FRANÇOIS BRUHAT

Points entiers sur les courbes de genre ≥ 1

Séminaire N. Bourbaki, 1964, exp. n° 247, p. 93-104

<http://www.numdam.org/item?id=SB_1962-1964__8__93_0>

Séminaire BOURBAKI
15e année, 1962/63, n° 247

Février 1963

POINTS ENTIERS SUR LES COURBES DE GENRE ≥ 1

par François BRUHAT

(d'après Serge LANG)

En 1929, SIEGEL montrait, en utilisant un théorème d'approximation diophantienne (théorème de Thue-Siegel) qu'une courbe affine de genre ≥ 1, définie sur un corps de nombres K, n'a qu'un nombre fini de points dont les coordonnées sont des entiers de K [7]. En 1934, MAHLER montrait que, pour une telle courbe de genre 1, il n'y a qu'un nombre fini de points dont les coordonnées sont dans un sous-anneau R de K, de type fini sur $\mathbb{Z}$ (c'est-à-dire ne faisant intervenir qu'un nombre fini de nombres premiers en dénominateur) [5]. En utilisant la théorie des jacobiennes et les résultats de ROTH [6], S. LANG reprend et généralise ces résultats au cas d'une courbe de genre ≥ 1 sur un corps K de type fini sur $\mathbb{Q}$.

I. Hauteurs.

1. Notations.

Dans tout l'exposé, la lettre K désignera un corps de caractéristique zéro qui est, soit un corps de nombres, extension algébrique finie de $\mathbb{Q}$ (cas I), soit le corps $k(V)$ des fonctions rationnelles sur une variété projective V non singulière en codimension 1, définie sur k (cas II).

Dans chacun de ces deux cas, on considère une famille $\mathcal{V}$ de valeurs absolues de K, vérifiant une formule du produit avec multiplicités $N(v) \geq 1$, c'est-à-dire satisfaisant à :

(1) $\forall\ x \in K^*$, on a $v(x) = 1$, sauf pour un nombre fini de $v \in \mathcal{V}$

(2) Il existe des entiers $N(v) \geq 1$ tels que

$$\prod_{v \in \mathcal{V}} v(x)^{N(v)} = 1 \quad \text{pour tout } x \in K^* .$$

On posera $\|x\|_v = v(x)^{N(v)}$, et on désignera par $\hat{K}_v$ le complété de K pour v.

Dans le cas I, on prend pour $\mathcal{V}$ la famille des valeurs absolues prolongeant soit la valeur absolue usuelle (notée $|\ |$), soit l'une des valeurs absolues p-adiques (notée $|\ |_p$) de $\mathbb{Q}$. On a alors $N(v) = [\hat{K}_v : \hat{\mathbb{Q}}_v]$.

Dans le cas II, on considère les diviseurs premiers p de K définis sur k, c'est-à-dire les cycles $\sum W^{\sigma}$, où W est une sous-variété irréductible de codimension 1 de V, définie sur une extension algébrique de k, et où W^{σ} décrit l'ensemble des conjuguées de W sur k. L'anneau local de p dans K est alors l'anneau d'une valuation discrète normée $x \leadsto \mathrm{ord}_p\, x$ de K. On choisit une constante c, avec $0 < c < 1$, et on pose :

$$v_p(x) = c^{(\mathrm{ord}_p\, x) \deg p}$$

où $\deg p$ désigne le degré projectif de p. La famille $\mathcal{V}$ des valeurs absolues v_p satisfait bien à (1) et (2) puisque le diviseur d'une fonction est de degré zéro.

