COMPOSITIO MATHEMATICA

ANTOINE CHAMBERT-LOIR

Extension universelle d'une variété abélienne et hauteurs des points de torsion

Compositio Mathematica, tome 103, nº 3 (1996), p. 243-267

<http://www.numdam.org/item?id=CM_1996__103_3_243_0>

Compositio Mathematica **103:** 243–267, 1996.

Extension universelle d'une variété abélienne et hauteurs des points de torsion

ANTOINE CHAMBERT-LOIR
École normale supérieure, Département de Mathématiques et Informatique, 45 rue d'Ulm, 75230 Paris Cedex 05, France, e-mail: chambert@ens.fr

Received 5 December 1994: accepted in final form 7 July 1995

Résumé. Nous évaluons la hauteur des points de torsion de l'extension universelle d'une variété abélienne définie sur un corps de nombres. Nous montrons en particulier que la moyenne des hauteurs des points d'ordre premier p croît comme $\log p$ quand p tend vers l'infini. Ceci généralise des résultats obtenus par P. Cohen pour les courbes elliptiques.

Pour cela, on utilise la théorie des hauteurs « à la Arakelov » qui permet de comprendre cette hauteur comme la somme d'une intersection sur un modèle entier convenable de l'extension universelle et d'un terme à l'infini. La p-partie, calculée grâce à la classification de Raynaud de certains schémas en groupes finis, fournit la principale contribution.

Nous donnons en appendice une application aux périodes p-adiques.

Mots clefs: théorie d'Arakelov, hauteurs, extension universelle, groupes p-divisibles, périodes, schémas en groupes finis

Table des matières

1. Introduction

Soient K un corps de nombres et A une variété abélienne définie sur K. Soit E l'extension vectorielle universelle de A. C'est un groupe algébrique commutatif, extension de A par l'espace cotangent ω_{A^*} de la variété abélienne duale A^* telle que toute extension vectorielle $0 \to V \to E' \to A \to 0$ en provienne par un unique morphisme $\omega_{A^*} \to V$.

Si n est un entier, nous noterons $[n]_A$ (resp. $[n]_E$) la multiplication par n dans A (resp. E).

D'après [13], on peut plonger E dans un espace projectif et ainsi considérer des *hauteurs de Weil* sur $E(\overline{\mathbf{Q}})$. On s'intéresse à la hauteur des points de torsion de E. Précisément, nous évaluons la moyenne des hauteurs des points annulés par un nombre premier p. Si g est la dimension de A, il y a p^{2g} tels points; en effet, la projection $\pi\colon E \to A$ induit un isomorphisme du sous-groupe de torsion de $E(\overline{\mathbf{Q}})$ sur le sous-groupe de torsion de $A(\overline{\mathbf{Q}})$.

Citons maintenant le théorème principal de cet article:

THÉORÈME 1.1 *Soit η une hauteur de Weil sur la compactification de E construite au paragraphe* 2.1. *Alors, il existe deux constantes strictement positives C_1 et C_2 telles que l'on ait l'inégalité, valable pour tout nombre premier p*

$$C_1 \log p - C_2 < \frac{1}{p^{2g}} \sum_{\substack{P \in E(\overline{\mathbf{Q}}) \\ [p]_E P = 0}} \eta(P) < C_1 \log p + C_2.$$

Si on se limite à cette extension vectorielle universelle, c'est pour éviter des phénomènes parasitaires du type suivant: prenons $A = A_1 \times A_2$ le produit de deux variétés abéliennes; alors le *pull-back* à A de l'extension universelle de A_1 possède « beaucoup » de points de torsion de hauteur nulle, à savoir ceux qui relèvent les points de torsion $(0, x_2) \in A$.

Donnons le plan de l'étude: d'abord nous construisons une hauteur particulièrement adaptée au problème. Celle-ci est construite à l'aide de la théorie d'Arakelov. Il nous faut un modèle entier de l'extension E, celui-ci nous est fourni par *l'extension canonique* du modèle de Néron de A, telle qu'elle est construite dans [6, Cor. 5.2, p. 54]. Après avoir compactifié E, nous exhibons un faisceau inversible relativement ample sur A et nous le munissons de métriques hermitiennes.

Nous calculons ensuite la composante archimédienne de la hauteur. Finalement, nous évaluons l'intersection à distance finie. Pour obtenir la minoration, nous nous ramenons comme dans [6] au cas d'une base où p est nilpotent. La théorie [11] de Raynaud appliquée au sous-schéma en groupe de p-torsion du schéma abélien nous permet de conclure.

Ce calcul local permet en outre dans certains cas d'évaluer les périodes p-adiques de Hodge–Tate d'une variété abélienne, telles qu'elles sont construites par Coleman. Nous donnons cette application en appendice.

Le Théorème 1.1 généralise les résultats [2, 3] de P. Cohen qui concernaient les courbes elliptiques, et le résultat de [1] où l'on faisait des hypothèses sur la réduction de la variété abélienne modulo p.

Signalons aussi que ce type de phénomènes ne se produit pas dans les variétés semi-abéliennes où un analogue du procédé de Tate permet de normaliser les hauteurs de sorte que la hauteur des points de torsion soit nulle (cf. la discussion dans l'introduction et l'appendice de [2]).

2. Construction de la hauteur

2.1. COMPACTIFICATION D'UNE EXTENSION VECTORIELLE

Soit S un schéma de dimension 1, irréductible et régulier, η son point générique. Soit A/S un schéma en groupes vérifiant:

— la fibre générique A_η est une variété abélienne;
— le schéma A/S est le modèle de Néron de A_η;

(ce qui est par exemple le cas si A/S est un schéma abélien). Soit V un groupe vectoriel de dimension n sur S et E une extension de A par V: c'est un schéma en groupes lisse sur S qui s'inscrit dans une suite exacte $0 \to V \to E \to A \to 0$. On notera $i\colon V \hookrightarrow E$ l'injection canonique, et $\pi\colon E \to A$ la projection.

À l'aide des arguments de [12, 13], nous allons construire une compactification lisse de E/S.

Pour cela, considérons E comme un espace principal homogène sur A, de groupe structural V: d'après [7, III. Sect. 4, Cor. 4.7] et [7, III. Sect. 3, Prop, 3.7], on a $\mathrm{Ext}^1_S(A, V) = H^1(A, \mathcal{O}_A \otimes_S V)$, d'où un recouvrement ouvert $\mathfrak{U}$ de A, et pour tous U_1 et $U_2 \in \mathfrak{U}$ une section $\sigma_{U_1U_2}$ du faisceau $\mathcal{O}_A \otimes V$ au-dessus de $U_1 \cap U_2$ vérifiant la condition de cocycle

$$\sigma_{U_1U_2} + \sigma_{U_2U_3} + \sigma_{U_3U_1} = 0, \quad \text{comme section de } \mathcal{O}_A \otimes V \text{ sur } U_1 \cap U_2 \cap U_3.$$

Réciproquement, de telles sections déterminent l'extension E de la façon suivante: si $U \in \mathfrak{U}$, notons $E_U = \pi^{-1}(U) \subset E$; alors il existe un isomorphisme $\varphi_U\colon E_U \to V \times_S U$ vérifiant $\varphi_{U_1} - \varphi_{U_2} = (\sigma_{U_1U_2}, 0)$. On obtient ainsi l'égalité $\mathrm{Ext}^1_S(A, V) = H^1(A, \mathcal{O}_A \otimes_S V)$. Or ce dernier groupe est canoniquement isomorphe à $\mathrm{Ext}^1(\mathcal{O}_A, \mathcal{O}_A \otimes_S V)$: en cohomologie de Čech, l'isomorphisme en question identifie le système de sections $(\sigma_{U_iU_j})$ aux matrices de transitions

$$\begin{pmatrix} I_n & \sigma_{U_iU_j} \\ 0 & 1 \end{pmatrix},$$

qui définissent un faisceau $\mathcal{F}$ sur A, localement libre de rang $n + 1$.

Posons alors $\overline{E} = \mathbf{P}(\mathcal{F})$. L'inclusion $V \hookrightarrow \mathcal{F}$ définit un sous-fibré isomorphe à $\mathbf{P}(V)$ de $\overline{E}$ qui est un diviseur D. En outre, on a une immersion ouverte $E \hookrightarrow \overline{E}$ dont l'image est précisément $\overline{E}\backslash D$. Notons $\mathcal{O}(1)$ le faisceau inversible $\mathcal{O}_{\mathbf{P}(\mathcal{F})}(1) = \mathcal{O}_{\overline{E}}(D)$. Il est par définition relativement ample sur A et est muni d'une section canonique $s_D \in \Gamma(\overline{E}, \mathcal{O}(1))$ telle que $\operatorname{div}(s_D) = D$.

LEMME 2.1 *Soit $P \in E_\eta(\eta)$. Alors, P s'étend uniquement en une section $\widetilde{P}$ (notée aussi $P^{\sim}$) $S \to \overline{E}$. En outre, l'image de $\widetilde{P}$ est l'adhérence de P dans $\overline{E}$.*

Preuve. Si le schéma $\overline{E}$ était propre sur S, ce serait une simple application du critère valuatif de propreté. Cependant, $\overline{E}$ est propre sur A (et même projectif), mais A n'est propre sur S que si c'est un schéma abélien.

Soit $Q = \pi(P) \in A_\eta(\eta)$. La propriété universelle du modèle de Néron entraîne que Q se prolonge uniquement en une section $\widetilde{Q}\colon S \to A$. Interprétons maintenant le point P comme une section rationnelle de $\mathbf{P}(\widetilde{Q}^*\mathcal{F})$, elle se prolonge alors de manière unique, d'après les hypothèses sur S et le critère valuatif de propreté, en une section régulière de $\mathbf{P}(\widetilde{Q}^*\mathcal{F})$, d'où une section $\widetilde{P}\colon S \to \mathbf{P}(\mathcal{F}) = \overline{E}$.

L'unicité de $\widetilde{P}$ résulte du fait que nécessairement $\pi(\widetilde{P})$ prolonge Q et est donc égal à $\widetilde{Q}$, si bien que $\widetilde{P}$ se factorise par un morphisme $S \to \mathbf{P}(\widetilde{Q}^*\mathcal{F})$. Or, le critère valuatif de propreté appliqué à $\overline{E} \to A$ entraîne que ce dernier morphisme est unique.

