Astérisque

JOSEPH OESTERLÉ

Courbes sur une variété abélienne

Astérisque, tome 121-122 (1985), Séminaire Bourbaki,
exp. n° 625, p. 213-224

<http://www.numdam.org/item?id=SB_1983-1984__26__213_0>

© Société mathématique de France, 1985, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (http://smf4.emath.fr/Publications/Asterisque/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Séminaire BOURBAKI
36e année, 1983-84, n° 625 Février 1984

COURBES SUR UNE VARIÉTÉ ABÉLIENNE
[d'après M. Raynaud]

par Joseph OESTERLÉ

INTRODUCTION

Soient A une variété abélienne définie sur un corps K de caractéristique 0, X une courbe propre absolument intègre de A définie sur K et non elliptique, Γ un sous-groupe de type fini de $A(\overline{K})$.

Nous nous proposons de décrire comment, à la suite de travaux de M. Raynaud et G. Faltings, l'énoncé suivant, conjecturé par S. Lang en 1965 ([La 1]), a été démontré.

THÉORÈME 1.– *L'ensemble des éléments* x *de* $X(\overline{K})$ *dont un multiple* nx *(avec* n *entier non nul) appartient à* Γ *est fini.*

M. Raynaud commence par démontrer le cas particulier de ce théorème où $\Gamma = \{0\}$:

THÉORÈME 2 (M. Raynaud).– *L'ensemble des éléments de* $X(\overline{K})$ *qui sont de torsion dans* $A(\overline{K})$ *est fini.*

Il démontre aussi que le théorème 1 est entraîné par le théorème 3 ci-dessous, apparemment plus faible. L'énoncé du théorème 3 est équivalent à la célèbre conjecture de Mordell qui affirme qu'une courbe absolument intègre Y définie sur une extension E de type fini de $\mathbb{Q}$ n'a qu'un nombre fini de points rationnels sur E si le corps de ses fonctions rationnelles est de genre ≥ 2. Cette conjecture a été récemment prouvée par G. Faltings, et on a donc :

THÉORÈME 3 (G. Faltings).– *L'ensemble* $X(\overline{K}) \cap \Gamma$ *est fini.*

Ceci achève la démonstration du théorème 1. Les travaux de G. Faltings ont fait l'objet d'exposés dans le précédent séminaire. Cet exposé est consacré à la démonstration par M. Raynaud du théorème 2 et de l'implication théorème 3 $\Rightarrow$ théorème 1 (cf. n° 4).

Au n° 1 nous donnons une démonstration, due à Bogomolov, de l'analogue du théorème 2 obtenu en remplaçant "torsion" par "torsion ℓ-primaire". Les n° 2 et 3 sont consacrés à des résultats de nature p-adique, en admettant un résultat technique démontré aux n° 5 et 6. Le n° 7 décrit diverses généralisations des théorèmes ci-dessus.

Signalons pour finir que l'on peut donner des énoncés de type "analytique complexe" équivalents aux énoncés précédents. Ainsi en remarquant que toute surface de Riemann S (compacte, connexe) est algébrisable et qu'une application analytique de S dans un tore complexe se factorise par la jacobienne de S, on vérifie aisément l'équivalence des énoncés du théorème 2 et du théorème 2' suivant :

THÉORÈME 2'.— *Soient* L *un réseau (de rang* $2g$*) de* $\mathbb{C}^g$, φ *une application analytique d'une surface de Riemann compacte connexe* S *dans* $\mathbb{C}^g/L$. *Si* $\varphi(S)$ *n'est contenue dans l'image d'aucune droite affine complexe de* $\mathbb{C}^g$, *son intersection avec* $\mathbb{Q}L/L$ *est finie.*

Il serait intéressant d'obtenir une démonstration purement transcendante du théorème précédent.

NOTATIONS

Etant donnée une variété abélienne A définie sur un corps K, un entier $n \geq 1$ et un nombre premier ℓ, on pose

$$A_n = \mathrm{Ker}(A(\overline{K}) \xrightarrow{n} A(\overline{K})),$$

$$A_{\ell^\infty} = \bigcup_{r \geq 1} A_{\ell^r},$$

$$T_\ell(A) = \varprojlim_r A_{\ell^r},$$

(l'application de transition $A_{\ell^r} \to A_{\ell^s}$ pour $r \geq s \geq 1$ étant la multiplication par ℓ^{r-s}).

Pour tout sous-groupe Γ de $A(\overline{K})$, on note $\mathrm{Div}(\Gamma)$ l'ensemble des "points de division de Γ", c'est-à-dire l'ensemble des $x \in A(\overline{K})$ dont un multiple nx (avec n entier non nul) appartient à Γ.

1. TORSION ℓ-PRIMAIRE, SUIVANT BOGOMOLOV

1.1. THÉORÈME (Bogomolov).— *Soient* A *une variété abélienne non nulle définie sur une extension de type fini* K *de* $\mathbb{Q}$ *et* ℓ *un nombre premier. Le groupe de Galois* $G_K = \mathrm{Gal}(\overline{K}/K)$ *opère sur le* $\mathbb{Z}_\ell$*-module* $T_\ell(A)$. *Son image dans* $\mathrm{Aut}(T_\ell(A))$ *contient un sous-groupe ouvert du groupe d'homothéties* $\mathbb{Z}_\ell^\times$.

