

# Remarques sur la taille des solutions de certaines équations algébriques

Lucien Szpiro

**0 – Introduction.** Les solutions de la conjecture de Mordell ([F2] puis [F3], [V1], [B]) ne donnent pas, à ce jour, une manière “effective” de trouver les points rationnels d’une courbe algébrique sur un corps de nombres. Par contre, diverses démonstrations de la même conjecture sur le corps de fonctions sont effectives ([Sz 1], [E,V], [V2]). Certaines de ces démonstrations ne sont valables qu’en caractéristique zéro, une en toute caractéristique. Nous donnons dans ce court article le résultat “*le plus effectif*”, à ce jour et à notre connaissance, qui soit valable en toute caractéristique sur les corps de fonctions d’une variable (Th. 2.1). La borne obtenue est **linéaire dans le genre du corps de fonctions et du second degré dans le genre de la courbe**. Nous montrons (Th 3.1) qu’un “**bon Mordell effectif**” de la forme précédente **pour une seule courbe, implique** sur les corps de nombres **la conjecture du discriminant** de [Sz 3]. Ce dernier résultat a été obtenu lors de conversations avec L. Moret–Bailly.

La “*règle du jeu*” dans ce papier est la suivante : sur un corps de fonctions d’une variable (ou un corps de nombres)  $K$ , une courbe projective, lisse, connexe  $X_K$  donne une surface projective  $X$  (ou arithmétique) fibrée sur une base  $B$  de dimension un. Sur cette surface nous utilisons la théorie des intersections des diviseurs (théorie d’Arakelov dans le cas arithmétique). On mesure la “*taille*” d’un point rationnel par la multiplicité d’intersection de la section de  $X$  sur  $B$  correspondante avec le faisceau dualisant relatif. Ce nombre est une bonne mesure de la taille car la courbe de départ est prise de genre au moins deux.

Au paragraphe un, nous introduisons une “**conjecture des petits points**” qui est plus **intrinsèque** que celles que nous avons proposées précédemment ([Sz2] par exemple). Nous montrons (lemme 1.1) que cette conjecture implique un “*bon Mordell effectif*”. Au paragraphe deux, nous montrons cette conjecture pour les corps de fonctions (Th. 2.1). Au paragraphe trois, nous montrons la moisson qu’apporterait un tel résultat sur les corps de nombres (Th. 3.1).

Nous avons utilisé sans sourciller la théorie d’Arakelov sur les surfaces arithmétiques. Les temps me semblent mûrs pour un emploi sans rappels de la dite théorie. Nous nous servons aussi de techniques standard de la géométrie algébrique des familles de courbes à un paramètre : changement de base, semi-stabilité, résolution des singularités. Les commutations de ces différentes opérations sont par exemple explicitées dans [Sz1].

## 1 – Une conjecture d’effectivité “intrinsèque”

Nous commençons par établir un lemme reliant les hauteurs de deux sections.

LEMME 1.1. — *Soit  $f : X \rightarrow B$  un morphisme projectif, plat, de fibre générique une courbe lisse et géométriquement connexe de genre  $g$ . Supposons que  $X$  soit un schéma régulier et  $B$  une courbe lisse et projective sur un corps  $k$  ou bien le spectre d’un anneau d’entiers algébriques. Alors si  $\omega_{X/B}$  désigne le faisceau dualisant relatif et si,  $E$  et  $E'$*

sont deux sections, on a :

$$-E^2 \leq -\omega_{X/B}^2 + 2(2g-1)(E \cdot E') - (2g-1)(2g+1)E'^2$$

Remarquons que la formule d'adjonction donne

$$-E^2 = (E \cdot \omega_{X/B})$$

pour toute section  $E$ . Pour montrer le lemme on considère dans  $\text{Pic}(X) \otimes \mathbb{R}$  le sous-espace engendré par :

$$\omega_{X/B}(E), \quad E' \quad \text{et} \quad F \quad \text{une fibre.}$$

La forme d'intersection sur cet espace a une signature possédant au moins un signe + car  $E' + \lambda F$ ,  $\lambda \in \mathbb{R}$  est de self intersection positive pour  $\lambda$  assez grand. Par le théorème de l'index le déterminant suivant est positif ou nul :

$$\begin{pmatrix} \omega_{X/B}^2 - E^2 & -E'^2 + (E' \cdot E') & 2g-1 \\ -E'^2 + (E' \cdot E) & E'^2 & 1 \\ 2g-1 & 1 & 0 \end{pmatrix}$$

ceci démontre le lemme 1.1.

