HAUTEUR ET TORSION DES MODULES DE DRINFELD DE RANG 2

par

Aurélien Galateau & Amílcar Pacheco

Résumé. — On étudie la hauteur dans le corps engendré par les points de torsion d'un module de Drinfeld de rang 2. Si ce module est de type CM ou non exceptionnel, on montre que lorsqu'elles ne s'annulent pas, la hauteur de Weil et la hauteur canonique sont minorées par une constante strictement positive.

1. Introduction

Cet article est consacré aux problèmes de hauteur dans les modules de Drinfeld. On s'intéresse en particulier au corps engendré par la torsion d'un module de Drinfeld de rang 2, et on cherche à minorer la hauteur d'un élément de ce corps lorsqu'elle ne s'annule pas.

Problème de Lehmer et propriété (B). — Ce type de problème est d'abord apparu dans le cadre des corps de nombres, puis des courbes elliptiques et des variétés abéliennes. Rappelons-en l'origine. Soit h la hauteur de Weil (logarithmique, absolue) sur $\bar{\mathbb{Q}}^*$. Par un théorème classique de Kronecker, la fonction h s'annule exactement en les racines de l'unité. Un célèbre problème, d'abord soulevé par Lehmer dans les années 30, consiste à trouver une minoration optimale pour h en dehors de son ensemble d'annulation. On peut formuler la conjecture suivante (voir **[26]**, §13, p. 476).

Conjecture 1.1 **(Lehmer)**. — *Il existe un nombre réel $c > 0$ tel que si $x \in \bar{\mathbb{Q}}^*$ n'est pas une racine de l'unité :*

$$h(x) \geq \frac{c}{[\mathbb{Q}[x] : \mathbb{Q}]}.$$

Nous remercions le programme MATH-AmSud (Capes et CNRS) pour son soutien financier. Le deuxième auteur remercie aussi CNPq - Brésil de lui avoir accordé une bourse de recherche.

Si ce problème est résolu dans un certain nombre de cas, il reste encore ouvert en général ; la meilleure borne inconditionnelle pour la hauteur est due à Dobrowolski (voir [**16**]).

On connaît certaines extensions infinies de $\mathbb{Q}$ sur lesquelles on peut donner une minoration absolue strictement positive pour la hauteur lorsqu'elle ne s'annule pas. C'est le cas pour la clôture abélienne $\mathbb{Q}^{\mathrm{ab}}$ de $\mathbb{Q}$ ([**3**]), pour la clôture abélienne K^{ab} d'un corps de nombres K ([**5**]), ou encore pour un corps totalement réel ([**34**]). Bombieri et Zannier ont proposé l'étude systématique des corps vérifiant cette propriété ([**9**]).

Définition 1.2. — On dit qu'un sous corps K de $\bar{\mathbb{Q}}$ a la propriété de Bogomolov, ou propriété (B), s'il existe $c(K) > 0$ tel que pour tout $x \in K^*$ qui n'est pas une racine de l'unité :

$$h(x) \geq c(K).$$

Remarquons que les corps de nombres vérifient la propriété (B) par Northcott. Les exemples intéressants sont donc à chercher parmi les extensions infinies de $\mathbb{Q}$. D'autres conditions suffisantes ont depuis été données (voir notamment [**2**] et [**11**]). Habegger a récemment étudié le corps $\mathbb{Q}(E_{\mathrm{tors}})$ engendré par le sous-groupe de torsion E_{tors} de $E(\bar{\mathbb{Q}})$, où E est une courbe elliptique (voir [**24**]).

Théorème 1.3 **(Habegger)**. — *Soit E une courbe elliptique définie sur $\mathbb{Q}$. Le corps $\mathbb{Q}(E_{\mathrm{tors}})$ vérifie la propriété (B).*

La contrainte portant sur le corps de définition de E est liée au théorème d'Elkies sur les places de réduction supersingulière d'une courbe elliptique définie sur $\mathbb{Q}$; le travail d'Habegger repose en grande partie sur les propriétés de la réduction de E aux premiers supersinguliers. Notons que par des méthodes assez proches, il parvient également à minorer la hauteur de Néron-Tate pour les points de E (d'ordre infini) définis sur $\mathbb{Q}(E_{\mathrm{tors}})$. Une autre minoration de la hauteur de Néron-Tate sur les variétés abéliennes a été donnée par Baker et Silverman dans le cas des extensions abéliennes (*cf.* [**7**]).

Hauteur et modules de Drinfeld. — Les problèmes analogues existent dans le cadre des modules de Drinfeld, pour lesquels on dispose en général de résultats plus faibles. Soit A l'anneau des polynômes sur un corps fini $\mathbb{F}_q$ tel que $\mathrm{car}(\mathbb{F}_q) \neq 2$, K son corps des fractions et ϕ un A-module de Drinfeld de rang $d \geq 1$ défini sur K et de caractéristique générique. On dispose d'une hauteur de Weil h sur $\bar{K}$ et d'une hauteur canonique $\hat{h}_\phi$ construite à partir de h par passage à la limite.

Si la conjecture de Lehmer est trivialement vraie pour la hauteur de Weil (voir (2.4) plus bas), elle reste ouverte pour $\hat{h}_\phi$. Denis a démontré l'analogue du théorème de Dobrowolski pour les extensions séparables sur un module de Carlitz ([**14**]). D'autres résultats ont depuis été donnés, notamment par Ghioca (*cf.* [**22**] pour une minoration en rang supérieur) et Ingram (voir [**25**] pour une minoration de type « Lang-Silverman »).

On peut également chercher des extensions (infinies) de K vérifiant la propriété (B) pour la hauteur canonique $\hat{h}_\phi$. Le premier cas étudié, suivant la stratégie développée par Amoroso et Dvornicich, a été celui des extensions abéliennes pour un module de Drinfeld de rang quelconque (voir [**13**]).

Théorème 1.4 **(David-Pacheco)**. — *La clôture abélienne K^{ab} de K vérifie la propriété (B) pour la hauteur $\hat{h}_\phi$.*

Récemment, Bauchère a donné de nouveaux exemples de corps vérifiant la propriété (B) pour la hauteur $\hat{h}_\phi$, inspirés par le travail d'Amoroso, David et Zannier ([**2**]), dans le cas où ϕ est de type CM (voir [**8**]).

Théorème 1.5 **(Bauchère)**. — *On suppose que ϕ est de type CM. Soit M/K une extension galoisienne de groupe de Galois G, et H un sous-groupe de $Z(G)$ fixant un sous-corps L de M. S'il existe une place finie de K au-dessus de laquelle les degrés locaux des places de L sont uniformément bornés, le corps M vérifie la propriété (B) pour la hauteur $\hat{h}_\phi$.*

Hauteur et torsion en rang 2. — À la suite du travail d'Habegger, on s'intéresse ici au corps K_{tors} engendré par la torsion de ϕ sur $\bar{K}$. Si ϕ est un module de Carlitz, le groupe de Galois de K_{tors}/K est abélien, et ce corps vérifie la propriété (B) pour $\hat{h}_\phi$. Le premier cas nouveau est celui des modules de Drinfeld de rang 2 sans multiplication complexe. On montre que la propriété de Bogomolov est vérifiée pour ces modules s'ils sont non exceptionnels (suivant la terminologie fixée par Poonen dans [**32**], qui corrige légèrement la définition donnée dans [**10**]).

L'hypothèse sur le rang, en plus de fournir un bon critère pour l'existence d'une infinité de premiers supersinguliers, joue un rôle important dans les propriétés de la représentation galoisienne associée à la torsion du module (voir en particulier le Lemme 4.6 plus bas, qui repose sur la classification des sous-groupes maximaux du groupe linéaire d'un espace vectoriel de dimension 2 sur un corps fini).

Théorème 1.6. — *Soit ϕ un module de Drinfeld de rang 2. Si ϕ est CM ou non exceptionnel, le corps K_{tors} satisfait la propriété (B) par rapport à la hauteur $\hat{h}_\phi$.*

Ce théorème est la conséquence immédiate de la Proposition 5.5, combinée avec le Corollaire 3.6 et le Théorème 3.7. Les méthodes employées nous permettent d'obtenir un énoncé analogue pour la hauteur de Weil.

Théorème 1.7. — *Soit ϕ un module de Drinfeld de rang 2. Si ϕ est CM ou non exceptionnel, il existe un réel $c(\phi) > 0$ tel que pour tout $x \in K_{\mathrm{tors}}$ non constant :*

$$h(x) \geq c(\phi).$$

Ce théorème se déduit directement de la Proposition 4.9, combinée avec le Corollaire 3.6 et le Théorème 3.7.

Les minorations obtenues sont dans les deux cas explicites. Elles dépendent de q (le cardinal du corps des constantes de K) et du degré d'un premier supersingulier « suffisamment grand »(dans un sens également explicite, faisant intervenir la constante de

comparaison entre hauteur de Weil et hauteur canonique, et la constante du Théorème 3.3 d'image ouverte dans le cas Drinfeld). On discutera au fil du texte la possibilité de rendre effectives toutes ces constantes ; il apparaît que le principal obstacle concerne le théorème de l'image ouverte.

La stratégie générale pour démontrer ces minorations est la même que dans le cas des courbes elliptiques : elle repose sur l'existence d'un premier supersingulier de degré assez grand. Les propriétés galoisiennes des modules de Tate en un tel premier $\mathfrak{p}$ permettent d'obtenir des estimations $\mathfrak{p}$-adiques très fortes, et d'en déduire une minoration absolue pour la hauteur.

Il convient de préciser que nos résultats sur les modules de Drinfeld de rang 2 sont partiels. En ce qui concerne les modules de type CM, si on fixe un ordre $\mathcal{O}$ d'un corps quadratique imaginaire, les j-invariants (singuliers) de modules de Drinfeld ayant multiplication complexe par $\mathcal{O}$ sont des entiers algébriques en nombre fini, qu'on peut expliciter grâce à la théorie du corps de classe du corps CM (voir par exemple [**21**], Theorem 9.3). D'autre part, comme le souligne Brown dans le commentaire suivant la formule (1.1.7) de [**10**], les j-invariants exceptionnels, pour lesquels notre méthode échoue, sont proportionnellement peu nombreux. Mais contrairement au cas des courbes elliptiques, on sait grâce aux travaux de Poonen (*cf.* [**32**]) que le théorème de Brown ne peut s'étendre à tous les modules de Drinfeld, même en rang 2. L'amélioration des résultats de cet article semble donc passer en premier lieu par l'analyse des premiers ordinaires. La première difficulté à résoudre apparaît dans le cas non ramifié, pour borner la taille d'une classe de Frobenius dans le groupe de Galois de l'extension K_{tors}/K.

Le cadre drinfeldien présente certains avantages, comme l'absence de places archimédiennes ou le caractère non conjectural d'un certain nombre d'énoncés (hypothèse de Riemann, théorème de l'image ouverte). L'absence des places archimédiennes nous permet de ne pas recourir à des énoncés d'équidistribution dans la minoration de la hauteur de Weil. On y parvient aussi pour la hauteur canonique, en utilisant un procédé d'accélération $\mathfrak{p}$-adique basé sur les propriétés de la « multiplication par $\mathfrak{p}$ »(Lemme 5.2).

Plan de l'article. — Pour toute la suite, on fixe $\mathbb{F}_q$ le corps fini à $q := p^\nu$ éléments (où $p \geq 3$ est un nombre premier et $\nu \geq 1$ est un nombre entier), et $A := \mathbb{F}_q[t]$ l'anneau des polynômes à une indéterminée sur $\mathbb{F}_q$, plongé dans son corps des fractions K.

On commencera par rappeler un certain nombre de généralités sur les modules de Drinfeld, leurs réductions, les modules de Drinfeld formels, et les différentes hauteurs avec lesquelles on travaillera. Puis on étudiera les propriétés galoisiennes de la torsion des modules de Drinfeld aux places supersingulières.

La quatrième partie sera consacrée à la minoration de la hauteur de Weil, moyennant l'existence d'un premier supersingulier bien choisi. L'étude du cas ramifié nous conduira à faire une descente sur la torsion basée sur des résultats de théorie des groupes et sur l'utilisation du théorème de l'image ouverte. Dans la dernière partie, on minorera la hauteur canonique sous une hypothèse de supersingularité comparable. La descente dans ce cadre est un peu plus compliquée, et on aura besoin pour conclure d'un dernier argument kummerien.

2. Généralités

On présente ici quelques résultats bien connus concernant les modules de Drinfeld (morphismes, réduction, modules de Drinfeld formels). On explique aussi comment construire une hauteur canonique compatible avec la structure de A-module.

2.1. Modules de Drinfeld et morphismes. — Commençons par rappeler quelques définitions de base sur les modules de Drinfeld. On renvoie à [**23**], 4 pour plus de détails.

Soit L un A-corps, c'est-à-dire un corps muni d'un morphisme d'anneaux $i : A \to L$. On dira que L est *de caractéristique générique* si le morphisme i est injectif. On peut munir le groupe additif $\mathbb{G}_a$ sur L d'une structure de A-module en se donnant un morphisme injectif $\phi : A \to \mathrm{End}(\mathbb{G}_a)$. Soit $\tau : x \to x^q$ l'endomorphisme de Frobenius sur $\mathbb{G}_a$. Le morphisme ϕ est entièrement caractérisé par l'image de la variable t, qui appartient à l'anneau $L\{\tau\}$ des polynômes (absolument) additifs en $\tau = x^q$ sur L. La multiplication sur les monômes de $L\{\tau\}$ est donnée par la règle suivante :

$$\forall(\lambda,\mu) \in L^2, (m,n) \in \mathbb{N}^2 \quad : \quad \lambda\tau^n\mu\tau^m = \lambda\mu^{q^n}\tau^{m+n}. \tag{2.1}$$

On écrit :

$$\phi(t) = a_0(t)\tau^0 + \cdots + a_d(t)\tau^d, \tag{2.2}$$

où les coefficients $a_0, \ldots, a_d$ sont dans L et vérifient : $a_0(t) = i(t)$ et $a_d(t) \neq 0$. Un tel module ϕ est appelé *module de Drinfeld*, et l'entier d est le *rang* de ϕ.