2. Hauteur dans l'espace projectif $\underset{\sim}{P}_n$.

Soit $x \in \underset{\sim}{P}_n$, rationnel sur K, et soit $(x_0, \dots, x_n) \in K^{n+1}$ un système de coordonnées de x. On appellera hauteur de x le nombre

$$h_K(x) = \prod_{v \in \mathcal{V}} \sup_i \|x_i\|_v \quad . \tag{3}$$

Vu (2), cela ne dépend pas du choix des coordonnées. En particulier, on plongera K dans $\underset{\sim}{P}_1$, et on posera pour $x \in K$:

$$h_K(x) = \prod_{v \in \mathcal{V}} \sup(1, \|x\|_v) \quad . \tag{4}$$

Si L est une extension algébrique finie, de degré r de K, la famille $\mathcal{W}$ des valeurs absolues w de L, prolongeant l'une quelconque des $v \in \mathcal{V}$, vérifie encore (1) et (2), avec $N(w) = [\hat{L}_w : \hat{K}_v]\, N(v)$. On montre alors facilement que, si $x \in \underset{\sim}{P}_n$ est rationnel sur K, on a :

$$h_L(x) = h_K(x)^r \quad .$$

Il en résulte que, pour $x \in \underset{\sim}{P}_n$, rationnel sur une extension algébrique finie L de K, le nombre $h_L(x)^{1/r}$ (avec $r = [L : K]$) ne dépend pas du choix de L. Ceci permet de prolonger la définition de h_K aux points de $\underset{\sim}{P}_n$ rationnels sur une extension algébrique de K.

3. Cas d'un corps de nombres.

Si $K = \underset{\sim}{Q}$ et si $x = \frac{a}{b}$, avec $a, b \in \underset{\sim}{Z}$ premiers entre eux, on a $h(x) = h((a, b))$. Pour tout nombre premier p, on a $|a|_p$ et $|b|_p \leqslant 1$ et l'un d'eux est égal à 1.

Par suite

(5) $$h(x) = \sup(|a|\ ,\ |b|) \quad .$$

De même si $x \in \underset{\sim}{P}_n$ est rationnel sur $\underset{\sim}{Q}$, $x = (x_o\ , \dots\ , x_n)$ avec $x_i \in \underset{\sim}{Z}$, premiers entre eux, on a :

(6) $$h(x) = \sup_i |x_i| \quad .$$

En particulier un <u>sous-ensemble de</u> $\underset{\sim}{P}_n$, <u>formé de points rationnels sur</u> $\underset{\sim}{Q}$ <u>et de hauteur bornée, est fini</u>.

Pour étendre ce résultat aux corps de nombres, on aura besoin d'une approximation du lemme de Gauss pour une valeur absolue archimédienne : soit $f \in K[X_1\ , \dots\ , X_n]$, $f = \sum c_\alpha X^\alpha$; posons pour $v \in \mathcal{V}$:

(7) $$v(f) = \sup_\alpha v(c_\alpha) \quad .$$

Le lemme de Gauss dit que l'on obtient ainsi une <u>valeur absolue</u> sur $K[X_1,\dots,X_n]$ lorsque v est non-archimédienne.

LEMME 1. - <u>Si</u> v <u>est archimédienne, l'on a</u> :

(8) $$4^{-d^n}\, v(fg) \leqslant v(f)\ v(g) \leqslant 4^{d^n}\, v(fg)$$

<u>pour</u> f , $g \in K[X_1\ , \dots\ , X_n]$ <u>avec</u> $\deg f + \deg g \leqslant d$.

On se ramène au cas d'une variable en posant $X_i = Y^{d^i}$.

Le lemme 1 résulte alors aussitôt du résultat suivant :

Si $f \in K[X]$, $f = \prod_{i=1}^{i=r} (X - \alpha_i)$ (avec $\alpha_i \in$ clôture algébrique K_a de K , à laquelle on prolonge v d'une manière quelconque), on a

(9) $$2^{-r} \prod_i \sup(1\ , v(\alpha_i)) \leqslant v(f) \leqslant 2^r \prod_i \sup(1\ , v(\alpha_i)) \quad .$$

Dans (9), l'inégalité de droite est triviale et celle de gauche se démontre par récurrence sur le nombre d'indices i tels que $v(\alpha_i) > 2$.