Nous renvoyons à [Bo] pour la démonstration de ce résultat : en fait la démonstration n'y est donnée que lorsque K est une extension finie de $\mathbb{Q}$, mais le cas général s'y ramène facilement par spécialisation. Signalons simplement que Bogomolov montre, en utilisant les propriétés des modules de Hodge-Tate, que l'image de G_K dans $\mathrm{Aut}(T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell)$ contient un sous-groupe ouvert de son enveloppe algébrique et d'après une remarque de Deligne l'algèbre de Lie de cette enveloppe algébrique contient les homothéties.

COROLLAIRE.— *Il existe un entier* $n > 1$ *et un élément* σ *de* G_K *tels que l'on ait* $\sigma(x) = nx$ *pour tout* $x \in A_{\ell^\infty}$.

1.2. L'énoncé qui suit est le cas particulier du théorème 2 que l'on obtient en se restreignant à la partie ℓ-primaire de la torsion.

THÉORÈME.— *Soient* A *une variété abélienne définie sur un corps* K *de caractéristique* 0, X *une courbe fermée absolument intègre de* A *définie sur* K *non elliptique,* ℓ *un nombre premier. L'ensemble* $X(\overline{K}) \cap A_{\ell^\infty}$ *est fini.*

Quitte à remplacer K par un sous-corps convenable sur lequel A et X sont définis, on peut supposer que K est de type fini sur $\mathbb{Q}$. Choisissons alors σ et n comme dans le corollaire au théorème 1.1. Pour tout $x \in X(\overline{K}) \cap A_{\ell^\infty}$ on a $nx = \sigma(x) \in X(\overline{K})$. Si $X(\overline{K}) \cap A_{\ell^\infty}$ était infini, X serait stable par l'endomorphisme n_A de multiplication par n dans A. On conclut grâce au lemme suivant :

Lemme.— Si X *est stable par* n_A *(avec* $n \geq 2$*),* X *est elliptique.*

Notons u le morphisme de X dans X induit par n_A. Son degré est égal à n^2 : en effet si l'on plonge K dans $\mathbb{C}$ et que l'on choisit une 1-forme différentielle holomorphe invariante ω sur $A(\mathbb{C})$ dont la restriction à l'ensemble $X'(\mathbb{C})$ des points lisses de $X(\mathbb{C})$ est non identiquement nulle, on a $n_A^*\omega = n\omega$, d'où

$$\deg(u)\int_{X'(\mathbb{C})} (\omega \wedge \overline{\omega}) = \int_{X'(\mathbb{C})} (n_A^*\omega \wedge \overline{n_A^*\omega}) = n^2 \int_{X'(\mathbb{C})} \omega \wedge \overline{\omega} .$$

Comme le morphisme $n_A : A \to A$ est galoisien de groupe A_n, l'ensemble des $a \in A_n$ tels que $X + a$ soit égal à X contient n^2 éléments. Ce raisonnement appliqué aux puissances de n montre que X est stable par une infinité de translations de A, donc est elliptique.

1.3. On peut préciser le théorème 1.2 par un énoncé "d'uniformité par rapport aux translations" :

THÉORÈME.— *Sous les hypothèses du théorème* 1.2, *il existe un entier* m *tel que pour toute extension* L *de* K *et tout* $a \in A(L)$ *le cardinal de* $(X + a)(\overline{L}) \cap A_{\ell^\infty}$ *soit majoré par* m.

Comme précédemment on peut supposer K de type fini sur $\mathbb{Q}$. La démonstration du théorème 1.2 montre que, si σ' désigne un automorphisme de $\overline{L}$ prolongeant σ, le cardinal de $(X + a)(\overline{L}) \cap A_{\ell^\infty}$ est majoré par le nombre d'éléments x de $(X + a)(\overline{L})$ tels que $nx \in (X + \sigma'(a))(\overline{L})$, ou encore, en notant b un élément de $A(\overline{L})$ tel que $(n-1)b = na - \sigma'(a)$, par le nombre d'éléments y de $(X + b)(\overline{L})$ tels que $ny \in (X + b)(\overline{L})$. Le théorème résulte alors du fait suivant : soit Y la sous-variété algébrique fermée $\{(b,y)/y - b \in X,\ ny - b \in X\}$ de $A \times A$; la première projection induit un morphisme propre de Y dans A, à fibres finies d'après le lemme de 1.2, et le cardinal de ses fibres est donc majoré.

Remarque.— Comme l'avait déjà remarqué S. Lang (cf. [La 1]) une démonstration analogue à la précédente permettrait d'obtenir le théorème 2 si l'on savait, sous les hypothèses du théorème 1.1, que l'image de G_K dans $\prod_\ell \mathrm{Aut}(T_\ell(A))$ contient un sous-groupe ouvert de $\hat{\mathbb{Z}}^\times = \prod_\ell \mathbb{Z}_\ell^\times$ (ce que J.-P. Serre conjecture dans [Se]).

2. VARIÉTÉS ABÉLIENNES SUR UN CORPS p-ADIQUE

2.0. Dans ce numéro, K *désigne un corps de caractéristique* 0, *complet pour une valuation discrète* v, R l'anneau de valuation de v, m l'idéal maximal de R. On suppose que *le corps résiduel* k *de* R *est algébriquement clos, de caractéristique* $p > 0$, que le groupe des valeurs de v est $\mathbb{Z}$ et on note e l'indice de ramification absolu $v(p)$ de R.

On note $\overline{K}$ une clôture algébrique de K, $\overline{v}$ la valuation de $\overline{K}$ qui prolonge v, $\overline{R}$ l'anneau de la valuation $\overline{v}$, $\overline{m}$ l'idéal maximal de $\overline{R}$.

