ALAIN ROBERT

Retour au théorème de Siegel-Mahler-Roth

Publications du Département de Mathématiques de Lyon, 1987, fascicule 1B
« Actes du colloque Jean Braconnier », , p. 61-74

<http://www.numdam.org/item?id=PDML_1987___1B_61_0>

RETOUR AU THEOREME DE SIEGEL-MAHLER-ROTH

par Alain Robert (Univ. de Neuchâtel)

1. INTRODUCTION

L'étude des solutions entières aux équations polynomiales remonte à la plus haute antiquité. Par contre, ce n'est qu'au XX^{e} siècle que des résultats généraux ont pu être obtenus. En voici un.

Théorème A (Siegel). Soit $P \in \mathbb{Z}[X,Y]$ un polynôme à coefficients entiers tel que l'équation $P(X,Y) = 0$ admette une infinité de solutions (x,y) à coordonnées entières. Alors, il existe une paramétrisation

$$x = a(t) \quad , \quad y = b(t)$$

de la courbe plane (réelle ou complexe) d'équation $P(X,Y) = 0$ avec deux fonctions a et b qui sont des polynômes de Laurent en t (i.e. des polynômes en t et $1/t$).

La même conclusion subsiste lorsqu'on suppose seulement que $P(X,Y) = 0$ admet une infinité de solutions (x,y) à coordonnées dans un anneau de nombres algébriques de type fini sur $\mathbb{Z}$, par exemple un anneau de la forme $\mathbb{Z}[1/n]$ où n est un entier strictement positif.

La conclusion du théorème A signifie que la courbe algébrique projective associée à la courbe affine plane d'équation $P(X,Y) = 0$ a au plus deux points à l'infini et est de genre nul (donc birationnellement isomorphe à une droite projective).

Dans cet exposé, nous donnerons les grandes lignes d'une version légèrement plus faible du théorème A en indiquant le rôle que peut y jouer l'analyse non standard. Le lecteur intéressé par le rôle plus spécifique de l'analyse non standard dans la démonstration du théorème A pourra se référer à [4]. Le théorème qui nous occupera ici constitue la partie birationnelle du théorème A et peut s'énoncer sous la forme suivante.

Théorème B. Soit R un sous-anneau de $\mathbb{Q}$, de type fini sur $\mathbb{Z}$, et $P \in R[X,Y]$. Supposons qu'il existe une infinité de points algébriques (x_i,y_i) sur la courbe d'équation $P(X,Y) = 0$ et une fonction rationnelle $f = f(X,Y)$ telle que $f(x_i,y_i) \in R$ pour tout i. Alors, il existe une paramétrisation $x = a(t)$, $y = b(t)$ de la courbe en question donnée par deux fonctions rationnelles de t.

Dans ce théorème B, nous ne supposons pas que les points (x_i,y_i) sur la courbe ont leurs coordonnées dans R, mais seulement dans la clôture algébrique $\bar{\mathbb{Q}}$ de $\mathbb{Q}$ dans $\mathbb{C}$. Mais si ces points ont tous une première coordonnée $x_i \in R$, on peut prendre pour fonction rationnelle f la fonction x satisfaisant l'hypothèse (resp. $f = y$ si tous les $y_i \in R$). Mais l'hypothèse plus faible du théorème B ne permet plus de donner de majoration pour le nombre de points à l'infini sur la courbe projective associée. (Pour être plus précis sur ce dernier point, il faudrait plutôt dire qu'un nombre fini de valeurs distinctes t_j du paramètre conduit à des points à l'infini sur la courbe projective associée, et que ce nombre de valeurs t_j ne peut être majoré sous les seules hypothèses du théorème B.)