Du lemme 1 résulte que si l'on pose $h(f) = h((c_\alpha))$, l'on a :

(10) $$4^{-d^n s}\, h(fg) \leqslant h(f)\ h(g) \leqslant 4^{d^n s}\, h(fg)$$

si $\deg f + \deg g \leqslant d$ et s'il y a s valeurs absolues archimédiennes dans $\mathcal{V}$.

Posons alors $d = [K : \underset{\sim}{Q}]$ et soit $x = (x_o\ , \dots\ , x_n) \in \underset{\sim}{P}_n$, rationnel sur K . Posons $f = \sum x_i X_i$; on a

$$h_K(x) = h_K(f) = h_{\underset{\sim}{Q}}(f)^d \quad .$$

Pour tout $\underset{\sim}{Q}$-isomorphisme σ de K dans la clôture algébrique de $\underset{\sim}{Q}$, on a

$$h_{\underset{\sim}{Q}}(f^{\sigma}) = h_{\underset{\sim}{Q}}(f) \quad .$$

Posons

$$g = \prod_{\sigma} f^{\sigma} \in \underset{\sim}{Q}[X_1 , \dots , X_n] \quad :$$

d'après (10), il existe une constante c, ne dépendant que de d, telle que

$$h_{\underset{\sim}{Q}}(g) \leqslant c\, h_{\underset{\sim}{Q}}(f)^d = c\, h_K(x) \quad .$$

Il en résulte que si x décrit un ensemble de hauteur bornée, les coefficients de g décrivent un ensemble fini. D'où :

THÉORÈME 1. - Pour tout entier d et toute constante k, l'ensemble des points x de $\underset{\sim}{P}_n$ satisfaisant à :

$$[\underset{\sim}{Q}(x) : \underset{\sim}{Q}] \leqslant d \qquad h_{\underset{\sim}{Q}}(x) \leqslant k$$

est fini.

COROLLAIRE. - Pour toute constante k, l'ensemble des points $x \in \underset{\sim}{P}_n$ rationnels sur le corps de nombres K, et satisfaisant à $h_K(x) \leqslant k$, est fini.

4. Hauteurs sur une variété.

Soit V une variété complète non-singulière définie sur K.

Si φ est un morphisme de V dans un projectif $\underset{\sim}{P}_n$, on posera :

$$h_{\varphi}(x) = h_K(\varphi(x))$$

(pour $x \in V$, rationnel sur une extension algébrique de K).

Si $\omega : W \to V$ est un morphisme, il est clair que :

(11)
$$h_{\varphi\circ\omega} = h_{\varphi} \circ \omega \quad .$$

Mais à un morphisme φ de V dans un projectif est associée une classe de diviseurs positifs sur V : on montre en effet que l'ensemble des diviseurs positifs X sur V, rationnels sur K, tels qu'il existe des fonctions rationnelles $(y_0 , y_1 , \dots , y_n)$ définissant φ et satisfaisant à :

$$(y_j) = X_j - X \,, \qquad X_j \geqslant 0 \,, \qquad X_o \cap \dots \cap X_n = \emptyset$$

est une classe de diviseurs positifs pour l'équivalence linéaire. On la notera $D(\varphi)$: on obtient un élément $X \in D(\varphi)$ en prenant par exemple un système $(y_o , \dots , y_n)$ définissant φ, et en posant $X = \sup$ des diviseurs polaires $\left(\frac{y_i}{y_o}\right)_{\infty}$.

THÉORÈME 2. — Soient φ , φ' , φ'' des morphismes de V dans des projectifs.

(i) Si $D(\varphi) = D(\varphi')$, alors $h_\varphi \sim h_{\varphi'}$ (ce qui signifie qu'il existe des constantes c_1 et $c_2 > 0$ avec $c_1\, h_\varphi \leqslant h_{\varphi'} \leqslant c_2\, h_\varphi$).

(ii) Si $D(\varphi) = D(\varphi') + D(\varphi'')$, alors $h_\varphi \sim h_{\varphi'}\, h_{\varphi''}$.