Un morphisme entre deux A-modules de Drinfeld ϕ et ψ sur L est donné par un polynôme $P \in L\{\tau\}$ vérifiant : $P \circ \phi(t) = \psi(t) \circ P$. L'anneau des endomorphismes d'un module ϕ sera noté $\mathrm{End}(\phi)$. C'est un A-module projectif de rang fini majoré par d^2, où d est le rang de ϕ. Si L est de caractéristique générique, cet anneau est commutatif et de rang au plus d (voir [**23**], Theorem 4.7.8 et [**20**], Proposition 2.3).

Un ordre d'une extension finie L de K est une A-algèbre incluse dans $\mathcal{O}_L$ dont le corps des fractions est L.

Définition 2.1. — On dit qu'un module ϕ de rang d est à multiplication complexe (CM) par un ordre $\mathcal{O}$ d'une extension finie L de K si $A \subsetneq O = \mathrm{End}(\phi)$ et $[L : K] = d$.

Remarque. Si ϕ est CM, le corps $L := \mathrm{End}(\phi) \times_A K$ est CM dans le sens suivant : il existe un seul idéal premier de $\mathcal{O}_L$ au-dessus de l'idéal « à l'infini »$(t)A$ (voir la preuve du Theorem 4.7.17 de [**23**]).

On se donne pour la suite de cette partie un module de Drinfeld ϕ de rang d défini sur $\bar{K}$. Quitte à remplacer K par une extension finie, on pourra toujours supposer que ϕ est défini sur K.

2.2. Torsion et séparabilité. — Un élément $b \in \bar{K}$ est dit de *torsion* pour ϕ s'il existe $a \in A \setminus \{0\}$ tel que $\phi(a) \cdot b = 0$. Si I est un idéal de A, on considérera par la suite :

$$\phi[I] := \{b \in \bar{K}, \forall a \in I \ : \phi(a) \cdot b = 0\},$$

et $\phi[I^\infty] = \bigcup_{n\geq 1} \phi[I^n]$. Si $a \in A$, on pose $\phi[a] := \phi[(a)A]$. On notera aussi ϕ_{tors} le sous-module de torsion de ϕ sur $\bar{K}$. Dans la suite, lorsqu'il n'y aura pas d'ambiguïté sur le module ϕ, on notera pour simplifier $K(I)$ l'extension de K engendrée par $\phi[I]$, et K_{tors} l'extension de K engendrée par ϕ_{tors}. Comme K est de caractéristique générique, on a l'isomorphisme de A-modules :

$$\phi[I] \simeq (A/I)^d,$$

et ce résultat est encore vrai si on remplace K par $A/\mathfrak{q}$, avec $\mathfrak{q}$ un idéal premier de A ne divisant pas I (*cf.* **[23]**, 4.5).

Lemme 2.2. — *L'extension $K(I)/K$ est galoisienne.*

Démonstration. — On peut supposer que $I = \mathfrak{p}^n$, où $\mathfrak{p}$ est premier et $n \geq 1$. Soit π un générateur de $\mathfrak{p}$. On a :

$$|\phi[\mathfrak{p}^n]| = |A/\mathfrak{p}^n|^d = q^{\deg(\pi)nd}.$$

Les points de $\mathfrak{p}^n$-torsion sont annulés par le polynôme $\phi(\pi^n)$, qui est de degré $q^{\deg(\pi)nd}$ en x. Ce polynôme s'annule donc exactement sur la $\mathfrak{p}^n$-torsion, et il est à racines simples dans son corps de décomposition, ce qui prouve le lemme. □

Remarque. Ce résultat nous sera d'une grande utilité pour étudier la hauteur dans $K(I)$. Les extensions inséparables de grand degré produisent des points de petite hauteur de Weil ; elles créent donc une obstruction naturelle lorsqu'on cherche une minoration absolue de la hauteur. Notons qu'il n'existe pour l'instant aucune minoration connue de la hauteur de Weil ou de la hauteur canonique dans les extensions galoisiennes. Mais les méthodes utilisées dans **[1]** et **[18]** devraient s'adapter au moins partiellement dans le cadre drinfeldien (voir aussi **[4]** pour un résultat récent sur les extensions galoisiennes des corps de nombres).

2.3. Hauteur de Weil et hauteur canonique. — On dispose sur $\bar{K}$ de la hauteur de Weil (absolue, logarithmique), qui est définie de la manière suivante. Si a appartient à une extension finie L de K, on pose :

$$h(a) := \frac{1}{[L:K]} \sum_{v\in M(L)} n_v \max\{0, -v(a)\},$$

où v varie parmi les places de L, et n_v est le degré résiduel en la place v, qu'on normalise en la prenant surjective : $L \to \mathbb{Z} \cup \{\infty\}$. Cette définition ne dépend pas du choix de L parmi les corps de définition de a. On a la formule du produit :

$$\forall a \in L^* : \sum_{v\in M(L)} n_v v(a) = 0. \tag{2.3}$$

La fonction h est sous-additive et vérifie la propriété de Northcott, qui caractérise les fonctions hauteurs : pour tous entiers D et H, il y a un nombre fini de points $a \in \bar{K}$ tels que $[K(a) : K] \leq D$ et $h(a) \leq H$. La hauteur de Weil vérifie aussi :

$$\forall a \in \bar{K}, \forall n \in \mathbb{Z} : h(a^n) = nh(a).$$

Il est alors facile de voir que cette hauteur s'annule exactement en le corps des constantes $\bar{k}$, dont le groupe multiplicatif est l'ensemble des éléments d'ordre fini de $\bar{K}^*$. Toute fonction rationnelle non constante ayant au moins une valuation non nulle, et donc au moins une valuation strictement négative par la formule (2.3) :

$$\forall a \in \bar{K} \setminus \bar{k} \quad : \quad h(a) \geq \frac{1}{[K(a) : K]}. \tag{2.4}$$

La conjecture de Lehmer est donc trivialement vraie dans ce cas.

On peut également construire une hauteur *canonique* sur $\bar{K}$, compatible avec la structure de module donnée par ϕ. Cette hauteur s'obtient à partir de h par un procédé de passage à la limite :

$$\hat{h}_\phi(a) := \lim_{n \to +\infty} \frac{h\big(\phi(t^n) \cdot a\big)}{q^{nd}}.$$

La fonction $\hat{h}_\phi$ vérifie la propriété suivante. Pour tout $a \in A$ de degré $r \geq 0$ et $b \in \bar{K}$:

$$\hat{h}_\phi\big(\phi(a) \cdot b\big) = q^{dr} \hat{h}_\phi(b).$$

De plus, la hauteur qu'on vient de construire est proche de la hauteur de Weil dans le sens suivant. Il existe $c_1(\phi) > 0$ tel que :

$$\forall x \in \bar{K} \qquad |h(x) - \hat{h}_\phi(x)| \leq c_1(\phi), \tag{2.5}$$

et la constante $c_1(\phi)$ peut être explicitée dans de nombreux cas (voir **[15]**, Théorème 4 et **[25]**, Theorem 1.6). La fonction $\hat{h}_\phi$ satisfait donc elle aussi la propriété de Northcott. Il est alors facile de montrer que la hauteur canonique s'annule exactement en les points de torsion de ϕ.

2.4. Réduction. — Soit $\mathfrak{p}$ un idéal premier de A et $S := A \setminus \mathfrak{p}$. L'idéal $\mathfrak{p}$ est engendré par un élément irréductible (unitaire) $\pi \in A$. On dit que le module ϕ défini par la formule (2.2) est *à coefficients entiers* en $\mathfrak{p}$ si pour tout $0 \leq i \leq d$, on a : $a_i \in S^{-1}A$. On dit qu'un module ψ est à réduction stable en $\mathfrak{p}$ si la classe d'isomorphisme de ψ sur L contient un module ϕ à coefficients $\mathfrak{p}$-entiers. Si on peut trouver un tel ϕ tel qu'en plus : $a_d \notin \mathfrak{p} \cdot S^{-1}A$ — avec les notations de (2.2) — on dit que ψ a *bonne réduction* en $\mathfrak{p}$.

Si ϕ a bonne réduction en $\mathfrak{p}$, on peut le supposer à coefficients $\mathfrak{p}$-entiers (quitte à prendre un module qui lui est isomorphe) et considérer le A-module $\phi_\mathfrak{p}$ défini sur le corps résiduel $A/\mathfrak{p} \simeq \mathbb{F}_{q^{\deg(\mathfrak{p})}}$ — le degré $\deg(\mathfrak{p})$ de $\mathfrak{p}$ étant le degré d'un générateur quelconque de cet idéal — par la formule :

$$\phi_\mathfrak{p}(t) := a_{0,\mathfrak{p}}(t)\tau^0 + \cdots + a_{d,\mathfrak{p}}(t)\tau^d,$$

où $a_{i,\mathfrak{p}}$ est la réduction de a_i modulo $\mathfrak{p}$ (pour $0 \leq i \leq d$). Il s'agit d'un module de Drinfeld de rang d.

2.5. Modules de Drinfeld formels. — Comme dans le cas des variétés abéliennes, il existe un outil puissant pour étudier les propriétés de la réduction en un idéal $\mathfrak{p}$ de A (et en particulier son noyau) : le module de Drinfeld formel. On suit ici [**33**].

Soit $\mathfrak{p}$ un idéal premier de A en lequel ϕ a bonne réduction. Le module ϕ induit alors un morphisme, noté $\hat{\phi}^{\mathfrak{p}}$:

$$A_{\mathfrak{p}} \longrightarrow A_{\mathfrak{p}}\{\{\tau\}\},$$

où $A_{\mathfrak{p}}$ est le complété de A en $\mathfrak{p}$ et $A_{\mathfrak{p}}\{\{\tau\}\}$ est l'anneau des séries formelles (absolument) additives en une variable sur $A_{\mathfrak{p}}$, le produit de deux séries formelles se déduisant de la règle (2.1) sur les monômes. Ce morphisme est construit de la manière suivante. Si $x = \frac{a}{b} \in S^{-1}A$ avec $b \notin \mathfrak{p}$, alors $\phi(b)$ est inversible en tant qu'élément de $S^{-1}A\{\{\tau\}\}$ et on peut poser :

$$\phi(x) := \phi(a)\phi(b)^{-1} \in S^{-1}A\{\{\tau\}\}.$$

Par continuité, ce morphisme s'étend en un morphisme $\hat{\phi}^{\mathfrak{p}}$ défini sur $A_{\mathfrak{p}}$, qui coïncide avec ϕ sur A. Il s'agit d'un $A_{\mathfrak{p}}$-module de Drinfeld formel, appelé complété formel de ϕ en $\mathfrak{p}$. Pour ne pas alourdir les notations, et lorsqu'il n'y aura pas d'ambiguïté sur l'idéal $\mathfrak{p}$, on notera $\hat{\phi}$ le complété formel de ϕ en $\mathfrak{p}$.

L'idéal $\mathfrak{p}A_{\mathfrak{p}}$ est un $A_{\mathfrak{p}}$-module de Drinfeld dont la loi est donnée par $\hat{\phi}$ ([**33**], 4 (1)). Si $a \in S$, le coefficient constant de $\hat{\phi}(a)$ est a, qui est inversible dans $A_{\mathfrak{p}}$. On en déduit que $\hat{\phi}(a) = \phi(a)$ est inversible dans $A_{\mathfrak{p}}\{\{\tau\}\}$, et que $\mathfrak{p}A_{\mathfrak{p}}$ considéré comme A-module n'a pas de $\mathfrak{q}$-torsion, pour un idéal premier $\mathfrak{q} \neq \mathfrak{p}$.

3. Torsion des modules de Drinfeld de rang 2 : aspects galoisiens

Les minorations de hauteurs que nous avons en vue reposent sur des estimations $\mathfrak{p}$-adiques précises, pour un certain idéal premier $\mathfrak{p}$ de A. Ces estimations reflètent des propriétés galoisiennes importantes de la torsion des modules de Drinfeld.

3.1. Modules de Tate et représentations galoisiennes. — On suppose désormais que ϕ est un module de rang 2 sur un A-corps L. Cette situation présente de nombreuses analogies avec celle d'une courbe elliptique définie sur un corps de caractéristique quelconque. On se donne également un premier $\mathfrak{p}$ de A ; son degré sera noté $\deg(\mathfrak{p})$.

Définition 3.1. — Le module de Tate $\mathfrak{p}$-adique de ϕ est la limite projective :

$$T_{\mathfrak{p}}(\phi) := \varprojlim \phi[\pi^n],$$

Le module de Tate $T_{\mathfrak{p}}(\phi)$ est un $A_{\mathfrak{p}}$-module de rang au plus 2. Si L est de caractéristique générique (resp. si $L = A/\mathfrak{q}$, avec $\mathfrak{q} \neq \mathfrak{p}$ un premier de A), ce rang vaut 2. Si $L = A/\mathfrak{p}$, la multiplication par π n'est plus séparable, et le rang chute (voir [**23**], 4.5).