Reste à montrer que l'adhérence de P dans $\overline{E}$ est précisément l'image de $\widetilde{P}$. D'abord, comme $\widetilde{P}$ est une section, cette image est fermée. Mais l'image de $\widetilde{Q}$ est déjà l'adhérence de Q dans A: elle est d'une part fermée, et comme A est localement quasi-projectif sur S, l'adhérence de Q est surjective sur S, ce qui entraîne $\overline{\{Q\}} \supset \widetilde{Q}$, d'où l'égalité. Finalement, le morphisme $\overline{E} \to A$ étant propre, l'adhérence $\overline{\{P\}}$ de P est fermée et surjective sur l'image de $\widetilde{Q}$, donc sur S, ce qui implique que $\overline{\{P\}} \supset \widetilde{P}$ et on a donc l'égalité. □

2.2. MÉTRIQUES HERMITIENNES

Dans ce paragraphe, on suppose que $S = \operatorname{Spec}\mathbf{C}$, si bien que A est une variété abélienne complexe. Ainsi, on peut identifier $A(\mathbf{C})$ à un tore complexe $\mathbf{C}^g/\Lambda$, Λ étant un réseau de $\mathbf{C}^g$, et $V \simeq \mathbf{C}^n$.

LEMME 2.2 *Il existe un homomorphisme $\rho\colon \Lambda \to V$ telle que $E(\mathbf{C})$ soit le quotient de $V \times \mathbf{C}^g$ par l'action de Λ donnée par*

$$\lambda \cdot (u, z) = (u + \rho(\lambda), z + \lambda), \qquad \lambda \in \Lambda.$$

Le fibré vectoriel $\mathcal{F}$ sur A est le quotient de $(\mathbf{C} \oplus V) \times \mathbf{C}^g$ par l'action

$$\lambda \cdot ((t, u), z) = ((t, u + t\rho(\lambda)), z + \lambda), \qquad \lambda \in \Lambda.$$

Preuve. L'extension de $\mathbf{C}^g$ par V obtenue par *pull-back* de E est scindée. Ainsi, on obtient une représentation ρ de $\Lambda = \pi_1(A)$ dans V (qui agit par translations sur lui-même). Réciproquement, étant donnée ρ, on reconstruit E, puis $\mathcal{F}$, à l'aide des formules indiquées. □

Avec les notations du lemme, le diviseur D est défini par l'équation $t = 0$; la section canonique s_D de $\mathcal{O}(1)$ est précisément représentée par t.

Le faisceau $\mathcal{O}(1)$ sur $\overline{E} = \mathbf{P}(\mathcal{F})$ est un quotient de $\pi^*\mathcal{F}$, π étant la projection $\overline{E} \to A$. Par conséquent, pour munir $\mathcal{O}(1)$ d'une métrique hermitienne, il suffit de construire une telle métrique h sur $\mathcal{F}$, et $\mathcal{O}(1)$ en héritera grâce à la formule

$$\|s_D\|_{([t,u],z)} = \frac{|t|}{h_z(t,u)^{1/2}}.$$

Il reste à construire h_z. Pour cela on remarque que la suite exacte de fibrés vectoriels $0 \to V \times A \to \mathcal{F} \to \mathbf{C} \times A$ admet une section $\mathcal{C}^\infty$. En effet, désignons encore par ρ le prolongement $\mathbf{R}$-linéaire de $\rho\colon \Lambda \to V$ en une application $\mathbf{C}^g \to V$ et posons $\varphi(t,z) = ((t, t\rho(z)), z)$. Pour tout $\lambda \in \pi_1(A)$

$$\lambda \cdot \varphi(t,z) = \lambda \cdot ((t, t\rho(z)), z) = ((t, t\rho(\lambda) + t\rho(z)), z + \lambda)\,,$$

tandis que

$$\varphi\left(\lambda \cdot (t,z)\right) = \varphi\left((t, z+\lambda)\right) = ((t, t\rho(z+\lambda)), z+\lambda)\,,$$

de sorte que $\varphi\colon \mathbf{C}\times\mathbf{C}^g \to (\mathbf{C}\oplus V)\times\mathbf{C}^g$ passe au quotient par l'action de $\pi_1(A)$. À la section φ est ainsi associé le scindage $\mathcal{C}^\infty$ $\Phi\colon \mathcal{F} \to (\mathbf{C}\oplus\mathcal{V})_A$ décrit sur le revêtement universel par $(t,u)_z \mapsto (t, u - t\rho(z))_z$, puisque $(t,u) = (t, t\rho(z)) + (0, u - t\rho(z))$.

Choisissons une métrique hermitienne $\|\cdot\|_V$ sur l'espace vectoriel V. Alors, grâce au scindage $\mathcal{C}^\infty$ que nous venons de construire, on peut munir $\mathcal{F}$ de la métrique somme directe orthogonale des métriques constantes $\|\cdot\|_V$ sur $V \times A$ et $|\cdot|$ sur $\mathbf{C} \times A$.

Nous avons ainsi établi la proposition:

PROPOSITION 2.3 *Une fois fixée une métrique hermitienne sur V, il existe une métrique hermitienne sur $\mathcal{O}(1)$ pour laquelle la norme de s_D est donnée par l'expression*

$$\|s_D\|_{([t,u],z)} = \frac{|t|}{\sqrt{\|u - t\rho(z)\|_V^2 + |t|^2}}.$$

(Si $u \in V$, $t \in \mathbf{C}$ et $z \in \mathbf{C}^g$, avec $(t,u) \neq (0,0)$, on note $([t,u],z)$ l'unique point de $\mathbf{P}(\mathcal{F})$ dont un relevé dans $(\mathbf{C} \oplus V) \times \mathbf{C}^g$ est (t,u,z).)

2.3. HAUTEURS LOCALES

Dans ce paragraphe et le suivant, $S = \operatorname{Spec} R$, où R est un anneau de Dedekind; on suppose que le corps des fractions de R, noté K est de caractéristique zéro. Nous reprenons les notations A, V et E du paragraphe 2.1

2.3.1. *Le cas non archimédien*

Soit $\mathfrak{p}$ un idéal maximal de R; soit v la valuation (normalisée) associée à $\mathfrak{p}$. On note $(\,\cdot\,)_v$ le produit d'intersection au-dessus de $\mathfrak{p}$ entre un 1-cycle et un diviseur transverses (cf. par exemple [14]).

DÉFINITION 2.1 Si $P \in \overline{E}(S)$ et $P \not\subset D$, on définit $h_{S,v}(P) = (P \cdot D)_v$.

Si $P \in E_K(K)$, alors son adhérence $\widetilde{P}$ dans $\overline{E}(S)$ n'est pas incluse dans D et on pose $h_{S,v}(P) = h_{S,v}(\widetilde{P})$.

2.3.2. *Le cas archimédien*

Pour tout plongement $\sigma\colon K \hookrightarrow \mathbf{C}$, on fixe une métrique hermitienne sur $V \otimes_\sigma \mathbf{C}$ et on note $\|\cdot\|^\sigma$ la métrique hermitienne sur $\sigma^*\mathcal{O}(1)$ construite comme au paragraphe précédent.

DÉFINITION 2.2 Si $P \in E_K(K)$, on définit $h_{S,\sigma}(P) = -\log \|s_D\|_P^\sigma$.

2.4. CHANGEMENT DE BASE

Soient K' une extension finie de K, R' la clôture intégrale de R dans K'. On note $S' = \mathrm{Spec} R'$. On définit A' comme le modèle de Néron de $A_K \otimes_K K'$; on note $V' = V \times_S S'$ et on se donne une extension E' de A' par V' dont la fibre générique vérifie $E'_{K'} = E_K \otimes_K K'$. Le but de ce paragraphe est de comparer $h_{S,\cdot}(P)$ et $h_{S',\cdot}(P')$ si $P \in E_K(K)$ et $P' = P \times_K K' \in E_{K'}(K')$.

2.4.1. *Le cas archimédien*

Soient $\sigma\colon K \hookrightarrow \mathbf{C}$ un plongement, et $\tau_1, \dots, \tau_d$ les $d = [K' : K]$ plongements de K' dans $\mathbf{C}$ qui prolongent σ.

PROPOSITION 2.4 *On suppose que les métriques hermitiennes sur $\tau_j^*\mathcal{O}(1)_{E'}$ sont obtenues par* pull-back *de celles sur $\sigma^*\mathcal{O}(1)_E$. Alors, on a la formule*

$$[K' : K] h_{S,\sigma}(P) = \sum_{j=1}^{d} h_{S',\tau_j}(P').$$

Preuve. Tous les termes $h_{S',\cdot}(P')$ du membre de droite sont égaux à $h_{S,\sigma}(P)$.

2.4.2. *Le cas non archimédien*

On se donne un idéal maximal $\mathfrak{p}$ de R et on note $\mathfrak{q}_1, \dots, \mathfrak{q}_r$ les idéaux premiers de R' au-dessus de $\mathfrak{p}$. On note v (resp. v'_j, pour $1 \leqslant j \leqslant r$) les valuations correspondantes. On note e_j l'indice de ramification de v'_j/v et $f_j = [R'/\mathfrak{q}_j : R/\mathfrak{p}]$ le degré résiduel.

PROPOSITION 2.5 *Faisons l'une des deux hypothèses suivantes:*

— *ou bien A/S est un schéma abélien et $E' = E \times_S S'$;*
— *ou bien A/S est semi-stable et E (resp. E') est* l'extension canonique *de A (resp. de A'), au sens de* [6, (5.2), Cor.] (*voir plus bas*).

Alors on a la formule

$$[K' : K]h_{S,v}(P) = \sum_{j=1}^{r} f_j h_{S',v'_j}(P').$$

Preuve. Dans le premier cas, on a $A' = A \times_S S'$, $E' = E \times_S S'$. Il en résulte, la construction de la compactification étant fonctorielle, que $\overline{E'} = \overline{E} \times_S S'$ et $\widetilde{P'} = \widetilde{P} \times_S S'$. Par conséquent, $h_{S',v'_j}(P') = e_j h_{S,v}(P)$ et la formule résulte de l'égalité classique $\sum_{j=1}^{r} e_j f_j = d = [K' : K]$.

Dans le second cas, rappelons la définition [6, (5.2), p. 54] de l'extension canonique. Soient B_K la variété abélienne duale de A_K et B son modèle de Néron sur S; de même, B' est le modèle de Néron de $B_K \otimes_K K'$ sur S'. On note B^0 (resp. B'^0) la composante neutre de B (resp. B'). L'extension canonique E est le schéma en groupes qui représente le foncteur $\mathbf{Extrig}_S(B^0, \mathbf{G}_m)$ des extensions de B^0 par le groupe multiplicatif $\mathbf{G}_m$ rigidifiées le long (du premier voisinage infinitésimal) de la section nulle, c'est-à-dire munies d'un scindage de la suite exacte des espaces tangents correspondante. On a ainsi une suite exacte

$$0 \to \omega_B \to E \to A \to 0,$$

où ω_B est le module des différentielles invariantes sur B. De même, on a une suite exacte

$$0 \to \omega_{B'} \to E' = \mathbf{Extrig}_{S'}(B'^0, \mathbf{G}_m) \to A' \to 0.$$

La propriété universelle des modèles de Néron entraîne l'existence d'un morphisme canonique $A \times_S S' \to A'$ qui se restreint en l'identité sur la fibre générique. Comme A/S est semi-stable, B/S l'est aussi (B_K est isogène à A_K) et la formation de la composante neutre commute au changement de base: $B'^0 = B^0 \times_S S'$.