Remarquons que nous avons déjà mis à profit le théorème de l'index pour comparer  $\omega_{X/B}$  et  $-E^2$  pour une section  $E$  dans [Sz 1]. Au vu de ce lemme il est "naturel" de poser le problème suivant :

**CONJECTURE 1.2.** — *Soit  $K_0$  un corps de nombres, ou un corps de fonctions d'une variable sur un corps  $k$ , et soit  $X$  une courbe lisse et géométriquement connexe de genre  $g \geq 2$  définie sur  $K_0$ . Alors pour tout entier  $n$ , il existe des constantes  $A(n)$  et  $B(n)$ , ne dépendant que de  $X$  sur  $K_0$  et de  $n$ , telles que, pour tout corps  $K$  extension finie de  $K_0$  de degré au plus  $n$  et pour tout point rationnel  $P$  de  $X$  sur  $K$ , il existe une extension finie  $K'$  de  $K$  et un point rationnel  $P'$  de  $X$  sur  $K'$  tel que les sections correspondantes  $E$  et  $E'$  du modèle minimal de  $X$  satisfassent à :*

$$(i) \quad -(E' \cdot E') \leq (A(n) \log D(K) + B(n))[K' : K_0]$$

$$(ii) \quad (E \cdot E') \leq (A(n) \log D(K) + B(n))[K' : K_0]$$

où  $\log D(K) = 2g-2$  si  $K$  est un corps de fonctions de genre  $g$ , et  $\log D(K) = \log |D_{K/\mathbb{Q}}|$  si  $K$  est un corps de nombres de discriminant  $D_{K/\mathbb{Q}}$ .

*Commentaires :*

a) Il est clair que le lemme et la conjecture qui précèdent impliquent :  $-E^2 \leq (2g - 1)(2g + 3)(A \log D(K) + B)$  i.e. un “Mordell effectif” très fort pour  $X$ . Remarquons que l’on a  $\omega_{X/B}^2 \geq 0$  cf. [Sz1] et [F1].

b) Nous appelons cette conjecture la *conjecture des petits points intrinsèque* “petit” à cause de la condition (i), “intrinsèque” car on demande l’existence de  $P'$  point de  $X$  sur  $\bar{K}$  et non plus un petit point sur chaque fibre de la fibration de Kodaira–Parshin comme dans [Sz1].

c) On ne peut avoir  $A(n) = 0$  comme il est facile de voir en prenant pour  $n$  le degré d’un morphisme fini de  $X$  dans la droite projective.

c) Exemple : on peut, en utilisant l’existence de points entiers sur le module des courbes de genre  $g$  donné, cf. [MB2], construire sur un anneau d’entiers algébriques  $\mathcal{O}_{K_0}$  une courbe  $f : X \rightarrow \text{Spec } \mathcal{O}_{K_0}$  lisse munie d’une involution  $\sigma$  sans point fixe. La distance entre un point  $P$  et  $\sigma(P)$  étant minorée par un réel strictement positif (sinon par compacité on aurait un point fixe), les sections correspondantes  $E$  et  $\sigma(E)$  sont telles que

$$(E \cdot \sigma(E)) \leq (\text{constante}) [K : \mathbb{Q}]$$

où  $K$  est le corps de rationalité de  $P$  et  $\sigma(P)$ . En effet la partie à distance fine de cette intersection est nulle car  $E$  et  $\sigma(E)$  ne se rencontrent modulo  $p$  pour aucun  $p$ , d’autre part la distance étant minorée, “la fonction de Green” est majorée. L’ennui est que  $E^2 = \sigma(E)^2$ .

d) Une des justifications de cette conjecture est que nous pouvons la démontrer sur les corps de fonctions, en toute caractéristique. C’est l’objet du paragraphe suivant.

