g \geq 2$). Ce n'est pas le cas du théorème de Faltings.

A part les résultats de Mordell et Weil cités plus haut, et avant les travaux de Faltings, on avait les résultats suivants de Siegel sur les points entiers :

DÉFINITION.– *Soit* K *un corps de nombres,* S *un ensemble fini de places de* K *et* X *une courbe* affine *lisse sur* K . *Un point entier de* X *sur* K *par rapport à* S *est un point rationnel de* X *sur* K *dont les coordonnées ont des dénominateurs à support dans* S .

On peut prendre pour exemple $K = \mathbb{Q}$, $S = \emptyset$, X une courbe plane dans $\mathbb{A}^2_K$ d'équation $F(X,Y) = 0$, un point entier est une solution entière de cette équation. La définition ne dépend pas du système de coordonnées affines choisies. En effet si $\widetilde{X} \longrightarrow \mathrm{Spec}\ \mathcal{O}$ ($\mathcal{O}$ = anneau des entiers de K) est le modèle régulier minimal de la compactification $\overline{X}$ de X , et si D est la fermeture schématique de $\overline{X} - X$, un point entier de X sur K par rapport à S assez grand n'est autre chose qu'une section du morphisme

$$\widetilde{X} - D \longrightarrow \mathrm{Spec}\ \mathcal{O} - S\ .$$

THÉORÈME [Si].– *Soit* K *un corps de nombres,* S *un ensemble fini de places de* K , X *une courbe* affine *et lisse sur* K *dont la compactification lisse* $\overline{X}$ *est de genre* g . *Alors les points entiers de* X *sur* K *par rapport à* S *sont en nombre fini dans les deux cas suivants :*

a) $g = 0$ *et* $\#(\overline{X} - X) \geq 3$.

b) $g > 0$.

Ce théorème ne donne pas, lui non plus, de borne effective pour la hauteur des points entiers. Cependant les travaux de Baker sur les équations dites de Thue

$$F(X,Y) = \mathrm{cste}\ ,$$

F polynôme homogène qui a trois racines distinctes, donnent une borne effective pour les solutions entières. Nous passerons pudiquement cette borne sous silence.

Disons enfin un mot des problèmes analogues où K est remplacé par un corps de fonctions K d'une courbe C sur un corps k , qui ne provient absolument pas de k (supposé algébriquement clos).

a) si $g = 0$, $C \simeq \mathbb{P}^1_K$ (théorème de Tsen).

b) $g = 1$, $C(K)$ est vide ou un groupe de type fini (Néron-Severi).

c) $g \geq 2$, $C(K)$ est fini ($k = \mathbb{C}$ Manin [Ma] caract $k = p > 0$ Samuel [Sa]).

Notons que Grauert a donné une autre démonstration du théorème de Manin dans [Gr], c'est cette démonstration qui a été adaptée par Samuel à la caractéristique positive. Une démonstration de ce dernier cas, plus dans la ligne de cet exposé, est fournie dans [S].

2. LE PROBLÈME DE SHAFAREVITCH

2.1. L'ensemble Ш$(B,\underline{F})$

Soit B (pour base) un schéma régulier (ici ce sera souvent un ouvert d'un anneau d'entiers algébriques ou un ouvert d'une courbe projective et lisse sur un corps k). Soit $\underline{F}$ (pour fibre) une description de variété algébrique et de ses dégénérescences éventuelles (par exemple $\underline{F}$ = courbe lisse et projective de genre g , à dégénérescence semi-stable ou $\underline{F}$ = variété abélienne de dimension g munie d'une polarisation de degré n). On appelle *ensemble de Shafarevitch* défini par B et $\underline{F}$ et on note Ш$(B,\underline{F})$ l'ensemble des classes de B isomorphismes de schémas

$$f : X \to B$$

dont les fibres sont décrites par $\underline{F}$.

Exemple 1.1.— Morphismes finis, cas arithmétique

Soit $\mathcal{O}$ un anneau d'entiers algébriques, S un ensemble fini de places de $\mathcal{O}$, $B = \operatorname{Spec} \mathcal{O} - S$ et n un entier positif. Une variation sur un théorème classique de Hermite permet d'affirmer que Ш$(B$, n points$)$ est fini. Nous reviendrons en 2.2 sur cet énoncé.

Exemple 1.2.— Morphismes finis de courbes (caract 0)

Soit C une courbe projective et lisse sur un corps k , S un ensemble fini de points de C et n un entier. On sait démontrer (essentiellement en utilisant le théorème d'unicité de Riemann) que Ш$(C - S$, n points$)$ est fini.

Exemple 1.3.— Le groupe de Tate-Shafarevitch

Soit K un corps de nombres et A une variété abélienne sur K . Alors l'ensemble des classes de K isomorphismes d'espaces principaux homogènes sous A qui deviennent isomorphes à A sur $\hat{K}$ pour chaque complétion de K est un groupe qu'on appelle le groupe de Tate-Shafarevitch. Il est compatible avec les notations habituelles de noter ce groupe Ш$(K$, formes de A , $\hat{K}$ iso à A pour tout $\hat{K})$. C'est une conjecture, non démontrée à l'heure actuelle, que Ш$(K$, $\hat{K}$ iso à $A)$ est un groupe fini.

Exemple 1.4.— Sur nos deux bases préférées $\operatorname{Spec} \mathcal{O} - S$ et $C - S$, les cas où S est vide sont intéressants. Par exemple $\#$Ш$(\operatorname{Spec} \mathbb{Z}$, n points$) = 1$ si $n \geq 2$ est un théorème de Minkowski qui se lit habituellement sous la forme : le discriminant d'un corps de nombres de degré au moins deux est en valeur absolue supérieur ou égal à deux.

Exemple 1.5.— A. Grothendieck a montré dans [Gro2] le théorème suivant :

Soit B un ouvert d'une courbe algébrique sur $\mathbb{C}$ et $P \in B$ et soit $A \xrightarrow{f} B$ un schéma abélien polarisé, alors si on fixe la fibre de P , le morphisme f est rigide. (On trouvera une autre preuve de ce fait dans [D2].) D'autre part G. Faltings a montré dans [F2] que l'ensemble de tels A est une famille limitée (nous en indiquons plus bas la démonstration de P. Griffiths [Gri]).

Exemple 1.6.– La conjecture de Shafarevitch [Sh1]

Shafarevitch dans son adresse au congrès international des mathématiciens de Stockholm a posé le problème suivant :

Soit K un corps de nombres, S un ensemble fini de places de K, g un entier supérieur ou égal à deux ; montrer que l'ensemble des classes de K isomorphismes de courbes lisses et projectives de genre g sur K ayant bonne réduction en dehors de S est fini.

Si $\mathcal{O}$ est l'anneau des entiers de K et $B = \operatorname{Spec} \mathcal{O} - S$ le problème de Shafarevitch peut s'énoncer : montrer que

$\# Ш(B,$ courbes lisses et proj de genre $g) < \infty$.

Rappelons qu'une courbe C, lisse et projective de genre $g \geq 1$ sur K, possède un modèle minimal unique régulier sur $\mathcal{O}$. C'est-à-dire qu'il existe un schéma régulier X et un morphisme projectif $X \xrightarrow{f} \operatorname{Spec} \mathcal{O}$ dont la fibre générique est C et tel qu'il n'y ait pas de $\mathbb{P}^1$ de self-intersection (-1) dans les fibres (Abhyankar [Ab] ou Lipman [Li] pour modèle régulier, Shafarevitch [Sh2] pour minimalité). On dit que C *a bonne réduction en* $\mathfrak{p} \in \operatorname{Spec} \mathcal{O}$ *si* $X(\mathfrak{p})$ *est lisse.*

On peut bien entendu faire la même conjecture dans le cadre géométrique :

$\# Ш(C - S,$ courbes lisses proj. genre $g) < \infty$.