Soit $0 \to \mathbf{G}_m \to H \to B^0 \to 0$ une extension rigidifiée. Par changement de base de S à S', on obtient ainsi une extension de B'^0 par $\mathbf{G}_m$, rigidifiée le long de la section nulle. On a ainsi une application canonique $E \times_S S' \to E'$ qui induit (par oubli de la rigidification) le morphisme canonique $A \times_S S' \to A'$ sur les modèles de Néron.

Il en résulte que $E \times_S S'$ est le *pull-back* de E' par l'application canonique $A \times_S S' \to A'$. Le reste de la construction est fonctorielle en l'extension vectorielle et l'on finit comme précédemment. □

2.5. HAUTEURS GLOBALES

On suppose maintenant que K est un corps de nombres; on note $\mathfrak{O} = \mathfrak{O}_K$ son anneau d'entiers et $S = \operatorname{Spec}\mathfrak{O}_K$. Soit A_K une variété abélienne sur K et A/S son modèle de Néron sur S, que l'on suppose semi-stable. D'après le théorème de réduction semi-stable, quitte à étendre les scalaires à une extension finie de K (en adjoignant les coordonnées des points de 12-torsion par exemple), cette hypothèse de semi-stabilité est vérifiée. Soit B_K la variété abélienne duale de A_K, et B son modèle de Néron sur S.

Soit E_K l'extension vectorielle universelle de A_K. C'est une extension $0 \to \omega_{B_K} \to E_K \to A_K \to 0$ universelle en ce sens que toute extension vectorielle $0 \to V \to E'_K \to A_K \to 0$ provient de E_K par *push-out* à l'aide d'un unique morphisme $\omega_{B_K} \to V$.

Soit E l'extension canonique de A par ω_B qui représente le foncteur $\mathbf{Extrig}(B^0, \mathbf{G}_m)$. C'est une extension vectorielle de A sur S qui prolonge E_K, mais ce n'est pas nécessairement l'extension vectorielle universelle de A/S (qui n'en possède pas forcément, cf. les contre-exemples de Breen et Raynaud dans [6, (5.6), p. 56–58]). Cependant, la restriction de E au plus grand ouvert de $\operatorname{Spec}\mathfrak{O}$ sur lequel A est un schéma abélien s'identifie canoniquement à son extension universelle.

Soit $\overline{E}$ la compactification de E construite comme au paragraphe 2.1. Pour tout plongement $\sigma : K \hookrightarrow \mathbf{C}$, munissons le faisceau inversible $\sigma^*\mathcal{O}(1)$ de métriques hermitiennes comme au paragraphe 2.2.

Soit $P \in E_K(K)$, $\widetilde{P} \in \overline{E}(S)$ son prolongement à $S = \operatorname{Spec}\mathfrak{O}_K$. Alors, le faisceau inversible $\widetilde{P}^*\mathcal{O}(1)$ sur S est aussi muni de métriques hermitiennes à l'infini. Nous noterons $\deg_{\mathrm{Ar}}$ son degré d'Arakelov (cf. par exemple [14]).

DÉFINITION 2.3 On appelle *hauteur relative* de P l'expression

$$h_K(P) = [K : \mathbf{Q}]^{-1} \deg_{\mathrm{Ar}} \widetilde{P}^*(\mathcal{O}(1), \|\cdot\|^\sigma).$$

(Elle dépend du choix des métriques hermitiennes sur ω_{B_K} que nous supposerons fixées une fois pour toutes, si bien que nous ne la faisons pas figurer dans la notation.)

PROPOSITION 2.6 *On a l'égalité*

$$h_K(P) = [K : \mathbf{Q}]^{-1} \left(\sum_v h_{S,v}(P) \log N(v) + \sum_\sigma h_{S,\sigma}(P) \right),$$

où $N(v)$ est le cardinal du corps résiduel en la place v. La sommation est sur toutes les places finies v de K et tous les plongements complexes $\sigma : K \hookrightarrow \mathbf{C}$.

Preuve. Si M est un $\mathfrak{O}_K$-module projectif de rang 1 métrisé, son degré d'Arakelov se calcule en choisissant une section non nulle m, et alors

$$\deg_{\mathrm{Ar}} M = \log \# \frac{M}{m\mathfrak{O}_K} - \sum_\sigma \log \|m\|_\sigma.$$

On choisit la section $\widetilde{P}^* s_D$ de $\widetilde{P}^*\mathcal{O}(1)$ qui est non nulle car $\widetilde{P} \not\subset D$. Par définition de l'intersection arithmétique, $(\widetilde{P} \cdot D)_v$ est la valuation de $s(P)$ pour une équation locale s de D. La proposition en résulte immédiatement. □

La formule précédente jointe aux Propositions 2.4 et 2.5 entraîne:

PROPOSITION 2.7 *Soit K' une extension finie de K et soit $P \in E_K(K) \subset E_K(K')$. Alors, $h_{K'}(P) = h_K(P)$. Par conséquent, h s'étend en une fonction sur $E_K(\overline{K})$.*

Le reste de l'article va se concentrer sur l'étude de la fonction h. Voici pourquoi:

PROPOSITION 2.8 *Il existe une hauteur de Weil sur $E_K(\overline{\mathbf{Q}})$ qui coïncide avec h sur l'ensemble des points de torsion de E_K annulés par un entier premier au conducteur de la variété abélienne A_K.*

Preuve. Soit $\mathcal{L}$ un faisceau inversible ample symétrique sur A_K et tel que $\mathcal{L}_1 := \pi^*\mathcal{L} \otimes \mathcal{O}(1)$ soit ample sur $\overline{E}_K$, ce qui est possible car $\mathcal{O}(1)$ est relativement ample pour $\pi : \overline{E}_K \to A_K$. Soient $\eta_{\mathcal{L}}$ et $\eta_{\mathcal{O}(1)}$ des hauteurs de Weil pour les fibrés en droites $\mathcal{L}$ sur A_K et $\mathcal{O}(1)$ sur $\overline{E}_K$. Alors, la fonction $\eta_{\mathcal{L}_1}$ sur $\overline{E}_K(\overline{\mathbf{Q}})$ définie par

$$\eta_{\mathcal{L}_1}(x) := \eta_{\mathcal{L}}(\pi(x)) + \eta_{\mathcal{O}(1)}(x),$$

est une hauteur de Weil pour $\mathcal{L}_1$. En vertu du théorème de Néron–Tate, quitte à rajouter à $\eta_{\mathcal{L}}$ une fonction bornée, nous pouvons supposer que $\eta_{\mathcal{L}}$ est une fonction quadratique sur $A_K(\overline{\mathbf{Q}})$. Par conséquent, si $x \in E_K(\overline{\mathbf{Q}})$ est un point d'ordre fini, on aura

$$\eta_{\mathcal{L}_1}(x) = \eta_{\mathcal{O}(1)}(x),$$

puisque $\pi(x) \in A_K(\overline{\mathbf{Q}})$ est aussi d'ordre fini. Il suffit donc de démontrer le lemme suivant:

LEMME 2.9 *Il existe une constante C telle que pour tout point $x \in E_K(\overline{\mathbf{Q}})$ d'ordre premier au conducteur de la variété abélienne A_K, on ait*

$$|h(x) - \eta_{\mathcal{O}(1)}(x)| \leqslant C.$$

Preuve du lemme. Pour clarifier les idées, donnons d'abord la preuve dans le cas où A_K admet bonne réduction sur l'anneau des entiers de K. L'extension vectorielle universelle compactifiée $\overline{E}$ du modèle de Néron est alors un modèle propre et plat de $\overline{E}_K$ sur l'anneau $\mathfrak{O}_K$; le faisceau $\mathcal{O}(1)$ est un prolongement sur $\overline{E}$ du faisceau de même nom sur $\overline{E}_K$ et nous l'avons muni de métriques hermitiennes aux places à l'infini. La théorie d'Arakelov nous dit alors que l'application

$$P \in \overline{E}_K(K') \longmapsto \frac{1}{[K' : K]} \deg_{\mathrm{Ar}} \tilde{P}^*\mathcal{O}(1) =: h(\mathcal{P}),$$

est une hauteur de Weil pour le fibré en droites $\mathcal{O}(1)$, ce qui termine la démonstration du lemme dans ce cas, une fois rappelé le fait que deux hauteurs de Weil pour le même fibré en droites diffèrent d'une fonction bornée.

Pour démontrer le cas général, il faut prendre garde au fait que les différentes extensions canoniques ne forment pas un unique modèle projectif de $\overline{E}_K$ mais une réunion croissante de modèles quasi-projectifs. De ce fait, on ne peut pas affirmer sans précautions que h est une hauteur de Weil pour le fibré en droites $\mathcal{O}(1)$.

Pour étudier h, nous allons revenir à la décomposition de h en hauteurs locales: $h = \sum_v h_v$. Nous allons construire une famille compatible $\{\eta_{D,v}\}$ de hauteurs locales pour le diviseur D (au sens de Serre, *Lectures on the Mordell–Weil theorem,* §6.2) telle que:

— pour toute place σ archimédienne, $\eta_{D,\sigma} = h_\sigma$;
— pour toute place v finie où A_K a bonne réduction, $\eta_{D,v} = h_v$;
— pour toute place v de mauvaise réduction, $\eta_{D,v}(P) = h_v(P)$ si $P \in E(\overline{K})$ est un point annulé par un entier premier à la caractéristique résiduelle de v.

Une fois cette construction de $\{\eta_{D,v}\}$ effectuée, la fonction $\eta_D(P) = \sum \eta_{D,v}(P)$ est une hauteur de Weil pour le diviseur D, si bien qu'il existe une constante C telle que $|\eta_D(P) - \eta_{\mathcal{O}(1)}(P)| \leqslant C$, d'où le lemme.

Si v est une place de bonne réduction ou une place infinie, l'interprétation de l'intersection arithmétique (2.3) comme une hauteur locale nous permet de poser $\eta_{D,v} = h_v$. Il reste donc à construire $\eta_{D,v}$ pour une place de mauvaise réduction, et pour cela, il est loisible de supposer que K est une extension finie de $\mathbf{Q}_p$. Nous notons R son anneau d'entiers et v la valuation de K étendue de manière unique en une valuation de $\overline{K}$. Enfin, A_K est une variété abélienne sur K et $0 \to V_K \to E_K \to A_K \to 0$ son extension vectorielle universelle.