Définition 3.2. — Supposons que $L = A/\mathfrak{p}$. On dit que ϕ est supersingulier si $T_{\mathfrak{p}}(\phi)$ est nul.

Remarque. Si ϕ n'est pas supersingulier, le rang du module de Tate vaut 1, et on dit que ϕ est *ordinaire*. On peut donner d'autres définitions équivalentes de la supersingularité. Par exemple, le module ϕ est supersingulier si et seulement si $\phi(\pi)$ est purement inséparable (*i.e.* est une puissance du Frobenius). Pour d'autres caractérisations impliquant l'anneau des endomorphismes de ϕ, on renvoie à **[20]**, 5.3.

Soit L^{sep} une clôture séparable de L. Le groupe de Galois $\mathrm{Gal}(L^{\mathrm{sep}}/L)$ agit linéairement sur la torsion de ϕ. Supposons ici que L est de caractéristique générique. On obtient alors une représentation :

$$\rho_{\mathfrak{p}^\infty} : \mathrm{Gal}(L^{\mathrm{sep}}/L) \longrightarrow \mathrm{GL}_2(A_{\mathfrak{p}}).$$

Si ϕ n'est pas de type CM, Pink a montré que l'image de cette représentation est ouverte (voir **[29]**). En se restreignant à la $\mathfrak{p}$-torsion, on obtient une autre représentation :

$$\rho_{\mathfrak{p}} : \mathrm{Gal}(L^{\mathrm{sep}}/L) \longrightarrow \mathrm{GL}_2(\mathbb{F}_{\mathfrak{p}}),$$

où $\mathbb{F}_{\mathfrak{p}} = A/\mathfrak{p}$ est le corps résiduel de cardinal $q_{\mathfrak{p}} = q^{\deg(\mathfrak{p})}$. On utilisera le théorème suivant (voir le résultat principal de **[31]**, qui est formulé de manière adélique) :

***Théorème 3.3* (Pink, Rütsche).** — *On suppose que ϕ n'est pas de type CM. Il existe un réel $c_2(\phi)$ tel que si $\deg(\mathfrak{p}) \geq c_2(\phi)$, la représentation $\rho_{\mathfrak{p}}$ est surjective.*

Remarques. Cet énoncé est l'analogue dans le cas drinfeldien des travaux de Serre sur les représentations données par la torsion des courbes elliptiques, dont il reprend la stratégie de preuve (*cf.* **[35]**). Il est encore valable en rang supérieur, et il existe aussi des résultats en caractéristique non générique (*cf.* par exemple **[30]**). Notons que les auteurs ne donnent pas de version explicite de leur théorème. Pour les courbes elliptiques, ce calcul a récemment été fait (voir **[27]**). La question de l'uniformité, qui consiste à chercher une borne indépendante de la courbe elliptique, est encore largement ouverte.

3.2. Distribution des premiers supersinguliers. — On suppose désormais que $L = K$, et on pose :

$$\phi(t) := t + g\tau + \Delta\tau^2,$$

où g, Δ sont dans K et $\Delta \neq 0$. Le j-invariant de ϕ est défini de la façon suivante :

$$j(\phi) := \frac{g^{q+1}}{\Delta} \in K.$$

La quantité $j(\phi)$ détermine ϕ à $\bar{K}$-isomorphisme près (voir **[20]**, Lemma 4.1).

Définition 3.4. — On dit que ϕ est exceptionnel si $tj(\phi)$ est un carré dans $\mathbb{F}_q((1/t))$.

Remarque. On reprend ici la définition de Poonen (**[32]**, 2), qui corrige celle donnée dans **[10]**, 1.

En rang 2, on a des résultats partiels sur la distribution des premiers en lesquels ϕ admet une réduction supersingulière. Cette distribution dépend de l'anneau des endomorphismes de ϕ. Dans le cas CM, l'analogue drinfeldien du critère de Deuring

assure l'existence de nombreux premiers supersinguliers, via l'analogue du théorème de Chebotarev pour les corps de fonctions sur un corps fini (voir [**17**], Theorem 6.3.1).

Théorème 3.5. — *Soit L/K une extension galoisienne finie et $\mathcal{C}$ une classe de conjugaison dans* $\mathrm{Gal}(L/K)$. *L'ensemble des idéaux premiers $\mathfrak{p}$ de $\mathcal{O}_K$ tels que $(\frac{L/K}{\mathfrak{p}}) = \mathcal{C}$ a une densité de Dirichlet, qui est égale à $\frac{|\mathcal{C}|}{[L:K]}$.*

Remarque. Dans cet énoncé, le « symbole d'Artin »$(\frac{L/K}{\mathfrak{p}})$ d'un idéal $\mathfrak{p}$ désigne la classe de conjugaison du Frobenius en un premier quelconque de $\mathcal{O}_L$ au-dessus de $\mathfrak{p}$.

Corollaire 3.6. — *Si le module ϕ est de type CM, il existe une infinité de premiers à réduction supersingulière.*

Démonstration. — Soit L le corps de la multiplication complexe. Le « critère de Deuring »([**10**], Lemma 2.9.3) affirme que les premiers supersinguliers sont ceux qui sont inertes ou ramifiés dans L. Par le Théorème 3.5, ils sont en nombre infini. □

Il est possible de préciser cet énoncé, en utilisant une version effective du théorème de Chebotarev. Si ϕ n'est pas de type CM, on dispose du résultat suivant :

***Théorème 3.7* (Brown)**. — *On suppose que $End(\phi) = A$. Si ϕ n'est pas exceptionnel, il admet une infinité de premiers à réduction supersingulière.*

Remarques. Brown donne en fait une version plus précise de son théorème, où il minore le nombre d'idéaux premiers de degré borné en lesquels la réduction est supersingulière. Cette estimation a ensuite été améliorée par David ([**12**]), en direction de l'analogue drinfeldien de la conjecture de Lang et Trotter. Poonen a construit des modules de Drinfeld en rang 2 n'ayant aucun premier de réduction supersingulière ([**32**], Proposition 1).

3.3. Extensions locales non ramifiées. — Soit $\mathfrak{p}$ un idéal premier de A, et $K_\mathfrak{p}$ le complété de K en $\mathfrak{p}$. Notons par $K_\mathfrak{p}^{\mathrm{sep}}$ une clôture séparable de $K_\mathfrak{p}$. Le corps résiduel $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ est isomorphe à $\mathbb{F}_\mathfrak{p} := \mathbb{F}_{q^{\deg(\mathfrak{p})}}$. Pour tout entier $n \geq 1$, on note $K_{\mathfrak{p}^n}$ la seule extension non ramifiée de $K_\mathfrak{p}$ de degré n dans $\bar{K}_\mathfrak{p}$. L'union :

$$K_\mathfrak{p}^{\mathrm{nr}} := \bigcup_{n\geq 1} K_{\mathfrak{p}^n}$$

est la plus grande extension non ramifiée de $K_\mathfrak{p}$ contenue dans $K_\mathfrak{p}^{\mathrm{sep}}$.

Lemme 3.8. — *On suppose que ϕ a bonne réduction en $\mathfrak{p}$. Soit I un idéal de A premier à $\mathfrak{p}$ et $n \geq 1$ un entier. L'extension $K_{\mathfrak{p}^n}(I)/K_\mathfrak{p}$ est non ramifiée.*

Démonstration. — L'extension $K_{\mathfrak{p}^n}/K_\mathfrak{p}$ étant non ramifiée, on peut supposer que $n = 1$. Quitte à composer les extensions, on peut aussi prendre $I = \mathfrak{l}^m$, où $\mathfrak{l}$ est un premier de A distinct de $\mathfrak{p}$ et $m \geq 1$. La réduction modulo $\mathfrak{p}$ induit un morphisme :

$$T_\mathfrak{l}(\phi) \longrightarrow T_\mathfrak{l}(\phi_\mathfrak{p})$$

dont le noyau est constitué d'éléments de $\mathfrak{l}^\infty$-torsion qui se réduisent sur 0 modulo $\mathfrak{p}$. Comme $\mathfrak{p} \neq \mathfrak{l}$, l'idéal $\mathfrak{p}A_\mathfrak{p}$ n'a pas de $\mathfrak{l}^\infty$-torsion (voir la conclusion du §2.5) et le

morphisme est injectif. Le groupe d'inertie en $\mathfrak{p}$ agit donc trivialement sur $T_{\mathfrak{l}}(\phi)$, et l'extension $K_{\mathfrak{p}}(\mathfrak{l}^m)/K_{\mathfrak{p}}$ est non ramifiée. □

Remarque. De façon équivalente, le lemme affirme que le corps $K_{\mathfrak{p}^n}(I)$ est inclus dans $K_{\mathfrak{p}}^{\mathrm{nr}}$. Pour tout premier $\mathfrak{l}$ de A, on dispose d'une représentation galoisienne :

$$\rho_{\mathfrak{l}^\infty} : \mathrm{Gal}(K_{\mathfrak{p}}^{\mathrm{sep}}/K_{\mathfrak{p}}) \to \mathrm{Aut}_{A_{\mathfrak{l}}} T_{\mathfrak{l}}(\phi).$$

On vient de démontrer que si $\mathfrak{p}$ est un premier de bonne réduction pour ϕ, alors $\rho_{\mathfrak{l}^\infty}$ est non ramifiée en $\mathfrak{p}$ pour tout $\mathfrak{l} \neq \mathfrak{p}$. Le critère de Néron-Ogg-Shafarevich pour les modules de Drinfeld affirme que ces deux propriétés sont en fait équivalentes (*cf.* **[6]**, Theorem 3.2 ou **[36]**, Theorem 1).

3.4. Groupes de ramification supérieure. — On fixe une extension finie L de $K_{\mathfrak{p}}$. Si M est une extension finie de L, on note $\mathcal{O}_M$ l'anneau des entiers de M, et $v : M \to \mathbb{Z}$ la valuation surjective sur M héritée de la valuation $\mathfrak{p}$-adique. On a une filtration du groupe $G := \mathrm{Gal}(M/L)$ donnée par les groupes de ramification, définis pour $i \geq -1$:

$$G_i(M/L) := \{\sigma \in G, \forall a \in \mathcal{O}_M : v(\sigma(a) - a) \geq i + 1\} ;$$

on remarque que $G_{-1}(M/L) = G$ est le groupe de Galois de l'extension, et $G_0(M/L)$ est son groupe d'inertie.

Une extension non ramifiée et une extension totalement ramifiée de L sont linéairement disjointes. Le lemme classique suivant précise le lien entre de telles extensions.

Lemme 3.9. — *Soient M et N deux extensions galoisiennes finies de L telles que M/L soit totalement ramifiée et N/L soit non ramifiée.*

1. *On a $M \cap N = L$ et l'application :*

$$\begin{array}{ccc} \mathrm{Gal}(MN/L) & \longrightarrow & \mathrm{Gal}(M/L) \times \mathrm{Gal}(N/L) \\ \sigma & \mapsto & (\sigma_{|M}, \sigma_{|N}) \end{array}$$

   est un isomorphisme de groupes.

2. *L'extension MN/M est non ramifiée de degré $[N : L]$ et l'extension MN/N est totalement ramifiée de degré $[M : L]$.*

3. *Soit $i \geq -1$. Si $\sigma \in \mathrm{Gal}(MN/N) \cap G_i(MN/L)$, alors $\sigma_{|M} \in G_i(M/L)$. De plus, l'application qui en résulte :*

$$\mathrm{Gal}(MN/N) \cap G_i(MN/L) \longrightarrow G_i(M/L)$$

   est un isomorphisme de groupes.

Démonstration. — La preuve du Lemma 2.1 de **[24]** s'adapte ici *mutatis mutandis*. Pour le premier point, il suffit de voir que l'extension de corps locaux $(M \cap N)/L$ est à la fois non ramifiée et totalement ramifiée, donc triviale. L'isomorphisme s'en déduit immédiatement.

Il suit de cela que l'extension MN/N est galoisienne, de groupe de Galois isomorphe à $\mathrm{Gal}(M/L)$. En particulier : $e := [MN : N] = [M : L]$. Le même argument montre que MN/M est une extension de degré $f := [N : L]$. On observe que MN/N et

MN/L ont le même indice de ramification e' car N/L est non ramifiée. Il en résulte : $e' \geq e$. Comme par ailleurs : $e' \leq [MN : N] = e$, on voit que $e' = e$ et que MN/N est totalement ramifiée. De même, l'extension MN/M est non ramifiée, ce qui achève de prouver le deuxième point.

Soit $\pi \in \mathcal{O}_M$ une uniformisante et soient $x_1, \ldots, x_f \in \mathcal{O}_N$ des relèvements d'une base vectorielle de l'extension résiduelle associée à N/L. On note $\mathcal{O} := \mathcal{O}_{MN}$. Par **[28]**, Proposition II.6.8 (et la remarque qui suit la preuve concernant les extensions inséparables), nous avons l'égalité suivante :

$$\mathcal{O} = \sum_{l=0}^{e-1} \sum_{m=1}^{f} \pi^l x_m \mathcal{O}_L.$$

On note w l'unique extension de la valuation surjective : $L \to \mathbb{Z} \cup \{\infty\}$ à une valuation surjective : $MN \to e^{-1}\mathbb{Z} \cup \{\infty\}$. Supposons que $\sigma \in \mathrm{Gal}(MN/N) \cap G_i(MN/L)$. Alors pour tout $a \in \mathcal{O}$:

$$e \cdot w(\sigma(a) - a) \geq i + 1,$$

car MN/L a un indice de ramification égal à e. D'autre part, M/L a aussi un indice de ramification égal à e, donc $\sigma_{|M} \in G_i(M/L)$, ce qui prouve la première partie du troisième point.