(iii) Si φ et φ' sont des plongements (biholomorphes) et si $D(\varphi)$ et $D(\varphi')$ sont algébriquement équivalents, alors pour tout $\varepsilon > 0$, il existe des constantes c_1 , $c_2 > 0$ telles que :

$$c_1\, h_\varphi^{1-\varepsilon} \leqslant h_{\varphi'} \leqslant c_2\, h_\varphi^{1+\varepsilon} \qquad \text{(on écrira } h_\varphi \approx h_{\varphi'}\text{)}$$

Démontrons (i) : Soit $X \in D(\varphi) = D(\varphi')$, et écrivons

$$\varphi = (f_0 , \dots , f_n) \qquad (f_j) = X_j - X \qquad X_0 \cap \dots \cap X_n = \emptyset \qquad X_j \geqslant 0$$

$$\varphi' = (g_0 , \dots , g_m) \qquad (g_k) = Y_k - X \qquad Y_k \geqslant 0 \qquad .$$

Posons $u_j = f_j/g_k$: on a $(u_j) = X_j - Y_k$ et par suite les fonctions $u_0 , \dots , u_n$ sont sans zéros communs. Comme V est complète, elles vérifient une relation du type

$$1 = \sum_{|\alpha|>0} a_\alpha\, u^\alpha \qquad . \tag{12}$$

Soit x un point de V_K , $x \notin X \cup Y_k$, et soit $v \in \mathcal{V}$: on déduit de (12) qu'il existe une constante $c(X , k)$ telle que l'on ait

$$\sup_i v(f_j(x)) \geqslant c(X , k)\; v(g_k(x)) \tag{13}$$

et on peut prendre $c = 1$, sauf pour un nombre fini de v , à savoir les v archimédiennes et celles pour lesquelles il y a un coefficient a_α avec $v(a_\alpha) > 1$. On peut donc former le produit des inégalités (13), et on obtient finalement l'existence d'une constante $\gamma(X)$ telle que :

$$h_\varphi(x) \geqslant \gamma(X)\; h_{\varphi'}(x) \quad \text{pour} \quad x \in V_K , \quad x \notin X \tag{14}$$

et on montre même aisément que (14) est valable pour $x \in V$, $x \notin X$ et x rationnel sur une extension algébrique de K .

On peut faire ceci en prenant successivement $X = X_0 , X_1 , \dots , X_n$, et on en déduit

$$h_\varphi(x) \geqslant \gamma h_{\varphi'}(x) \tag{15}$$

pour $x \in V$ rationnel sur une extension algébrique de K , avec $\gamma = \inf\limits_i \gamma(X_i)$. D'où (i).

(ii) est immédiat : On considère le morphisme

$$u : (x_0 , \dots , x_n) \times (y_0 , \dots , y_m) \rightsquigarrow (x_i\, y_j)$$

de $\underset{\sim}{P}_n \times \underset{\sim}{P}_m$ dans $\underset{\sim}{P}_{(n+1)(m+1)-1}$. Alors le morphisme $u \circ (\varphi' \times \varphi'')$ a pour classe de diviseurs $D(\varphi') + D(\varphi'')$ et pour hauteur $h_{\varphi'}\, h_{\varphi''}$.

Pour démontrer (iii), on utilise le résultat suivant : Si $X \in D(\varphi)$ et si φ est un plongement, il existe un entier $e > 0$ tel que pour tout diviseur Z algébriquement équivalent à zéro, le diviseur $Z + eX$ est associé à un plongement. Soit $X' \in D(\varphi')$. Pour tout entier $n \geqslant 0$, il existe donc un plongement φ_n tel que :

$$n(X - X') + eX \in D(\varphi_n) \qquad .$$

Si $X_n \in D(\varphi_n)$, on a donc

$$(n + e)\, X \sim nX' + X_n$$

d'où

$$h_{\varphi}^{n+e} \sim h_{\varphi'}^{n}\, h_{\varphi_n}$$

et

$$h_{\varphi}^{1+(e/n)} \sim h_{\varphi'}\, h_{\varphi_n}^{1/n} \geqslant h_{\varphi'} \quad \text{car} \quad h_{\varphi_n} \geqslant 1 \qquad .$$

On en déduit aussitôt (iii).