2.2. Les deux méthodes pour borner un ensemble de Shafarevitch

2.2.1. Hauteurs, degré

2.2.1.1. *Cas géométrique* C courbe sur le corps k. La technique employée dans les cas géométriques se divise en deux :

a) famille limitée,

b) rigidité.

a) Pour les familles de variétés abéliennes ou de courbes $X \xrightarrow{f} C$ on réussit en terme de S et g, à borner d = - degré sur C de l'algèbre de Lie de la variété abélienne ou de la jacobienne de la courbe (S est lieu de mauvaise réduction qu'on a supposé semi-stable). Par exemple si $f : X \to C$ est une famille de courbes de genre $g \geq 2$ dont la classe de Kodaira-Spencer n'est pas nulle : $12d \leq 8g(g-1)(q-1+\frac{s}{2})$ où q = genre de C et $s = \# S$ (*cf.* [S]). Si le corps de base est $\mathbb{C}$ Arakelov [A1] a une borne plus fine

$$d \leq (g - g_0)(q - 1 + \frac{s}{2})$$

où g_0 est la dimension de la partie fixe de la jacobienne. Pour les familles de variétés abéliennes Griffiths dans [Gri] nous a montré : $d \leq 8\pi g(q-1+\frac{s}{2})$. Cette dernière inégalité sur $\mathbb{C}$, est aussi démontrée quand $S = \emptyset$, pour les familles de variétés abéliennes dans [M-B,S]. Une borne moins explicite est donnée dans [F2].

Une famille $X \in Ш(C-S,\ldots)$ correspond à un morphisme de C dans M_g (ou A_g). Les graphes Γ de ces morphismes sont des sous-variétés de $C \times M_g$ (ou $C \times A_g$). Le fait d'avoir borné d permet - plus ou moins facilement - de montrer qu'il existe un faisceau ample L sur $C \times M_g$ (ou $C \times A_g$) dont le degré sur Γ est borné. On a donc une variété de Chow W, de type fini sur le corps de base k qui "paramétrise" l'ensemble des $X \in Ш(C-S,\ldots)$.

b) Dans le cas des *familles de courbes* non constantes (ou ce qui revient presqu'au même à classe de Kodaira-Spencer non nulle) on montre que $f : X \to C$ semi-stable, S fixé est rigide ([A1], [S]). Pour cela on remarque avec Arakelov [A1] que les déformations infinitésimales de f sont paramétrées par $H^1(X,\omega_{X/C}^{-1})$. Si on est en caractéristique zéro, Arakelov ayant montré que $\omega_{X/C}$ est numériquement positif (i.e. presque ample), il conclut par le "vanishing theorem" de Kodaira-Ramanujam. En caractéristique positive, on montre dans [S] que les mêmes énoncés sont valables. Il a fallu faire plus attention car le "vanishing de Kodaira" n'est pas vrai en caractéristique positive (*cf.* [Mu], [R3], [S]).

On vérifie alors que $Ш(C-S$, courbes de genre g, semi-stables) est fini car dans chaque composante connexe de W on a un seul élément de $Ш$. On n'a aucune information sur le nombre de ces composantes connexes.

En caractéristique zéro on déduit par 2.1 exemple 1.2 et le théorème de Grothendieck du § 3 (réduction semi-stable) que $\# Ш(C-S$, courbes de genre g$) < \infty$.

En caractéristique positive 2.1 exemple 1.2 n'est pas vrai et, en fait, on ne peut retirer l'hypothèse de semi-stabilité comme on le voit par un contre-exemple dans [S].

2.2.1.2. *Cas arithmétique* : K corps de nombres, $\mathcal{O}$ son anneau d'entiers.

a) *Hauteur naïve*

Soit P un point de l'espace projectif $\mathbb{P}^n$. Soient $x_0,\ldots,x_n$ des coordonnées homogènes de P que l'on suppose dans $\mathbb{Z}$ et sans facteur commun. On pose $H(P) = \sup_i |x_i|$. Il est évident que l'ensemble des points P de $\mathbb{P}^n(\mathbb{Q})$ tels que $H(P)$ soit borné est fini.

Si on est sur un corps de nombres K, P un point de coordonnées $(x_0,\ldots,x_n)$, on pose $H(P) = \prod_{\sigma\in\Phi} \sup_i |x_i|_\sigma^{\varepsilon_\sigma}/N(\Sigma x_i\mathcal{O})$ où Φ est l'ensemble des places archimédiennes de K, $\varepsilon_\sigma = 1$ (resp. 2) si σ est réelle (resp. complexe). $H(P)$ ne dépend pas du choix des coordonnées par la formule du produit : $\prod_\sigma |f|_\sigma^{\varepsilon_\sigma} = N(f)$, $f \in K$. L'ensemble des points de $\mathbb{P}^n(K)$ tel que $H(P)$ soit borné est fini.

Il est clair qu'on a le même énoncé de finitude si on remplace $\sup|x_i|$ par $\sqrt{\Sigma|x_i|^2}$. En réinterprétant par exemple

$$\prod_{\sigma\in\Phi} \left(\sqrt{\Sigma|x_i|_\sigma^2}\right)^{\varepsilon_\sigma}/N(\Sigma x_i\mathcal{O})$$

on introduit des hauteurs plus "sophistiquées".

b) *Hauteur arakélovienne* ([W2], [A1])

On veut une notion de "hauteur" qui a des propriétés proches de celles du degré dans l'analogue géométrique. Nous en donnons ici le yoga.

Soit K un corps de nombres, $\mathcal{O}$ son anneau d'entiers, $n = d^\circ(K/\mathbb{Q})$, D = valeur absolue du discriminant. Soit L un faisceau inversible sur $\mathcal{O}$ muni pour chaque place archimédienne σ d'une forme hermitienne

$$< , >_\sigma : L \otimes_\sigma \mathbb{C} \otimes \overline{L \otimes_\sigma \mathbb{C}} \longrightarrow L \otimes_\sigma \mathbb{C} .$$

Soit $s \in L$, on pose

$$d^\circ(L) = \log \frac{\# L/sL}{\prod_\sigma \|s\|_\sigma^{\varepsilon_\sigma}} ,$$

$d^\circ(L)$ ne dépend pas de s (formule du produit). Les classes de faisceaux inversibles hermitiens, modulo isométries, forment un groupe noté

$$\operatorname{Pic}_c(\mathcal{O}) .$$

On a une suite exacte

$$0 \longrightarrow \mathbb{R}^{r_1+r_2}/\log \mathcal{O}^\times \longrightarrow \operatorname{Pic}_c(\mathcal{O}) \longrightarrow \operatorname{Cl}(\mathcal{O}) \longrightarrow 0$$

où r_1 = nombre de places réelles, r_2 = nombre de places complexes, $\mathcal{O}^\times$ unités de $\mathcal{O}$. On voit facilement que $d^\circ : \operatorname{Pic}_c(\mathcal{O}) \to \mathbb{R}$ est additif.

On introduit une "caractéristique d'Euler-Poincaré" $\chi(L) = -\log \operatorname{vol} \mathbb{R}^n/L$ où $L \to \mathbb{R}^n$ par $\mathbb{R}^n \simeq \oplus_\sigma L \otimes_\sigma K_\sigma$, $K_\sigma = \mathbb{R}$ (resp. $K_\sigma = \mathbb{C}$) si σ réelle (resp. σ complexe), et où le volume est mesuré par les métriques euclidiennes associées à $< , >_\sigma$.