Soit X un modèle propre, de type fini et plat de A_K sur l'anneau R (par exemple, l'adhérence de A_K dans un espace projectif $\mathbf{P}^n_R$ convenable). On choisit aussi un R-schéma propre, de type fini et plat Y qui prolonge $A_K \times A_K$ et est muni d'applications p_1, p_2, $m : Y \to X$ qui prolongent respectivement la première projection, la seconde projection et la multiplication $A_K \times A_K \to A_K$ (par exemple, on peut prendre pour Y l'adhérence dans X^3 de l'image A_K^2 par la composition $A_K^2 \xrightarrow{(p_1,p_2,m)} A_K^3 \hookrightarrow X^3$.) Choisissons enfin un R-module libre V tel que $V \otimes_R K = V_K$.

Soit (U_i) un recouvrement ouvert affine fini de X, U_{ij} l'intersection de U_i et U_j qui est aussi un ouvert affine; soient donc $U_i = \operatorname{Spec} A_i$ et $U_{ij} = \operatorname{Spec} A_{ij}$. Les $U_{i,K}$ sont des ouverts affines de A_K sur lesquels le V_K-torseur $E_K|_{U_{i,K}}$ est trivial, d'où une section $\sigma_i \colon U_{i,K} \to E_K$. Sur $U_{i,K} \cap U_{j,K}$, la différence $\sigma_i - \sigma_j$ est une fonction régulière f_{ij} à valeurs dans V_K. Ainsi, $f_{ij} \in A_i \otimes V \otimes K$. Par conséquent, il existe un entier N tel que $N f_{ij} \in A_i \otimes V$; les $N f_{ij}$ vérifient encore la condition de cocycle, ce qui permet de prolonger E_K en un V-torseur E au-dessus de X. Comme au paragraphe 2.1, cela nous donne un faisceau $\mathcal{F}$ sur X, extension de $\mathcal{O}_X$

par $V \otimes \mathcal{O}_X$, une compactification $\overline{E} = \mathbf{P}(\mathcal{F})$, un diviseur à l'infini relativement ample D, etc.

Comme X est propre sur R, on a $X(\overline{R}) = A(\overline{K})$ et l'ensemble des points entiers de X est muni d'une structure de groupe. En revanche, E n'est pas propre sur R et l'ensemble $E(\overline{R})$ n'est pas a priori un sous-groupe de $E_K(\overline{K})$. Nous allons toutefois nous ramener à ce cas, quitte à remplacer l'entier N par un de ses multiples.

Il existe des trivialisations de E sur les ouverts affines U_i que nous notons toujours σ_i. Soit Ω_{ijk} l'ouvert $(p_1,p_2)^{-1}(U_i \times U_j) \cap m^{-1}(U_k)$ de Y et $\Omega_{ijk,K}$ sa fibre générique. On a une fonction $\Omega_{ijk,K} \to V_K$ définie par

$$f_{ijk}(x,x') = \sigma_i(x) \oplus_E \sigma_j(x') \ominus_E \sigma_k(x \oplus_A x'),$$

si bien que $f_{ijk} \in \Gamma(\Omega_{ijk}) \otimes V \otimes K$ et qu'il existe un dénominateur commun à toutes ces fonctions. Ainsi, quitte à multiplier les fonctions de transitions f_{ij} par un entier non nul, ce qui multiplie les fonctions f_{ijk} par ce même entier, on peut supposer que

$$f_{ijk} \in \Gamma(\Omega_{ijk}) \otimes V.$$

De même, on peut aussi supposer que l'élément neutre de E_K se prolonge en un point entier, quitte encore à remplacer l'extension par un multiple.

Dans ces conditions, montrons que $E(\overline{R})$ est un groupe: Soient e et $e' \in E(\overline{R})$, $x = \pi(e)$ et $x' = \pi(e')$. On peut trouver i, j et k tels que $(p_1,p_2)^{-1}(x,x') \in \Omega_{ijk}$. Alors, dire que e est entier revient à dire que $e \ominus_E \sigma_i(x) \in V \otimes_R \overline{R}$, de même pour e'. On constate alors que

$$e \oplus_E e' = (e \ominus \sigma_i(x)) + (e' \ominus \sigma_j(x')) + f_{ijk}(x,x') + \sigma_k(x \oplus x'),$$

ce qui prouve que $e \oplus e'$ est un point de $E(\overline{R})$. De même, on prouve que $e \ominus e'$ est un point de $E(\overline{R})$, si bien que $E(\overline{R})$ est un groupe.

On associe alors aux choix de X, Y, V, $\overline{E}$ une hauteur locale en la place v sur $E_K(\overline{K})$ par la formule

$$\eta_{D,v}(P) = (D \cdot \tilde{P})_v,$$

calculée sur ce modèle $\overline{E}$, où $P \in \overline{E}_K(\overline{K}) \setminus |D|$, $\tilde{P}$ est l'unique point entier de $\overline{E}(\overline{R})$ qui prolonge P et $(\ \cdot\ )_v$ est l'intersection arithmétique du diviseur D et du 1-cycle $\tilde{P}$ (qui sont bien transverses).

Évaluons $\eta_{D,v}([n]_E P) - \eta_{D,v}(P)$: soit e un point entier dans la fibre de P, $e' = [n]e$ qui est un point entier dans la fibre de $[n]P$. Alors, $\eta_{D,v}(P)$ est la valuation du dénominateur de $P \ominus_E e$ et $\eta_{D,v}([n]P)$ est la valuation du dénominateur de $[n]P - e' = n(P \ominus e)$, si bien que

$$\eta_{D,v}([n]P) \leqslant \eta_{D,v}(P) \leqslant \eta_{D,v}([n]P) + v(n).$$

Si l'on suppose de plus que $[n]P = 0$, où n est un entier premier à la caractéristique résiduelle de v, on constate que $\eta_{D,v}(P) = 0$.

Or, on prouve au Corollaire 4.3 – de manière bien sûr indépendante – que $h_v(P) = 0$ pour de tels points. La fonction $\eta_{D,v}$ construite vérifie donc la condition requise, ce qui établit le lemme et du même coup achève la preuve de la proposition. □

3. Le calcul archimédien

On reprend les notations des paragraphes 2.1 et 2.2. En particulier, on fixe des normes hermitiennes $\|\cdot\|_{V,\sigma}$ sur $V \otimes_\sigma \mathbf{C}$ et on note $\|\cdot\|^\sigma$ la métrique hermitienne correspondante sur $\mathcal{O}(1)$. Le but de cette section est de démontrer la proposition:

PROPOSITION 3.1 *Soit E une extension vectorielle d'une variété abélienne complexe A. Soit n un entier non nul et $P \in E(\mathbf{C})$ un point tel que $[n]P = 0$. Alors, on a*

$$\|s_D\|_P = 1.$$

Preuve. Comme l'extension de $\mathbf{C}^g$ par V obtenue par *pull-back* est scindée, le même calcul que dans la Proposition 2.2 montre que la loi de groupe sur E se déduit par passage au quotient par l'action de $\pi_1(A)$ de l'opération

$$(u, z) \oplus (u', z') \mapsto (u + u', z + z')$$

sur $V \times \mathbf{C}^g$. Vue comme loi de groupe rationnelle sur $\overline{E}$, elle provient de l'opération

$$([t, u], z) \oplus ([t', u'], z') \mapsto ([tt', t'u + tu'], z + z') .$$

Par conséquent, la multiplication par n sur E provient de l'application rationnelle $([t, u], z) \mapsto ([t, nu], nz)$ sur $\overline{E}$. Il en résulte que si n est un entier non nul, les coordonnées des points de n-torsion de E, lues sur le revêtement universel, sont $([1, \rho(\lambda)/n], \lambda/n)$ avec $\lambda \in \pi_1(A)$.

La Proposition 2.3 affirme alors que

$$\|s_D\|_P = |t|(\|u - t\rho(z)\|_V^2 + |t|^2)^{-(1/2)},$$

alors que l'on a $u = \rho(\lambda)/n$, $t = 1$ et $z = \lambda/n$, si bien que $\|s_D\|_P = 1$.

4. Le calcul aux places finies

Le but de cette section est d'évaluer les termes $h_{S,v}$ pour une place finie v de S. On supposera donc que S est le spectre d'un anneau de valuation discrète R, complet et de corps résiduel k algébriquement clos. Soit K le corps des fractions de R.

On note A/S est le modèle de Néron d'une variété abélienne A_K/K et E une extension vectorielle de A par un groupe vectoriel V/S.

4.1. PRÉLIMINAIRES

Le *push-out* de l'extension E via la multiplication par λ sur V nous donne une extension $[\lambda]_*E$ avec un morphisme u_λ: $E \to [\lambda]_*E$: si l'on considère la suite exacte

$$0 \to V \xrightarrow{(i,-\lambda)} E \times V \xrightarrow{p_\lambda} [\lambda]_*E \to 0$$

qui définit $[\lambda]_*E$, le morphisme u_λ est la restriction de p_λ à $E \times \{0\} = E$. Si λ n'est pas une unité, l'application u_λ ne s'étend pas à $\overline{E}$. Cependant, on peut définir, en reprenant la notation du Lemme 2.1:

DÉFINITION 4.1 Soit $P \in E_K(K)$. On définit $u_\lambda(\widetilde{P})$ comme $(u_\lambda(P))\widetilde{\ }$, où $u_\lambda(P)$ est calculé sur la fibre générique.

PROPOSITION 4.1 *Soit $P \in E_K(K)$. Alors, on peut calculer la multiplicité d'intersection $(\widetilde{P} \cdot D)_v$ par la formule*

$$(\widetilde{P} \cdot D)_v = \min\{v(\lambda); \quad \lambda \in R \setminus \{0\},\ u_\lambda(\widetilde{P}) \in [\lambda]_*E(S) \hookrightarrow u_\lambda(E_K(K))\}.$$

Preuve. Soit $\mathfrak{U}$ un recouvrement ouvert de A et $\eta = (\eta_{UU'})$ un cocycle qui représente la classe de l'extension E dans $H^1(A, \mathcal{O}_A \otimes_S V)$. Si f: $S \to A$ est un S-point de A un S-point σ de E au-dessus de f est alors une famille de morphismes $\sigma_U : f^{-1}(U) \to V$ pour $U \in \mathfrak{U}$ vérifiant $\sigma_U - \sigma_{U'} = \eta_{UU'} \circ f$. L'extension $[\lambda]_*E$ correspond à la classe $\lambda\eta$ et le S-point $u_\lambda(\sigma)$ de $[\lambda]_*E$ est représenté par les morphismes $\lambda\sigma_U$.

Comme R est principal, un S-point de $\overline{E} = \mathbf{P}(\mathcal{F})$ au-dessus de f est un couple $(\{\sigma_U\}, t)$ défini à multiplication par une unité de R près et tel que $\sigma_U - \sigma_{U'} = t\eta_{UU'} \circ f$, pour tous U et $U' \in \mathfrak{U}$, et $(\sigma_U, t) \notin \mathfrak{p}V \times \mathfrak{p}$, $\mathfrak{p}$ étant l'idéal maximal de R.