COROLLAIRE. - Supposons que V soit une courbe. Soient $X \in D(\varphi)$ et $X' \in D(\varphi')$. Posons $d =$ degré de X , $d' =$ degré de X' . Alors on a :

$$h_{\varphi} \approx h_{\varphi'}^{d/d'} \qquad .$$

On sait en effet que sur une courbe, deux diviseurs sont algébriquement équivalents si et seulement s'ils ont même degré.

Remarque. - La théorie des hauteurs est due essentiellement à SIEGEL [7] dans le cas des courbes (corollaire du théorème 2) et à WEIL [8]. Le (iii) du théorème 2 est dû, en dimension > 1 , à LANG [3].

II. Le théorème de Roth.

5. Un énoncé du théorème de Thue-Siegel-Roth.

Nous conservons les notations précédentes. Soit K_a une clôture algébrique de K et choisissons pour toute $v \in \mathcal{V}$ une valeur absolue (notée encore v) de K_a prolongeant v .

THÉORÈME 3. – Soit S une partie finie de $\mathcal{V}$. Pour tout $v \in S$, soit $\alpha_v \in K_a$. Soit c, $\rho > 0$. L'ensemble des $x \in K$ tels que :

$$(16) \qquad \prod_{v \in S} \inf(1 \, , \, v(X - \alpha_v)^{N(v)}) \leq c \, h_K(x)^{-2-\rho}$$

est de hauteur bornée.

Il n'est pas question de donner ici la moindre indication sur la démonstration : voir [4], chapitre VI. Indiquons comment on retrouve à partir du théorème 3 l'énoncé "classique" du théorème de Roth : on prend $K = \mathbb{Q}$, S se composant de la seule valeur absolue usuelle. On trouve que, pour $\alpha \in \mathbb{Q}_a$, l'ensemble des $\frac{m}{n} \in \mathbb{Q}$ satisfaisant à

$$|\alpha - \frac{m}{n}| \leq c \, h(\frac{m}{n})^{-2-\rho}$$

est fini. Mais

$$h(\frac{m}{n}) = \sup(|m| \, , \, |n|) \qquad (\text{si} \quad (m \, , \, n) = 1 \,)$$

et si $\frac{m}{n}$ est voisin de α, $|n|$ et $h(\frac{m}{n})$ sont équivalents.

On trouve donc qu'il n'y a qu'un nombre fini d'éléments $\frac{m}{n} \in \mathbb{Q}$ tels que $|\alpha - \frac{m}{n}| \leq \frac{c}{n^{2+\rho}}$.

6. Formulation géométrique du théorème de Roth.

THÉORÈME 4. – Soit W une courbe projective non-singulière, définie sur K. Soit $f \in K(W)$, non constante, et soit r l'ordre maximum des pôles de f. Soit $\lambda > 2$ et $c > 0$. L'ensemble F des points $x \in W$, rationnels sur K et vérifiant :

$$(17) \qquad \|f(x)\|_v \geq c \, h(x)^{\lambda r}$$

est de hauteur bornée.

(h est évidemment la hauteur relative au plongement projectif donné de W.) On commence par choisir une $g \in K(W)$, c'est-à-dire un morphisme de W dans $\mathbb{P}_1$, telle que $h \sim h_g$, que g n'ait ni zéros ni pôles aux pôles de f et prenne des valeurs distinctes en ces pôles : il suffit de prendre

$$g = \frac{a_o x_o + \dots + a_n x_n}{b_o x_o + \dots + b_n x_n} \qquad a_i \, , \, b_i \in K$$

(où $(x_o \, , \, \dots \, , \, x_n)$ sont les coordonnées sur W) les a_i et les b_j n'annulant pas certains polynômes. Naturellement, on utilise le corollaire du théorème 2.