2. EXEMPLES ELEMENTAIRES

Les exemples les plus intéressants sont ceux où le polynôme de définition de la courbe plane est de degré deux. Voici quelques cas caractéristiques.

a) Considérons l'hyperbole d'équation $x^2 - 2y^2 = 1$. Elle contient une infinité de points (x_i,y_i) à coordonnées entières. On les obtient de

la façon usuelle en partant de l'unité fondamentale $u = 3 + 2\sqrt{2}$ du corps quadratique $\mathbb{Q}(\sqrt{2})$. La norme de cette unité est

$$N(u) = (3 + 2\sqrt{2})(3 - 2\sqrt{2}) = 9 - 8 = 1.$$

Les puissances entières $u^i = x_i + y_i\sqrt{2}$ de u ont des composantes x_i et y_i entières (lorsque i est positif, ceci résulte simplement du fait que les coefficients binomiaux permettant de calculer la i^e puissance de $3 + 2\sqrt{2}$ sont entiers). De plus

$$x_i^2 - 2\,y_i^2 = N(x_i + y_i\sqrt{2}) = N(u^i) = N(u)^i = 1$$

prouve que tous les points (x_i,y_i) sont sur l'hyperbole considérée.

b) Sur l'hyperbole d'équation $y^2 - x^2 - xy = 1$, il y a aussi une infinité de points à coordonnées entières. On peut les construire de la façon suivante. Les nombres de Fibonacci sont définis inductivement par

$$f_o = 0,\ f_1 = 1,\ \ldots\ f_{n+1} = f_n + f_{n-1}\ .$$

Ainsi par exemple,

$$f_2 = 1,\ f_3 = 2,\ f_4 = 3,\ f_5 = 5,\ f_6 = 8,\ f_7 = 13,\ \ldots$$

Le lecteur pourra vérifier que les points

$$(x_i,y_i) = (f_{2i},f_{2i+1}) \qquad i = 0, 1, \ldots$$

sont tous sur l'hyperbole citée. Les points (f_{2i+1},f_{2i+2}) sont au contraire sur l'hyperbole d'équation $y^2 - x^2 - xy = -1$. Ces deux hyperboles ont d'ailleurs pour asymptotes communes les droites $y = mx$ de pentes m satisfaisant $m^2 - m - 1 = 0$, à savoir $m = \frac{1}{2}(1 \pm \sqrt{5})$. Les quotients f_{i+1}/f_i tendent vers $\frac{1}{2}(1 + \sqrt{5})$ lorsque $i \to \infty$ (resp. vers $\frac{1}{2}(1 - \sqrt{5})$ lorsque $i \to -\infty$).

Dans les deux exemples a) et b), il est facile de trouver une paramétrisation de l'hyperbole à l'aide de polynômes de Laurent en t.

c) Sur l'hyperbole d'équation $xy = 1$, il n'y a visiblement qu'un nombre fini de points dont les deux coordonnées sont entières. Mais en prenant un anneau de type fini de la forme $R = \mathbb{Z}[1/p]$ (où p est par exemple un nombre premier), les points

$$(x_i,y_i) = (2^i,1/2^i)$$

ont leur deux coordonnées dans R et le théorème A (formulé avec R au lieu de $\mathbb{Z}$) est encore applicable.

Donnons encore quelques exemples en degré supérieur à deux.

d) Sur les courbes d'équation $y = a_n x^n + \ldots + a_o$ il y a une infinité de points ayant leur deux coordonnées entières (on suppose que les coefficients a_i sont entiers, de sorte que toute valeur entière de x conduit à une valeur entière de y !). Une paramétrisation polynomiale de ces courbes saute aux yeux :

$$x = t \ , \ y = a_n t^n + \ldots + a_o \ .$$

e) Prenons finalement N entiers n_j distincts et considérons la courbe d'équation

$$y \prod_{1 \leqslant j \leqslant N} (x - n_j) = 1 \ .$$

Cette courbe peut être paramétrisée par

$$x = t, \ y = \prod_{1 \leqslant j \leqslant N} (t - n_j)^{-1} \ .$$

Les valeurs entières de t conduisent à des valeurs entières de x et il y a ainsi une infinité de points ayant première coordonnée entière sur cette courbe. Le théorème B est applicable. Mais les N + 1 valeurs $t = t_j$ et $t = \infty$ doivent être exclues et le théorème A ne serait applicable que si $N + 1 \leqslant 2$, i.e. $N \leqslant 1$ (ce cas illustre la précision apportée en fin de l'introduction).