On introduit une caractéristique modifiée $\chi'(L) = -\log \dfrac{2^n \operatorname{vol}(\mathbb{R}^n/L)}{2^{r_1}\pi^{r_2}}$ qui se justifie par le lemme 3 ci-dessous. Par exemple on a : $\chi'(\mathcal{O}) = r_2 \log \frac{\pi}{2} - \frac{1}{2} \log D$. On a aussi une notion de sections

$$H^\circ(L) = \{ s \in L \mid \|s\|_\sigma \le 1 \quad \forall \sigma \} .$$

Par exemple $H^\circ(\mathcal{O}) = \{0\} \cup \mu(\mathcal{O})$; $\mu(\mathcal{O})$ = les racines de l'unité dans $\mathcal{O}$. ($\mathcal{O} \otimes_\sigma \mathbb{C}$ est muni de la métrique telle que $\|1\|_\sigma = 1 \quad \forall \sigma$.)

On interprète géométriquement $\chi'(L)$ de la façon suivante :

$$\chi'(L) = \log \lim_{t \to \infty} 2^{-n} \# H^\circ(L_t)/t^n$$

où L_t est obtenu à partir de L en multipliant les métriques par t^{-1}.

Pour montrer qu'on se rapproche de la théorie du degré sur les courbes algébriques citons quatre lemmes dont les trois premiers sont de démonstration immédiate (le quatrième étant une reformulation du lemme de Minkovski sur les points d'un réseau dans un compact convexe symétrique).

Lemme 0 (Riemann-Roch !).— $\chi'(L) = \deg L + \chi'(\mathcal{O})$.

Lemme 1.— *Si* $d^\circ(L) < 0$ *alors* $H^\circ(L) = 0$.

Lemme 2.— *Si* $d^\circ(L) = 0$ *et* $H^\circ(L) \neq 0$ *alors* $L \cong \mathcal{O}$ *(comme faisceaux métrisés)* $\mathcal{O}$ *faisceau métrisé trivial.*

Lemme 3 (Minkowski).– *Si* $\deg(L) \geq -\chi'(\mathcal{O})$ *alors* $H^{o}(L) \neq 0$.

On peut retrouver facilement les théorèmes élémentaires de théorie des nombres (discriminant plus grand que un, théorème des unités, finitude de $Cl(\mathcal{O})$ et l'exemple 1.1 du § 2...) à partir de ces quatre lemmes.

Soit X une variété algébrique sur $\mathcal{O}$: $X \xrightarrow{f} \mathcal{O}$. Supposons que X soit projective, i.e. munie d'une immersion fermée

$$X \longrightarrow \mathbb{P}^N_{\mathcal{O}} .$$

Soit $P \in X(K)$ un point rationnel, il lui correspond une section $E \hookrightarrow X$ du morphisme f . $E \simeq \operatorname{Spec} \mathcal{O}$. Supposons que $\mathcal{O}_X(1)$ soit muni de métriques hermitiennes aux places à l'infini. Alors $\mathcal{O}_X(1)/E$ est un faisceau inversible métrisé sur $\mathcal{O}$ comme plus haut. Il a donc un degré : définissons : $d^o\mathcal{O}_X(1)/E = h(P)$.

PROPOSITION.– *L'ensemble des points* P *de* $X(K)$ *tels que* $h(P)$ *est borné est un ensemble fini.*

Pour vérifier cette proposition notons d'abord que l'énoncé ne dépend pas des métriques hermitiennes choisies car $X_{\mathbb{C}}$ est compacte. On prend alors sur $\mathcal{O}_X(1)$ une métrique de Fubini-Study et on constate avec plaisir que

$$\exp h(P) = \prod_{\sigma\in\Phi} \left(\sqrt{\Sigma\, |x_i^2|}\right)^{\varepsilon_\sigma} / N(\Sigma\, x_i\mathcal{O})$$

comme à la fin du a) !

2.2.2. Représentation du π_1 ou du groupe de Galois

2.2.2.1. *Cas géométrique*. Soit C une courbe, S un ensemble fini de points. On connait le groupe fondamental $\pi_1(C-S)$. On peut donc à partir de ses représentations avoir des informations sur les ensembles $Ш(C-S,\ldots)$.

Exemple 2.1.– Morphismes finis (caract. zéro)

Par le théorème d'unicité de Riemann un quotient de $\pi_1(C-S)$ de cardinal n correspond biunivoquement à $C' \to C$ étale sur $C-S$, galoisien de $d^o n$. On peut, en prenant la clôture galoisienne, remplacer un élément de $Ш(C-S, n \text{ points})$ par un revêtement galoisien d'ordre $n!$. On en conclut que $Ш(C-S, n \text{ points})$ est fini car l'ensemble des quotients de $\pi_1(C-S)$ de cardinal $n!$ est un ensemble fini (exemple 1.2 de 2.1).

Notons que la borne obtenue par Griffiths dans [Gri] utilise aussi cette technique.

2.2.2.2. *Cas arithmétique* : c'est le groupe de Galois de la clôture algébrique $\overline{K}/K$ qui joue le rôle du groupe fondamental.

Exemple 2.2.– Esquisse de démonstration de l'exemple 1.1 du § 2

Outre que cet exemple est d'un emploi constant dans cet exposé, la démonstration a l'avantage d'utiliser les deux techniques pour borner un ensemble $Ш$. Il s'agit ici de $Ш(\operatorname{Spec} \mathcal{O} - S, n \text{ points})$.

a) Hermite a montré que l'ensemble des surcorps K' de K de discriminant D donné est fini. Dans le langage de 2.2.1.2 b), on met sur le faisceau inversible $\mathcal{O}'$ des métriques $\| \ \|'_{\sigma}$ qui lui donnent un degré $= -\chi'(\mathcal{O}')$, $(-\chi'(\mathcal{O}') = \frac{1}{2}\log D' - r'_2 \log \frac{\pi}{2})$ de la façon suivante (on suppose pour simplifier qu'il n'y a que des places complexes) :

$$\|1\|'_{\sigma_1} = (\tfrac{2}{\pi})^{r'_2/2} D'^{-1/4} 2^{1-r'_2} \quad ; \quad \|1\|'_{\sigma_i} = 2 \ , \quad \forall i \neq 1 \ .$$

Par le lemme 3, il existe $x \in \mathcal{O}$ tel que

$$|\sigma_1(x)| \leq (\tfrac{2}{\pi})^{-r'_2/2} D'^{+1/4} 2^{r_2-1} \quad ; \quad |\sigma_i(x)| \leq \frac{1}{2} \ ,$$

où $| \ |_{\sigma_i}$ est la métrique usuelle. Un tel élément x est un élément primitif de K' sur K (en fait sur $\mathbb{Q}$) ; en effet

$$\Pi |\sigma_i(x)| = N(x) \geq 1$$

car $x \in \mathcal{O}'$. On a alors $|\sigma_1(x)| > 1$ et $\sigma_1(x)$ ne peut être égal à aucun $\sigma_j(x)$, $j \neq 1$.

On a donc montré que pour un discriminant donné il existe un élément primitif de hauteur bornée.

b) Il reste à montrer que pour $n = \deg K'/K$ fixé et $S = \text{Support } D_{K'/K}$ fixé, le discriminant est borné. On peut supposer (quitte à remplacer n par $n!$) que K'/K est galoisienne. On utilise alors la seconde méthode : analyser le groupe de Galois. Ceci est fait dans Serre [Se1] à l'aide des groupes de ramification supérieure. On se ramène à une situation locale : $K \to L$ galoisien de groupe G, complet pour une valuation discrète, de degré n, d'indice de ramification absolu e . Soit $\mathfrak{P}$ l'idéal de la valuation de L . On note G_i le sous-groupe de G qui opère trivialement sur $\mathcal{O}_L/\mathfrak{P}^{i+1}$.