Soit D le cycle des pôles de f et soit $\mathcal{O}$ l'anneau local de D dans $K(f)$. Puisque f n'est pas constante, $K(W)$ est algébrique sur $K(f)$, et puisque g n'a pas de pôle sur D, g est entière sur $\mathcal{O}$. Soit P le polynôme minimal de g sur $K(f)$: on a :

$$P(X) = Q(X) + f^{-1} A(f^{-1}, X)$$

avec $Q \in K[X]$ et $A \in K[Y, X]$.

Posons $Q(X) = \prod(X - \alpha_i)^{r_i}$ (avec $\alpha_i \in K_a$) : on montre (en utilisant le fait que g prend des valeurs distinctes aux points de D) que les ordres de multiplicité r_i sont $\leqslant r$.

Soit alors $x_n \in F$, avec $h(x_n) \to +\infty$. On peut supposer que $v(g(x_n))$ reste <u>borné</u> : sinon, on extraira une suite partielle telle que $v(g(x_{n_k})) \to \infty$ et on remplacera g par $\frac{1}{g}$. Pour n grand, $v(f^{-1}(x_n))$ est voisin de zéro d'après (17) et $v(A(f^{-1}(x_n)), g(x_n))$ reste <u>borné</u>. Comme $P(f) = 0$, il en résulte qu'il existe une constante $c_1 > 0$ telle que

$$(18) \qquad \prod_i \|f(x_n) - \alpha_i\|_v^{r_i} = \|Q(f(x_n))\|_v \leqslant c_1 \|f^{-1}(x_n)\|_v \leqslant \frac{c_1\, c^{-1}}{h(x_n)^{\lambda r}} .$$

L'un des facteurs du premier membre de (18) est donc très petit, et par extraction de suite, on se ramène au cas où $\|f(x_n) - \alpha_1\|_v$, par exemple, tend vers zéro. On a alors

$$\prod_{i \geqslant 2} \|f(x_n) - \alpha_i\|_v^{r_i} \geqslant c_2 > 0$$

d'où

$$\|f(x_n) - \alpha_1\|_v^{r_1} \leqslant \frac{c_3}{h(x_n)^{\lambda r}}$$

et puisque $r_1 \leqslant r$, on en déduit

$$\|f(x_n) - \alpha_1\|_v \leqslant \frac{c_4}{h(x_n)^{\lambda}} \qquad (\lambda > 2)$$

ce qui contredit le théorème 3.

III. Cas des courbes de genre $\geqslant 1$.

On garde les notations de II, et on suppose de plus que W est de <u>genre</u> $\geqslant 1$.

7. Amélioration du théorème 4.

Supposons que W ait un point rationnel sur K. La jacobienne J de W est alors définie sur K, et nons désignerons par J_K le groupe des points de J rationnels sur K. On sait (forme faible du théorème de Mordell-Weil) que pour tout entier $m \geq 1$, le groupe quotient J_K/mJ_K est fini, à condition, dans le cas II, de supposer le corps des constantes k algébriquement clos, ce que nous supposons dans ce numéro (voir par exemple [4], chapitre 5).

THÉORÈME 5. - Soit $f \in K(W)$, non constante. Pour tous $c, \rho > 0$, l'ensemble F des points de W, rationnels sur K, tels que

$$v(f(x)) \geq c\, h(x)^{\rho} \tag{19}$$

est de hauteur bornée.

Vu le corollaire du théorème 2, il suffit de démontrer le théorème 5 pour un plongement projectif particulier de W : on supposera choisi un plongement projectif de J, et on considèrera W comme plongée dans J (on sait qu'il existe une famille de plongements canoniques de W dans J, définis à une translation près de J).

Soit alors $x_n \in F$, avec $h(x_n) \to \infty$. Puisque J_K/mJ_K est fini, on peut supposer que les x_n appartiennent tous à la même classe $a + mJ_K$.

Considérons alors le revêtement non ramifié $\omega : J \to J$ défini par $\omega(u) = a+mu$, et considérons sa restriction à W. On obtient un revêtement non ramifié irréductible $\omega_o : U \to W$, défini sur K (cf. [1], § 4). On a $x_n \in \omega_o(U_K)$ et on peut donc choisir $y_n \in U_K$ avec $x_n = \omega_o(y_n)$.