Par définition, l'intersection arithmétique $(\widetilde{P} \cdot D)_v$ est alors égale à $v(t)$, si bien que $\widetilde{P} \in E(S)$ si et seulement si $v(t) = 0$. D'après ce qu'on vient de voir, $u_\lambda(\widetilde{P})$ correspond à la famille $(\{\sigma_U\}, t/\lambda)$ tant que $v(t/\lambda) \geqslant 0$, et à $(\{\frac{\lambda}{t}\sigma_U\}, 1)$ quand $v(\lambda/t) \geqslant 0$, d'où la proposition. □

LEMME 4.2 *Soit $P \in E_K(K)$. Alors $(\widetilde{P} \cdot D)_v \geqslant 0$.*

Si de plus $[n]_E P$ se prolonge en $([n]_E P)\widetilde{\ } \in E(S)$, par exemple si $[n]_E P = 0$, alors $(\widetilde{P} \cdot D)_v \leqslant v(n)$.

Preuve. La première partie est évidente. Pour démontrer la seconde, on utilise la structure affine de E: soient $Q_1 = \pi(P)$, $Q_2 = \pi([n]_E P) = [n]_A Q_1$, $P_1 \in E(S)$ tel que $\pi(P_1) = Q_1$ (il en existe car R est principal) et $P_2 = ([n]_E P)\widetilde{\ }$. Alors, il existe $x \in V \otimes K$ tel que $P_1 + i(x) = P$ (rappelons que i est l'inclusion $V \hookrightarrow E$). La multiplicité d'intersection $(\widetilde{P} \cdot D)_v$ est alors égale à

$$\min\{v(\lambda); \quad \lambda \in R,\ \lambda x \in V \subset V \otimes K\}.$$

Par hypothèse, $[n]_E P$ se prolonge en $P_2 \in E(S)$. Par conséquent, $nx = i^{-1}(P_2 - [n]_E P_1)$ est entier et $(\widetilde{P} \cdot D)_v \leqslant v(n)$. □

COROLLAIRE 4.3 *Si $P \in E_K(K)$ est un point de n-torsion, $(\widetilde{P} \cdot D)_v = 0$ pour toutes les places v dont la caractéristique résiduelle ne divise pas n.*

4.2. GROUPES FINIS

Soient B un schéma et H un schéma en groupes fini et plat sur B. D'après [6, (1.2), p. 3], il existe une application universelle $\alpha_H : H \to \omega_{H^*}$ de H dans un faisceau quasi-cohérent, où H^* est le dual de Cartier de H, et ω_{H^*} le faisceau des différentielles invariantes sur H^*.

Rappelons une construction de cette application: Soit $P \in H(B)$. La dualité de Cartier permet de voir P comme un B-morphisme $\varphi\colon H^* \to \mathbf{G}_m$ et $\alpha_H(P) = \varphi^*(\mathrm{d}t/t) \in \omega_{H^*}$. (Rappelons que $\mathrm{d}t/t$ est la différentielle invariante sur $\mathbf{G}_m = \mathrm{Spec}B[t, t^{-1}]$.) En effet, selon [6, (1.2), p. 4], α_H est la composition

$$H \xrightarrow{\sim} \mathrm{Hom}(H^*, \mathbf{G}_m) \to \mathrm{Hom}_{B-\text{schémas } B-\text{pointés}}(\mathrm{Inf}^1(H^*), \mathbf{G}_m) = \omega_{H^*},$$

$\mathrm{Inf}^1(H^*)$ désignant le premier voisinage infinitésimal de l'élément neutre dans H^*. Comme les différentielles invariantes s'identifient canoniquement aux éléments de l'espace cotangent en l'origine et comme $\mathrm{d}t/t$ est une base de $\omega_{\mathbf{G}_m}$, cette dernière flèche est bien donnée par $\varphi \mapsto \varphi^*(\mathrm{d}t/t)$.

Nous notons $A(n)$ le sous-schéma en groupes $\mathrm{Ker}[p^n]_A$ de A.

PROPOSITION 4.4 *Soit E l'extension vectorielle canonique d'un schéma abélien A/S. Soient $P \in E_K(K)$ un point annulé par p^n, $\widetilde{P}$ son adhérence (construite au Lemme 2.1) et $\widetilde{Q} = \pi(\widetilde{P}) \in A(S)$. Alors, $\widetilde{Q} \in A(n)(S)$ et on a pour tout $\lambda \in R \setminus \{0\}$ l'équivalence*

$$h_{S,v}(P) \leqslant v(\lambda) \iff \lambda\alpha_{A(n)}(\widetilde{Q}) = 0.$$

Preuve. Tout d'abord, on remarque que E/S est l'extension vectorielle universelle de A/S. En effet, le schéma abélien dual B s'identifie à la composante neutre du modèle de Néron de la variété abélienne duale B_K de A_K. Par conséquent, l'extension canonique qui représente le foncteur $\mathbf{Extrig}_S(B, \mathbf{G}_m)$ est canoniquement isomorphe à l'extension vectorielle universelle de A qui représente, d'après [6, Proposition (2.6.7)], le même foncteur.

D'après la Proposition 4.1, l'inégalité $(\widetilde{P} \cdot D)_v \leqslant v(\lambda)$ est vraie si et seulement si $\widetilde{Q}$ se relève en un point de p^n-torsion dans l'extension vectorielle $[\lambda]_* E$. Or, pour vérifier ce dernier fait, il n'est pas restrictif d'effectuer le changement de base de $S = \mathrm{Spec} R$ à $S_n = \mathrm{Spec}(R/p^n R)$. En effet, l'équation à résoudre s'écrit, une fois choisie comme dans la démonstration du Lemme 4.2 une origine P_1 dans la fibre affine au-dessus de $\widetilde{Q}$, $p^n x = v$, où $v = -[p^n] P_1$, et cette équation possède une solution $x \in \omega_{A^*}$ si et seulement si $v \in p^n \omega_{A^*}$, c'est-à-dire s'il y a une solution après changement de base à S_n.

De même, la condition de droite est vraie si et seulement si elle est vraie après changement de base à S_n car les groupes abéliens $\omega_{A(n)^*}(S)$ et $\omega_{A(n)^*}(S_n)$ sont égaux.

Pour simplifier les notations, on notera de la même manière les S-schémas et les S_n schémas obtenus par extension des scalaires de S à S_n.

D'après [6, (2.6.3), p. 22], la suite exacte

$$0 \to A(n) \to A \xrightarrow{[p^n]_A} A \to 0,$$

de S_n-schémas en groupes donne par le *push-out* par l'application $\alpha_{A(n)}$: $A(n) \to \omega_{A(n)^*}$ une extension

$$0 \to \omega_{A(n)^*} \to E \to A \to 0,$$

qui est l'extension vectorielle universelle de A/S_n (Remarque: comme $p^n = 0$ dans S_n, $\omega_{A(n)^*} = \omega_B$ est un S_n-groupe vectoriel).

Par conséquent, sur S_n, l'extension $[\lambda]_* E$ est obtenue par *push-out* de l'extension $0 \to A(n) \to A \overset{[p^n]}{\to} A \to 0$ par l'application $\lambda \alpha_{A(n)}$, c'est-à-dire le quotient de $\omega_{A(n)^*} \times A$ par le sous-groupe engendré par les points de la forme $(-\lambda \alpha_{A(n)}(x), x)$ pour $x \in A(n)$ (cf. [4, III, Déf. 1.3.1]; le quotient est le faisceau associé au préfaisceau (pour la topologie plate)

$$T \mapsto \frac{\omega_{A(n)^*}(T) \times_{S_n(T)} A(T)}{\{(-\lambda \alpha_{A(n)}(x), x); x \in A(n)(T)\}},$$

pour tout $T \to S_n$ plat et de présentation finie.)

Localement, la recherche du point de p^n torsion $\widetilde{z}$ relevant $\widetilde{Q}$ dans l'extension $[\lambda]_* E$ se ramène donc au problème suivant: soit $T \to S_n$ plat et de présentation finie, on cherche $v_T \in \omega_{A(n)^*}(T)$ et $\xi_T \in A(T)$ tels que $(p^n v_T, [p^n]\xi_T) = (-\lambda \alpha_{A(n)}(x_T), x_T)$ pour un certain $x_T \in \omega_{A(n)^*}(T)$. Comme (v_T, ξ_T) doit relever le point $\widetilde{Q}_T \in A(n)(T)$, on a $[p^n]\xi_T = \widetilde{Q}_T$. Donc $x_T = \widetilde{Q}_T$ et on a une solution si et seulement si $p^n v_T = -\lambda \alpha_{A(n)}(\widetilde{Q}_T)$ a une solution $v_T \in \omega_{A(n)^*}(T)$, c'est-à-dire si et seulement si $0 = \lambda \alpha_{A(n)}(\widetilde{Q}_T) \in \omega_{A(n)^*/T}$.

Si l'on a une solution globale $\tilde{z}$, il en résulte que $\lambda\alpha_{A(n)}(\widetilde{Q}_T) = 0$ pour un morphisme $T \to S_n$ fidèlement plat et de présentation finie, et donc que $\lambda\alpha_{A(n)}(\widetilde{Q}) = 0$.

Réciproquement, si $\lambda\alpha_{A(n)/S_n}(\widetilde{Q})$ est nul, les $\tilde{z} = (v, \xi) = (0, \widetilde{Q}) \in \omega_{A(n)^*}(S_n) \times A(S)$ représentent un point annulé par $[p^n]$ dans le *préfaisceau* quotient, et donc $\widetilde{Q}$ se relève a fortiori en un S_n-point de p^n-torsion dans le *faisceau* quotient $[\lambda]_* E$. □

4.3. Exemple des schémas en groupes d'ordre p

On note $\overline{R}$ la clôture intégrale de R dans une clôture algébrique $\overline{K}$ de K. On pose $\overline{S} = \mathrm{Spec}\overline{R}$. On note encore v l'unique valuation sur $\overline{K}$ qui prolonge la valuation de K. On suppose enfin que $v(p) > 0$.

Le but de ce paragraphe est d'étudier l'application α_G quand G est un schéma en groupes d'ordre p. On utilise la classification donnée par Oort et Tate [10].

4.3.1. $G = \mu_p$, $G^* = \mathbf{Z}/p$

Le schéma en groupes G^* est étale, donc $\omega_{G^*} = 0$ et $\alpha_G = 0$.