f) Sur la cubique d'équation $x^3 - y^2 = 2$ il n'y a que deux points $(x,y) = (3, \pm 5)$ à coordonnées entières (ce résultat était déjà connu de Fermat). Mais on peut voir qu'il y a une infinité de points à coordonnées rationnelles. L'ensemble des points réels ou complexes de cette courbe ne peut pas être paramétré à l'aide de fonctions rationnelles (la courbe n'est pas "unicursale"). Par contre, cette courbe peut être paramétrée à l'aide de fonctions transcendantes de Weierstrass. Elle est de genre 1: on dit que c'est une courbe elliptique. Le théorème de Faltings (ex-conjecture de Mordell) montre qu'une courbe algébrique ayant une infinité de points rationnels est de genre inférieur ou égal à 1. Le genre 1, où il n'y a qu'un nombre fini de points entiers, mais où il peut y avoir une infinité de points rationnels est crucial (cf. [8]).

Son étude n'est pas terminée.

3. PRINCIPES D'ANS

Pour démontrer une propriété classique telle que le théorème de Siegel, il suffit de l'établir lorsque toutes ses données sont standard. L'ensemble des points entiers sur une courbe algébrique standard est standard et on utilise le principe général suivant.

(3.1) Principe. Si E est un ensemble standard, E est infini si et seulement si E possède un élément non standard.

Ce principe nous permet de traduire le théorème de Siegel en ANS et conduit à étudier les points entiers non standard sur les courbes algébriques (dans quel cas peut-il y en avoir?). Plus généralement, si nous désirons traiter de points ayant une coordonnée dans un anneau $R \subset \mathbb{Q}$ de type fini, il faut indiquer la signification du terme standard pour de tels anneaux.

(3.2) Proposition. Soit $a \in \mathbb{Q}$ un nombre rationnel et $R = \mathbb{Z}[a]$. Alors l'anneau R est standard exactement lorsque les seuls diviseurs premiers du dénominateur de a sont tous standard.

Continuons notre liste de principes d'ANS par l'énoncé suivant.

(3.3) Principe. Soit $f : E \longrightarrow F$ une application standard entre ensembles (standard). Si $x \in E$ est un élément standard, alors $y = f(x)$ est aussi un élément standard de F.

La proposition suivante résulte des principes énoncés.

(3.4) Proposition. Soit $f : E \longrightarrow F$ une application standard entre ensembles (standard). Prenons $x \in E$ et posons $y = f(x)$. Alors

a) y non standard $\Longrightarrow$ x non standard,

b) x non standard et $f^{-1}(y)$ fini $\Longrightarrow$ y non standard.

Nous appliquerons librement cette proposition dans le cadre suivant : E et F sont des courbes algébriques standard (ou l'ensemble des points à coordonnées algébriques sur ces courbes) et f est une application régulière non constante et standard entre ces courbes. Donc f est de degré fini, ses fibres sont des ensembles finis. La proposition montre qu'un point algébrique P sur la première courbe est non standard si et seulement son image dans la deuxième l'est. Le cas particulier de ce résultat obtenu en prenant pour F la droite projective est suffisamment important

pour mériter une mention particulière.

(3.5) Théorème. Soit C une courbe algébrique standard définie sur un corps de nombres (standard). Choisissons et fixons un point P non standard sur C et à coordonnées algébriques : $P \in C(\bar{\mathbb{Q}})$. Dénotons par F le corps $\bar{\mathbb{Q}}(C)$ des fonctions rationnelles $C \longrightarrow \mathbb{P}^1$ définies sur $\bar{\mathbb{Q}}$. Alors