2.1. *Soit* A *une variété abélienne définie sur* K *ayant bonne réduction en* v : cela signifie qu'il existe un R-schéma abélien A dont A est la fibre générique (et un tel A est unique à isomorphisme unique près). La fibre spéciale A_o de A est une variété abélienne définie sur k.

2.2. On a une *application de spécialisation* de $A(K) = A(R)$ dans $A_o(k)$. Elle est surjective car A est lisse sur R et s'étend d'ailleurs en une application de spécialisation de $A(\overline{K}) = A(\overline{R})$ dans $A_o(k)$. Etant donnée une extension finie $K' \subset \overline{K}$ de K, l'ensemble des éléments de $A(K')$ qui se spécialisent en 0 s'identifie à l'ensemble des points à coordonnées dans $\overline{m} \cap K'$ d'un groupe formel défini sur R : cet ensemble est *un groupe standard sur* K' au sens de ([LIE], III, § 7, n° 3). Pour tout $\lambda \in \mathbb{R}_+$, nous noterons $A_{(\lambda)}(K')$ l'ensemble des points de ce groupe standard dont les coordonnées ont une valuation strictement supérieure à λ. On pose $A_{(\lambda)}(\overline{K}) = \bigcup_{K'} A_{(\lambda)}(K')$.

2.3. PROPOSITION.– a) *La restriction de l'application de spécialisation à l'ensemble des points de torsion de* $A(K)$ *a un noyau fini d'ordre une puissance de* p ; *elle est injective si* $e < p - 1$.

b) *Soit* M *une partie de* $\mathrm{Div}(A(K))$. *Si les degrés* $[K(x):K]$ *sont bornés lorsque* x *décrit* M, *il existe un entier* $r \geq 0$ *tel que* $p^r M$ *soit contenu dans* $A(K)$.

Posons $\lambda = \frac{e}{p-1}$. Il résulte des propriétés de l'application exponentielle ([LIE], III, § 7, n° 6, prop. 14) que $A_{(\lambda)}(\overline{K})$ est sans torsion et qu'on a $A_{(\lambda)}(\overline{K}) \cap \mathrm{Div}(A(K)) = A_{(\lambda)}(K)$. D'autre part pour tout $\mu \in]0,\lambda]$, $A_{(\mu)}(\overline{K})/A_{(\lambda)}(\overline{K})$ est annulé par une puissance de p (*loc. cit.*, n° 4).

L'assertion a) résulte de ce qui précède car le noyau de l'application de spécialisation $A(K) \longrightarrow A_o(k)$ est contenu dans $A_{(\mu)}(K)$ pour tout $\mu < 1$.

Prouvons b). Quitte à translater les éléments de M par des éléments de $A(K)$, on se ramène au cas où ils se spécialisent en 0. Les degrés des extensions $K(x)$ de K où x décrit M étant bornés, il en est de même de leurs indices de ramification ; ceci entraîne que M est contenu dans $A_{(\mu)}(\overline{K})$ pour un $\mu > 0$ convenable et b) résulte des remarques faites au début de la démonstration.

3. RÉSULTATS p-ADIQUES

3.0. Dans ce numéro, nous conservons les notations du numéro précédent. Nous supposons en outre que *l'indice de ramification absolu* e *de* R *est égal à* 1 .

3.1. On se donne de plus une courbe X sur A , absolument intègre, définie sur K . On suppose que X est la fibre générique d'une R-courbe propre et plate $\mathcal{X}$ de $\mathcal{A}$ vérifiant les hypothèses techniques suivantes :

(i) La fibre spéciale X_0 de $\mathcal{X}$ est intègre, la normalisée $\widetilde{\mathcal{X}}$ de $\mathcal{X}$ est lisse sur R , à fibres de genre ≥ 2 . En particulier la fibre spéciale de $\widetilde{\mathcal{X}}$ est la normalisée de X_0 .

(ii) Soit J la jacobienne de $\widetilde{\mathcal{X}}$ et $a : J \to A$ le morphisme d'Albanese associé au morphisme composé $\widetilde{\mathcal{X}} \to \mathcal{X} \to \mathcal{A}$. On suppose que a est surjectif, que son noyau N est lisse et que le groupe des composantes connexes de N est d'ordre premier à p .

3.2. Les hypothèses précédentes entraînent les résultats suivants :

a) *Si* a *est un élément de* $A(\overline{K}) - A(K)$, *il existe* $\sigma \in \mathrm{Gal}(\overline{K}/K)$ *tel que* $X - a \neq X - \sigma(a)$ *(en fait on a même* $X - a \neq X - \sigma(a)$ *pour tout* $\sigma \in \mathrm{Gal}(\overline{K}/K)$ *tel que* $\sigma(a) \neq a$ *).*

C'est une conséquence facile du fait que $\widetilde{X}_0$ n'a pas d'automorphismes infinitésimaux non triviaux puisqu'elle est de genre ≥ 2 (cf. [Ra 1], dém. de la prop. 6.4.2).

b) *L'ensemble* $X(R/p^2R) \cap pA(R/p^2R)$ *est fini.*

Cette assertion est le point crucial de la démonstration de M. Raynaud. Nous la démontrerons aux numéros 5 et 6 : plus précisément, d'après les hypothèses de 3.1, l'hypothèse (H) du numéro 5.4 est satisfaite par la courbe intègre X_0 de A_0 , et la normalisée $\widetilde{X}_0$ de X_0 est de genre ≥ 2 . Ceci permet d'appliquer la proposition 5.5 à X_0 . Le résultat que nous cherchons à démontrer est alors conséquence de la proposition 6.5, appliquée au R/p^2R-schéma abélien $A \times_R R/p^2R$ et à la courbe $X \times_R R/p^2R$: les hypothèses de cette proposition sont vérifiées d'après l'assertion (C1) de 5.4.