L'injectivité du morphisme suit du premier point. Il reste à prouver que tout $\sigma' \in G_i(M/L)$ appartient à l'image de ce morphisme. Par le premier point, il existe un unique relèvement $\sigma \in \mathrm{Gal}(MN/N)$ tel que $\sigma_{|M} = \sigma'$. Prouvons que $\sigma \in G_i(MN/L)$.

Soit $a \in \mathcal{O}$. Par la décomposition de $\mathcal{O}$, on peut écrire :

$$a = \sum_{l,m} \pi^l x_m a_{l,m},$$

avec $a_{l.m} \in \mathcal{O}_L$. On observe que :

$$e \cdot w(\sigma(\pi^l) - \pi^l) = e \cdot w(\sigma'(\pi^l) - \pi^l) \geq i + 1,$$

car $\pi \in \mathcal{O}_M$. L'inégalité triangulaire ultramétrique nous donne alors :

$$\begin{aligned} e \cdot w(\sigma(a) - a) &= e \cdot w\Big(\sum_{l,m} (\sigma(\pi^l x_m a_{l,m}) - \pi^l x_m a_{l,m}\Big) \\ &= e \cdot w\Big(\sum_{l,m} ((\sigma(\pi^l) - \pi^l) x_m a_{l.m})\Big) \\ &\geq \min_{l,m} \{e \cdot w((\sigma(\pi^l) - \pi^l) x_m a_{l,m})\} \geq i + 1, \end{aligned}$$

donc $\sigma \in G_i(MN/L)$ et le lemme est entièrement démontré. □

3.5. Extensions totalement ramifiées en un premier supersingulier. — On donne maintenant une description explicite de certaines extensions locales totalement ramifiées et de leurs groupes de ramification supérieure. En un premier de réduction supersingulière, on peut y parvenir en utilisant la théorie des modules de Lubin-Tate.

On fixe pour ce paragraphe un premier $\mathfrak{p} := \pi A$ de bonne réduction supersingulière pour ϕ. Les propriétés galoisiennes qui nous intéressent supposent de se placer au-dessus de l'extension non ramifiée $K_\mathfrak{q} := K_{\mathfrak{p}^2}$ de $K_\mathfrak{p}$. On notera $\mathbb{F}_\mathfrak{q}$ et $\mathbb{F}_\mathfrak{p}$ leurs corps résiduels respectifs, ainsi que $q_\mathfrak{q} = q^{2\deg(\mathfrak{p})}$ et $q_\mathfrak{p} = q^{\deg(\mathfrak{p})}$ les ordres de ces corps.

Le groupe $\mathrm{Gal}(K_\mathfrak{p}^{\mathrm{nr}}/K_\mathfrak{p})$ ayant un sous-groupe d'inertie trivial, il contient un unique relèvement du morphisme de Frobenius d'ordre $q_\mathfrak{p}$ (resp. $q_\mathfrak{q}$), qu'on notera $F_\mathfrak{p}$ (resp. $F_\mathfrak{q}$). Si $\mathfrak{l} \neq \mathfrak{p}$ est un autre idéal premier de A, le morphisme $F_\mathfrak{q}$ agit $A_\mathfrak{l}$-linéairement sur le module de Tate $T_\mathfrak{l}(\phi)$ via $\rho_\mathfrak{l}$. Les coefficients du polynôme caractéristique de $\rho_\mathfrak{l}(F_\mathfrak{q})$ ne dépendent pas du choix de $\mathfrak{l} \neq \mathfrak{p}$. Quitte à choisir un autre générateur pour $\mathfrak{p}$, on peut écrire ce polynôme sous la forme suivante :

$$\chi_{\phi,\mathfrak{p}}(X) = X^2 - a_\mathfrak{p} X - \pi,$$

et la trace $a_\mathfrak{p}$ est un élément de A qui satisfait à :

$$\deg(a_\mathfrak{p}) \leq \frac{\deg(\pi)}{2} = \frac{\deg(\mathfrak{p})}{2},$$

par **[20]**, Proposition 5.1. Comme $\mathfrak{p}$ est supersingulier, on a aussi : $a_\mathfrak{p} \equiv 0 \pmod{\mathfrak{p}}$, ce qui force : $a_\mathfrak{p} = 0$ (*cf.* **[20]**, Lemma 5.2). Par le théorème de Cayley-Hamilton, on en déduit que pour tout idéal premier $\mathfrak{l} \neq \mathfrak{p}$ de A :

$$\rho_\mathfrak{l}(F_\mathfrak{q}) = \rho_\mathfrak{l}(F_\mathfrak{p})^2 = \pi. \tag{3.1}$$

Soit $n \geq 1$ un entier fixé. On peut désormais décrire précisément la structure galoisienne des extensions de $K_\mathfrak{q}$ engendrées par la $\mathfrak{p}^n$-torsion. On rappelle que $\mathbb{F}_q$ est un corps fini de degré ν sur son corps premier $\mathbb{F}_p$.

Lemme 3.10. — *1. L'extension $K_\mathfrak{q}(\mathfrak{p}^n)/K_\mathfrak{q}$ est totalement ramifiée de degré $q_\mathfrak{q}^{n-1} \cdot (q_\mathfrak{q} - 1)$, et son groupe de Galois est donné par :*

$$\mathrm{Gal}(K_\mathfrak{q}(\mathfrak{p}^n)/K_\mathfrak{q}) \cong \mathbb{Z}/(q_\mathfrak{q} - 1)\mathbb{Z} \times (\mathbb{Z}/p^{n-1}\mathbb{Z})^{2\deg(\mathfrak{p})\nu}.$$

2. Soit $1 \leq k \leq n$ et i tel que $q_\mathfrak{q}^{k-1} \leq i \leq q_\mathfrak{q}^k - 1$. On a :

$$G_i(K_\mathfrak{q}(\mathfrak{p}^n)/K_\mathfrak{q}) \cong \mathrm{Gal}(K_\mathfrak{q}(\mathfrak{p}^n)/K_\mathfrak{q}(\mathfrak{p}^k)) \cong (\mathbb{Z}/p^{n-k}\mathbb{Z})^{2\deg(\mathfrak{p})\nu}.$$

3. Soit I un idéal de A premier à $\mathfrak{p}$. L'image de la représentation galoisienne :

$$\mathrm{Gal}(K_\mathfrak{q}(\mathfrak{p}^n)/K_\mathfrak{q}) \to \mathrm{Aut}_{A_\mathfrak{q}} \phi[\mathfrak{p}^n]$$

contient la multiplication par les éléments de $\phi(I)$ et agit transitivement sur $\phi[\mathfrak{p}^n]$.

Démonstration. — On note $A_\mathfrak{q}$ la fermeture intégrale de $A_\mathfrak{p}$ dans $K_\mathfrak{q}$. Soit

$$\hat{\phi}_\mathfrak{p} : A_\mathfrak{p} \longrightarrow A_\mathfrak{p}\{\{\tau\}\} \subset A_\mathfrak{q}[[x]]$$

le complété formel de ϕ en $\mathfrak{p}$ (voir §2.5). Comme $\hat{\phi}_\mathfrak{p}$ s'identifie à ϕ sur A, on a :

$$\hat{\phi}_\mathfrak{p}(\pi) - \pi x \quad \in \quad x^2 A_\mathfrak{q}[[x]].$$

Si $\mathfrak{l} \neq \mathfrak{p}$ est un premier de A, l'application naturelle :

$$\mathrm{End}(\phi_\mathfrak{p}) \otimes A_\mathfrak{l} \to \mathrm{End}_{A_\mathfrak{l}}(T_\mathfrak{l}(\phi_\mathfrak{p}))$$

est injective (voir [**20**], la remarque qui précède la Proposition 5.1, et qui est une conséquence du Lemma 2.2). En réduisant (3.1) modulo $\mathfrak{p}$, on en déduit :

$$\hat{\phi}_{\mathfrak{p}}(\pi) - x^{q_{\mathfrak{q}}} \quad \in \quad \mathfrak{p}A_{\mathfrak{q}}[[x]].$$

Le module formel $\hat{\phi}_{\mathfrak{p}}$ est donc un module de Lubin-Tate pour l'idéal premier $\mathfrak{p} \cdot A_{\mathfrak{q}}$ de $A_{\mathfrak{q}}$ (*cf.* [**28**] V, Definition 4.5). Comme ϕ a réduction supersingulière en $\mathfrak{p}$, on a : $T_{\mathfrak{p}}(\phi) = 0$. Il en résulte que $K_{\mathfrak{q}}(\mathfrak{p}^n)$ est le corps des points de π^n-division du module de Lubin-Tate $\hat{\phi}_{\mathfrak{p}}$.

On peut appliquer le Theorem 5.4 de [**28**] V, qui affirme que l'extension $K_{\mathfrak{q}}(\mathfrak{p}^n)/K_{\mathfrak{q}}$ est totalement ramifiée de degré $(q_{\mathfrak{q}} - 1)q_{\mathfrak{q}}^{n-1}$, et que :

$$\mathrm{Gal}(K_{\mathfrak{q}}(\mathfrak{p}^n)/K_{\mathfrak{q}}) \cong A_{\mathfrak{q}}^{\times}/A_{\mathfrak{q}}^{(n)},$$

où $A_{\mathfrak{q}}^{(n)}$ est le groupe des n-unités de $A_{\mathfrak{q}}^{\times}$. On a une suite exacte :

$$1 \to A_{\mathfrak{q}}^{(1)}/A_{\mathfrak{q}}^{(n)} \to A_{\mathfrak{q}}^{\times}/A_{\mathfrak{q}}^{(n)} \to A_{\mathfrak{q}}^{\times}/A_{\mathfrak{q}}^{(1)} \to 1.$$

Par la Proposition 3.10 de [**28**] II (on renvoie au paragraphe précédant cette proposition pour la définition du groupe des n-unités), le quotient de droite est isomorphe au groupe multiplicatif de $\mathbb{F}_{\mathfrak{q}}$, qui est cyclique d'ordre $q_{\mathfrak{q}} - 1$; et les quotients successifs $A_{\mathfrak{q}}^{(k)}/A_{\mathfrak{q}}^{(k+1)}$ sont tous isomorphes au groupe additif de $\mathbb{F}_{\mathfrak{q}}$, qui est un espace vectoriel de dimension $2\deg(\mathfrak{p})\nu$ sur son corps premier $\mathbb{F}_p$. Par une récurrence immédiate, le quotient de gauche est isomorphe à $(\mathbb{Z}/p^{n-1}\mathbb{Z})^{2\deg(\mathfrak{p})\nu}$. La suite exacte est scindée, car les quotients considérés sont d'ordres premiers entre eux. Le point 1 est donc entièrement démontré.

Le premier isomorphisme du point 2 est la Proposition 6.1 de [**28**] V, et le second est une conséquence du point 1 (en considérant le quotient du groupe de Galois de la n-division par le groupe de Galois de la k-division).

Pour le point 3, on considère le morphisme induit par la loi de réciprocité locale :

$$(\cdot, K_{\mathfrak{q}}(\mathfrak{p}^n)/K_{\mathfrak{q}}) : K_{\mathfrak{q}}(\mathfrak{p}^n)^* \longrightarrow \mathrm{Gal}(K_{\mathfrak{q}}(\mathfrak{p}^n)/K_{\mathfrak{q}}).$$

Tout élément $a \in I$ est une unité dans $A_{\mathfrak{q}}$ et par [**28**] V, Theorem 5.5, on a :

$$\forall b \in K_{\mathfrak{q}}(\mathfrak{p}^n) \quad : \quad (a^{-1}, K_{\mathfrak{q}}(\mathfrak{p}^n)/K_{\mathfrak{q}})(b) = \phi(a) \cdot b.$$

La Proposition 5.2 de [**28**] V montre que $\mathfrak{p}^n$ est un $A_{\mathfrak{q}}/\mathfrak{p}^n A_{\mathfrak{q}}$-module libre de rang 1, sur lequel le groupe de Galois agit linéairement et transitivement. □

3.6. Extensions locales engendrées par un idéal de torsion. — On peut désormais traiter le cas « mixte » des extensions locales engendrées par un idéal de torsion quelconque. Soit J un idéal de A premier avec $\mathfrak{p}$; on note $I := \mathfrak{p}^n J$, pour un entier $n \geq 0$.

Lemme 3.11. — *1. Le compositum $K_{\mathfrak{q}}(\mathfrak{p}^n)K_{\mathfrak{q}}(J)$ est égal à $K_{\mathfrak{q}}(I)$.*

2. L'extension $K_{\mathfrak{q}}(I)/K_{\mathfrak{q}}(\mathfrak{p}^n)$ est non ramifiée et l'extension $K_{\mathfrak{q}}(I)/K_{\mathfrak{q}}(J)$ est totalement ramifiée.

3. *La restriction à $K_{\mathfrak{q}}(\mathfrak{p}^n)$ induit un isomorphisme de groupes :*

$$\mathrm{Gal}(K_{\mathfrak{q}}(I)/K_{\mathfrak{q}}(J)) \xrightarrow{\sim} \mathrm{Gal}(K_{\mathfrak{q}}(\mathfrak{p}^n)/K_{\mathfrak{q}}).$$

En particulier, l'extension $K_{\mathfrak{q}}(I)/K_{\mathfrak{q}}(J)$ est abélienne.