a) Pour toute $f \in F$,

$$f \text{ standard et } f \neq 0 \implies 0 \neq f(P) \neq \infty,$$

b) Pour toute $f \in F$,

$$f \text{ standard et non constante} \implies f(P) \text{ non standard},$$

c) Pour deux fonctions $f, g \in F$

$$f \text{ et } g \text{ standard}, f \neq g \implies f(P) \neq g(P) .$$

Quelques commentaires s'imposent. Comme l'ensemble $C(\bar{\mathbb{Q}})$ est toujours infini, on peut donc trouver un point P non standard dans cet ensemble. Un tel point joue le rôle de "point générique" du moins si l'on se restreint aux fonctions rationnelles standard. La propriété c) montre de façon précise comment on passe fidèlement des fonctions standard aux valeurs qu'elles prennent en P. Les propriétés algébro-géométriques de la courbe C peuvent donc être traduites en propriétés arithmétiques des valeurs f(P) des fonctions rationnelles standard sur C. D'autre part, les coordonnées du point P engendrent un corps de nombres k. Si possible, on choisira P de façon que ce corps de nombres soit standard. Ceci n'est possible (d'après le résultat de Faltings) que si le genre de la courbe C est $\leqslant 1$. De même, lorsque la courbe C est affine, disons donnée par une équation polynomiale à coefficients entiers, on peut essayer de choisir le point P de façon que ses coordonnées engendrent un anneau R (nécessairement de type fini) standard. Ceci n'est possible (d'après le résultat de Siegel) que si la courbe C a un genre nul.
On voit bien comment l'hypothèse que C a une infinité de points entiers ou à coordonnées dans un anneau standard $R \subset \mathbb{Q}$ et de type fini sur $\mathbb{Z}$ se traduit sur la possibilité de choisir le point P convenablement dans le théorème ci-dessus.

4. HAUTEURS PROJECTIVES

La hauteur d'un nombre rationnel a écrit sous forme réduite $a = m/n$ (i.e. n et m sont deux entiers relativement premiers et $n \geqslant 1$) est par définition l'entier positif $H(a) = \mathrm{Max}(|m|,n)$. On voit donc que

$H(a)$ entier $\geqslant 1$,

$H(1/a) = H(a)$ si $a \neq 0$,

pour toute constante c $\{a \in \mathbb{Q} : H(a) \leqslant c\}$ est fini.

Lorsque la constante c est standard, l'ensemble $\{a \in \mathbb{Q} : H(a) \leqslant c\}$ est standard et fini, ne contient que des éléments standard. Par conséquent,

a rationnel non standard $\Longrightarrow$ H(a) illimité.

La notion de hauteur s'étend à l'espace projectif $\mathbb{P}^n$ comme suit. Si $a = [a_0:a_1: \ldots :a_n] \in \mathbb{P}^n(\mathbb{Q})$, on peut supposer que la représentation choisie de a est telle que les $a_i \in \mathbb{Z}$ sont des entiers relativement premiers: ceci fixe le choix de la représentation au signe près. On pose

$H(a) = \mathrm{Max}\{|a_i|\}$ entier $\geqslant 1$.

Lorsque n = 1, on retrouve la définition précédente en plongeant $\mathbb{Q}$ dans $\mathbb{P}^1(\mathbb{Q})$ de la façon usuelle $a = m/n \longmapsto [m:n]$. Comme ci-dessus, on a encore

$a \in \mathbb{P}^n(\mathbb{Q})$ et a non standard $\Longrightarrow$ H(a) illimité

du moins lorsque l'entier n est standard, ce que nous supposerons parfois implicitement dans de tels énoncés.