## 2 – Corps de fonctions.

Si  $K$  est un corps de fonctions, les techniques développées dans [Sz 1] (utilisation de la classe de Kodaira–Spencer et négativement d’un “vanishing” à la Kodaira) permettent de montrer la conjecture 1 – 2 avec des coefficients  $A$  et  $B$  très simples. Par rapport à [Sz 1] nous ne faisons essentiellement qu’un changement de présentation : nous montrons la conjecture des petits points “intrinsèque” au lieu d’extrinsèque. Le gain est qu’on obtient un “Mordell effectif” avec une borne pour la hauteur des points rationnels du **second degré dans le genre de la courbe** et du premier degré dans le genre du corps de base. En caractéristique zéro on sait que A.N. Parshin [P] a noté que l’inégalité de Bogomolov–Miyaoaka  $c_1^2 \leq 3c_2$  donne une borne linéaire en le genre de la courbe. Rappelons que la manière de calculer explicitée dans [Sz 1] donnait une borne exponentielle en ce genre.

**THÉORÈME 2.1.** — *Soit  $K$  un corps de fonctions d’une variable de genre  $g$ . Soit  $X_K$  une courbe lisse géométriquement connexe de genre  $g \geq 2$  sur  $K$ . Soit  $X$  le modèle entier sur la courbe lisse  $C$  sur  $k$  de corps de fonctions  $K$ . Supposons que  $X$  soit une famille semi-stable sur  $C$ , dont la classe de Kodaira–Spencer est non nulle et qui ait*

$s$  fibres géométriques singulières. Alors pour tout point rationnel  $P$  de  $X_K$  sur  $K$  la section correspondante  $E_P$  de  $X$  sur  $C$  satisfait à :

$$-E_P^2 \leq 2(2g-1)(2g+3)(2q-1+s).$$

REMARQUE 1. — Si on est **en caractéristique zéro** dire que la classe de Kodaira-Spencer d'une famille est non nulle c'est dire que la famille est non constante. En effet la classe de Kodaira-Spencer correspond à l'application tangente de la base de la famille dans le "module" des fibres. Si on est **en caractéristique**  $p > 0$  on doit multiplier l'inégalité du théorème par  $p^e$ , l'entier  $e$  est le degré d'inséparabilité du morphisme de  $C$  dans le module  $\overline{\mathcal{M}}_g$  des courbes de genre  $g$ , obtenu à partir de  $X \rightarrow C$ .

REMARQUE 2. — Par le théorème de réduction semi-stable d'A. Grothendieck (cf. par exemple [Sz 1] exposé 2 de M. Deschamps) quitte à "grandir"  $K$  par une extension finie (et contrôlable), on peut supposer que  $X$  a réduction semi-stable quand on se préoccupe de la hauteur des points rationnels.

*Démonstration du théorème :* Comme dans [Sz 1] la construction de Kodaira-Parshin permet d'obtenir le diagramme commutatif suivant :

$$Y \xrightarrow{\rho} X \xrightarrow{h} C' \xrightarrow{\pi} C$$

où  $\pi$  est un morphisme fini étale,  $\rho$  est fini et n'est ramifié qu'au-dessus de  $E_P$ . De plus on a  $\omega_{Y/C'}^{\otimes 2} = \rho^*(\omega_{X/C}^{\otimes 2} \otimes \mathcal{O}_X(E_P))$ . Dans l'exposé 3, §3, démonstration du théorème 3 de [Sz 1], en utilisant les deux techniques rappelées au début de §2, on montre que  $\omega_{Y/C'} \otimes T_{C'}^1(-\pi^*S)$  n'est pas numériquement positif (où  $T_{C'}^1$  est le tangent de  $C'$  sur  $k$  et  $S$  est le diviseur positif réduit de  $C$  dont les fibres sont non lisses). Par définition l'une des inégalités suivantes est satisfaite :

$$\text{a) } (\omega_{Y/C'} \otimes T_{C'}^1(-\pi^*S))^2 \leq 0$$

$$\text{b) } ((\omega_{Y/C'} \otimes T_{C'}^1(-\pi^*S)).D) < 0 \text{ pour un diviseur effectif } D.$$

Par un exercice classique de la théorie des surfaces algébriques (valable aussi en théorie d'Arakelov) dans le cas a) il existe un diviseur  $D$  tel que  $(D.\omega_{Y/C'} \otimes T_{C'}^1(-\pi^*S - F)) \leq 0$  où  $F$  est une fibre (exercice : un fibré en droite qui coupe chaque diviseur effectif non négativement est de self intersection non négative).