4. *On suppose que $n \geq 1$. Alors :*

$$\mathrm{Gal}(K_{\mathfrak{q}}(I)/K_{\mathfrak{q}}(I/\mathfrak{p})) \cong \begin{cases} (\mathbb{Z}/p\mathbb{Z})^{2\deg(\mathfrak{p})\nu} & \text{si} \quad n \geq 2 \\ \mathbb{Z}/(q_{\mathfrak{q}}-1)\mathbb{Z} & \text{si} \quad n = 1. \end{cases}$$

Démonstration. — Par Bézout, on a une décomposition de A-modules :

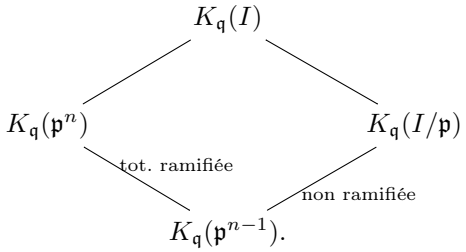
$$\phi[I] = \phi[\mathfrak{p}^n] \oplus \phi[J],$$

ce qui démontre le premier point.

Le second point suit du Lemme 3.9 (2), combiné respectivement avec le Lemme 3.8 pour la partie non ramifiée, et avec le Lemme 3.10 (1) pour la partie totalement ramifiée.

L'isomorphisme du troisième point est une conséquence immédiate du Lemme 3.9 (1), et l'extension considérée est abélienne par le Lemme 3.10 (1).

Passons au dernier point. On a : $K_{\mathfrak{q}}(I/\mathfrak{p}) = K_{\mathfrak{q}}(\mathfrak{p}^{n-1})K_{\mathfrak{q}}(J)$ par le premier point. Le second point nous donne le diagramme suivant :



Par le Lemme 3.9 (1), la restriction donne un isomorphisme :

$$\mathrm{Gal}(K_{\mathfrak{q}}(I)/K_{\mathfrak{q}}(I/\mathfrak{p})) \cong \mathrm{Gal}(K_{\mathfrak{q}}(\mathfrak{p}^n)/K_{\mathfrak{q}}(\mathfrak{p}^{n-1})).$$

Il suffit alors d'appliquer le Lemme 3.10 (1) dans le cas $n = 1$ et (2) dans le cas $n \geq 2$ pour conclure. □

4. Hauteur de Weil sur les corps engendrés par la torsion

On donne maintenant une borne inférieure pour la hauteur de Weil sur les éléments d'ordre infini de l'extension K_{tors} de K engendrée par la torsion de ϕ sur $\bar{K}$. Celle-ci est en grande partie basée sur des estimations $\mathfrak{p}$-adiques traduisant les propriétés galoisiennes énoncées dans la partie précédente. Dans le cas des extensions non ramifiées en un premier $\mathfrak{p}$ de réduction supersingulière dont le degré est borné, l'information $\mathfrak{p}$-adique s'avère suffisante. Dans le « cas ramifié », plus délicat, on devra faire une descente sur la torsion et utiliser des résultats assez fins de théorie des groupes.

4.1. Borne pour la hauteur de Weil dans le cas non ramifié. — On suppose dans ce paragraphe que le module ϕ admet un premier $\mathfrak{p} = \pi A$ de réduction supersingulière, et on considère un idéal I de A premier à $\mathfrak{p}$. On note $|\cdot|_\mathfrak{p} := q^{-v_\mathfrak{p}(\cdot)}$ la norme sur le corps local $K_\mathfrak{q}(I)$ et $\mathcal{O}$ son anneau d'entiers. L'estimation métrique suivante reflète les propriétés du morphisme de Frobenius dans le cas non ramifié.

Lemme 4.1. — *Pour tout $\alpha \in K_\mathfrak{q}(I)$, on a :*

$$|F_\mathfrak{q}(\alpha) - \alpha^{q_\mathfrak{q}}|_\mathfrak{p} \leq q^{-1} \max\{1, |F_\mathfrak{q}(\alpha)|_\mathfrak{p}\} \max\{1, |\alpha|_\mathfrak{p}\}^{q_\mathfrak{q}}.$$

Démonstration. — Par le Lemme 3.8, l'extension locale $K_\mathfrak{q}(I)/K_\mathfrak{q}$ est non ramifiée. On distingue deux cas, selon que α appartient ou non à $\mathcal{O}$. Si c'est le cas, on a : $|\alpha|_\mathfrak{p} \leq 1$ et $F_\mathfrak{q}(\alpha) - \alpha^{q_\mathfrak{q}} \in \mathfrak{p}\mathcal{O}$. Il vient :

$$|F_\mathfrak{q}(\alpha) - \alpha^{q_\mathfrak{q}}|_\mathfrak{p} \leq |\pi|_\mathfrak{p} = q^{-1},$$

et l'inégalité annoncée est vraie dans ce cas. Si $\alpha \notin \mathcal{O}$, alors $\alpha^{-1} \in \mathcal{O}$ et :

$$|F_\mathfrak{q}(\alpha^{-1}) - \alpha^{-q_\mathfrak{q}}|_\mathfrak{p} \leq q^{-1}.$$

On obtient alors :

$$|\alpha^{-q_\mathfrak{q}}(F_\mathfrak{q}(\alpha) - \alpha^{q_\mathfrak{q}})|_\mathfrak{p} = |(F_\mathfrak{q}(\alpha^{-1}) - \alpha^{-q_\mathfrak{q}})\, F_\mathfrak{q}(\alpha)|_\mathfrak{p} \leq q^{-1}\, |F_\mathfrak{q}(\alpha)|_\mathfrak{p},$$

et l'inégalité du lemme est encore vérifiée. □

On est en mesure de donner une première borne pour la hauteur. L'argument crucial dont on se sert ici est que dans le cas supersingulier, le relèvement du Frobenius est dans le centre du groupe $\mathrm{Gal}(K(I)/K)$, ce qui a pour effet de propager à toute l'orbite galoisienne la propriété $\mathfrak{p}$-adique donnée par le lemme précédent.

Proposition 4.2. — *Si $\mathfrak{p}$ est un premier où ϕ a réduction supersingulière et I un idéal de A premier à $\mathfrak{p}$, pour tout $\alpha \in K(I)^*$ non constant :*

$$h(\alpha) \geq \frac{\deg(\mathfrak{p})}{q^{2\deg(\mathfrak{p})} + 1}.$$

Démonstration. — On commence par fixer une place $v|\mathfrak{p}$ de $K(I)$ et on note $F_\mathfrak{q}$ le morphisme de Frobenius d'ordre $q_\mathfrak{q}$ associé. Soit $\mathfrak{l}$ un diviseur premier de I et $m \geq 1$ un entier. Par (3.1), le morphisme $F_\mathfrak{q}$ agit sur $\phi[\mathfrak{l}^m]$ comme la multiplication par π. Le lemme de Bézout montre que le module $\phi[I]$ est une somme directe de tels modules. Comme $F_\mathfrak{q}$ agit linéairement sur $\phi[I]$, on en déduit que $F_\mathfrak{q}$ appartient au centre de $\mathrm{Gal}(K(I)/K)$.

On considère $\beta := F_\mathfrak{q}(\alpha) - \alpha^{q_\mathfrak{q}} \in K(I)$, et on remarque d'abord que $\beta \neq 0$. Si β était nul, comme la hauteur est invariante sous Galois, on aurait :

$$h(\alpha) = h(F_\mathfrak{q}(\alpha)) = h(\alpha^{q_\mathfrak{q}}) = q_\mathfrak{q} h(\alpha),$$

puis : $h(\alpha) = 0$, ce qui est impossible car on a supposé que α est d'ordre infini pour la structure multiplicative. On peut donc appliquer la formule du produit (2.3) à β :

$$\sum_{w \in M(K(I))} n_w w(\beta) = - \sum_{w \in M(K(I))} n_w \log_q |\beta|_w = 0. \tag{4.1}$$

Puisque l'extension $K(I)/K$ est galoisienne (voir le Lemme 2.2), pour $w|\mathfrak{p}$ une place de $K(I)$, on peut trouver $\sigma \in \mathrm{Gal}(K(I)/K)$ tel que $w = \sigma^{-1}v$. Comme $F_\mathfrak{q}$ et σ commutent, on a :

$$|\beta|_w = |\sigma F_\mathfrak{q}(\alpha) - \sigma(\alpha^{q_\mathfrak{q}})|_v = |F_\mathfrak{q}(\sigma\alpha) - (\sigma\alpha)^{q_\mathfrak{q}}|_v.$$

On peut maintenant estimer le terme de droite avec le Lemme 4.1 :

$$\begin{aligned}|\beta|_w &\leq q^{-1}\max\{1, |F_\mathfrak{q}(\sigma\alpha)|_v\}\max\{1, |\sigma\alpha|_v\}^{q_\mathfrak{q}}\\ &= q^{-1}\max\{1, |\sigma F_\mathfrak{q}(\alpha)|_v\}\max\{1, |\sigma\alpha|_v\}^{q_\mathfrak{q}}\\ &= q^{-1}\max\{1, |F_\mathfrak{q}(\alpha)|_w\}\max\{1, |\alpha|_w|\}^{q_\mathfrak{q}}.\end{aligned}$$

Si $w \nmid \mathfrak{p}$ est une autre place de $K(I)$, l'inégalité ultramétrique donne immédiatement :

$$|\beta|_w \leq \max\{|F_\mathfrak{q}(\alpha)|_w, |\alpha^{q_\mathfrak{q}}|_w\} \leq \max\{1, |F_\mathfrak{q}(\alpha)|_w\}\max\{1, |\alpha|_w\}^{q_\mathfrak{q}}.$$

Avec la formule (4.1), on obtient finalement :

$$\begin{aligned}0 &= \sum_{w|\mathfrak{p}} n_w \log_q|\beta|_w + \sum_{w\nmid\mathfrak{p}} n_w \log_q|\beta|_w\\ &\leq -\sum_{w|\mathfrak{p}} n_w\log_q(q) + \sum_{w\in M(K(I))} n_w \log_q\big(\max\{1, |F_\mathfrak{q}(\alpha)|_w\}\max\{1, |\alpha|_w\}^{q_\mathfrak{q}}\big).\end{aligned}$$

On divise par $[K(I) : K]$ et on utilise l'égalité $\sum_{w|\mathfrak{p}} n_w = \deg(\mathfrak{p})[K(I) : K]$ pour trouver :

$$\deg(\mathfrak{p}) \leq h(F_\mathfrak{q}(\alpha)) + q_\mathfrak{q} h(\alpha),$$

Puisque la hauteur est invariante sous l'action de Galois, l'inégalité du lemme suit immédiatement. □

4.2. Cas ramifié : estimation métrique et première globalisation. — On suppose encore ici que ϕ admet un premier supersingulier $\mathfrak{p} = \pi A$, mais on prend cette fois un idéal I de A divisible par $\mathfrak{p}$. Soit $\mathfrak{P}$ l'idéal maximal de l'anneau des entiers de $K_\mathfrak{q}(I)$ et $e_{\mathfrak{P}|\mathfrak{p}}$ l'indice de ramification de $\mathfrak{P}$ sur $\mathfrak{p}$. On obtient une propriété $\mathfrak{P}$-adique impliquant des éléments du groupe de ramification maximale.

Lemme 4.3. — *Soit $\alpha \in K_\mathfrak{q}(I)$. Si $\psi \in \mathrm{Gal}\big(K_\mathfrak{q}(I)/K_\mathfrak{q}(I/\mathfrak{p})\big)$, on a :*

$$|\psi(\alpha) - \alpha|_\mathfrak{P} \leq q^{\frac{-e_{\mathfrak{P}|\mathfrak{p}}}{q_\mathfrak{q}-1}}\ \max\{1, |\psi(\alpha)|_\mathfrak{P}\}\ \max\{1, |\alpha|_\mathfrak{P}\}.$$

Démonstration. — Soit n la puissance maximale de $\mathfrak{p}$ dans la décomposition de I en facteurs premiers. Notons $L := K_\mathfrak{q}(\mathfrak{p}^n)$ et $M := K_\mathfrak{q}(I/\mathfrak{p}^n)$. Par le point 1 du Lemme 3.11, on a : $LM = K_\mathfrak{q}(I)$, et par le point 2, on sait que $K_\mathfrak{q}(I)/L$ est non ramifiée.

On suppose d'abord que α est un entier dans $K_\mathfrak{q}(I)$. On a :

$$\psi_{|L} \in \mathrm{Gal}(L/K_\mathfrak{q}(\mathfrak{p}^{n-1})),$$

et par le point 2 du Lemme 3.10, on peut supposer que $\psi_{|L}$ appartient au groupe de ramification $G_i(L/K_\mathfrak{q})$, avec $i = q_\mathfrak{q}^{n-1} - 1$ (cet indice de ramification étant maximal).

Le morphisme ψ est l'unique relèvement de $\psi_{|L}$ à $K_{\mathfrak{q}}(I)$ qui se restreint à l'identité sur M. Par le point 3 du Lemme 3.9, on en déduit que $\psi \in G_i(K_{\mathfrak{q}}(I)/K_{\mathfrak{q}})$, ce qui implique :

$$\psi(\alpha) - \alpha \in \mathfrak{P}^{q_{\mathfrak{q}}^{n-1}}.$$

Le point 1 du Lemme 3.10 et le point 3 du Lemme 3.11 donnent : $e_{\mathfrak{P}|\mathfrak{p}} = q_{\mathfrak{q}}^{n-1}(q_{\mathfrak{q}}-1)$. On a donc :

$$|\psi(\alpha) - \alpha|_{\mathfrak{P}} \leq q^{-q_{\mathfrak{q}}^{n-1}} = q^{\frac{-e_{\mathfrak{P}|\mathfrak{p}}}{q_{\mathfrak{q}}-1}},$$

et le lemme est démontré dans ce cas.