4.3.2. $G = \mathbf{Z}/p$, $G^* = \mu_p$

Soit $x = 1 \in G(S)$. Le morphisme correspondant $G^* \to \mathbf{G}_m$ est le plongement identique. Par suite, $\varphi^*(\mathrm{d}t/t) = \mathrm{d}t/t$ est annulé exactement par p.

4.3.3. *Cas général*

Soient a et c deux éléments de R tels que $ac = p$. On définit un schéma en groupes $G_{a,c}$ sur $S = \mathrm{Spec}R$ de la façon suivante

$$G_{a,c} = \mathrm{Spec}\frac{R[X]}{(X^p - aX)}, \quad m^*(X) = 1 \otimes X + X \otimes 1 + c\sum_{i=1}^{p-1} \frac{X^i}{w_i} \otimes \frac{X^{p-i}}{w_{p-i}},$$

où les w_i sont des éléments canoniques de R (vérifiant $w_i \equiv i! \pmod{p}$). Le dual de $G_{a,c}$ est $G_{cw_{p-1}, a/w_{p-1}}$ et la dualité de Cartier est donnée par

$$T \mapsto 1 + \frac{1}{1-p}\sum_{i=1}^{p-1} \frac{(X \otimes Y)^i}{w_i}.$$

Posons $G = G_{a,c}$ et notons G^* le dual de G. Soient $\mathcal{A}$ et $\mathcal{A}^*$ les algèbres affines de G et G^*. Le module des différentielles de G^* est engendré par $\mathrm{d}Y$, avec la relation $(pY^{p-1} - cw_{p-1})\,\mathrm{d}Y = 0$. Or, $1 - \frac{a}{w_{p-1}}Y^{p-1}$ est inversible dans l'algèbre affine de G^*, si bien que

$$\Omega^1_{G^*/R} = \mathcal{A}^*/(c)\,\mathrm{d}Y.$$

Soit $0 \neq x \in G(\overline{S})$, c'est-à-dire une solution de $x^{p-1} = a$. Le $\overline{R}$-morphisme correspondant $\varphi_x : G^* \to \mathbf{G}_m$ est donné par $T \mapsto 1 + \frac{1}{1-p} \sum \frac{x^i}{w_i} Y^i$, si bien que $\alpha_G(x)$ est la forme différentielle invariante

$$\frac{x}{1-p} \frac{\sum_{i=1}^{p-1} \frac{ix^{i-1}}{w_i} Y^{i-1}}{1 + \frac{1}{1-p} \sum \frac{x^i}{w_i} Y^i} \mathrm{d}Y.$$

Le dénominateur, étant égal à $\varphi_x^*(T)$, est inversible par construction.

LEMME 4.5 *Supposons que c ne soit pas une unité. Alors, tout élément de $\mathcal{A}^*$ de la forme $1 + a_1 Y + \cdots + a_{p-1} Y^{p-1}$ est inversible.*

Preuve. En effet, si l'on spécialise Y en toutes les solutions de $Y^p = cw_{p-1}Y$, l'expression devient une unité de R. Par conséquent, la fonction concernée n'appartient à aucun idéal maximal de $\mathcal{A}^*$ et est inversible. □

Ainsi, $\varphi_x^*(\mathrm{d}t/t)$ est, à une unité de $\mathcal{A}^*$ près, la forme différentielle $x\,\mathrm{d}Y$. La valuation de x est égale à $v(a)/(p-1)$. Par conséquent, pour tout $\lambda \in R$,

$$\lambda \alpha_G(x) = 0 \Longleftrightarrow v(\lambda) \geqslant v(c) - \frac{v(a)}{p-1} = v(p) - \frac{p}{p-1} v(a).$$

Remarque 1. Le cas où $G = \mu_p$ correspond à $a = p$ et $c = 1$ auquel cas l'assertion de droite est vraie pour tout $\lambda \in R$. Le cas où $G = \mathbf{Z}/p$ est obtenu pour $a = 1$ et $c = p$. On a $v(a) = 0$ et on retrouve le résultat obtenu par une analyse directe.

COROLLAIRE 4.6 (cf. [1]) *Soient G/S un schéma en groupes fini et plat annulé par p et $G \xrightarrow{\pi} G^{et}$ son quotient étale maximal. Soit $x \in G(\overline{S})$ tel que $\pi(x) \neq 0$. Alors, si $\lambda \in R$ est tel que $\lambda \alpha_G(x) = 0$, on a $\lambda \in pR$.*

Preuve. En effet, soit $G \xrightarrow{\pi_x} H$ un quotient étale d'ordre p de G^{et} tel que $y = \pi_x(x) \neq 0$. Comme $\lambda \alpha_G(x) = 0$, on a $\lambda \alpha_H(y) = 0$. Comme y est non nul, les calculs précédents entraînent que $\lambda \in pR$. □

Remarque 2. On trouve déjà dans [6], au bas de la page 56, un argument de ce type qui montre qu'il n'y a pas, sur l'extension universelle elle-même, de point d'ordre p relevant un point étale.

4.4. SCHÉMAS EN GROUPES DE TYPE $(p, \ldots, p)$

Le problème que posent les schémas en groupes d'ordre premier p est qu'ils se prêtent mal au dévissage des schémas en groupes annulés par p, à moins d'admettre des extensions ramifiées. Ce sont les schémas en groupes vectoriels étudiés par Raynaud dans [11] qui nous permettront de conclure.

Dans ce paragraphe, on suppose que R absolument non ramifié, c'est-à-dire que p est une uniformisante de R.

PROPOSITION 4.7 *Soit G un schéma en groupes simple défini sur R. On suppose que G^* n'est pas étale et que R est absolument non ramifié. Alors, si $y \in G(\overline{K})$ est non nul et $\lambda \in \overline{R}$ est tel que $\lambda \alpha_G(y) = 0$, on a l'inégalité $v(\lambda) > \frac{p-2}{p-1} v(p)$.*

Preuve. Notons $q = \#G$ et soit r l'entier tel que $p^r = q$. Soit $\mathbf{F}$ le corps fini à q éléments. Les Propositions 3.2.1 et 3.3.2 de [11] impliquent que G est un schéma en groupes en $\mathbf{F}$-vectoriels vérifiant la condition $(\star\star)$ de [11, p. 246].

Soit w l'élément de R défini en [11, (17), p. 242]. D'après [11, Corollaire 1.5.1], il existe r couples (γ_i, δ_i), indexés par $\mathbf{Z}/r\mathbf{Z}$, d'éléments de R tels que $\gamma_i \delta_i = w$ et vérifiant les propriétés suivantes: l'algèbre affine de G est

$$\mathcal{A} = R[X_i; i \in \mathbf{Z}/r\mathbf{Z}]/(X_i^p - \delta_i X_{i+1}; i \in \mathbf{Z}/r\mathbf{Z});$$

le dual de Cartier G^* de G est défini par les couples (δ_i, γ_i), la dualité $G \times G^* \to \mathbf{G}_m$ étant donnée par

$$T \mapsto 1 + \sum_{\substack{a_i=0 \\ (a_i)\neq(0,\ldots,0)}}^{p-1} \left(\prod_i X_i^{a_i}\right) \otimes \left(\prod_i Y_i^{a_i}\right),$$

(pour alléger l'écriture, on *notera* $\sum_\chi$ la sommation sur les (a_i) tels que $0 \leqslant a_i \leqslant (p-1)$ et $(a_i) \neq (0, \ldots, 0)$); on peut aussi donner explicitement la comultiplication, mais nous n'en aurons pas besoin.

Le module des différentielles de G^* est engendré sur $\mathcal{A}^*$ par les $\mathrm{d}Y_i$, $i \in \mathbf{Z}/r\mathbf{Z}$, avec les relations $pY_i^{p-1}\,\mathrm{d}Y_i = \gamma_i\,\mathrm{d}Y_{i+1}$. Par conséquent, le module ω_{G^*} des différentielles invariantes, qui s'identifie au module des différentielles en l'origine, est donné par

$$\omega_{G^*} = \bigoplus_{i\in\mathbf{Z}/r\mathbf{Z}} \frac{R}{(\gamma_{i-1})}\,\mathrm{d}Y_i.$$

Soit $x = (x_i) \in G(\overline{R})$ un point d'ordre p. Le morphisme $\varphi_x : G^* \to \mathbf{G}_m$ est donné par la formule

$$T \mapsto 1 + \sum_\chi \prod_i x_i^{a_i} \prod_i Y_i^{a_i}.$$

Il en résulte que

$$\varphi_x^*(\mathrm{d}t/t) = \sum_i \frac{P_i}{Q}\,\mathrm{d}Y_i, \qquad Q = \varphi_x^*(T),$$

et

$$P_i = \sum_{\chi} a_i \left(\prod_j x_j^{a_j} \right) Y_i^{a_i - 1} Y_{i+1}^{a_{i+1}} \cdots Y_{i+r-1}^{a_{i+r-1}}.$$

Par restriction à la section nulle, $Q = 1$ et $P_i = x_i$. Par suite, on a $\varphi_x^*(\mathrm{d}t/t) = \sum x_i \, \mathrm{d}Y_i \in \omega_{G^*}$.

Posons $A_i = \gamma_{i-1}/x_i$ et définissons A_i^* par $A_i^* = A_i$ si $A_i \in R$ et $A_i^* = 1$ sinon. On a alors $\lambda\alpha_G(x) = 0$ si et seulement si $v(\lambda) \geqslant v(A_i^*)$ pour tout i.

Comme $x_i^p = \delta_i x_{i+1}$, la valuation de A_i est égale à

$$\begin{aligned} v(A_i) &= v(\gamma_{i-1}) - \frac{1}{q-1}(p^{r-1}v(\delta_i) + \cdots + v(\delta_{i+r-1})) \\ &= v(p) - \frac{p}{q-1}(v(\delta_{i-2}) + pv(\delta_{i-3}) + \cdots + p^{r-2}v(\delta_i) + p^{r-1}v(\delta_{i-1})) \end{aligned}$$

c'est-à-dire

$$v(A_{i+1}) = v(p) - \frac{1}{q-1}\sum_{h=1}^{r} p^h v(\delta_{i-h}) = \frac{1}{q-1}\sum_{h=1}^{r} v(\gamma_{i-h})p^h - \frac{v(p)}{p-1}.$$

Si tous les γ_i sont des unités, on a $v(A_i) < 0$ pour tout i, si bien que $\alpha_G(x) = 0$. Mais dans ce cas, G^* est étale donc isomorphe à $(\mathbf{Z}/p)^r$ et G est isomorphe à μ_p^r.