3.3. PROPOSITION.— *Il existe un entier* $r \geq 0$ *tel que l'on ait* $p^r x \in A(K)$ *pour tout* $x \in X(\overline{K}) \cap \mathrm{Div}(A(K))$.

Soit x un élément de $X(\overline{K}) \cap \mathrm{Div}(A(K))$. Il existe d'après la proposition 2.3, b), un entier $r(x) \geq 0$ tel que $p^{r(x)}x$ appartienne à A(K) . Pour tout $\sigma \in \mathrm{Gal}(\overline{K}/K)$, on a donc

$$\sigma(x) - x \in (X - x)(\overline{K}) \cap A_{p^\infty} .$$

Compte tenu du théorème 1.3, le nombre de conjugués $\sigma(x)$ de x , et donc le degré $[K(x):K]$, est majoré indépendamment de x . La proposition 2.3, b), permet de conclure.

3.4. PROPOSITION.— *Soit* Ω *la réunion d'une famille finie de classes de* $A(\overline{K})$ *modulo* pA(K) . *Le sous-groupe de torsion du groupe engendré par* $X(\overline{K}) \cap \Omega$ *est fini.*

Il existe une extension finie K' de K telle que Ω soit contenue dans $A(K')$. D'après la proposition 2.3, a) et b), la restriction de l'application de spécialisation $A(\overline{K}) \longrightarrow A_0(k)$ à l'ensemble des points de torsion de $A(K')$ a un noyau fini. Il suffit donc pour démontrer la proposition 3.4 de montrer que l'image de $X(\overline{K}) \cap \Omega$ dans $A_0(k)$ par l'application de spécialisation est finie, et pour cela on peut supposer que Ω est réduite à une classe $a + pA(K)$, avec $a \in A(\overline{K})$.

a) Supposons que a appartienne à $A(K)$. L'image de $X(\overline{K}) \cap \Omega = X(R) \cap (a + pA(R))$ dans $A_0(k)$ par l'application de spécialisation est alors finie d'après 3.2, b), appliqué à la courbe $X - a$ translatée de X.

b) Supposons que a n'appartienne pas à $A(K)$. D'après 3.2, a), il existe $\sigma \in \mathrm{Gal}(\overline{K}/K)$ tel que $X - a$ soit distinct de $X - \sigma(a)$. Or si $x = a + \mu$ est un élément de $X(\overline{K}) \cap (a + pA(K))$, $\mu = x - a = \sigma(x) - \sigma(a)$ appartient à $(X - a)(\overline{K}) \cap (X - \sigma(a))(\overline{K})$. Ceci montre que $X(\overline{K}) \cap \Omega$ est fini et achève la démonstration.

3.5. PROPOSITION.— *Soit Γ un sous-groupe de type fini de $A(K)$. Le sous-groupe de torsion du groupe engendré par $X(\overline{K}) \cap \mathrm{Div}(\Gamma)$ est fini.*

D'après la proposition 3.3, il existe un entier $r \geq 0$ tel que l'on ait $p^r x \in A(K)$ pour tout $x \in X(\overline{K}) \cap \mathrm{Div}(\Gamma)$. Posons $\Gamma' = \mathrm{Div}(\Gamma) \cap A(K)$. Pour démontrer la proposition il suffit d'après 3.4 de montrer que l'ensemble des classes modulo $pA(K)$ qui rencontrent $X(\overline{K}) \cap \mathrm{Div}(\Gamma)$ est fini. Or on déduit de l'application $x \mapsto p^r x$ une application à fibres finies de cet ensemble dans $\Gamma'/p^{r+1}\Gamma'$ et on a :

Lemme.— Le groupe $\Gamma'/p^{r+1}\Gamma'$ est fini.

En effet on a une suite exacte

$$1 \longrightarrow A(K)_{\mathrm{tors}} \longrightarrow \Gamma' \longrightarrow W \longrightarrow 1$$

où W s'identifie à un sous-groupe du $\mathbb{Q}$-espace vectoriel de dimension finie $\Gamma \otimes_{\mathbb{Z}} \mathbb{Q}$. Or $M/p^{r+1}M$ est fini pour tout sous-groupe M de $\Gamma \otimes_{\mathbb{Z}} \mathbb{Q}$ ou de $A(\overline{K})_{\mathrm{tors}}$. Le lemme en résulte.

4. DÉMONSTRATION DU THÉORÈME 2 ET DE L'IMPLICATION THÉORÈME 3 ⇒ THÉORÈME 1

4.0. Nous nous plaçons dans la situation décrite dans l'introduction : on a une variété abélienne A définie sur un corps K de caractéristique 0, une courbe X propre absolument intègre de A, définie sur K et non elliptique, un sous-groupe Γ de $A(\overline{K})$ de type fini.