Soit D le discriminant de L sur K . On a

- $v_L(D) = \sum_0^{\infty}(\# G_i - 1)$,
- G_i/G_{i+1} est un sous-groupe de $\mathfrak{P}^i/\mathfrak{P}^{i+1}$,
- $G_i = (1)$ si $i > e/p-1$.

3. PASSAGE AUX VARIÉTÉS ABÉLIENNES

Si C est une courbe lisse et projective sur $\mathbb{C}$, sa *jacobienne* $J(C)$ est la variété abélienne principalement polarisée dont le tore complexe sous-jacent est :

$$H^0(C,\Omega^1_C)^{\vee}/H_1(C,\mathbb{Z})$$

[on envoie un lacet γ dans la forme linéaire sur les différentielles définie par l'application $\gamma \longrightarrow (\omega \longmapsto \int_{\gamma}\omega)$].

La jacobienne paramétrise les diviseurs de degré zéro sur C à équivalence rationnelle près. Cette dernière définition se généralise en caractéristique positive : $J(C) = \mathrm{Pic}^0(C)$. Pour une famille de courbes projectives dont l'espace de paramètres est par exemple un anneau d'entiers algébriques ou une courbe projective et lisse sur un corps,

$$X \xrightarrow{f} B ,$$

on a encore une notion de jacobienne relative : $J(X) = \mathrm{Pic}^{\circ}(X/B)$ qui est la composante neutre du schéma de Picard relatif $R^1 f_*(\mathcal{O}_X^*)$. $J(X)$ est un schéma en groupes sur B : $J(X) \to B$. On dit qu'un schéma en groupes de ce type a bonne réduction en un point P de B si la fibre $J(X)/P$ est une variété abélienne.

Lemme.— Soit C *une courbe projective, lisse, géométriquement connexe sur un corps* K . *Soit* B *un schéma de dimension* 1 *dont le corps de fonctions est* K *et* P *un point de* B . *Alors si* C *a bonne réduction en* P , $J(C)$ *a bonne réduction en* P .

On voit ainsi qu'en prenant une courbe sur un corps de nombres C/K on a construit une *variété abélienne* A *principalement polarisée* $J(C)/K$ vérifiant les trois conditions suivantes :

1) La dimension de A est fixée (égale au genre g de C).
2) A est une variété abélienne définie sur K .
3) L'ensemble de bonne réduction de A contient celui de C .

En fait le théorème de Torelli permet de reconstruire une courbe à partir de sa jacobienne. Une analyse moderne de ce théorème se trouve dans Oort [O]. Nous en donnons la forme la plus efficace pour notre problème. Nous avons d'abord à introduire les modules :

- $M_{g,n}$ est l'espace de modules des courbes lisses, connexes de genre g sur un corps k , munies d'une base sur $\mathbb{Z}/n\mathbb{Z}$ des points de division par n $(n \geq 3)$ dans sa jacobienne (rigidification). $M_{g,n}$ est une variété algébrique lisse de dimension $3g-3$ sur k qui possède une courbe universelle.
- $A_{g,n}$ est l'espace de modules des variétés abéliennes principalement polarisées, de dimension g sur un corps k munies d'une base sur $\mathbb{Z}/n\mathbb{Z}$ des points de division par n $(n \geq 3)$. $A_{g,n}$ est une variété algébrique de dimension $\frac{g(g+1)}{2}$ sur k qui possède une variété abélienne principalement polarisée universelle.

THÉORÈME (Torelli).— *Pour* $n \geq 3$ *premier à la caractéristique, l'application des périodes*

$$M_{g,n} \to A_{g,n}$$

qui à une courbe associe sa jacobienne, est un morphisme quasi-fini.

La "conjecture de Shafarevitch pour les variétés abéliennes" s'énonce de la façon suivante :

Soit K *un corps de nombres,* S *un ensemble fini de places de* K , g *et* n *des entiers positifs. Montrer que l'ensemble des variétés abéliennes sur* K *de dimension* g , *munies d'une polarisation de degré* n *et ayant bonne réduction en dehors de* S *est un ensemble fini modulo* k *isomorphismes.*

On peut résumer cette conjecture par :

$\#\,Ш(\mathrm{Spec}\,\mathcal{O} - S$, var. ab. dim g , pol. de $d^{\circ}n) < \infty$.

Rappelons qu'une variété abélienne A sur K possède un modèle de Néron unique [N], $X \longrightarrow \operatorname{Spec} \mathcal{O}$, qui est un schéma en groupes commutatif et lisse, et qui est caractérisé par la propriété universelle suivante : l'application canonique

$$A(R_K) \longleftarrow X(R)$$

est une bijection pour tout schéma R lisse sur $\mathcal{O}$.

On dit que A/K a bonne réduction en dehors de S, si son modèle de Néron a bonne réduction en dehors de S.

Grâce à l'exemple 1.1 du § 2 et au théorème de Torelli on voit que "Shafarevitch pour les variétés abéliennes" implique "Shafarevitch pour les courbes". En effet fixons $n \geq 3$. L'extension K' de K, où les points de division par n sont rationnels, est de degré plus petit que $n^{(2g)^2}$ et n'est ramifiée qu'en $S \cup \{n\}$.

En fait quand on introduit les points de division par $n \geq 3$ dans une variété abélienne sa mauvaise réduction "n'est pas si mauvaise" : elle est "semi-stable".

DÉFINITION.– *Soit* V *un anneau de valuation discrète de corps de fractions* K *et corps résiduel* k. *Soit* A *(resp.* C *) un schéma en groupes à fibres connexes (resp. une courbe) sur* Spec V. *Supposons que* A_K *(resp.* C_K *) soit une variété abélienne (resp. une courbe projective, lisse, géométriquement connexe) ; on dit que* A *(resp.* C *) a réduction semi-stable si la fibre spéciale* A_k *(resp.* C_k *) est une extension d'une variété abélienne par un groupe de type multiplicatif (resp. est une courbe réduite dont les singularités sont des points doubles ordinaires, et qui ne contienne pas de* $\mathbb{P}^1$ *qui se contracte dans* C *). Il revient au même de dire que la monodromie est unipotente.*

THÉORÈME (A. Grothendieck [G2]).– *Soit* V *un anneau de valuation discrète de corps de fractions* K *et soit* A_K *une variété abélienne sur* K. *Alors si pour un entier* $n \geq 3$, *premier à la caractéristique résiduelle, les points de divisions par* n *dans* A_K *sont rationnels sur* K, *le modèle de Néron de* A_K *a réduction semi-stable.*

A. Grothendieck a montré le premier qu'une variété abélienne a "potentiellement" réduction semi-stable (i.e. après un changement de base fini). Les efforts conjugués de Serre, Tate et Raynaud permettent d'énoncer le théorème de réduction semi-stable sous cette forme simple.

Remarque.– Nous avons invoqué plus haut le plongement d'une courbe dans sa jacobienne. On peut rêver d'une stratégie pour démontrer le théorème de Mordell-Faltings, résumée dans la conjecture suivante (S. Lang) :

Soit A *une variété abélienne sur* $\mathbb{C}$ *et* L *un* $\mathbb{Z}$ *module libre de type fini dans* A. *Soit* C *une courbe dans* A *; alors* $\bigcup_n (C \cap n^{-1}L)$ *est fini.*

Cette conjecture a été montrée directement dans le cas $\operatorname{rang}(L) = 0$ par M. Raynaud [R2] (points de torsion). Dans ce même article Raynaud montre que le théorème de Mordell-Faltings (encore à l'état de conjecture lors de la parution de [R2]) implique l'énoncé ci-dessus.