Si α n'est pas entier dans $K_{\mathfrak{q}}(I)$, on applique la dernière égalité à α^{-1} et on a :

$$|\alpha^{-1}(\psi(\alpha) - \alpha)|_{\mathfrak{P}} = |\psi(\alpha)(\psi(\alpha^{-1}) - \alpha^{-1})|_{\mathfrak{P}} \leq q^{\frac{-e_{\mathfrak{P}|\mathfrak{p}}}{q_{\mathfrak{q}}-1}} |\psi(\alpha)|_{\mathfrak{P}},$$

ce qui achève la preuve. □

L'extension $K(I)/K$ est galoisienne et le groupe $H := \mathrm{Gal}(K(I)/K(I/\mathfrak{p}))$ est distingué dans $G := \mathrm{Gal}(K(I)/K)$. Soit

$$\rho_{\mathfrak{p}^n} : \mathrm{Gal}(K^{\mathrm{sep}}/K) \longrightarrow \mathrm{GL}_2(A/\mathfrak{p}^n).$$

la représentation galoisienne associée à la $\mathfrak{p}^n$-torsion. Si $\sigma \in H$, alors :

$$\rho_{\mathfrak{p}^n}(\sigma) = I_2 + \pi^{n-1}\mathcal{M}_\sigma,$$

où $\mathcal{M}_\sigma \in \mathrm{M}_2(A)$ est bien définie modulo $\mathfrak{p}$. On en déduit une injection $\mathcal{M} : H \hookrightarrow \mathrm{M}_2(\mathbb{F}_{\mathfrak{p}})$, et on a en particulier :

$$|H| \leq q_{\mathfrak{p}}^4.$$

Dès que $n \geq 2$, on a :

$$\begin{aligned} \rho_{\mathfrak{p}^n}(\sigma\sigma') &= (I_2 + \pi^{n-1}\mathcal{M}_\sigma)(I_2 + \pi^{n-1}\mathcal{M}_{\sigma'}) \\ &= I_2 + \pi^{n-1}(\mathcal{M}_\sigma + \mathcal{M}_{\sigma'}) + \pi^n M', \end{aligned}$$

avec $M' \in \mathrm{M}_2(A)$. L'application $\mathcal{M}$ est donc un morphisme de groupes.

On se donne désormais une place $v|\mathfrak{p}$ dans $K(I)$, et un élément ψ du groupe de décomposition H_v en v de H. Afin de propager la propriété métrique obtenue à un nombre suffisant de places au-dessus de $\mathfrak{p}$, on va minorer la taille de l'orbite O_v de v sous l'action du centralisateur :

$$C(\psi) := \{\sigma \in G, \sigma\psi = \psi\sigma\}.$$

Ceci est possible car $\psi \in H$, qui est un sous-groupe distingué de G suffisamment petit.

Lemme 4.4. — *On a la minoration suivante :*

$$|O_v| \geq \frac{1}{q_{\mathfrak{p}}^4} \frac{[K(I) : K]}{[K_{\mathfrak{p}}(I) : K_{\mathfrak{p}}]}.$$

Démonstration. — Le groupe $C(\psi)$ est le stabilisateur de ψ pour l'action de G sur lui-même par conjugaison, et l'orbite de ψ pour cette action est contenue dans H. Il suit :

$$|C(\psi)| \geq \frac{|G|}{|H|} \geq \frac{[K(I) : K]}{q_{\mathfrak{p}}^4}.$$

Comme l'extension $K(I)/K$ est galoisienne, le nombre total des places de $K(I)$ divisant $\mathfrak{p}$ est donné par le quotient :

$$\frac{[K(I):K]}{[K_{\mathfrak{p}}(I):K_{\mathfrak{p}}]}.$$

Le groupe G agit transitivement sur les places de $K(I)$ divisant $\mathfrak{p}$, et on obtient :

$$|O_v| \geq \frac{1}{[G:C(\psi)]} \frac{[K(I):K]}{[K_{\mathfrak{p}}(I):K_{\mathfrak{p}}]} \geq \frac{1}{q_{\mathfrak{p}}^4} \frac{[K(I):K]}{[K_{\mathfrak{p}}(I):K_{\mathfrak{p}}]}.$$

□

On peut donner une première minoration conditionnelle de la hauteur dans le cas ramifié. Les exceptions sont les points qui sont définis sur une extension *locale* moins ramifiée. L'étape suivante consistera à globaliser cette descente sur la torsion. Pour simplifier les notations, on suppose que $K(I)$ est plongé dans $K_{\mathfrak{p}}^{\mathrm{sep}}$ de telle sorte que $|\cdot|_{\mathfrak{p}}$ corresponde à la place v qu'on a fixée.

Proposition 4.5. — *Si $\mathfrak{p}$ est un premier où ϕ a réduction supersingulière et I est un idéal de A divisible par $\mathfrak{p}$, pour tout $\alpha \in K(I) \setminus K_{\mathfrak{q}}(I/\mathfrak{p})$:*

$$h(\alpha) \geq \frac{\deg(\mathfrak{p})}{2q^{6\deg(\mathfrak{p})}}.$$

Démonstration. — Par hypothèse, on peut choisir $\psi \in H_v$ tel que : $\psi(\alpha) \neq \alpha$. On pose :

$$\beta := \psi(\alpha) - \alpha.$$

Cet élément est dans $K(I)$ qui est une extension galoisienne de K. On peut appliquer la formule (2.3) :

$$\sum_{w \in M(K(I))} n_w \log_q |\beta|_w = 0.$$

Si $w \in O_v$, on pose : $w = \sigma^{-1}v$, avec $\sigma \in C(\psi)$. On a alors :

$$|\beta|_w = |\sigma\psi(\alpha) - \sigma\alpha|_v = |\psi(\sigma\alpha) - \sigma\alpha|_v$$

On peut maintenant utiliser le Lemme 4.3, ce qui donne :

$$\begin{aligned} |\beta|_w &\leq q^{\frac{-e_{w|\mathfrak{p}}}{q_{\mathfrak{q}}-1}} \max\{1, |\psi(\sigma\alpha)|_v\} \max\{1, |\sigma\alpha|_v\} \\ &= q^{\frac{-e_{w|\mathfrak{p}}}{q_{\mathfrak{q}}-1}} \max\{1, |\psi(\alpha)|_w\} \max\{1, |\alpha|_w\}. \end{aligned}$$

Si w est une autre place de $K(I)$, l'inégalité ultramétrique donne immédiatement :

$$|\beta|_w \leq \max\{1, |\psi(\alpha)|_w\} \max\{1, |\alpha|_w\}.$$

On en déduit l'inégalité suivante, par la formule (2.3) :

$$\frac{1}{q_{\mathfrak{q}}-1} \sum_{w \in O_v} n_w e_{w|\mathfrak{p}} \leq \sum_{w \notin O_v} n_w \log_q(\max\{1, |\psi(\alpha)|_w\} \max\{1, |\alpha|_w\}).$$

Comme l'extension $K(I)/K$ est galoisienne, on a $n_w = n_v$ pour toute place $w \in O_v$. Par le Lemme 4.4, il en résulte :

$$\frac{\deg(\mathfrak{p})}{q_{\mathfrak{p}}^4(q_{\mathfrak{q}}-1)} \leq \frac{1}{[K(I):K]} \sum_{w \in M(K(I))} n_w \log_q(\max\{1, |\psi(\alpha)|_w\} \max\{1, |\alpha|_w\}).$$

La hauteur étant invariante sous l'action de Galois, on obtient finalement :

$$h(\alpha) \geq \frac{\deg(\mathfrak{p})}{2q_{\mathfrak{p}}^6},$$

et la proposition suit. □

4.3. Cas ramifié : la descente. — Le travail effectué jusqu'à présent nous permet, pour les éléments de $K(I)$ dont la hauteur n'est pas correctement minorée, de descendre localement le long de la $\mathfrak{p}^n$-torsion. Nous allons maintenant rendre cette descente globale, pour pouvoir nous ramener à des éléments de $K(J)$, où J est un idéal de A premier à $\mathfrak{p}$, et utiliser nos résultats sur le cas non ramifié.

Cette stratégie repose sur certaines propriétés des sous-groupes de Cartan non déployés de $\mathrm{GL}_2(\mathbb{F}_{\mathfrak{p}})$, c'est-à-dire de ses sous-groupes cycliques d'ordre $q_{\mathfrak{p}}^2 - 1 = q_{\mathfrak{q}} - 1$.

Lemme 4.6. — *On suppose que* $\deg(\mathfrak{p}) \geq 3$. *Soit C un sous-groupe de Cartan non déployé de* $\mathrm{GL}_2(\mathbb{F}_{\mathfrak{p}})$, *et soit $\mathcal{S}$ la réunion des classes de conjugaison de C sous l'action de* $\mathrm{GL}_2(\mathbb{F}_{\mathfrak{p}})$. *Alors $\mathcal{S}$ engendre* $\mathrm{GL}_2(\mathbb{F}_{\mathfrak{p}})$ *pour la structure multiplicative, et* $\mathrm{M}_2(\mathbb{F}_{\mathfrak{p}})$ *pour la structure additive.*

Démonstration. — Le normalisateur de C est d'ordre $2(q_{\mathfrak{q}} - 1)$, et l'orbite de C sous l'action de $\mathrm{GL}_2(\mathbb{F}_{\mathfrak{p}})$ par conjugaison est de cardinal :

$$\frac{|\mathrm{GL}_2(\mathbb{F}_{\mathfrak{p}})|}{2(q_{\mathfrak{q}} - 1)}.$$

Si $C' \neq C$ dans cette orbite, alors C' est aussi un sous-groupe de Cartan non déployé de $\mathrm{GL}_2(\mathbb{F}_{\mathfrak{p}})$, et $\{0\} \cup (C \cap C') = \mathbb{F}_{\mathfrak{p}}$, la droite des matrices scalaires. On a donc :

$$|\mathcal{S}| \geq (q_{\mathfrak{q}} - q_{\mathfrak{p}}) \frac{|\mathrm{GL}_2(\mathbb{F}_{\mathfrak{p}})|}{2(q_{\mathfrak{q}} - 1)} = \frac{(q_{\mathfrak{p}} - 1)^2 q_{\mathfrak{p}}^2}{2}.$$

Le groupe multiplicatif $G_{\mathcal{S}}$ engendré par $\mathcal{S}$ contient C et est d'ordre $> q_{\mathfrak{p}}^3$. Il n'est donc pas inclus dans un groupe de Borel ou dans le normalisateur d'un groupe de Cartan. Par la Proposition 16 de **[35]**, si l'ordre de $G_{\mathcal{S}}$ est premier à p, son image dans le groupe projectif est un groupe exceptionnel d'ordre $> q_{\mathfrak{p}}^2 > 60$ (par l'hypothèse faite sur $\mathfrak{p}$), ce qui est impossible. L'ordre de $G_{\mathcal{S}}$ est donc divisible par p. Comme ce groupe n'est pas inclus dans un Borel, il contient $\mathrm{SL}_2(\mathbb{F}_{\mathfrak{p}})$ par la Proposition 15 de **[35]** - dont la preuve, de nature géométrique, est valable pour le groupe linéaire d'ordre 2 sur un corps de caractéristique p. Comme $C \subset G_{\mathcal{S}}$, on a $\det(G_{\mathcal{S}}) = \mathbb{F}_{\mathfrak{p}}^*$ et finalement $G_{\mathcal{S}} = \mathrm{GL}_2(\mathbb{F}_{\mathfrak{p}})$.

Un calcul immédiat et le fait que $q_{\mathfrak{p}} \geq 8$ montre que le groupe additif M engendré par $\mathcal{S}$ est d'ordre $> q_{\mathfrak{p}}^4/3$, donc d'indice < 3. Si ce groupe était distinct de $\mathrm{M}_2(\mathbb{F}_{\mathfrak{p}})$, il serait d'indice $\geq p \geq 3$. Le lemme est donc entièrement démontré. □

Remarque. Cette propriété additive des groupes de Cartan est fausse en caractéristique 2. Par exemple, pour $\mathbb{F}_\mathfrak{p} = \mathbb{F}_2$, il n'y a qu'un seul Cartan non déployé, engendré par un élément d'ordre 3, et il engendre un groupe additif d'indice 4 dans $M_2(\mathbb{F}_2)$.

Afin de pouvoir utiliser le lemme précédent, on va faire une hypothèse supplémentaire sur $\mathfrak{p}$. On rappelle que l'action du groupe de Galois sur $\phi[\mathfrak{p}]$ induit une représentation :

$$\rho_\mathfrak{p} : \mathrm{Gal}(K^{\mathrm{sep}}/K) \longrightarrow \mathrm{GL}_2(\mathbb{F}_\mathfrak{p}).$$

Lemme 4.7. — *On suppose que* $\deg(\mathfrak{p}) \geq 3$ *et que le morphisme* $\rho_\mathfrak{p}$ *est surjectif. Alors le groupe* H *est engendré par* $\{gH_vg^{-1},\ g \in G\}$.