4.1. PROPOSITION (M. Raynaud).— *Le sous-groupe de $A(\overline{K})$ engendré par $X(\overline{K}) \cap \mathrm{Div}(\Gamma)$ est de type fini.*

Quitte à remplacer A par une sous-variété abélienne, on se ramène au cas où A est engendré par les différences des points de X. Des réductions élémentaires de

géométrie algébrique pour le détail desquelles nous renvoyons à [Ra 1] montrent qu'il existe :

(i) un sous-corps E de type fini sur $\mathbb{Q}$ sur lequel A et X sont définis et tel que Γ soit contenu dans $A(E)$;

(ii) un nombre premier p et une extension K' de E tels que les hypothèses de 2.0, 2.1, 3.0, 3.1 soient satisfaites pour le corps K', la variété abélienne $A \times_E K'$ et la courbe $X \times_E K'$.

D'après la proposition 3.5 le sous-groupe de torsion T du groupe engendré par $X(\overline{K}) \cap \mathrm{Div}(\Gamma) = X(\overline{K}') \cap \mathrm{Div}(\Gamma)$ est fini. Soit n son ordre. Pour tout $x \in X(\overline{K}) \cap \mathrm{Div}(\Gamma)$ et tout $\sigma \in \mathrm{Gal}(\overline{E}/E)$ on a $\sigma(x) - x \in T$, d'où $\sigma(nx) = nx$, et $nx \in A(E)$. Or $A(E)$ est un groupe de type fini (théorème de Mordell-Weil-Néron). Ceci entraîne la proposition.

4.2. Le théorème 2 résulte de la proposition 4.1 appliquée au cas où $\Gamma = \{0\}$ et le théorème 1 résulte de la proposition 4.1 lorsqu'on sait que l'intersection de $X(\overline{K})$ et d'un sous-groupe de type fini de $A(\overline{K})$ est finie, ce qui est l'énoncé du théorème 3.

5. APPLICATIONS DE GAUSS

Dans ce numéro, k désigne un corps algébriquement clos.

5.1. Soient X une courbe propre intègre définie sur k, V un k-espace vectoriel de dimension finie et γ un morphisme d'un ouvert non vide de X dans l'espace projectif $\mathbb{P}(V)$ des droites de V : un tel morphisme s'étend canoniquement en un morphisme $\tilde{\gamma}$ de la normalisée $\tilde{X}$ de X dans $\mathbb{P}(V)$. On appelle degré de l'application rationnelle γ et on note $\deg(\gamma)$ le degré de la classe de diviseurs sur $\tilde{X}$ image inverse par $\tilde{\gamma}$ de la classe des diviseurs hyperplans de $\mathbb{P}(V)$. De même si $u : Y \to X$ est une application rationnelle non constante d'une courbe propre intègre Y dans X on appelle degré de u et on note $\deg(u)$ le degré du morphisme fini $\tilde{u} : \tilde{Y} \to \tilde{X}$ défini par u.

5.2. Avec les notations précédentes, on a :

(i) $\deg(\gamma \circ u) = \deg(\gamma)\deg(u)$;

(ii) pour tout espace vectoriel W contenant V le degré de l'application rationnelle composée $X \xrightarrow{\gamma} \mathbb{P}(V) \to \mathbb{P}(W)$ est égal à celui de γ ;

(iii) pour tout sous-espace vectoriel V' de V tel que $\mathbb{P}(V')$ ne contienne pas l'image de γ, le degré de l'application rationnelle composée $X \xrightarrow{\gamma} \mathbb{P}(V) \to \mathbb{P}(V/V')$ est inférieur à celui de γ : il lui est égal si $\mathbb{P}(V')$ ne rencontre pas $\tilde{\gamma}(\tilde{X})$.

5.3. Soit X une courbe intègre d'une variété abélienne A définie sur k. Par translation on identifie l'espace tangent en un point quelconque de A à l'espace tangent à l'origine $\mathrm{Lie}(A)$. En associant à tout point lisse x de X le point de

$\mathbb{P}(\mathrm{Lie}\,A)$ défini par la tangente à X en x on obtient une application rationnelle $\gamma_X : X \to \mathbb{P}(\mathrm{Lie}\,A)$ appelée l'"application de Gauss" associée à X.

5.4. Supposons désormais que le corps algébriquement clos k soit de caractéristique $p > 0$. Soit X une courbe propre intègre d'une variété abélienne A définie sur k.

Soit $A \xrightarrow{v} B \xrightarrow{u} A$ la factorisation de l'endomorphisme $p_A : A \to A$ de multiplication par p, dans laquelle v est étale et u radicielle. Notons Y et Z les images réciproques réduites de X par p_A et u respectivement. Soit r le plus petit entier ≥ 0 tel que le noyau de u soit annulé par la puissance r-ième du Frobenius, $F^r : B \to B^{(r)}$ (où $B^{(r)}$ est la variété abélienne déduite de B par le changement de base $a \mapsto a^{p^r}$ de k dans k) : l'isogénie $F^{(r)}$ admet une factorisation $B \xrightarrow{u} A \xrightarrow{w} B^{(r)}$ par u, et w induit un morphisme de X dans $Z^{(r)}$.

Supposons que X vérifie l'hypothèse suivante, où J désigne la jacobienne de la normalisée $\widetilde{X}$ de X :

(H) Le morphisme d'Albanese $a : J \to A$ associé au morphisme composé $\widetilde{X} \to X \to A$ est surjectif, son noyau N est lisse, et le groupe des composantes connexes de N est d'ordre premier à p.

On en déduit alors facilement les conséquences suivantes ([Ra 1]) :

(C1) La courbe Y et la courbe Z sont intègres.

(C2) Le morphisme $w_{|X} : X \to Z^{(r)}$ est birationnel.