4. LE PROBLÈME DE TATE

4.1. Énoncé de la conjecture

On a vu au § précédent l'importance des variétés abéliennes et de leurs points de division. Nous introduisons dans ce paragraphe le "module de Tate" construit à partir d'iceux. C'est en fait le H_1 ℓ-adique de la variété abélienne et la conjecture de Tate dit qu'on espère retrouver beaucoup sur la variété abélienne A, quand on "connait" $H_1(A,\mathbb{Z}_\ell)$.

DÉFINITION.— *Soit* A *une variété abélienne définie sur un corps* K *et soit* ℓ *un nombre premier. On appelle module de Tate de* A, *et on note* $\mathbb{T}_\ell(A)$ *la limite projective sur* n *des noyaux de la multiplication par* ℓ^n *dans* $A_{\overline{K}}$. *Si* ${}_{\ell^n}A = \operatorname{Ker} A \xrightarrow{\ell^n} A$, *on a* ${}_{\ell^{n+1}}A \xrightarrow{\ell} {}_{\ell^n}A$).

Si G est le groupe de Galois de la clôture algébrique $\overline{K}$ de K, sur K, $\mathbb{T}_\ell(A)$ est un $\mathbb{Z}_\ell[G]$-module.

La conjecture de Tate pour les homomorphismes de variétés abéliennes est un cas particulier de sa conjecture sur les cycles algébriques qui "remplace" en cohomologie ℓ-adique la conjecture de Hodge.

Conjecture de Tate.— *Soit* K *un corps de type fini sur son corps premier,* G *le groupe de Galois de* $\overline{K}$ *sur* K, *soient* A *et* B *deux variétés abéliennes définies sur* K *et soit* ℓ *un nombre premier (premier à la caractéristique de* K). *Alors l'homomorphisme canonique :*

$$\operatorname{Hom}_K(A,B) \otimes \mathbb{Z}_\ell \longrightarrow \operatorname{Hom}_G(\mathbb{T}_\ell(A),\mathbb{T}_\ell(B))$$

est un isomorphisme. De plus le G-*module* $\mathbb{T}_\ell(A) \otimes \mathbb{Q}_\ell$ *est semi-simple.*

Cette conjecture est à l'heure actuelle démontrée :

a) Si K est de caractéristique positive, par Zarhin [Z] (S. Mori pour $p = 2$).

b) Si K est de caractéristique zéro, par Faltings [F1], [F2], [F3].

On trouvera dans l'exposé de Deligne ([D]) dans ce séminaire la démonstration de b) (notamment quand K est un corps de nombres). Nous expliquons ci-dessous la réduction, due à Tate et Zarhin [T], [Z], de cette conjecture à un énoncé de finitude qui est un cas particulier de "la conjecture de Shafarevitch pour les variétés abéliennes".

Il faut noter que pour les courbes elliptiques, la semi-simplicité est démontrée dans Serre [Se2]. Dans ce même livre, Serre donne la démonstration de la conjecture de Shafarevitch pour les courbes elliptiques. L'idée est de Shafarevitch lui-même et utilise le théorème de Siegel cité au § 1.

4.2. Réduction de la conjecture de Tate à un énoncé de finitude

On se ramène rapidement (par passage au produit $A \times B$ et au graphe d'un homomorphisme) à montrer :

$$\mathrm{End}_K(A) \otimes \mathbb{Q}_\ell \xrightarrow{\sim} \mathrm{End}_G(\mathbb{T}_\ell(A) \otimes \mathbb{Q}_\ell) .$$

Soit L un faisceau ample sur A (une polarisation) ; on sait lui associer depuis A. Weil (*cf.* par exemple D. Mumford [Mu]) une forme bilinéaire antisymétrique, dite de Riemann :

$$E^L = \mathbb{T}_\ell(A) \times \mathbb{T}_\ell(A) \longrightarrow \mathbb{Z}_\ell(1) = \varprojlim \mu_{\ell^n}$$

qui est non dégénérée car L est ample. Soit W un sous-G-module isotrope maximal de $\mathbb{T}_\ell(A) \otimes \mathbb{Q}_\ell$ et soit K_n l'image de $\mathbb{T}_\ell(A) \cap W$ dans

$$\mathbb{T}_\ell(A)/\ell^n\mathbb{T}_\ell(A) = {}_{\ell^n}A =: \mathrm{Ker}\ A \xrightarrow{\ell^n} A .$$

On a un diagramme commutatif

$$\begin{tikzcd} A \arrow[r, "\pi_n"] \arrow[dr, "\ell^n"'] & A/K_n = A_n \arrow[d, "\lambda_n"] \\ & A \end{tikzcd}$$

PROPOSITION 1 (Tate, Zarhin).— *Si une infinité de* A_n *sont* K *isomorphes, il existe* $u \in \mathrm{End}_K(A) \otimes \mathbb{Q}_\ell$ *tel que*

$$\mathbb{T}_\ell(u)(\mathbb{T}_\ell(A) \otimes \mathbb{Q}_\ell) = W .$$

Soit n_0 tel qu'il y ait une infinité de A_n K-isomorphes à A_{n_0} : $v_n : A_n \xrightarrow{\sim} A_{n_0}$. On prend $u_n = \lambda_n \circ v_n \circ \lambda_{n_0}^{-1} \in \mathrm{End}_K(A) \otimes \mathbb{Q}_\ell$ et $u = \lim u_n$ dans $\mathrm{End}_K(A) \otimes \mathbb{Q}_\ell$. Il est facile de vérifier que $\mathbb{T}_\ell(u)$ satisfait à la condition de l'énoncé.

PROPOSITION 2 (Zarhin).— *Supposons l'hypothèse de la proposition* 1 *vérifiée pour chaque sous-G-module isotrope maximal de* $\mathbb{T}_\ell(A^8) \otimes \mathbb{Q}_\ell$. *Alors :*

1) *Pour tout sous-G-module* W *de* $\mathbb{T}_\ell(A) \otimes \mathbb{Q}_\ell$, *il existe* u *dans* $\mathrm{End}_K(A) \otimes \mathbb{Q}_\ell$ *tel que* $u^2 = u$ *et* $u(\mathbb{T}_\ell(A) \otimes \mathbb{Q}_\ell) = W$.

2) $\mathbb{T}_\ell(A) \otimes \mathbb{Q}_\ell$ *est un* G *module semi-simple.*

Il est clair qu'on déduit la proposition 2 de la proposition 1 en construisant un sous-groupe isotrope maximal ad hoc pour W . Indiquons cette construction :

Soit L ample sur A et $M = \bigotimes_1^8 p_i^*L$, $N = \bigotimes_1^4 p_i^*L$, $p_i : A^8 \to A$ les projections. Soient a , b , c , d dans $\mathbb{Q}_\ell$ tels que $a^2 + b^2 + c^2 + d^2 = -1$. Soit

$$I = \begin{pmatrix} a & -b & -c & -d \\ b & a & d & -c \\ c & -d & a & b \\ d & c & -b & a \end{pmatrix} .$$

On vérifie que $I\,{}^tI = -1$. On considère I comme élément de $\mathrm{End}_G(\mathbb{T}_\ell(A^4)) \otimes \mathbb{Q}_\ell$ et on pose

$$W_1 = \{x, Ix \mid x \in W^4\} ,$$

$$W_2 = \{x, -Ix \mid x \in W^{\perp 4}\} ,$$

$W^{\perp 4}$ étant défini par la forme commutateur associée à N sur A^4. On a

- $W_1 \cap W_2 = 0$,
- W_1 et W_2 sont orthogonaux pour E^M, et
- $W_1 + W_2$ est un sous-G-module isotrope maximal pour E^M.