Démonstration. — Puisque $H \trianglelefteq G$, le groupe Γ engendré par $\{gH_vg^{-1},\ g \in G\}$ est inclus dans H. On va montrer que ces deux groupes sont égaux. On rappelle que $\rho_{\mathfrak{p}^n}$ est la représentation galoisienne induite par l'action de Galois sur la $\mathfrak{p}^n$-torsion. On a le diagramme commutatif suivant :

$$\begin{array}{ccc} G & \xrightarrow{\rho_{\mathfrak{p}^n}} & \mathrm{GL}_2(A/\mathfrak{p}^n) \\ \downarrow & \searrow^{\rho_\mathfrak{p}} & \downarrow \\ \mathrm{Gal}(K(\mathfrak{p})/K) & \longrightarrow & \mathrm{GL}_2(\mathbb{F}_\mathfrak{p}), \end{array} \tag{4.2}$$

où la flèche de droite est la surjection naturelle et celle de gauche est la restriction.

On traite d'abord le cas $n = 1$. Par le point 4 du Lemme 3.11, le groupe H_v est cyclique d'ordre $q_\mathfrak{q} - 1$, et c'est aussi le cas de $\rho_\mathfrak{p}(H_v)$ car la restriction de $\rho_\mathfrak{p}$ à H_v est injective. Le groupe $\rho_\mathfrak{p}(H_v)$ est donc un sous-groupe de Cartan non déployé de $\mathrm{GL}_2(\mathbb{F}_\mathfrak{p})$. Puisqu'on a supposé que $\rho_\mathfrak{p}(G) = \mathrm{GL}_2(\mathbb{F}_\mathfrak{p})$, le Lemme 4.6 donne :

$$\rho_\mathfrak{p}(\Gamma) = \mathrm{GL}_2(\mathbb{F}_\mathfrak{p}).$$

Mais H s'injecte dans $\mathrm{Gal}(K(\mathfrak{p})/K)$ par la restriction naturelle, donc la restriction de $\rho_\mathfrak{p}$ à H est aussi injective et il vient immédiatement : $\Gamma = H$.

On suppose maintenant que $n \geq 2$. Par le point 4 du Lemme 3.11, on a :

$$|\mathcal{M}(H_v)| = |H_v| = q_\mathfrak{p}^2,$$

et $\mathcal{M}(H_v)$ contient une matrice non scalaire θ. Par le point 3 du Lemme 3.10, le groupe $\rho_{\mathfrak{p}^n}(H_v)$ contient les homothéties de $\mathrm{GL}_2(A/\mathfrak{p}^n)$; on en déduit que $\mathcal{M}(H_v)$ contient le sous-groupe $\mathbb{F}_\mathfrak{p}$ des matrices scalaires de $\mathrm{M}_2(\mathbb{F}_\mathfrak{p})$. Comme $\mathcal{M}(H_v)$ est un sous-groupe de $\mathrm{M}_2(\mathbb{F}_\mathfrak{p})$ d'ordre $q_\mathfrak{p}^2$, on a :

$$\mathcal{M}(H_v) = \mathbb{F}_\mathfrak{p} + \mathbb{F}_\mathfrak{p}\theta.$$

Le théorème de Cayley-Hamilton montre alors que $\theta^2 \in \mathcal{M}(H_v)$, et $\mathcal{M}(H_v)$ est une $\mathbb{F}_\mathfrak{p}$-algèbre commutative. On va prouver que c'est un corps.

On affirme d'abord que θ n'a pas de valeurs propres dans $\mathbb{F}_\mathfrak{p}$. D'après le point 3 du Lemme 3.11, l'extension $K_\mathfrak{q}(I)/K_\mathfrak{q}(I/\mathfrak{p}^n)$ est abélienne. Le centralisateur $C(\theta)$ contient donc $\rho_\mathfrak{p}(\mathrm{Gal}(K_\mathfrak{q}(\mathfrak{p})/K_\mathfrak{q}))$. Par le point 1 du Lemme 3.10 et l'injectivité de $\rho_\mathfrak{p}$,

on voit que $q_\mathfrak{q} - 1$ divise $|C(\theta)|$. Si θ a une valeur propre dans $\mathbb{F}_\mathfrak{p}$, il existe $\lambda, \mu \in \mathbb{F}_\mathfrak{p}$ tels que θ est conjugué sur $\mathbb{F}_\mathfrak{p}$ à :

$$\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix} \text{ ou } \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}.$$

Un rapide calcul des centralisateurs montre que θ est scalaire, ce qui est absurde.

Si une matrice non nulle de $\mathbb{F}_\mathfrak{p} + \theta\mathbb{F}_\mathfrak{p}$ n'est pas inversible, c'est un diviseur de 0 et on en déduit que le polynôme caractéristique de θ est scindé. On a donc :

$$\mathcal{M}(H_v)^\times = \mathcal{M}(H_v) \setminus \{0\}.$$

C'est un sous-groupe de Cartan non déployé de $\mathrm{GL}_2(\mathbb{F}_\mathfrak{p})$, et $\mathcal{M}(H_v)$ est un corps à $q_\mathfrak{q}$ éléments. Si $\sigma \in G$ et $\psi \in H_v$, alors $\sigma\psi\sigma^{-1} \in H$, et on vérifie que :

$$\mathcal{M}(\sigma\psi\sigma^{-1}) = \rho_{\mathfrak{p}^n}(\sigma)\mathcal{M}(\psi)\rho_{\mathfrak{p}^n}(\sigma)^{-1}.$$

Le groupe additif $\mathcal{M}(\Gamma)$ contient tous les conjugués du groupe de Cartan $\mathcal{M}(H_v)^\times$. Il est donc égal à $\mathrm{M}_2(\mathbb{F}_\mathfrak{p})$ par le Lemme 4.6. Comme $\mathcal{M}$ est injective, on en déduit que $\Gamma = H$. □

Remarque. Si ϕ est à multiplication complexe par un ordre $\mathcal{O}$, le module de Tate $T_\mathfrak{p}(\phi)$ est naturellement muni d'une structure de $\mathcal{O}_\mathfrak{p}$-module libre de rang 1, avec $\mathcal{O}_\mathfrak{p} = \mathcal{O} \otimes_A A_\mathfrak{p}$. Puisque $\rho_{\mathfrak{p}^\infty}(H)$ commute aux éléments de $\mathcal{O}_\mathfrak{p}$, on a :

$$\rho_{\mathfrak{p}^\infty}(H) \subset \mathcal{O}_\mathfrak{p}^*.$$

Par le point 4 du Lemme 3.11, les groupes H et H_v ont même ordre. Ils sont donc égaux, et la conclusion du lemme est encore vraie dans ce cas.

Ce résultat sur l'orbite du groupe de décomposition se traduit immédiatement dans l'énoncé suivant, qui permet de globaliser la descente.

Corollaire 4.8. — *On suppose que* $\deg(\mathfrak{p}) \geq 3$ *et que le morphisme* $\rho_\mathfrak{p}$ *est surjectif. Soit* $\alpha \in K(I)$ *tel que* $\sigma(\alpha) \in K_\mathfrak{q}(I/\mathfrak{p})$ *pour tout* $\sigma \in G$. *Alors* $\alpha \in K(I/\mathfrak{p})$.

Démonstration. — L'hypothèse faite ici signifie que α est fixé par tous les conjugués de H_v sous l'action de G. Par le Lemme 4.7, on en déduit que α est fixé par H. □

4.4. Minoration de la hauteur de Weil dans les modules génériques. — On est maintenant en mesure de démontrer une borne pour la hauteur de Weil dans les extensions de K engendrées par la torsion d'un module de Drinfeld ϕ de rang 2 admettant un premier supersingulier de degré assez grand.

Proposition 4.9. — *On suppose qu'il existe un premier* $\mathfrak{p}$ *supersingulier pour* ϕ *tel que :* $\deg(\mathfrak{p}) \geq \max\{3, c_2(\phi)\}$. *Soit* $\alpha \in K^*_{\mathrm{tors}}$ *non constant. On a :*

$$h(\alpha) \geq \frac{\deg(\mathfrak{p})}{2q^{6\deg(\mathfrak{p})}}.$$

Démonstration. — On écrit : $\alpha \in K(I)$, avec $I = \mathfrak{p}^n J$. L'idéal J est premier à $\mathfrak{p}$, et on prend $n \geq 0$ minimal. Par la Proposition 4.2, on peut prendre $n \geq 1$.

Supposons par l'absurde que l'inégalité annoncée est fausse. La Proposition 4.5 montre que $\alpha \in K_{\mathfrak{q}}(I/\mathfrak{p})$, où $K_{\mathfrak{q}}$ est l'unique extension non ramifiée de la complétion $\mathfrak{p}$-adique $K_{\mathfrak{p}}$ de K. La hauteur de Weil étant invariante sous l'action de Galois, on a encore : $\sigma(\alpha) \in K_{\mathfrak{q}}(I/\mathfrak{p})$ pour tout $\sigma \in \mathrm{Gal}(K(I)/K)$. Le Corollaire 4.8 contredit alors la minimalité de n. □

5. Hauteur canonique sur les corps engendrés par la torsion

On se concentre maintenant sur la hauteur canonique $\hat{h}_\phi$, qu'on va également minorer sur K_{tors} lorsqu'elle ne s'annule pas. La stratégie générale est la même, mais on doit tenir compte de certaines spécificités. La première est que $\hat{h}_\phi$ et h ne s'annulent pas en les mêmes éléments de $\bar{K}$. La seconde est que ces deux hauteurs sont proches à une constante près, qui ne dépend que de ϕ.

5.1. Borne pour la hauteur canonique dans le cas non ramifié. — La méthode employée ici est très proche de celle qui nous a permis de minorer la hauteur de Weil. On suppose que le module ϕ admet un premier $\mathfrak{p} = \pi A$ de réduction supersingulière tel que :

$$\deg(\mathfrak{p}) \geq 2(c_1(\phi) + 1).$$

Cette hypothèse sur la taille de $\mathfrak{p}$ nous permettra de gommer la différence entre hauteur de Weil et hauteur canonique, qui est majorée par la constante $c_1(\phi)$. On considère un idéal I de A premier à $\mathfrak{p}$.

Proposition 5.1. — *Soit $\alpha \in K(I) \setminus \phi_{\mathrm{tors}}$. Alors :*

$$\hat{h}_\phi(\alpha) \geq \frac{1}{q^{2\deg(\mathfrak{p})} + 1}.$$

Démonstration. — Un problème spécifique se pose lorsque α n'est pas v-entier pour un grand nombre de places $v|\mathfrak{p}$. On le résout en utilisant un principe de tiroirs. On note :

$$\mathcal{P} := \{v|\mathfrak{p} \in M(K(I))\} = \{v, v(\alpha) \geq 0\} \dot{\cup} \{v, v(\alpha) < 0\} = \mathcal{P}^+ \dot{\cup} \mathcal{P}^-.$$

On observe que l'union est disjointe, et on suppose d'abord que $|\mathcal{P}^-| \geq |\mathcal{P}|/2$. On peut alors directement minorer la hauteur de α :

$$h(\alpha) \geq \frac{1}{[K(I) : K]} \sum_{v \in \mathcal{P}^-} n_v \geq \frac{\deg(\mathfrak{p})}{2} \geq c_1(\phi) + 1,$$

et on obtient :

$$\hat{h}_\phi(\alpha) \geq h(\alpha) - c_1(\phi) \geq 1.$$

La proposition est donc démontrée dans ce cas.

On peut donc supposer que $|\mathcal{P}^+| > |\mathcal{P}|/2$. On fixe une place $v \in \mathcal{P}^+$ et on note $F_{\mathfrak{q}}$ le Frobenius associé. Soit

$$\beta := F_{\mathfrak{q}}(\alpha) - \phi(\pi) \cdot \alpha.$$

Si $\beta = 0$, comme la hauteur canonique est invariante sous l'action de Galois :

$$\hat{h}_\phi(\alpha) = \hat{h}_\phi\big(\phi(\pi)\cdot\alpha\big) = q^{2\deg(\mathfrak{p})}\hat{h}_\phi(\alpha),$$

et α annule la hauteur canonique, ce qui contredit le choix de α. On peut donc appliquer la formule du produit à β.

Commençons par la norme v-adique. L'égalité (3.1) couplée avec l'injectivité de l'application naturelle : $\mathrm{End}(\phi_\mathfrak{p}) \otimes A_\mathfrak{l} \to \mathrm{End}_{A_\mathfrak{l}}(T_\mathfrak{l}(\phi_\mathfrak{p}))$ montre que :

$$\phi(\pi)\cdot x - x^{q_\mathfrak{q}} \in \mathfrak{p}A[x], \tag{5.1}$$

et ce polynôme est de degré au plus $q_\mathfrak{q} - 1$. On en déduit :

$$|\beta|_v \leq q^{-1}\max\{1, |\alpha|_v\}^{q_\mathfrak{q}} \leq q^{-1}.$$

L'extension $K(I)/K$ étant galoisienne, si $w \in \mathcal{P}^+$, on peut trouver $\sigma \in \mathrm{Gal}(K(I)/K)$ tel que $w = \sigma^{-1}v$. On sait que σ commute à $F_\mathfrak{q}$, et il est immédiat que σ commute à l'action de π qui est définie sur K. On a donc :

$$\begin{aligned} |\beta|_w &= |\sigma F_\mathfrak{q}(\alpha) - \sigma(\phi(\pi)\cdot\alpha)|_v = |F_\mathfrak{q}(\sigma\alpha) - \phi(\pi)\cdot(\sigma\alpha)|_v \\ &\leq q^{-1}\max\{1, |\sigma\alpha|_v\}^{q_\mathfrak{q}} \leq q^{-1}. \end{aligned}$$

Si w est une place quelconque de $K(I)$, on se contente de la majoration triviale :

$$|\beta|_w \leq \max\{1, |\beta|_w\}.$$

Par la formule du produit (2.3) et la comparaison entre hauteurs, on obtient :

$$\hat{h}_\phi(\beta) \geq h(\beta) - c_1(\phi) \geq \frac{\deg(\mathfrak{p})}{2} - c_1(\phi) \geq 1.$$

On finit la preuve en comparant les hauteurs canoniques de α et β (en remarquant par passage à la limite que $\hat{h}_\phi$ est sous-additive et invariante sous Galois puisque ces propriétés sont vraies pour h) :

$$\hat{h}_\phi(\beta) \leq \hat{h}_\phi(F_\mathfrak{q}(\alpha)) + \hat{h}_\phi(\phi(\pi)\cdot\alpha) \leq (1 + q_\mathfrak{q})\hat{h}_\phi(\alpha),$$

ce qui achève la démonstration. □

5.2. Cas ramifié : une première borne. — On s'attaque pour finir au cas ramifié. La comparaison entre hauteur de Weil et hauteur canonique introduit une nouvelle difficulté. Dans un premier temps, on parvient à descendre localement à une extension kummerienne près.