(C3) L'application qui à une 1-forme différentielle sur A associe son image réciproque sur $\widetilde{X}$ est injective. En particulier si $\dim A \geq 2$ (ce qui équivaut, vu (H), à dire que le genre de $\widetilde{X}$ est ≥ 2), l'application de Gauss γ_X n'est pas constante.

Comme p_A n'est pas étale, on a $r \geq 1$ et il résulte alors de (C2) que l'on a $\deg(u_{|Z}) = p^r > 1$, d'où :

(C4) On a $\deg(v_{|Y}) < \deg(p_{A|Y})$.

5.5. PROPOSITION.– *Supposons que X vérifie l'hypothèse* (H) *et que $\widetilde{X}$ soit de genre ≥ 2. Notons γ_X et γ_Y les applications de Gauss* (5.3) *associées à X et Y. Les applications rationnelles γ_Y et $\gamma_X \circ (p_{A|Y})$ ne sont pas égales.*

Puisque v est étale, on a un diagramme commutatif

$$\begin{array}{ccc} Y & \xrightarrow{\gamma_Y} & \mathbb{P}(\mathrm{Lie}\,A) \\ {\scriptstyle v_{|Y}}\downarrow & & \downarrow \\ Z & \xrightarrow{\gamma_Z} & \mathbb{P}(\mathrm{Lie}\,B)\ . \end{array}$$

où la flèche de droite est l'isomorphisme déduit de l'application tangente à v. On en déduit l'égalité

$$\deg(\gamma_Y) = \deg(\gamma_Z \circ v_{|Y}) = \deg(\gamma_Z)\deg(v_{|Y})\ . \tag{1}$$

De même, puisque $w_{|X}$ est birationnel ((C2)) on a un diagramme commutatif d'applications rationnelles composables

$$\begin{array}{ccccc} X & \xrightarrow{\gamma_X} & \mathbb{P}(\mathrm{Lie}\,A) & \longrightarrow & \mathbb{P}((\mathrm{Lie}\,A)/M) \\ {\scriptstyle w_{|X}}\downarrow & & & & \downarrow \\ Z^{(r)} & & \xrightarrow{\gamma_{Z(r)}} & & \mathbb{P}(\mathrm{Lie}\,B^{(r)}) \end{array}$$

où M est le noyau de l'application tangente à $w : A \to B^{(r)}$.

On en déduit d'après 5.2

$$\deg(\gamma_X) \geq \deg(\gamma_{Z(r)} \circ w_{|X}) = \deg(\gamma_{Z(r)}) \quad . \tag{2}$$

Par transport de structure le degré de γ_Z est égal à celui de $\gamma_{Z(r)}$ et il résulte de (1) et (2) l'inégalité

$$\deg(\gamma_Y) \leq \deg(\gamma_X)\deg(v_{|Y}) \quad .$$

Or l'application γ_X est non constante d'après (C3), donc a un degré non nul ; d'autre part on sait par (C4) que le degré de $v_{|Y}$ est strictement inférieur à celui de $p_{A|Y}$. Ainsi le degré de γ_Y est strictement inférieur à $\deg(\gamma_X)\deg(p_{A|Y}) = \deg(\gamma_X \circ p_{A|Y})$.

6. ÉTUDE MODULO p^2

Dans ce numéro, k *désigne un corps algébriquement clos de caractéristique* $p > 0$ et R un anneau local de corps résiduel k dont l'idéal maximal est non nul, engendré par p , de carré nul : autrement dit R *est isomorphe à l'anneau des vecteurs de Witt de longueur* 2 *sur* k .

6.1. Soit S une R-algèbre. On note $y \mapsto [y]^p$ et $y \mapsto p[y]$ les applications de S/pS dans S déduites par passage au quotient des applications $x \mapsto x^p$ et $x \mapsto px$ de S dans S (et on utilisera les notations analogues pour les faisceaux de R-algèbres). *Lorsque* S *est plat sur* R *et que l'anneau* S/pS *est réduit, l'application* $(y,y') \longmapsto [y]^p + p[y']$ *de* $(S/pS)^2$ *dans* S *est injective et son image est* $S^p + pS$.

6.2. *Soit* $A = (\underline{A},\mathcal{O}_A)$ *un* R*-schéma abélien.* Sa réduction modulo p , $A_o = (\underline{A},\mathcal{O}_{A_o})$, est une variété abélienne sur k . Notons $p_A = (\underline{p},u)$ l'endomorphisme de multiplication par p dans A . Sa réduction p_{A_o} modulo p a une différentielle nulle. Par suite le $\underline{p}$-morphisme de faisceaux u de $\mathcal{O}_A$ dans $\mathcal{O}_A$ induit un $\underline{p}$-morphisme de faisceaux de $\mathcal{O}_A$ dans $\mathcal{O}_A^p + p\mathcal{O}_A$. Puisque A est plat sur R et A_o réduit, u s'écrit (cf. 6.1)

$$u = [u']^p + p[u'']$$

où u' et u'' sont des $\underline{p}$-morphismes de faisceaux d'ensembles $\mathcal{O}_A$ dans $\mathcal{O}_{A_o}$.

6.3. Soit S une R-algèbre. De la surjection canonique $S \to S_o = S/pS$ on déduit un homomorphisme de groupes $\pi_S : A(S) \to A(S_o) = A_o(S_o)$; cet homomorphisme est surjectif car A est lisse sur R .