Il existe donc par la proposition 1, $u_1, \ldots, u_8 \in \mathrm{End}_K(A) \otimes \mathbb{Q}_\ell$ tel que

$$\sum_1^8 u_i(\mathbb{T}_\ell(A) \otimes \mathbb{Q}_\ell) = W_1 + W_2 .$$

L'idéal à droite engendré par les u_i dans $\mathrm{End}_K(A) \otimes \mathbb{Q}_\ell$ est engendré par idempotent u car ce dernier anneau est semi-simple. On voit facilement que u vérifie ce qu'on veut.

Il nous reste donc à analyser l'hypothèse de la proposition 2. On voit facilement que si la polarisation de A est de degré d, les A_n sont aussi munies d'une polarisation de degré d (car W est isotrope maximal). Les A_n étant toutes isogènes à A par une isogénie de degré une puissance de ℓ et étant définies sur K elles aussi, on voit que l'hypothèse de la proposition est un cas particulier de "la conjecture de Shafarevitch pour les variétés abéliennes".

5. LA STRATÉGIE APPLIQUÉE PAR FALTINGS [F2]

5.1. Le théorème de Faltings

Faltings démontre dans son article la "conjecture de Shafarevitch pour les variétés abéliennes".

Soit A_K une variété abélienne de dimension g sur un corps de nombres et $A \xrightarrow{f} \mathrm{Spec}\, \mathcal{O}$ son modèle de Néron sur l'anneau des entiers $\mathcal{O}$ de K. Faltings munit - suivant une idée arakélovienne - le fibré inversible $\omega_A = \bigwedge^g f_* \Omega^1_{A/\mathcal{O}}$ de métriques hermitiennes pour chaque place à l'infini de la façon suivante :

$$|\alpha|_\sigma^2 = 2^{-g} \left| \int_{A_\sigma(\mathbb{C})} \alpha \wedge \bar{\alpha} \right| ;$$

ω_A a donc un degré d au sens de 2.2.1.2 b). On définit la *hauteur modulaire* de A_K par

$$h(A_K) = d^o\omega_A/[K:\mathbb{Q}] .$$

L'avantage de h sur d tient à ce que $h(A_K) = h(A_{K'})$ quand A_K est semi-stable et K' une extension finie de K.

La démonstration comporte quatre parties :

1) Montrer que si on borne le degré d de ω_A (au sens ci-dessus) on n'a qu'un nombre fini de variétés abéliennes A sur K de dimension g munies d'une polarisation de degré n. C'est sans doute la partie la moins éclairante (quoique attendue) du papier cité. On en trouvera un traitement résumé, mais rigoureux, dans [D] ; on pourra aussi profiter de la lecture de [Zi].

2) Montrer que le degré d_n de ω_{A_n}, pour les variétés abéliennes A_n introduites dans le § 4, proposition 1, est borné (ce qui implique la conjecture de Tate). On

notera que j'ai bien écrit "borné" et non "constant".

3) Montrer qu'alors l'ensemble des classes d'isogénie de variétés abéliennes à mauvaise réduction fixée est un ensemble fini. C'est un résultat qui lui, a passé le crible de la critique.

4) Montrer que dans chaque classe d'isogénie le degré d de ω_A est borné.

J'ai, dans cet exposé, montré que ces quatre points impliquent les conjectures de Tate, et Shafarevitch.

La nouveauté "stratégique" de Faltings se trouve dans le fait que 2) ⇒ 3) qui est de toute beauté. Sinon le modèle géométrique pré-existant s'applique entièrement. La technique pour "borner d " dans 2) et 4) utilise essentiellement, pour mesurer la variation de d (ou de la hauteur modulaire) par isogénie, l'article [R1] de Raynaud et les "conjectures de Weil" pour les variétés abéliennes [W2].

On trouvera dans l'exposé de Deligne [D] la démonstration de ces quatre points.

5.2. <u>La construction de Kodaira-Parshin</u> [K], [P]

Cette construction permet de déduire la conjecture de Mordell de celle de Shafarevitch pour les courbes.

Nous utilisons les notations de 2.1.6. Soit K un corps de nombres et C une courbe sur K ayant bonne réduction en dehors de Σ . Nous allons construire une application à *fibres finies* : $P \rightsquigarrow C_P$,

$$C(K) \longrightarrow \coprod(\operatorname{Spec} \mathcal{O}' - S' , g')$$

où $\mathcal{O}'$ est l'anneau d'entiers d'un corps K' extension finie de K , S' est l'image réciproque de $S = \Sigma \cup (\bigcup_{\mathfrak{p}|2} \mathfrak{p})$ dans $\mathcal{O}'$, et g' est défini par $2g' - 2 = 2^{2g}(4g-3)$.

<u>Construction de</u> C_P

On envoie C dans sa jacobienne J en associant à un point Q le faisceau inversible $\mathcal{O}_C(Q-P)$. On définit ainsi une courbe C_1 par "pull-back" de la multiplication par deux dans J

$$\begin{tikzcd} J \arrow[r, ".2"] & J \\ C_1 \arrow[u] \arrow[r] \arrow[ur, phantom, "\square"] & C \arrow[u] \end{tikzcd}$$

La courbe C_1 est lisse de genre g_1' tel que $2g_1' - 2 = 2^{2g}(2g-2)$. C_1 est aussi définie sur K . L'image réciproque D de P est un diviseur de degré 2^{2g} . La courbe C_1 a bonne réduction sur Spec $\mathcal{O} - S$.

Quitte à faire une extension finie K_1' de K de degré $2^{2g'}$, étale en dehors de S , on peut supposer que $\mathcal{O}_{C_1}(D) \simeq L^{\otimes 2}$ pour un faisceau inversible L sur C_1 (défini sur K_1'). On prend alors pour $C_P \xrightarrow{\alpha} C_1$ le revêtement de C_1 ramifié de degré deux en D , étale sur $C_1 - D$ caractérisé par le fait que $\mathcal{O}_{C_P}(\alpha^{-1}(D)_{\text{réduit}}) = \alpha^* L$.

La courbe $C_p \xrightarrow{\pi} C$ aura bonne réduction en dehors de l'image réciproque de S. L'ensemble des corps K'_1 est fini (exemple 1.1 § 2) ; on prend alors K' le plus petit corps contenant la réunion des K'_1.

En fait une variante, due à D. Mumford, permet d'être plus économique sur le corps de base K' (mais pas sur le genre) :

On construit C_1 comme plus haut et on considère la courbe singulière C' où l'on a contracté (pincé) $D-(0,P)$ en un seul point P'.

On plonge alors par $(0,P) \longrightarrow 0$, $C'-P'$ dans sa jacobienne J' et on obtient une courbe C'' par le diagramme cartésien suivant :

$$\begin{tikzcd} J' \arrow[r, ".2"] & J' \\ C'' \arrow[u] \arrow[r] \arrow[ur, phantom, "\square"] & C'-P' \arrow[u] \end{tikzcd}$$

On prend alors pour C_p la normalisée de la fermeture projective de C''.

On voit facilement que $C(K) \longrightarrow Ш(\mathrm{Spec}\ \mathcal{O}'-S', g')$ est à fibres finies. En effet :

a) $C_p \longrightarrow C$ n'est ramifié qu'en P.

b) Il n'y a qu'un nombre fini de morphismes entre deux courbes algébriques de genre au moins deux.