Comme  $\pi : C' \rightarrow C$  est étale on a  $T_{C'}^1 = \pi^*T_C^1$ . D'autre part si

$$(D.\omega_{X/C} \otimes \pi^*T_C^1(-S - F)) \leq 0$$

on vérifie facilement que  $D$  ne peut être vertical. Il existe donc un diviseur horizontal  $\rho_*D$  sur  $X$  tel que

$$(\rho_*D \cdot \omega_{X/C}^{\otimes 2} \otimes \mathcal{O}_X(E_P) \otimes (T_C^1(-S - F))^{\otimes 2}) \leq 0.$$

Quitte à faire un changement de base  $C'' \xrightarrow{\pi''} C$  on obtient donc une section  $E''$   $X \times_C C'' \rightarrow C''$  telle que

$$(E'' \cdot (\omega_{X''/C''}^{\otimes 2} \pi''^* \mathcal{O}_X(E_P))) \leq 2 \cdot \deg \pi''(2q - 1 + s).$$

Si  $E''$  n'est pas égal à  $E_P$  (sur  $C''$ ) on obtient  $-E''^2 \leq \deg \pi''(2q - 1 + s)$

$$(E'' \cdot E_P) \leq 2 \deg \pi''(2q - 1 + s)$$

i.e. la conjecture 1.2 avec  $A = 2$  et  $B = 2(s + 1)$ . Si  $E''$  est égal à  $E_P$  on obtient  $-E''^2 = -E_P^2 \leq 2 \deg \pi''(2q - 1 + s)$  et  $E'' \cdot E_P = +E''^2 < 0$  donc les mêmes  $A$  et  $B$  que plus haut !! Le commentaire a) de la conjecture 1.2 montre alors le théorème.

### 3 – “Mordell effectif” pour une seule courbe suffit

**DÉFINITION 3.1.** — Soit  $C$  une courbe algébrique définie sur  $\overline{\mathbb{Q}}$  munie d'une hauteur  $h$  associée à un faisceau inversible ample. On dit que  $C$  satisfait à un **bon Mordell effectif** si, pour tout entier  $n$  il existe des constantes  $\alpha(n)$  et  $\beta(n)$  telles que, pour tout corps de nombres  $K$  de degré au plus  $n$  sur  $\mathbb{Q}$ , on ait : pour tout  $P \in C(K)$   $h(P) \leq \alpha(n) \log |D_{K/\mathbb{Q}}| + \beta(n)$  où  $D_{K/\mathbb{Q}}$  est le discriminant de  $K$  sur  $\mathbb{Q}$ .

Cette définition appelle plusieurs remarques :

0) Nos hauteurs sont toujours logarithmiques.

1) Si  $h'$  est une hauteur associée à un autre fibré inversible ample sur  $C$  il existe des constantes  $\alpha$  et  $\beta$  – ne dépendant que de  $C$  et des deux fibrés amples – telles que

$$h'(P) \leq \alpha h(P) + \beta \text{ pour tout } P \in C(\overline{\mathbb{Q}}).$$

2) Si  $C$  satisfait à un bon Mordell effectif alors son genre géométrique est au moins deux (c'est un exercice de montrer qu'en genre un ou zéro il existe un corps de nombres où la courbe acquiert une infinité de points rationnels, donc de hauteur non bornée).

Le résultat qui suit a été obtenu lors de discussions avec L. Moret-Bailly. Des cas particuliers (i.e. pour des courbes explicites) avaient été établis par différents auteurs :

P. Vojta (courbe  $X^4 + Y^4 = z^4$ ) [V3]

L. Moret-Bailly (courbe  $Y^2 + Y = X^5$ ) [M-B 1]

A.N. Parshin (courbes modulaires) [P]

**THÉORÈME 3.2.** — S'il existe une courbe algébrique sur  $\overline{\mathbb{Q}}$  satisfaisant à un bon Mordell effectif alors la conjecture du discriminant est vraie.