Lemme.– Il existe une unique application $\alpha_S : A_o(S_o) \longrightarrow A(S)$ *rendant commutatif le diagramme*

(1)
$$\begin{array}{ccc} A(S) & \xrightarrow{p.1_{A(S)}} & A(S) \\ {\scriptstyle \pi_S}\downarrow & \nearrow_{\alpha_S} & \downarrow{\scriptstyle \pi_S} \\ A_o(S_o) & \xrightarrow{p.1_{A_o(S_o)}} & A_o(S_o) \end{array} .$$

L'unicité de α_S résulte de la surjectivité de π_S . Il suffit pour prouver l'existence de α_S de montrer que l'image par $p.1_{A(S)}$ d'un élément x de $A(S)$ ne dépend que de $\pi_S(x)$. Un élément x de $A(S)$ est un couple $(\underline{x},v)$ où $\underline{x}$ est une application continue $\mathrm{Spec}(S) \longrightarrow \underline{A}$ et v un $\underline{x}$-morphisme de $\mathcal{O}_A$ dans $\mathcal{O}_S$. Alors $\pi_S(x)$ est égal à $(\underline{x},v_o)$, où v_o est le $\underline{x}$-morphisme de $\mathcal{O}_{A_o}$ dans $\mathcal{O}_{S_o}$ déduit de v par réduction modulo p . Quant à l'image de x par $p.1_{A(S)}$, elle est égale d'après 6.2 à $(\underline{y},w)$ où $\underline{y} = \underline{p} \circ \underline{x}$ et où w est le $\underline{y}$-morphisme de $\mathcal{O}_A$ dans $\mathcal{O}_S$ donné par la formule

(2) $$w = [v_o \circ u']^p + p[v_o \circ u''] .$$

Ceci prouve le lemme.

6.4. Conservons les notations précédentes. *Soit en outre* X *une courbe de* A *propre et plate sur* R *; notons* X_o *la courbe de* A_o *déduite de* X *par réduction modulo* p *; supposons que* X_o *et son image réciproque réduite* Y_o *par* p_{A_o} *sont intègres.*

Étudions le diagramme (1) lorsque S est l'algèbre des nombres duaux $R[\varepsilon]$. Dans ce cas le groupe $A_o(S_o) = A_o(k[\varepsilon])$ est le groupe des points à valeurs dans k du fibré tangent de A_o : il s'identifie canoniquement au groupe produit $A_o(k) \times \mathrm{Lie}(A_o)$. De manière analogue $A(S) = A(R[\varepsilon])$ s'identifie à $A(R) \times \mathrm{Lie}\, A$; le R-module $\mathrm{Lie}\, A$ est libre de rang fini et $\mathrm{Lie}(A_o)$ s'identifie à $\mathrm{Lie}\, A/p\,\mathrm{Lie}\, A$. Par passage au quotient on déduit de la multiplication par p dans $\mathrm{Lie}(A)$ un isomorphisme, noté $\xi \longmapsto p[\xi]$, de $\mathrm{Lie}\, A_o$ sur $p\,\mathrm{Lie}\, A$.

Les identifications précédentes étant faites, soit y_o un point lisse de $Y_o(k)$ et ξ un élément de $\mathrm{Lie}\, A_o$. Pour que l'élément (y_o,ξ) de $A_o(k[\varepsilon])$ appartienne à $Y_o(k[\varepsilon])$ il faut et il suffit que ξ appartienne à la droite $\gamma_{Y_o}(y_o)$, où γ_{Y_o} est l'application de Gauss associée à Y_o (cf. 5.3). Vu la commutativité du diagramme (1), l'image de (y_o,ξ) par $\alpha_{R[\varepsilon]}$ est $(x,p[\xi])$, avec $x = \alpha_R(y_o)$, et le point x de $A(R)$ relève l'élément $x_o = py_o$ de $X_o(k)$. Supposons maintenant de plus que x_o est un point lisse de $X_o(k)$. Alors si η est un élément de $\mathrm{Lie}\, A$, pour que l'élément (x,η) de $A(R[\varepsilon])$ appartienne à $X(R[\varepsilon])$ il faut et il suffit que x appartienne à $X(R)$ et que η appartienne à l'espace tangent à X le long de la section x (que l'on identifie par translation à un facteur direct libre $\gamma_X(x)$ de rang 1 du R-module $\mathrm{Lie}\, A$). La droite de $\mathrm{Lie}\, A_o$ déduite de $\gamma_X(x)$ par réduction modulo p est $\gamma_{X_o}(x_o)$: en particulier si η appartient à $p\,\mathrm{Lie}\, A \cap \gamma_X(x)$ il est de la forme $p[\eta_o]$ avec $\eta_o \in \gamma_{X_o}(x_o)$.

De la discussion précédente, nous tirons la conclusion suivante : *si l'image de* $Y_o(k[\varepsilon])$ *par* $\alpha_{R[\varepsilon]}$ *est contenue dans* $X(R[\varepsilon])$ *, les applications rationnelles*

γ_{Y_o} *et* $\gamma_{X_o} \circ p_{A_o|Y_o}$ *de* Y_o *dans* $\mathbb{P}(\mathrm{Lie}\, A_o)$ *sont égales.*

6.5. PROPOSITION.— *Sous les hypothèses de* 6.4, *l'une des conditions suivantes est satisfaite :*

a) *L'ensemble* $pA(R) \cap X(R)$ *est fini.*

b) *Les applications rationnelles* γ_{Y_o} *et* $\gamma_{X_o} \circ p_{A_o|Y_o}$ *de* Y_o *dans* $\mathbb{P}(\mathrm{Lie}\, A_o)$ *sont égales.*