Par ailleurs, on sait que si X est un diviseur positif sur J, l'application $\alpha \rightsquigarrow \alpha^{-1}(X)$ du $\mathbb{Z}$-module des endomorphismes de J dans le groupe des classes de diviseurs modulo l'équivalence algébrique est quadratique (cf. par exemple [2], p. 92). Il en résulte que si X est un diviseur positif associé au plongement choisi φ de J (c'est-à-dire une section hyperplane de J), le diviseur $\omega^{-1}(X)$, qui est associé au plongement $\varphi \circ \omega$ de J, est algébriquement équivalent à $m^2(X - a)$, ou encore à $m^2 X$, car X et le translaté $X - a$ sont algébriquement équivalents. Le théorème 2 entraîne alors que :

$$h_{\varphi}^{m^2} \approx h_{\varphi\circ\omega} = h_{\varphi} \circ \omega .$$

Prenons alors m suffisamment grand pour que $(m^2 - 1)\rho > 3r$, où r est l'ordre maximum des pôles de f, ou encore de $f \circ \omega$. On a

$$h_\varphi(x_n) = h_\varphi(\omega(y_n)) \geqslant c_1\ h_\varphi(y_n)^{m^2-1}$$

et

$$v(f \circ \omega(y_n)) = v(f(x_n)) \geqslant c_2\ h_\varphi(y_n)^{(m^2-1)\rho}$$

avec $h(y_n) \to \infty$, ce qui contredit le théorème 4.

8. Où l'on montre que les points entiers sont de hauteur bornée.

Soit $\mathfrak{W}$ un sous-ensemble fini de $\mathfrak{V}$, contenant toutes les valeurs absolues archimédiennes de $\mathfrak{V}$ et soit R un sous-anneau de K, dont les éléments a sont entiers pour toutes les valeurs absolues v (nécessairement non-archimédiennes) de $\mathfrak{V}$ n'appartenant pas à $\mathfrak{W}$ (i. e. vérifiant $v(a) \leqslant 1$) pour toutes les valeurs absolues v (nécessairement non-archimédiennes) de $\mathfrak{V}$ n'appartenant pas à $\mathfrak{W}$.

THÉORÈME 6. - Soit W une courbe projective non-singulière de genre ≥ 1 définie sur K et soit $f \in K(W)$, non constante. L'ensemble F des points de W, rationnels sur K, qui ne sont pas des pôles de f et où f prend une valeur appartenant à R est de hauteur bornée.

Si l'on est dans le cas II, on peut supposer k algébriquement clos puisque les hauteurs ne dépendent pas des corps des constantes. On pourra donc appliquer le théorème 5.

Soit $x_n \in F$ avec $h(x_n) \to +\infty$. On a

$$\begin{aligned} h(f(x_n)) &= \prod_{v\in\mathfrak{V}} \sup(1\ ,\ v(f(x_n))^{N(v)}) \\ &= \prod_{v\in\mathfrak{W}} \sup(1\ ,\ v(f(x_n))^{N(v)}) \end{aligned} \quad .$$

Mais (corollaire du théorème 2) $h(f(x_n)) \approx h(x_n)^\delta$ avec $\delta > 0$, et par suite $h(f(x_n)) \to +\infty$. Posons

$$N = \sum_{v\in\mathfrak{W}} N(v)$$

pour tout n assez grand, il existe une $v \in \mathfrak{W}$ avec $v(f(x_n)) \geqslant h(f(x_n))^{1/N}$ et on peut supposer que c'est toujours la même v, par extraction de suite. On a alors $v(f(x_n)) \geqslant h(x_n)^{\delta/2N}$ pour n grand, ce qui contredit le théorème 5.

COROLLAIRE. - Soit K un corps de nombres et soit R un sous-anneau de K, de type fini sur $\mathbb{Z}$. Soit W une courbe projective non-singulière de genre ≥ 1 définie sur K, et soit $f \in K(W)$, non constante. L'ensemble des points de W, rationnels sur K, qui ne sont pas des pôles de f et où f prend une valeur appartenant à R est fini.