Nous montrerons ci-dessous la conjecture du discriminant sous la forme “ $a, b, c$ ” (faible) pour tout corps de nombres (cf. [Sz 3] ou [O]).

Soit  $C_{K_0}$  une courbe algébrique sur un corps de nombres  $K_0$  satisfaisant à un bon Mordell effectif. Par le théorème de Beily [Be] on peut réaliser  $C_{K_0}$  comme un revêtement

de la droite projective  $\mathbb{P}_{K_0}^1$  ramifié seulement en trois points. Soit  $\pi : C \rightarrow \mathbb{P}_{K_0}^1$  un modèle entier de ce morphisme de Beily avec  $\pi$  fini de degré  $d$ . Par une transformation homographique on peut supposer que les trois points de ramification de  $\pi_{K_0}$  sont les points de coordonnées projectives  $(1, 0)$ ,  $(0, 1)$  et  $(1, -1)$ . Soit  $(a, b) \in \mathbb{P}^1(\mathcal{O}_K)$  où  $K$  est un corps de nombres contenant  $K_0$ . Soit  $R$  le lieu de ramification dans  $\mathbb{P}_{\mathcal{O}_{K_0}}^1$  du morphisme  $\pi$ . On a par hypothèse  $R_{K_0} = \{(1, 0), (0, 1), (1, -1)\}$ . Donc on sait que  $R$  est contenu dans la réunion des trois sections  $(1, 0)$ ;  $(0, 1)$ ;  $(1, -1)$  et d'un diviseur vertical  $V$ .

Le support de  $(a, b) \cap R$  est donc contenu dans l'ensemble des places  $v$  qui divisent  $(a, b) \cap (1, 0)$ ;  $(a, b) \cap (0, 1)$ ;  $(a, b) \cap (1, -1)$  et  $V$ . Ces places sont contenues parmi celles divisant  $a$ ;  $b$ ;  $(a + b)$  et support  $(V) = V_0$ .

Le corps  $K$  étant fixé un point de  $\mathbb{P}^1(K)$  donne par image réciproque des points de  $C_K$  rationnels sur des corps  $K'$  de degré au plus  $d$  sur  $K$ . Les corps  $K'$  sont ramifiés sur  $K$  au plus en les places qui divisent  $(a, b) \cap R$ . Donc pour  $v|a.b(a+b).V_0$ .

Par un théorème de Hensel (cf. par exemple J.-P. Serre [Se]) il existe un entier  $\tau(K)$  tel que le discriminant  $D_{K'/\mathbb{Q}}$  satisfasse à

$$|D_{K'/\mathbb{Q}}| \leq \left( \prod_{v|ab(a+b)V_0} N(v) \right)^{\tau(K)}$$

où  $N(v)$  est le cardinal du corps résiduel de  $v$ .

Prenons comme hauteur sur  $C$  la hauteur du point image par  $\pi$ , soit dans notre cas  $\log \prod_{\rho \in \infty(K)} \sup(|a|_\rho, |b|_\rho)$ . Par hypothèse on a un bon Mordell effectif sur  $C$  donc :

$$\prod_{\rho \in \infty(K)} \sup(|a|_\rho, |b|_\rho) \leq \left( \prod_{v|ab(a+b)} N(v) \right)^{\alpha(d[K:\mathbb{Q}])\tau(K)} e^{\beta(d[K:\mathbb{Q}])} N(V_0)^{\tau(K)\alpha(d[K:\mathbb{Q}])}$$

qui donne l'inégalité suivante (en posant  $c = a + b$ ) :

$$N(abc) \leq \text{Constante}(K) \left( \prod_{v|abc} N(v) \right)^{\sigma(K)}$$

où  $\sigma$  est une constante ne dépendant que de  $K$ . □

**Note.** E. Bombieri nous a signalé que N. Elkies a obtenu une sorte de réciproque du th. 3.2 : la conjecture “ $a, b, c$  forte” implique “Mordell effectif”.