Il est encore utile d'étendre la notion de hauteur aux points à coordonnées algébriques. Pour cela, on observe que dans $\mathbb{Q}$ d'abord, si $a = m/n$ est une expression réduite,

$$H(a) = \mathrm{Max}(|m|,n) = \prod_v \mathrm{Max}(|a|_v , 1)$$

où v parcourt l'ensemble des places de $\mathbb{Q}$: ce sont les nombres premiers p et la place archimédienne v donnant lieu à la valeur absolue usuelle. En effet, lorsque p parcourt l'ensemble des nombres premiers, le produit des valeurs absolues $|a|_p > 1$ reconstitue le dénominateur n de a . Le produit définissant H(a) sera donc égal à n si $|a| = |a|_v < 1$ et à $n \cdot |a|_v = n|m/n| = |m|$ si $|a| > 1$ comme on le souhaite. Lorsque $a = [a_0:a_1: \ldots :a_n] \in \mathbb{P}^n(\bar{\mathbb{Q}})$ a des coordonnées algébriques, disons dans un corps de nombres k fixé, on pose

$$H(a)^{[k:\mathbb{Q}]} = \prod_v \mathrm{Max}(|a_0|_v , |a_1|_v , \ldots , |a_n|_v)$$

où v parcourt l'ensemble des places de k. La formule du produit montre que le choix d'une représentation particulière de a n'influence pas le résultat du calcul de maximum. D'autre part, l'exposant est choisi de façon telle que le résultat ne dépend pas du choix du corps de nombres k dans lequel on peut trouver une représentation de a.

Lorsqu'une courbe algébrique est plongée ou immergée dans un espace projectif, elle hérite une notion de hauteur simplement par transport. Il convient d'étudier comment le choix d'un plongement ou d'une immersion influence le comportement de la hauteur qui en résulte.

Rappelons qu'une application algébrique de degré d entre espaces projectifs $\mathbb{P}^n$ et $\mathbb{P}^m$ est tout simplement une application

$$f : [a_0:a_1: \ldots :a_n] \longmapsto [b_0:b_1: \ldots :b_m]$$

qui peut être exprimée en composantes

$$b_j = f_j(a_0,a_1, \ldots ,a_n)$$

à l'aide de formes homogènes f_j ayant toutes le même degré d. Ceci dit, le premier résultat fondamental est le suivant (cf.).

(4.1) Théorème. Soit f une application $\mathbb{P}^n \longrightarrow \mathbb{P}^m$ algébrique de degré d. Alors il existe une constante $c > 0$ telle que

$$c^{-1} H(P)^d \leqslant H(f(P)) \leqslant c\, H(P)^d$$

pour tous les points $P \in \mathbb{P}^n(\bar{\mathbb{Q}})$.

On abrège souvent les inégalités ci-dessus en utilisant la notation $H(f(P)) \asymp H(P)^d$. En utilisant le logarithme de la hauteur

$$h(P) = \log H(P) ,$$

la conclusion du théorème peut être récrite

$$h(f(P)) - d\, h(P) \text{ est bornée pour } P \in \mathbb{P}^n(\bar{\mathbb{Q}}) .$$

Supposons maintenant que f est standard (donc n, m et d sont standard). On peut donc trouver un majorant standard de la fonction $h(f(P)) - d\,h(P)$. Si P est non standard, H(P) et h(P) sont illimités et

$$h(f(P))/h(P) = d + \text{infinitésimal},$$

c'est à dire

$$\operatorname{st} h(f(P))/h(P) = d.$$

Mais observons d'emblée que cette égalité est plus faible que la conclusion du théorème puisqu'elle ne permettrait que de retrouver les inégalités

du théorème à ε près dans le sens suivant. Pour tout $\varepsilon>0$, il existe une constante $c_\varepsilon > 0$ telle que

$$c_\varepsilon^{-1} H(P)^{d-\varepsilon} \leqslant H(f(P)) \leqslant c_\varepsilon H(P)^{d+\varepsilon}.$$

C'est précisément ce genre d'inégalités qui ont été établies par A. Weil dans un cadre plus général (cf. [9]). Dans le cas des courbes, nous pouvons donc reformuler les résultats de Weil comme suit en utilisant l'ANS.

(4.2) Théorème. Soit C une courbe algébrique et f,g deux immersions de C dans des espaces projectifs. Nous supposerons toutes les données standard et définies sur $\bar{\mathbb{Q}}$. Alors si $P \in C(\bar{\mathbb{Q}})$ est un point non standard,

$$\operatorname{st} \frac{h(f(P))}{h(g(P))} = \frac{\deg(f)}{\deg(g)} .$$

Le degré d'une application non constante $f : C \longrightarrow \mathbb{P}^n$ peut être vu comme le nombre "générique" de points d'intersection de f(C) avec un hyperplan de $\mathbb{P}^n$.