5.3. Comment obtenir les théorèmes de finitude

On peut réinterpréter la construction de Kodaira-Parshin en notant qu'on a construit un *revêtement étale*

$$\tilde{C} \to C$$

et un morphisme fini

$$\tilde{C} \longrightarrow A_{g',n}$$

(espace de module des variétés abéliennes avec structure de niveau $n \geq 3$) pour toute courbe lisse C de genre g sur un corps de caractéristique ne divisant pas 2. $\tilde{C} \to C$ étant étale, $\tilde{C}(K)$ fini équivaut à $C(K)$ fini. $A_{g'}(K,S)$ étant fini pour tout corps K par le théorème de Faltings, $\tilde{C}(K)$ est donc fini.

Deligne a fait la remarque suivante : soit X un quotient compact d'un espace de Siegel par un groupe discret sans torsion. Par le théorème de Margoulis, le groupe en question est arithmétique et il existe donc un morphisme fini d'un revêtement étale $\tilde{X}$ de X dans un $A_{g,n}$. Ainsi $\#X(K) < \infty$ pour tout corps de nombres.

Par exemple l'ensemble des variétés abéliennes avec structure de niveau $n \geq 3$ de dimension donnée sur un corps de nombres K, ayant de la multiplication par une algèbre de quaternions totalement réelle, est fini à K isomorphismes près.

6. TABLEAU DES RÉSULTATS

Nous donnons sous forme de tableau les résultats obtenus à ce jour sur $C-S$ ou $\mathrm{Spec}\ \mathcal{O}-S$. Nous avons indiqué aussi ce qu'on sait sur les familles ayant bonne réduction partout $(S=\emptyset)$.

En fait on a la généralisation suivante des résultats de Faltings qui a été remarquée indépendamment par Faltings lui-même, Deligne et Parshin-Zarhin.

THÉORÈME 2 (Faltings).– *Soit* B *un schéma régulier, intègre et de type fini sur* $\mathbb{Q}$ *, de corps de fractions* K *dont la clôture algébrique est notée* $\overline{K}$ *. Soit* G *le groupe de Galois de* $\overline{K}$ *sur* K *. Alors*

a) *Si* A *et* B *sont des variétés abéliennes sur* K *,*

a-1) *la représentation de* G *dans* $\mathbb{T}_\ell(A)\otimes\mathbb{Q}_\ell$ *est semi-simple pour tout* ℓ *,*

a-2) *on a un isomorphisme canonique pour tout* ℓ *:*

$$\mathrm{Hom}_K(A,B)\otimes\mathbb{Z}_\ell \xrightarrow{\sim} \mathrm{Hom}_G(\mathbb{T}_\ell(A),\mathbb{T}_\ell(B)) .$$

b) *L'ensemble des classes de* K *isomorphismes de* K*-variétés abéliennes de dimension* g *ayant bonne réduction sur* B *est un ensemble fini.*

On notera que dans b) il n'y a plus de degré de polarisation fixé. On s'en passe à l'aide du lemme suivant dont Deligne m'a donné une démonstration.

Lemme (Zarhin).– *Soit* A *une variété abélienne sur un corps* k *. Sur* $A^4\times(A^*)^4$ *il existe une polarisation principale.*

Dans ce tableau, sur la ligne variété abélienne, dans la colonne K corps de nombres $B=\mathrm{Spec}\ \mathcal{O}-S\ \ldots$, une notation comme

$$Ш(B,g,n)$$

signifie : l'ensemble de Shafarevitch des variétés abéliennes sur B , de dimension g , munies d'une polarisation de degré n . (Voir tableau au verso.)

base / fibre	Corps de nombres K d'anneau d'entiers $\mathcal{O}$ S ensemble fini de places $B = \operatorname{Spec} \mathcal{O} - S$	C courbe algébrique sur $\mathbb{C}$ S ensemble fini de points $B = C - S$, K corps de fonctions de C	C courbe algébrique sur un corps k de caractéristique $p > 0$ S ensemble fini de points $B = C - S$, K corps de fonctions de C
n points	$\#\text{Ш}(\operatorname{Spec} \mathbb{Z}, \text{n points}) = 1$ (*Minkovski*) $\#\text{Ш}(B, \text{n points}) < \infty$ (*Hermite*)	$\#\text{Ш}(\mathbb{P}^1, \text{n points}) = 1$ $\#\text{Ш}(\mathbb{A}^1, \text{n points}) = 1$ $\#\text{Ш}(B, \text{n points}) < \infty$ (*Riemann*)	$\#\text{Ш}(\mathbb{P}^1, \text{n points}) = 1$ $\#\text{Ш}(\mathbb{A}^1, \text{n points, modéré}) = 1$ $\#\text{Ш}(B, \text{n points, modéré}) < \infty$ mais $\text{Ш}(\mathbb{A}^1, \text{n points})$ est infini
X Courbe lisse project. connexe de genre $g \geq 2$	$\#X(K) < \infty$ (*conj. Mordell, th. Faltings*) $\Uparrow$ *Kodaira-Parshin* $\#\text{Ш}(B,g) < \infty \quad \forall g \geq 2$ $\Uparrow$ *Torelli*	$\#X(K) < \infty$ si X non constante (*Manin*) $\Uparrow$ *Kodaira-Parshin* $\#\text{Ш}(B,g, \text{non constante}) < \infty \quad \forall g \geq 2$ (*Parshin-Arakelov*) $\#\text{Ш}(\mathbb{P}^1\text{-2 points},g,\text{s.s,non cste}) = 0$ $\#\text{Ш}(\text{cbe ellipt.},g,\text{s.s,non cste}) = 0$	$\#X(K) < \infty$ si X non constante (*Samuel*) $\Uparrow$ *Kodaira-Parshin* $\#\text{Ш}(B,g,\text{non constante,semi-stable}) < \infty$, $\forall g \geq 2$ [S] $\#\text{Ш}(\mathbb{P}^1\text{- 2 points},g,\text{s.s,non cste}) = 0$ [S] $\#\text{Ш}(\text{cbe ellipt.},g,\text{s.s,non cste}) = 0$ [S]
A variété abélienne de dim g, munie d'une polarisation de degré n	$\#\text{Ш}(B,g,n) < \infty$ (*Faltings*) $\Downarrow$ *Zarhin-Tate* $\operatorname{Hom}_K(A,A') \otimes \mathbb{Z}_\ell \xrightarrow{\sim} \operatorname{Hom}_G(T_\ell(A), T_\ell(A'))$ et $T_\ell(A) \otimes \mathbb{Q}_\ell$ semi-simple (*conj. Tate, th. Faltings*) $\Downarrow$ *Faltings* $\#\text{Ш}(B,g,n)/\text{isogénies} < \infty$ *Faltings* A(K) est un groupe commutatif de type fini (*Mordell-Weil*)	$\text{Ш}(B,g,n)$ est une famille limitée, éventuellement infinie (*Faltings*) $\#\text{Ш}(\mathbb{P}^1\text{- 3 points}, g, n) = 1$ $\#\text{Ш}(B,g,n, \text{une fibre fixée}) < \infty$ (*A. Grothendieck*)	$\text{Ш}(B,g,n,d)$ est une famille limitée (*Moret-Bailly*) $\Downarrow$ *Zarhin-Tate* Conjecture de Tate (*th. Zarhin*) $\#\text{Ш}(\mathbb{P}^1, g=2, n=1, \text{non constante}) \neq 0$ (*Moret-Bailly*)

7. ET MAINTENANT ?

La démonstration de Faltings de la conjecture de Mordell ne donne pas une borne effective pour la hauteur des points rationnels d'une courbe parce qu'on ne connaît pas la hauteur modulaire d pour un représentant d'une classe d'isogénie.