Notons I (resp. J_o) le faisceau d'idéaux de $\mathcal{O}_A$ (resp. $\mathcal{O}_{A_o}$) qui définit X (resp. Y_o) et J_o' le faisceau d'idéaux de $\mathcal{O}_{A_o}$ engendré par J_o et les images de I par les p-morphismes de faisceaux u' et u'' (cf. 6.2). Notons Y_o' le sous-schéma fermé de Y_o défini par J_o'. Distinguons deux cas :

a) On a $J_o \not\subseteq J_o'$. Dans ce cas $Y_o'(k)$ est fini puisque Y_o est par hypothèse une courbe intègre. Or il résulte du diagramme (1) que $pA(R) \cap X(R)$ est égal à $\alpha_R(Y_o(k)) \cap X(R)$. D'après la formule (2) cet ensemble est égal à $\alpha_R(Y_o'(k))$. La condition a) de la proposition est donc satisfaite.

b) On a $J_o = J_o'$. Dans ce cas il résulte de la formule (2) que l'on a $\alpha_S(Y_o(S_o)) \subset X(S)$ pour toute R-algèbre S. En prenant $S = R[\varepsilon]$, on voit d'après 6.4 que la condition b) est satisfaite.

7. GÉNÉRALISATIONS

7.1. La conjecture suivante, formulée par S. Lang ([La 2], p. 221) généralise de façon naturelle l'énoncé du théorème 1 :

Conjecture.— Soit A un groupe algébrique commutatif, extension d'une variété abélienne par un tore, défini sur un corps algébriquement clos K de caractéristique 0. Soient X une sous-variété algébrique fermée de A et Γ un sous-groupe de type fini de $A(K)$. L'ensemble des éléments x de $X(K)$ dont un multiple nx (avec n entier non nul) appartient à Γ est contenu dans la réunion d'une famille finie de sous-variétés de X qui sont des translatées de sous-groupes algébriques de A.

On connaît les résultats partiels suivants :

a) *Cas où* A *est un tore* : la conjecture a été démontrée par P. Liardet ([Li]) lorsque X est une courbe, puis par M. Laurent ([Lt]) dans le cas général.

b) *Cas où* $\Gamma = \{0\}$ ("points de torsion sur X") *et* A *est une variété abélienne* : la conjecture a été démontrée par M. Raynaud ([Ra 2]). Lorsqu'on se restreint à la torsion ℓ-primaire, les démonstrations de Bogomolov exposées au n° 2 se généralisent également ([Bo] et [Ra 2]).

c) *Cas où* A *est une variété abélienne et où* X *ne contient aucun translaté de sous-variété abélienne non nulle de* A : M. Raynaud montre ([Ra 3]) qu'alors $X(K) \cap \mathrm{Div}(\Gamma)$ engendre un sous-groupe de type fini de $A(K)$.

7.2. Plaçons-nous dans les hypothèses du théorème 2. Pour toute extension L de K et tout $a \in A(L)$, l'ensemble des points de $(X + a)(\overline{L})$ qui sont de torsion dans

$A(\overline{L})$ est fini. On peut se demander s'il existe un majorant du nombre de ces points indépendant de a : M. Raynaud déduit de 7.1, b) qu'il en est bien ainsi lorsque X n'est pas contenu dans une surface abélienne de A .

Addendum : A l'aide d'une théorie de l'intégration p-adique, R. Coleman montre, dans un article à paraître intitulé " p-adic abelian integrals and torsion points on curves", que, sous les hypothèses du théorème 2, et en supposant en outre que K *est un corps de nombres* et que A *est à multiplications complexes*, on peut donner des bornes effectives simples du nombre de points de $X(\overline{K})$ qui sont de torsion dans $A(\overline{K})$.

BIBLIOGRAPHIE

[Bo] F.A. BOGOLOMOV - *Sur l'algébricité des représentations l-adiques*, C.R. Acad. Sci. Paris, t. 290(1980), 701-704.

[La 1] S. LANG - *Division points on curves*, Annali di Matematica Pura ed Applicata, serie quarta, tomo LXX(1965), 229-234.

[La 2] S. LANG - Fundamentals of diophantine geometry, Springer-Verlag, New York, 1983.

[Li] P. LIARDET - *Sur une conjecture de S. Lang*, Soc. Math. Fr., Astérisque 24-25 (1975), 187-209.

[LIE] N. BOURBAKI - Groupes et algèbres de Lie, C.C.L.S. Diffusion, Paris, 1982.

[Lt] M. LAURENT - *Équations diophantiennes exponentielles*, C.R. Acad. Sci. Paris, t. 296(1983), 945-947.

[Ra 1] M. RAYNAUD - *Courbes sur une variété abélienne et points de torsion*, Invent. Math. 71(1983), 207-233.

[Ra 2] M. RAYNAUD - *Sous-variété d'une variété abélienne et points de torsion*, Arithmetic and Geometry, Papers dedicated to I.R. Shafarevich, Birkhäuser (1983).

[Ra 3] M. RAYNAUD - *Around the Mordell conjecture for function fields and a conjecture of Serge Lang*, Proc. of the Japan-France Conf. held at Tokyo and Kyoto, Springer-Verlag, Lect. Notes in Math. 1016(1982), 1-19.

[Se] J.-P. SERRE - *Représentations l-adiques*, Kyoto Symposium on Algebraic Number Theory, Japan Society for the Promotion of Science (1977), 177-193.

Joseph OESTERLÉ

École Normale Supérieure
E.R.A. 589
45 rue d'Ulm
F-75230 PARIS CEDEX 05