5. VALUATIONS

Soit C une courbe (irréductible) standard définie sur $\mathbb{Q}$ et F son corps de fonctions rationnelles. Supposons qu'il existe un point P non standard de $C(\mathbb{Q})$ et prenons une fonction rationnelle standard $f \in F - \mathbb{Q}$ non constante. Il existe une place v de $\mathbb{Q}$ telle que $|f(P)|_v$ est illimité: nous supposerons qu'il est possible de choisir v standard avec cette propriété. Avec ces conventions et notations, on a alors le résultat suivant.

(5.1) Théorème. Il y a une unique valuation standard m_v de F telle que

$$m_v(g) = - \operatorname{st}(\log|g(P)|_v / \log|f(P)|_v)$$

pour toute fonction standard $g \in F - \{0\}$. Cette valuation est triviale sur $\mathbb{Q}$.

Démonstration. Lorsque g est standard, on montre facilement que le quotient des logarithmes est limité et il est donc légitime d'en prendre la partie standard. La fonction m_v est parfaitement bien définie.

L'additivité du logarithme fournit

$$m_v(g_1 g_2) = m_v(g_1) + m_v(g_2)$$

(d'abord pour des g_i standard). L'application m_v est un homomorphisme $F \longrightarrow \mathbb{R}^+$. Il reste à vérifier

$$m_v(g_1 + g_2) \geqslant \mathrm{Inf}(m_v(g_1), m_v(g_2))$$

lorsque les deux membres sont définis. On peut supposer les g_i standard. Cette inégalité est évidemment satisfaite lorsque la place v est non archimédienne puisque dans ce cas

$$|g_1(P) + g_2(P)|_v \leqslant \mathrm{Max}\,(|g_1(P)|_v, |g_2(P)|_v)\ .$$

Dans le cas où v est archimédienne, on a encore

$$|a + b| \leqslant |a| + |b| \leqslant 2\,\mathrm{Max}(|a|, |b|)$$

et $\log 2 / \log|f(P)| \simeq 0$ montre que le facteur 2 disparaît lors de la prise de partie standard. (Pour la place complexe définie par $|a|_{\mathbb{C}} = a\bar{a} = |a|^2$ on a $|a + b|_{\mathbb{C}} \leqslant 4\,\mathrm{Max}(|a|_{\mathbb{C}}, |b|_{\mathbb{C}})$ et le même raisonnement s'appliquerait.) Démontrons finalement que m_v est triviale sur les constantes. Comme cette fonction m_v est standard, il suffit de vérifier que $m_v(c) = 1$ pour toute constante c standard non nulle. Par définition, on a

$$m_v(c) = -\,\mathrm{st}\,\log|c|_v \,/\, \log|f(P)|_v = 0$$

puisque $|c|_v$ et $\log|c|_v$ sont limités.

Lorsque la courbe C est projective et donc complète, la valuation m_v est associée à un point $P_v \in C(\bar{\mathbb{Q}})$ de la façon suivante. Il existe une constante $r_v > 0$ telle que

$$\mathrm{ord}_{P_v}(g) = r_v m_v(g) \quad \text{pour } g \in F^{\times}\ .$$

En prenant $g = f$, on trouve $r_v = -\,\mathrm{ord}_{P_v}(f)$ et

$$\mathrm{ord}_{P_v}(g)/\mathrm{ord}_{P_v}(f) = \mathrm{st}\left\{\log|g(P)|_v \,/\, \log|f(P)|_v\right\} \tag{5.2}$$

pour g standard. Plus précisément, comme les coordonnées de P_v sont algébriques, la valuation m_v est associée au cycle premier rationnel (standard) $Z_v = \sum P_v^{\sigma}$ somme des conjugés de P_v sur $\mathbb{Q}$. L'exposant parcourt l'ensemble fini de plongements $\mathbb{Q}(P_v) \longrightarrow \bar{\mathbb{Q}}$ du corps engendré par les coordonnées de P_v et pour toute $g \in F^{\times}$, les ordres de g en P_v et P_v^{σ} sont les mêmes, ce qui permet de définir l'ordre de g sur Z_v comme étant l'ordre de g en un quelconque des P_v^{σ}.