La seule piste que j'aie pour l'effectivité est la suivante :

Arakelov dans [A2] a introduit une théorie des intersections sur une surface arithmétique $X \xrightarrow{f} \operatorname{Spec} \mathcal{O}$ où la bonne mesure de la hauteur d'un point est l'opposé de la self-intersection de la section correspondante : $-E^2$. J'aimerais proposer la conjecture suivante :

Conjecture des petits points.— *Soit* K *un corps de nombres,* C *une courbe lisse sur* K *de genre* $g \geq 2$ *, semi-stable et ayant bonne réduction en dehors d'un ensemble* S *de places. Alors il existe un point rationnel* P *de* C *sur un corps* K' *extension de degré* n *de* K *telle que la section* E *correspondante ait la propriété suivante :*

$$-\frac{E^2}{n} \leq f(K,g,S)$$

où f *est une fonction* effectivement calculable.

A l'aide de la construction de Kodaira-Parshin et du théorème de l'index sur les surfaces arithmétiques (Faltings [F3] et Hriljac [H]), je peux montrer que cette conjecture implique la "conjecture de Mordell effective". J'ai montré dans [S] que la classe de Kodaira-Spencer dans le cas géométrique, permet de construire un petit point P, dont la section correspondante E de $X \xrightarrow{f} C$, satisfait la relation suivante :

$$-\frac{E^2}{n} \leq (2q-2+s)$$

où $s = \# S$ et q = genre de C.

Rajouté le 15 octobre 1984

1) M. Raynaud a montré, depuis les travaux de Faltings ici rapportés, qu'on peut borner effectivement la variation de la hauteur modulaire dans une classe d'isogénie

2) A.N. Parshin, en utilisant un article de D. Mumford (Am. J. of Math., 1965) traduit en termes d'intersections d'Arakelov, a montré que la démonstration de Faltings donne une borne "effective" pour le nombre de points rationnels d'une courbe sur un corps de nombres.

3) Il est à noter que S. Zucker a obtenu, dans le cas géométrique, une borne effective pour le degré de l'algèbre de Lie relative (cf. aussi : Loring W. Tu, Memoirs of the A.M.S., 1983, vol. 43, n° 279).

BIBLIOGRAPHIE

[Ab] S. ABHYANKAR - *Resolution of singularities of arithmetical surfaces*, Proc. Conf. on Arithm. Alg. Geometry, Purdue, 1963.

[Ar1] S.Ju. ARAKELOV - *Families of algebraic curves with fixed degeneracies*, Math. USSR Izvestija vol. 15(1971), n° 6.

[Ar2] S.Ju. ARAKELOV - *Intersection theory on arithmetical surfaces*, Math. USSR Izvestija vol. 8(1974), n° 6.

[D1] P. DELIGNE - *Preuve des conjectures de Tate et Shafarevitch [d'après G. Faltings]*, ce volume.

[D2] P. DELIGNE - *Hodge II* , Public. Math. IHES n° 40.

[F1] G. FALTINGS - *Arakelov's theorem for abelian varieties*, Inventiones Math. vol. 73, fasc. 3(1983).

[F2] G. FALTINGS - *Eindlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Inventiones Math. vol. 73, fasc. 3(1983).

[F3] G. FALTINGS - *Calculus on arithmetic surfaces*, à paraître dans Annals of Math.

[Gra] H. GRAUERT - *Mordell's Vermutung über rationale Punkte auf algebraischen Kurven...*, Publ. Math. IHES, 1965.

[Gri] P. GRIFFITHS - Lettre à l'auteur, 18 mars 1983.

[Gro1] A. GROTHENDIECK - S.G.A. 7.I, exp. 9, Springer-Verlag, Lecture Notes in Math. vol. 288, 1972.

[Gro2] A. GROTHENDIECK - *Un théorème sur les homomorphismes de schémas abéliens*, Inventiones Math. 2(1966), p. 59.

[H] P. HRILJAC - Thèse, MIT 1982, à paraître dans American Journal of Math.

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

[L] J. LIPMAN - *Desingularisation of two dimensional schemes*, Annals of Math. 107 (1978), 151-207.

[Ma] Iu.I. MANIN - *Rational points of algebraic curves over function fields*, Transl. A.M.S. (2) 50(1966), p. 189.

[M-B1] L. MORET-BAILLY - *Familles de courbes et de variétés abéliennes* I et II , dans Astérisque n° 86.

[M-B2] L. MORET-BAILLY - Thèse, Orsay, à paraître.

[M-B & S] L. MORET-BAILLY et L. SZPIRO - *Pinceaux de variétés abéliennes ayant bonne réduction*, à paraître.

[Mo] L.J. MORDELL - *On the rational solutions of the indeterminate equation of the third and fourth degree*, Proc. Cambridge Phil. Soc. t. 21(1922), p. 179.

[Mu1] D. MUMFORD - *Abelian varieties*, Oxford Univ. Press, Bombay 1970.

[Mu2] D. MUMFORD - *Pathologies III*, American Journal of Math. 89(1967).

[N] A. NERON - *Modèles minimaux des variétés abéliennes sur les corps locaux et globaux*, Publ. Math. IHES n° 21.

[O-S] F. OORT and J. STEENBRINK -*The local Torelli problem for algebraic curves*, Géom. Alg. à Angers, Sigthoff-Noordhoff Alphen, 1980.

[P] A.N. PARSHIN - *Curves over function fields*, Izv. Acad. Nauk USSR 32(1968).

[R1] M. RAYNAUD - *Schémas en groupes de type* p.p.p..., Bull. SMF t. 102(1974), 241-280.

[R2] M. RAYNAUD - *Courbes sur une variété abélienne et points de torsion*, Invent. Math. 71(1983), 207-233.

[R3] M. RAYNAUD - *Contrexemples au "vanishing de Kodaira"*, Volume Ramanujan, Oxford Univ. Press, Bombay 1980.

[Sa] P. SAMUEL - *Complément à un article de H. Grauert sur la conjecture de Mordell*, Publ. Math. IHES n° 29(1966).

[Se1] J.-P. SERRE - *Corps locaux*, Publ. Inst. Math. Univ. Naucago VIII, Hermann, 1962.

[Se2] J.-P. SERRE - *Abelian ℓ-adic representations and elliptic curves*, Benjamin, 1968.

[Sh1] I.R. SHAFAREVITCH - *Algebraic number fields*, Proc. Int. Cong. Stockholm, 1962.

[Sh2] I.R. SHAFAREVITCH - *Minimal models.. of two dimensional schemes*, TIFR, Bombay, n° 37.

[Si] C.L. SIEGEL - Oeuvres complètes, vol. 1, Springer-Verlag (1966), p. 209.

[S] Séminaire sur les Pinceaux de courbes de genre au moins deux (L. Szpiro), Astérisque n° 86(1981).

[T1] J. TATE - *Algebraic cycles and poles of zeta functions*, Arithm. Alg. Geom., Purdue, 1963.

[T2] J. TATE - *Endomorphisms of abelian varieties over finite fields*, Invent. Math. 2(1966), 134-144.

[W1] A. WEIL - *Sur l'analogie entre les corps de nombres et les corps de fonctions*, Revue Scient. n° 77(1939), dans Oeuvres complètes I, Springer-Verlag.

[W2] A. WEIL - *Courbes algébriques et variétés abéliennes*, Hermann 2e édition, Paris, 1971.

[Za] J. ZARHIN - *Endomorphisms of abelian varieties over fields of finite characteristic*, Math. USSR Izv. vol. 9(1975), n° 2.

[Zi] A. ZINOVIEV - *Les hauteurs béantes*, L'âge d'homme, Lausanne, 1977.

Lucien SZPIRO

Ecole Normale Supérieure
45 rue d'Ulm
F-75230 PARIS CEDEX 05