Dans le cas contraire, comme R est absolument non ramifié, $v(\gamma_i) \in \{0, 1\}$ pour tout i; on peut choisir i tel que $v(\gamma_i) = 1$, et alors

$$v(A_{i+1}) \geqslant \frac{p^r}{p^r - 1} - \frac{1}{p-1} = \frac{p-2}{p-1} + \frac{1}{p^r - 1}.$$

4.5. Fin du calcul

PROPOSITION 4.8 *Soit R un anneau de valuation v discrète, de corps des fractions K de caractéristique 0, de corps résiduel k de caractéristique p. On suppose que R est absolument non ramifié. Soient K' une extension finie de K, R' la clôture intégrale de R dans K' ; soit v' une place de S' au-dessus de v. On note $S = \mathrm{Spec} R$ et $S' = \mathrm{Spec} R'$.*

Soit E l'extension universelle d'un schéma abélien A/S de dimension g. Alors au moins $p^{2g} - p^{2g-1}$ points P d'ordre p dans $E_{K'}(K')$ vérifient

$$h_{S',v'}(P) > \frac{p-2}{p-1} v'(p).$$

Preuve. Sans restreindre la généralité, nous pouvons supposer que R est complet et que son corps résiduel k est algébriquement clos.

Supposons que le sous-groupe G de p-torsion de A admet un quotient étale non trivial. Dans ce cas, le Corollaire 4.6 montre que pour tous les points $P \in E_{K'}(K')$

tels que $\pi(P) \in A(S')$ est non trivial dans ce quotient, on a $(\widetilde{P} \cdot D)_{v'} \geqslant v'(p)$. Or, au plus p^{2g-1} points de A annulés par p peuvent être d'image nulle dans le quotient étale, d'où la proposition dans ce cas.

Dans le cas contraire, G n'admet pas non plus de quotient toroïdal (on se ramène à la fibre spéciale où l'on applique [9, Sect. 15, p. 147]). D'après [11, Corollaire 3.3.7], comme R est non ramifié et strictement hensélien, le dernier quotient H d'une suite de Jordan–Hölder de G/S est alors un schéma en groupes simple auquel la Proposition 4.7 s'applique. Au plus p^{2g-1} points de G sont d'image nulle dans H. Pour les autres points P, si l'on note P' leur image dans H et que $\lambda\alpha_G(P) = 0$, on a $\lambda\alpha_H(P') = 0$, si bien que $v'(\lambda) > \frac{p-2}{p-1}v'(p)$ d'après la Proposition 4.7. Ainsi, sauf pour au plus p^{2g-1} points, on a $(\widetilde{P} \cdot D)_{v'} > v'(p)(p-2)/(p-1)$. □

Remarque 3. Les arguments de l'exemple [11, 3.4] permettent de traiter plus complètement le cas des courbes elliptiques supersingulières. Avec les hypothèses de la Proposition 4.8, supposons en outre que A/S soit une courbe elliptique de réduction A_k/k supersingulière. Soit G le sous-groupe de p-torsion de A/S. Alors G est simple, car sinon il admettrait un sous-groupe d'ordre p, lequel serait étale ou toroïdal, conformément à la classification des groupes d'ordre p sur une base non ramifiée; mais ceci est incompatible avec l'hypothèse que la courbe elliptique est supersingulière. Ensuite, comme G est simple et S non ramifié, c'est un groupe en $\mathbf{F}$-vectoriels du type étudié par Raynaud. Il correspond à $r = 2$ ($\mathbf{F} = \mathbf{F}_{p^2}$) et on a nécessairement $v(\gamma_1) = 0$ et $v(\gamma_2) = 1$ (ou le contraire), car sinon G serait étale ou toroïdal. Par suite, $\lambda\alpha_G(y) = 0$ si et seulement si $y = 0$ ou $v(\lambda) \geqslant (p^2 - p - 1)/(p^2 - 1)$.

Cela redonne par une méthode totalement différente une partie des résultats de [2, 3].

5. Démonstration du théorème principal

Nous pouvons maintenant démontrer le théorème principal de cet article, dans lequel h désigne la hauteur relative (Déf. 2.3):

THÉORÈME 5.1 *Soient K un corps de nombres, $\mathfrak{O}$ son anneau d'entiers, $S = \operatorname{Spec}\mathfrak{O}$. Soit A_K une variété abélienne sur K, A/S son modèle de Néron supposé semi-stable. Soit E_K l'extension vectorielle universelle de A_K. Alors, pour tout nombre premier p ne divisant ni le conducteur de A ni le discriminant de K, on a*

$$\left(1 - \frac{2}{p}\right) \log p \leqslant \frac{1}{p^{2g}} \sum_{\substack{P \in E_K(\overline{K}) \\ [p]_E P = 0}} h(P) \leqslant \log p.$$

Preuve. Choisissons p assez grand de sorte que pour tout nombre premier $\ell > p$, l'extension $K/\mathbf{Q}$ soit ramifiée en ℓ et A ait bonne réduction en toutes les places au-dessus de ℓ. Soit K' une extension de K telle que le sous-groupe de p-torsion de A soit rationnel sur K' et soit $S' = \mathrm{Spec}\mathfrak{O}_{K'}$.

D'après la Proposition 3.1, $h_{S',\sigma}(P) = 0$ pour tout point P de torsion dans $E_{K'}(K')$ et tout plongement $\sigma\colon K' \hookrightarrow \mathbf{C}$.

Fixons une place v' de K'. Si la caractéristique résiduelle de v' est différente de p, alors les hauteurs locales des points de p-torsion en v' sont nulles d'après le Corollaire 4.3.

En revanche, si la caractéristique résiduelle de v' est p, comme $h_{S',v'}(P) \geqslant 0$ pour tout P, la minoration 4.8 implique que la somme $\sum_{[p]_E P=0} h_{S',v'}(P)$ est minorée par

$$(p^{2g} - p^{2g-1})\frac{p-2}{p-1}v'(p) \geqslant p^{2g}\left(1 - \frac{2}{p}\right) v'(p).$$

La Proposition 2.6 entraîne alors l'inégalité

$$\begin{aligned}
\sum_{[p]_E P=0} h(P) &= \frac{1}{[K':\mathbf{Q}]}\sum_{v'}\sum_{[p]_E P=0} h_{S',v'}(P)\log N(v') \\
&\quad + \frac{1}{[K':\mathbf{Q}]}\sum_{\sigma}\sum_{[p]_E P=0} h_{S',\sigma}(P) \\
&= \frac{1}{[K':\mathbf{Q}]}\sum_{v'|p}\sum_{[p]_E P=0} h_{S',v'}(P) f_{v'}\log p \\
&\geqslant \frac{1}{[K':\mathbf{Q}]}\sum_{v'|p} p^{2g}\left(1 - \frac{2}{p}\right) f_{v'}v'(p)\log p \\
&\geqslant p^{2g}\left(1 - \frac{2}{p}\right)\log p,
\end{aligned}$$

puisque

$$\sum_{v'|p} f_{v'}v'(p) = [K':\mathbf{Q}].$$

D'autre part, on a, d'après le Lemme 4.2, l'inégalité $h_{S',v'}(P) \leqslant v'(p)$ pour toute place v' de S'. Finalement, comme $\sum_{v'} v'(p)\log N(v') = [K':\mathbf{Q}]\log p$, on a pour tout point $P \in E_K(\overline{K})$ d'ordre p l'inégalité $h(P) \leqslant \log p$, ce qui entraîne la majoration du théorème. □

THÉORÈME 5.2 *Soit A_K une variété abélienne sur un corps de nombres K, $\overline{E}_K$ la compactification de son extension vectorielle universelle* (cf. Sect. 2.1). *Soit η*

une hauteur de Weil sur $\overline{E}_K$. Alors, il existe deux constantes strictement positives C_1 et C_2 telles que l'on ait l'inégalité, valable pour tout nombre premier p

$$C_1 \log p - C_2 < \frac{1}{p^{2g}} \sum_{\substack{P \in E_K(\overline{K}) \\ [p]_E P = 0}} \eta(P) < C_1 \log p + C_2.$$

Preuve. Sans restreindre la généralité, on peut supposer que A admet un modèle de Néron semi-stable sur l'anneau des entiers de K. Soit $\mathcal{L}$ un fibré ample sur $\overline{E}_K$. La structure du groupe de Picard des fibrés projectifs (cf. par exemple [5, Exercice II.7.9]) entraîne qu'il existe un unique fibré inversible $\mathcal{L}_0$ sur A_K et un unique entier $m \in \mathbf{Z}$ tel que $\mathcal{L} = \pi^* \mathcal{L}_0 \otimes \mathcal{O}(m)$. Comme $\mathcal{L}$ est ample, on a $m > 0$.

Si η est une hauteur de Weil associée à $\mathcal{L}$, la Proposition 2.8 entraîne alors qu'il existe une constante C telle que $|\eta(P) - mh(P)| \leqslant C$ pour tout point $P \in E_K(\overline{K})$ d'ordre premier. D'après le théorème précédent, l'expression

$$\frac{1}{p^{2g}} \sum_{[p]_E P = 0} h(P) - \log p,$$

est bornée quand p parcourt l'ensemble des nombres premiers. Il existe ainsi une constante C' telle que l'on ait, pour tout nombre premier p, l'inégalité

$$\left| \frac{1}{p^{2g}} \sum_{[p]_E P = 0} \eta(P) - m \log p \right| \leqslant C',$$

d'où le théorème. □

Appendice: Lien avec les périodes p-adiques

Les méthodes exposées ci-dessus permettent également d'étudier les points d'ordre une puissance de p. On déduit aisément de la Proposition 4.4 que pour tout nombre premier p ne divisant ni le conducteur de A, ni le discriminant de K, et pour tout entier $n \geqslant 1$, la moyenne des hauteurs des points d'ordre divisant p^n est minorée par $(n - \frac{2}{p}) \log p$.

Dans [3], P. Cohen retraduit ce type de résultats (sur les courbes elliptiques) dans le langage des périodes p-adiques. Nous faisons de même dans le cas des variétés abéliennes en exprimant en ces termes les conséquences de la Proposition 4.7.

Soient $\mathbf{C}_p$ le complété de la clôture algébrique $\overline{\mathbf{Q}}_p$ de $\mathbf{Q}_p$ et $\mathcal{O}_p$ la clôture intégrale de $\mathbf{Z}_p$ dans $\mathbf{C}_p$. Notons v la valuation normalisée de $\mathbf{C}_p$, telle que $v(p) = 1$. Soient R un sous-anneau de $\mathcal{O}_p$ tel que $v(R \setminus \{0\})$ est discret et $K \subset \mathbf{C}_p$ son corps de fractions. Notons k le corps résiduel de R qui est de caractéristique p. Finalement, désignons par Γ le groupe des automorphismes continus de $\mathbf{C}_p / K$.

Soit A un schéma abélien sur R; rappelons que nous notons $A(n)$ le noyau de la multiplication par p^n sur A. Soit $T_p(A) = \varprojlim A(n)(\mathbf{C}_p)$ le module de Tate de A. Nous noterons par ailleurs $\tilde{A}/k$ la variété abélienne sur k obtenue par réduction de A modulo l'idéal maximal de R.