6. ESQUISSE DE DEMONSTRATION

Pour donner une idée de la démonstration du théorème B, plaçons-nous dans le cas particulier suivant. La courbe C est projective, irréductible (non singulière) définie sur $\mathbb{Q}$, standard et de genre $g \geqslant 1$. On suppose que $C(\bar{\mathbb{Q}})$ contient un point non standard P avec une coordonnée $f(P) \in \mathbb{Q}$ rationnelle (f est donc une fonction rationnelle standard non constante). L'hypothèse sur le genre implique que C admet des revêtements non ramifiés de degré arbitrairement grands. Ceci a pour conséquence que le dénominateur de f(P) est lui aussi "grand". Pour simplifier, nous supposerons que C admet un grand revêtement standard $\pi : \widetilde{C} \longrightarrow C$ de degré m et défini sur $\mathbb{Q}$, avec une fonction rationnelle $\widetilde{f}$ sur $\widetilde{C}$ de même degré que f et aussi définie sur $\mathbb{Q}$. Supposons finalement qu'il est possible de trouver un point $\widetilde{P} \in C(\bar{\mathbb{Q}})$ avec $\widetilde{f}(\widetilde{P}) \in \mathbb{Q}$ et au-dessus de P : $\pi(\widetilde{P}) = P$. En résumé, on a donc la situation décrite dans le diagramme ci-dessous.

$$\begin{array}{ccccc} \widetilde{P} \in \widetilde{C}(\bar{\mathbb{Q}}) & \xrightarrow{\widetilde{f}} & \mathbb{P}^1(\bar{\mathbb{Q}}) \ni \widetilde{f}(\widetilde{P}) & = & \widetilde{a} \in \mathbb{Q} \\ \pi \big\downarrow \deg m & & & & \\ P \in C(\bar{\mathbb{Q}}) & \xrightarrow{f} & \mathbb{P}^1(\bar{\mathbb{Q}}) \ni f(P) & = & a \in \mathbb{Q} \end{array} .$$

Le résultat (4.2) de Weil donne

$$\text{st } h(a)/h(\widetilde{a}) = \deg f \circ \pi / \deg \widetilde{f} = \deg \pi = m$$

puisque f et $\widetilde{f}$ ont même degré. D'autre part, le résultat (5.2) nous donne une estimation du quotient logarithmique des valeurs absolues $|\widetilde{a}|_v$ et $|a|_v$ en lesquelles elles sont illimitées

$$\text{st } \frac{\log|a|_v}{\log|\widetilde{a}|_v} = \text{st } \frac{\log|f(P)|_v}{\log|f(\widetilde{P})|_v} = \text{st } \frac{\log|f\circ\pi(\widetilde{P})|_v}{\log|f(\widetilde{P})|_v} =$$

$$= \frac{\text{ord}_{Z_v}(f\circ\pi)}{\text{ord}_{Z_v}(f)} = r \qquad (1 \leqslant r \leqslant \deg f) .$$

Par comparaison

(6.1) $\quad \text{st } h(a)/\log|a|_v = (m/r)\ \text{st } h(\widetilde{a})/\log|\widetilde{a}|_v$.

La quantité $h(a)/\log|a|_v$ s'interprète comme "étalement" du dénominateur de a. Prenons en effet pour v la place avec $|a|_v$ maximal. On a alors

$$|a|_v \leqslant H(a) \leqslant |a|_v^s$$

où s désigne le nombre de places w avec $|a|_w > 1$. En prenant les logarithmes, on arrive à

$$1 \leqslant h(a)/\log|a|_v \leqslant s \quad .$$

Donc (6.1) fournit

$$s \geqslant \text{st } h(a)/\log|a|_v \geqslant m/r \quad .$$

Comme l'entier m est arbitraire (mais standard), on conclut que

s est illimité.