L'ensemble des valeurs absolues non-archimédiennes, qui ne sont pas toujours $\leqslant 1$ sur R, est en effet fini.

9. Cas des corps de fonctions.

L'interprétation de la condition "de hauteur bornée" fait appel dans le cas fonctionnel (cas II) aux propriétés des jacobiennes et de leurs " K/k-traces" (voir par exemple [4], chapitre V). Enonçons le résultat :

THÉORÈME 7. - *Soient K un corps de fonctions sur k et W une courbe projective non-singulière de genre $\geqslant 1$ définie sur K. Si F est un sous-ensemble infini de points de W, rationnels sur K et de hauteur bornée, alors il existe une courbe W_0 définie sur k et une transformation birationnelle $T : W_0 \to W$ définie sur K. Si le genre de W est $\geqslant 2$, tous les points de F, sauf un nombre fini, sont images par T de points de W_0 rationnels sur k. Si le genre est 1, alors les points de F se trouvent sur un nombre fini de classes modulo l'image par T du groupe des points de W_0 rationnels sur k.*

Des théorème 6 et 7, on déduit le théorème suivant :

THÉORÈME 8. - *Soient K un corps de type fini sur $\mathbb{Q}$ et R un sous-anneau de K de type fini sur $\mathbb{Z}$. Soit W une courbe projective non-singulière de genre $\geqslant 1$ définie sur K. Soit $f \in K(W)$, non constante. L'ensemble F des points de W, rationnels sur K, qui ne sont pas des pôles de f et où f prend une valeur appartenant à R, est fini.*

Supposons F infini ; et soit k la fermeture algébrique de $\mathbb{Q}$ dans K. Les théorèmes 6 et 7 permettent de supposer que W est *définie sur* k et que l'ensemble F' des points de F, *rationnels sur* k, est infini. On raisonne alors par récurrence sur la dimension algébrique n de K sur $\mathbb{Q}$, le cas $n = 0$ étant le corollaire du théorème 6. Si $n > 0$, on prend un corps L avec $k \subset L \subset K$ et K de degré de transcendance 1 sur L. Soit $\mathcal{O}$ un anneau de valuation discrète de K, contenant R et L, tel que le corps résiduel $K' = \mathcal{O}/m$ soit algébrique sur L et que la "réduction" f' de f modulo m ne soit pas constante. En réduisant toutes les données modulo m, les points de F' donnent un ensemble infini de points rationnels sur K' où f' prend des valeurs appartenant à l'image R' de R dans K', d'où, etc.

BIBLIOGRAPHIE

[1] LANG (Serge). - Unramified class field theory over function fields in several variables, Annals of Math., Series 2, t. 64, 1956, p. 285-325.

[2] LANG (Serge). - Abelian varieties. - New York, Interscience Publishers, 1959 (Interscience Tracts in pure and applied Mathematics, 7).

[3] LANG (Serge). - Integral points on curves. - Paris, Presses universitaires de France, 1960 (Institut des Hautes Etudes scientifiques, Publications mathématiques, 6 ; p. 27-43).

[4] LANG (Serge). - Diophantine geometry. - New York, Interscience Publishers, 1962 (Interscience Tracts in pure and applied Mathematics, 11).

[5] MAHLER (K.). - Über die rationalen Punkte auf Kurven vom Geschlecht Eins, J. für die reine und angew. Math., t. 170, 1934, p. 168-178.

[6] ROTH (K. F.). - Rational approximations to algebraic numbers, Mathematika, t. 2, 1955, p. 1-20.

[7] SIEGEL (C. L.). - Über einige Anwendungen Diophantischer Approximationen, 2ter Teil : Über Diophantische Gleichungen, Abh. Preuss. Akad. Wiss., Phys.-math. Kl., 1929, p. 41-70.

[8] WEIL (André). - Arithmetic on algebraic varieties, Annals of Math., Series 2, t. 53, 1951, p. 412-444.