Les périodes p-adiques dont il s'agit sont données par une application $\mathbf{C}_p$-linéaire et Γ-équivariante

$$\theta_A : \mathbf{C}_p \otimes_{\mathbf{Z}_p} T_p(A) \to \mathbf{C}_p \otimes_R H^0(A^*, \Omega^1_{A^*}) = \mathbf{C}_p \otimes_R \omega_{A^*},$$

dont Coleman (« Hodge–Tate periods and p-adic abelian integrals », *Invent. Math.*, **78**, 1984, p. 351–379) donne la description suivante:

THÉORÈME A.1 (Coleman). *Soit E l'extension vectorielle universelle de A sur R. Soit $a = (a_n)_{n \in \mathbf{N}} \in T_p(A)$. Choisissons pour tout n un point $b_n \in E(\mathcal{O}_p)$ relevant a_n. Alors $\theta_A(a) = \lim_{n \to \infty} [p^n]_E b_n$.*

La dualité canonique $\langle \cdot, \cdot \rangle$ (cf. [9, Sect. 13, Corollary 3, p. 130]) entre $H^1(A, \mathcal{O}_A)$ et $H^0(A^*, \Omega^1)$ permet de récrire cette application θ_A comme un accouplement entre $H^1_{\mathrm{DR}}(A)/H^0(\Omega^1)$ (dont on peut représenter les éléments par des formes différentielles de seconde espèce) et $T_p(A)$, après extension des scalaires à $\mathbf{C}_p$. Si $a \in T_p(A)$ et $\eta \in H^1_{\mathrm{DR}}(A)$, nous noterons $\int_a \eta = \langle \eta, \theta_A(a) \rangle$ l'élément de $\mathcal{O}_p$ correspondant.

Le Théorème A.1 et la non-nullité de θ_A (qui possède un inverse à droite, cf. l'article de Coleman), joints aux calculs aux places archimédiennes (Proposition 3.1) et aux places finies ne divisant pas p (Corollaire 4.3) entraînent que la moyenne des hauteurs des points de p^n-torsion est minorée par une expression de la forme $(n - C_p) \log p$. Mais il ne permet pas de préciser la dépendance de C_p en fonction de p, ni a fortiori de minorer la moyenne des hauteurs des points de p-torsion.

Inversement, il n'est pas surprenant que l'on puisse, en utilisant les techniques des paragraphes 4.2 et 4.4, préciser l'énoncé de Coleman. Ainsi elles entraînent en particulier:

THÉORÈME A.2 *Soit $a = (a_1, \ldots \in T_p(A)$.*

(i) *Supposons que le corps K est absolument non ramifié. Alors, sauf pour au plus p^{2g-1} valeurs de* $a \bmod pT_p(A)$, *il existe une forme différentielle de seconde espèce $\eta \in H^1_{\mathrm{DR}}(A)$ telle que $\int_a \eta \in \mathcal{O}_p$ est de valuation inférieure à $1/(p-1)$.*

(ii) *Si l'image de a_1 dans $\tilde{A}$ est non nulle, alors il existe une forme différentielle de seconde espèce η telle que $\int_a \eta$ est une unité de $\mathcal{O}_p$.*

Le point (ii) étend aux variétés abéliennes un théorème de B. Perrin–Riou (« Périodes p-adiques », *C.R. Acad. Sc. Paris,* 300, 1985, Corollaire 6) sur les périodes p-adiques des courbes elliptiques ordinaires. Signalons par ailleurs les évaluations bien plus précises obtenues par P. Colmez (« Périodes des variétés abéliennes à multiplication complexe », *Ann. of Math.*, 138, 1993, p. 625–683) pour les périodes p-adiques des variétés abéliennes de type CM.

Soit ι_n l'immersion fermée $A(n) \hookrightarrow A$, d'où la suite exacte

$$0 \to p^n\omega_{A^*} \to \omega_{A^*} \xrightarrow{\iota_n^*} \omega_{A(n)^*} \to 0.$$

LEMME A.3 *Soit $a_n \in A(\mathcal{O}_p)$ tel que $[p^n]_A a_n = 0$ et $b_n \in E(\mathcal{O}_p)$ qui relève a_n. Alors $\alpha_{A(n)}(a_n) = -\iota_n^*([p^n]_E b_n)$.*

Preuve. (Cf. Crew, « Universal extensions and p-adic periods of elliptic curves », *Comp. Math.*, 73, 1990, pp. 107–119)

Soit B_n l'anneau $\mathcal{O}_p/p^n\mathcal{O}_p$. Les groupes abéliens $\omega_{A(n)^*/\mathcal{O}_p}(\mathcal{O}_p)$ et $\omega_{A(n)^*/B_n}(B_n)$ sont égaux, si bien qu'il est loisible, pour démontrer ce lemme, d'étendre les scalaires à B_n. Comme ι_n^* est un isomorphisme sur B_n, il reste à montrer le fait suivant: soit $a \in A(n)(B_n)$ et $b \in E(B_n)$ qui relève a. Alors, l'élément $[p^n]b$ de ω_{A^*/B_n} est égal à $-\alpha(a)$.

Comme on l'a vu dans la démonstration de la Proposition 4.4, le point b est défini par un couple $(\beta, v) \in \omega_{A^*} \times A(B_n)$ modulo les points de la forme $(-\alpha(\xi), \xi)$ pour $\xi \in A(n)(B_n)$. Avec ces notations, b relève le point $[p^n]_A\beta$ de A et $[p^n]_E b = (p^n v, [p^n]_A\beta) = (0, [p^n]_A\beta)$. Comme on a supposé que b relève a, on voit que $[p^n]_E b$ est donné par le couple $(0, a) \in \omega_{A^*} \times A(B_n)$, lequel point est dans la même classe que $(-\alpha(a), 0)$, d'où le lemme. $\square$

Preuve du théorème. Soient $n \geqslant 1$ et $k \geqslant 0$; comme b_{n+k} relève a_{n+k}, le point $[p^k]_E b_{n+k}$ relève le points a_n et $[p^k]_E b_{n+k} - b_n \in \omega_{A^*}$, ce qui montre que $[p^{n+k}]_E b_{n+k}$ et $[p^n]_E b_n$ sont congrus modulo $p^n\omega_{A^*}$ (et entraîne en particulier la convergence de la suite définissant $\theta_A(a)$).

Par suite, si $\lambda \in \mathcal{O}_p$ n'est pas multiple de p, $\theta_A(a) \in \lambda\omega_{A^*}$ si et seulement si $[p]_E b_1 \in \lambda\omega_{A^*}$, ce qu'on peut vérifier après extension des scalaires à $\mathcal{O}_p/p\mathcal{O}_p$. Autrement dit, $\theta_A(a) \in \lambda\omega_{A^*}$ équivaut à l'annulation de $(p\lambda^{-1})\alpha_{A(1)}(a_1) \in \omega_{A(1)^*}$.

Démonstration de (i)

Comme dans la preuve de la Proposition 4.8, le corps K étant absolument non ramifié sur $\mathbf{Q}_p$, le dernier quotient d'une suite de Jordan–Hölder du R-schéma en groupes $A(1)$ est justiciable de la Proposition 4.7. Notons $\varpi : A(1) \to H$ ce quotient. Si $\varpi(a_1) \neq 0$, on a ainsi $v(p/\lambda) > \frac{p-2}{p-1}v(p)$, d'où la majoration

$$v(\lambda) < \frac{1}{p-1}v(p).$$

Cela signifie exactement qu'il existe une forme différentielle de seconde espèce η telle que $v(\int_a \eta) < \frac{1}{p-1}$.

Comme au plus p^{2g-1} points $a \in T_p(A)/pT_p(A)$ sont tels que $\varpi(a_1) = 0$, ceci conclut la démonstration de la première partie du théorème.

Démonstration de (ii)
La non-nullité de a_1 dans $\tilde{A}$ signifie que $A(1)$ admet un quotient étale $\varpi: A(1) \to H$ non trivial et $\varpi(a_1) \neq 0$. Si $(p/\lambda)\alpha_{A(1)}(a_1) = 0$, la Proposition 4.6 entraîne que $v(p/\lambda) \geqslant v(p)$, et donc $v(\lambda) = 0$, ce qui signifie comme précédemment qu'il existe une forme de seconde espèce η telle que $v(\int_a \eta) = 0$. □

Remarque 4. J'ai constaté depuis la rédaction de cet article que le théorème principal 5.2 s'étend à toutes les extensions vectorielles non triviales. Par ailleurs la Proposition 2.8 est valable pour tous les points de torsion, cf. « Extensions vectorielles, périodes et hauteurs », *thèse*, Univ. Paris 6, décembre 1995.

Remerciements

Je voudrais remercier P. Cartier pour de nombreuses remarques, ainsi que J.B. Bost pour m'avoir signalé une erreur dans une première version de cet article.

Références

1. Chambert-Loir, A.: Extension universelle et hauteurs, *C.R.A.S.*, 318 (juin 1994), 1067–1070.
2. Cohen, P.: Heights of torsion points on commutative group varieties, *Proc. London Math. Soc.*, 52 (1986), 427–444.
3. —, Heights of torsion points on commutative group varieties II, *Proc. London Math. Soc.*, 62 (1991), 99–120.
4. Giraud, J.: *Cohomologie non abélienne*, Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen, Band 179, Springer, 1971.
5. Hartshorne, R.: *Algebraic Geometry*, Graduate Texts in Mathematics 52, Springer.
6. Mazur, B. and Messing, W.: *Universal Extensions and One Dimensional Crystalline Cohomology*, Lecture Notes in Mathematics 370, Springer.
7. Milne, J. S.: *Étale Cohomology*, Princeton University Press, 33, 1980.
8. Moret-Bailly, L.: *Princeaux de variétés abéliennes*, Astérisque 129.
9. Mumford, D.: *Abelian Varieties*, Oxford University Press, 1974.
10. Oort, F. and Tate, J.: Group schemes of prime order, *Ann. Sci. E.N.S.* 3 (1970), 1–21.
11. Raynaud, M.: Schémas en groupes de type $(p, \ldots, p)$, *Bull. S.M.F.*, 102 (1974), 241–280.
12. Serre, J.-P.: *Groupes algébriques et corps de classes*, Hermann, 1960.
13. —, Quelques propriétés des groupes algébriques commutatifs, in *Nombres transcendants et groupes algébriques*, M. Waldschmidt, Astérisque 69–70, 191–202.
14. Szpiro, L.: Degrés, intersections, hauteurs, in *Séminaire sur les princeaux arithmétiques: la conjecture de Mordell*, Astérisque 127, 11–28.
15. Tate, J.: p-divisible groups, in *Proceedings of a Conference on Local Fields*, Driebergen, 1967, 158–183.