Cela montre bien dans ce cas pourquoi la première coordonnée a = f(P) de P ne saurait être entière.

7. OBJECTIONS ET CONCLUSION

En général, lorsqu'on considère un revêtement $\pi : \tilde{C} \longrightarrow C$ un point $\tilde{P}$ au-dessus de P aura des coordonnées dans un corps de nombres (extension finie de $\mathbb{Q}$). Par définition de la hauteur du nombre algébrique $\tilde{a} = \tilde{f}(\tilde{P})$, on aura seulement

$$|\tilde{a}|_v \leqslant H(\tilde{a})^{[k:\mathbb{Q}]}$$

d'où

$$h(\tilde{a}) \,/\, \log|\tilde{a}|_v \geqslant 1/[k:\mathbb{Q}] \quad .$$

Ceci n'est plus suffisant pour conclure à l'étalement du dénominateur de a : lorsque le degré m du revêtement augmente, le degré $[k:\mathbb{Q}]$ pourrait augmenter aussi ! Le théorème de Roth fournit par contre une minoration universelle, indépendante du degré du nombre algébrique considéré. Elle s'écrit

$$\text{st } h(a)/\log|a|_v \geqslant \tfrac{1}{2}$$

pour toute place v de $\bar{\mathbb{Q}}$ et tout nombre algébrique non standard $a \in \bar{\mathbb{Q}}$.

D'autre part, la construction explicite de revêtements de C peut être effectuée en plongeant C dans sa jacobienne A et en prenant pour $\tilde{C}$ l'image réciproque de C par la multiplication par un entier r.

$$\begin{array}{ccc} \widetilde{C} = [r]^{-1}(C) & \longrightarrow & C \\ \downarrow & & \downarrow \\ A & \longrightarrow & A \end{array} \quad \text{(de degré } m = r^2\text{)} .$$

$$P \longmapsto P + P + \ldots + P = [r]\,P$$

En utilisant la partie faible du théorème de Mordell-Weil

pour tout corps de nombres k et toute variété abélienne A définie sur k, les groupes $A(k)/[r]A(k)$ sont finis, on montre comment les hypothèses faites au numéro précédent peuvent être réalisées. Le lecteur intéressé par les détails dans le cas du genre 1 (courbes elliptiques) pourra se référer au livre de Silvermann [8] .

Alain Robert
Institut de Mathématiques
Chantemerle 20
CH-2000 NEUCHATEL

REFERENCES

[1] Lang S., Integral Points on Curves,
Publ. Math. I.H.E.S. n.6 (1960), 319-335

[2] Mahler K., Uber die rationalen Punkte auf Kurven vom Geschlecht Eins,
J. Reine u. Angew. Math., 170 (1934), 168-178

[3] Robert A., Analyse non standard, Presses Polytechniques Romandes (1985)

[4] Robert A., Integral Points on Curves and NSA
L'Enseignement Mathématique (à paraître)

[5] Robinson A., Roquette P., On the Finiteness Theorem of Siegel and Mahler concerning Diophantine Equations,
J. of Nb. Theory 7, n.2 (1975), 121-176

[6] Siegel K.L., Approximation algebraischer Zahlen
M. Zeitschrift 10 (1921), 173-213
(Complete Works, vol.1 p.6-...)

[7] Siegel K.L., The Integer Solutions of the Equation $y^2 = \ldots$
J. of the London Math. Soc. 1 (1926), 66-68
(Complete Works, vol.1 p.207-208)

[8] Silvermann J.H., The Arithmetic of Elliptic Curves
Graduate Text in Math. nb.106, Springer-Verlag 1986

[9] Weil A., Arithmetic on Algebraic Varieties
Ann. of Math. 53, nb.3 (1951) 412-444