On suppose que le module ϕ admet un premier $\mathfrak{p} = \pi A$ de réduction supersingulière tel que :

$$\deg(\mathfrak{p}) \geq 3(c_1(\phi) + 1).$$

On reprend les notations du 4.2. En particulier, on se donne un idéal I de A divisible par $\mathfrak{p}$, et on fixe une place $v|\mathfrak{p}$. On note $H_v := \mathrm{Gal}(K_\mathfrak{q}(I)/K_\mathfrak{q}(I/\mathfrak{p}))$ le groupe de décomposition en v. On obtient d'abord une minoration conditionnelle de la hauteur canonique.

Lemme 5.2. — *Soit $\alpha \in K(I)$. S'il existe $\psi \in H_v$ tel que : $\psi(\alpha) - \alpha \notin \phi[\mathfrak{p}^\infty]$, on a :*

$$\hat{h}_\phi(\alpha) \geq \frac{1}{2q^{4\deg(\mathfrak{p})q_\mathfrak{q}^2}}.$$

Démonstration. — On pose :

$$\beta := \phi(\pi^{2q_{\mathfrak{q}}^2}) \cdot \big(\psi(\alpha) - \alpha\big),$$

qui est non nul par hypothèse. La formule (2.3) donne :

$$\sum_{w \in M(K(I))} n_w \log_q |\beta|_w = 0.$$

On utilise de nouveau un principe de tiroirs, dans lequel on distingue trois cas. Notons $\mathfrak{P}$ l'idéal correspondant à v. L'orbite $\mathcal{O}_v$ de v sous l'action du centralisateur $C(\psi)$ de ψ dans G s'écrit comme une union disjointe :

$$\begin{array}{rcccccc} \mathcal{O}_v & := & \left\{w, w(\alpha) \geq 0\right\} & \cup & \left\{w, 0 > w(\alpha) \geq -\dfrac{e_{\mathfrak{P}|\mathfrak{p}}}{4q_{\mathfrak{q}}}\right\} & \cup & \left\{w, w(\alpha) < -\dfrac{e_{\mathfrak{P}|\mathfrak{p}}}{4q_{\mathfrak{q}}}\right\} \\ & = & \mathcal{O}_v^{(1)} & \cup & \mathcal{O}_v^{(2)} & \cup & \mathcal{O}_v^{(3)}. \end{array}$$

Examinons d'abord le cas : $|\mathcal{O}_v^{(1)}| \geq |\mathcal{O}_v|/3$. Si $w \in O_v^{(1)}$, on pose : $w = \sigma^{-1}v$, où $\sigma \in C(\psi)$. On a : $|\sigma\alpha|_v = |\alpha|_w \geq 0$, donc $\sigma\alpha$ est $\mathfrak{P}$-entier et :

$$\gamma := \psi(\sigma\alpha) - \sigma\alpha \in \mathfrak{P}^{q_{\mathfrak{q}}^{n-1}},$$

ce qui d'un point de vue métrique se traduit par : $|\gamma|_v \leq q^{\frac{-e_{\mathfrak{P}|\mathfrak{p}}}{q_{\mathfrak{q}}-1}}$. En utilisant (5.1), on observe que : $|\phi(\pi) \cdot \gamma|_v \leq q^{-e_{\mathfrak{P}|\mathfrak{p}}}$. Comme de plus :

$$\phi(\pi) \cdot x - \pi x \in x^q A[x],$$

une récurrence immédiate montre que : $|\phi(\pi^{2q_{\mathfrak{q}}^2}) \cdot \gamma|_v \leq q^{-q_{\mathfrak{q}}^2 e_{\mathfrak{P}|\mathfrak{p}}}$. Puisque $\sigma \in C(\psi)$ et commute à l'action de ϕ, il suit :

$$|\beta|_w \leq q^{-q_{\mathfrak{q}}^2 e_{\mathfrak{P}|\mathfrak{p}}}.$$

Si w est une autre place de $K(I)$, on se contente de la majoration :

$$|\beta|_w \leq \max\{1, |\beta|_w\}.$$

On en déduit l'inégalité suivante, par la formule (2.3) :

$$q_{\mathfrak{q}}^2 \sum_{w \in O_v^1} n_w e_{w|\mathfrak{p}} \leq \sum_{w \notin O_v^1} n_w \log_q(\max\{1, |\beta|_w\},$$

puis par le Lemme 4.4 et la comparaison entre hauteur de Weil et hauteur canonique :

$$1 + c_1(\phi) \leq \frac{\deg(\mathfrak{p})}{3} \leq h(\beta) \leq \hat{h}_\phi(\beta) + c_1(\phi).$$

La hauteur canonique étant quadratique pour l'action de ϕ, invariante sous l'action de Galois et sous-additive, on obtient finalement :

$$\begin{array}{rcl} 1 \leq \hat{h}_\phi(\beta) & \leq & q^{4\deg(\mathfrak{p})q_{\mathfrak{q}}^2}\big(\hat{h}_\phi(\alpha) + \hat{h}_\phi(\psi\alpha)\big) \\ & \leq & 2q^{4\deg(\mathfrak{p})q_{\mathfrak{q}}^2}\hat{h}_\phi(\alpha) \end{array}$$

et l'inégalité de la proposition suit.

Passons maintenant au cas : $|\mathcal{O}_v^{(2)}| \geq |\mathcal{O}_v|/3$, qui est plus délicat car on doit tenir compte des dénominateurs. Si $w \in O_v^{(2)}$, on pose $w = \sigma^{-1}v$, avec $\sigma \in C(\psi)$, et $\delta = \sigma\alpha$. On a : $|\sigma\alpha|_v = |\alpha|_w \leq 0$, donc δ^{-1} est $\mathfrak{P}$-entier. Pour $l \geq 0$, on pose :

$$f(\delta, l) := \psi(\delta^{-q_\mathfrak{q}^l}) - \delta^{-q_\mathfrak{q}^l},$$

qui est de valuation : $v\left(f(\delta,l)\right) \geq e_{\mathfrak{P}|\mathfrak{p}} q_\mathfrak{q}^l/(q_\mathfrak{q}-1)$. On a :

$$\psi(\delta^{q_\mathfrak{q}^l}) - \delta^{q_\mathfrak{q}^l} = \frac{-f(\delta,l)}{\delta^{-q_\mathfrak{q}^l}(\delta^{-q_\mathfrak{q}^l} + f(\delta,l))} = \frac{-\delta^{2q_\mathfrak{q}^l} f(\delta,l)}{1+\delta^{q_\mathfrak{q}^l} f(\delta,l)}.$$

Par hypothèse, on a :

$$2q_\mathfrak{q}^l v(\delta) + v(f(\delta,l)) \geq 2q_\mathfrak{q}^l w(\alpha) + q_\mathfrak{q}^{l-1} e_{\mathfrak{P}|\mathfrak{p}} \geq \frac{l}{2} e_{\mathfrak{P}|\mathfrak{p}}.$$

Ceci implique au passage que le dénominateur est une $\mathfrak{P}$-unité, et il vient :

$$v\left(\psi(\delta^{q_\mathfrak{q}^l}) - \delta^{q_\mathfrak{q}^l}\right) \geq \frac{l}{2} e_{\mathfrak{P}|\mathfrak{p}}.$$

Une récurrence immédiate basée sur (5.1) montre par ailleurs que pour tout $m \geq 1$:

$$\phi(\pi^m)\cdot x = \sum_{i=0}^{m} \pi^i P_{i,m}\left(x^{q_\mathfrak{q}^{m-i}}\right), \tag{5.2}$$

où $P_{i,m} \in A[x]$ est additif de degré $< q_\mathfrak{q}^i$, sans terme constant, et $P_{0,m}(x) = x$. En évaluant terme à terme, il en résulte que :

$$w(\beta) = v(\sigma\beta) \geq e_{\mathfrak{P}|\mathfrak{p}} \min_{0\leq i\leq 2q_\mathfrak{q}^2} \{i + (2q_\mathfrak{q}^2 - i)/2\} = e_{\mathfrak{P}|\mathfrak{p}} q_\mathfrak{q}^2.$$

Comme dans le cas précédent, on applique la formule du produit à β avec les majorations triviales aux places n'appartenant pas à $\mathcal{O}_v^{(2)}$. On trouve une nouvelle fois :

$$h(\beta) \geq 1 + c_1(\phi),$$

et on en déduit la borne annoncée pour la hauteur canonique de α.

Il reste à traiter le cas : $|\mathcal{O}_v^{(3)}| \geq |\mathcal{O}_v|/3$. Beaucoup de conjugués de α ont un gros dénominateur, et on peut ici se passer de ψ. Si $w = \sigma^{-1}v \in \mathcal{O}_v^{(2)}$, l'identité (5.2) montre que :

$$w\left(\phi(\pi^4)\cdot\alpha\right) = v\left(\phi(\pi^4)\cdot\sigma\alpha\right) \leq -q_\mathfrak{q}^2 e_{\mathfrak{P}|\mathfrak{p}}.$$

On peut alors minorer directement la hauteur de Weil :

$$\begin{aligned} h(\phi(\pi^4)\cdot\alpha) &\geq \frac{q_\mathfrak{q}^2}{[K(I):K]} \sum_{w\in\mathcal{O}_v^3} n_w e_{\mathfrak{P}|\mathfrak{p}} \\ &\geq \frac{\deg(\mathfrak{p}) q_\mathfrak{q}^2}{3q_\mathfrak{p}^4} \\ &\geq c_1(\phi) + 1. \end{aligned}$$

On en déduit finalement une borne pour la hauteur canonique :

$$\hat{h}_\phi(\alpha) = \frac{\hat{h}_\phi(\phi(\pi^4)\cdot\alpha)}{q^{8\deg(\mathfrak{p})}} \geq \frac{1}{q^{8\deg(\mathfrak{p})}}.$$

Cette inégalité est plus forte que celle du lemme. La démonstration est donc achevée. □

Remarque. On a utilisé ici un procédé d'accélération p-adique en multipliant α par une puissance importante de π. L'inconvénient de cette méthode est qu'on obtient une borne exponentielle en $q_\mathfrak{q}$.

5.3. Cas ramifié : préparatifs kummeriens. — Les conditions sont presque réunies pour descendre le long de la $\mathfrak{p}^n$-torsion, comme on l'a déjà fait pour minorer la hauteur de Weil. La seule différence pour l'instant est qu'on arrive à faire descendre localement un multiple assez grand du point dont on veut minorer la hauteur. On aura besoin de contrôler la $\mathfrak{p}^\infty$-torsion dans $K_\mathfrak{q}(I)$, puis de construire un élément particulier du centre de $\mathrm{Gal}(K(I)/K)$. On écrit $I = \mathfrak{p}^n J$, avec J premier à $\mathfrak{p}$.

Lemme 5.3. — *On a :* $K_\mathfrak{q}(I) \cap \phi[\mathfrak{p}^\infty] = \phi[\mathfrak{p}^n]$.

Démonstration. — Le membre de droite est inclus dans celui de gauche par construction. Montrons l'autre inclusion. Supposons que $x \in K_\mathfrak{q}(I) \cap \phi[\mathfrak{p}^m]$ pour un certain entier $m \geq n$. Si $m = 0$, il n'y a rien à démontrer. Par le point 3 du Lemme 3.10, on voit que $\mathrm{Gal}(K_\mathfrak{q}(I)/K_\mathfrak{q})$ agit transitivement sur $\phi[\mathfrak{p}^m]$, donc que $\phi[\mathfrak{p}^m] \subset K_\mathfrak{q}(I)$.

On peut alors utiliser le point 1 du Lemme 3.10 pour comparer les indices de ramification. Comme $m \geq 1$, l'indice de ramification de $K_\mathfrak{q}(I)/K_\mathfrak{q}$ est $\geq q_\mathfrak{q}^{m-1}(q_\mathfrak{q}-1)$. On en déduit que $n \geq 1$ et que :

$$q_\mathfrak{q}^{n-1}(q_\mathfrak{q}-1) \geq q_\mathfrak{q}^{m-1}(q_\mathfrak{q}-1),$$

donc que $m = n$, ce qui achève la preuve. □

On se donne maintenant un idéal premier $\mathfrak{m}$ de A engendré par un élément irréductible μ. On suppose que $\mathfrak{m} \neq \mathfrak{p}$.

Lemme 5.4. — *Il existe un élément σ_μ du centre de G tel que l'action de σ_μ sur $\phi[\mathfrak{p}^n]$ soit donnée par $\phi(\mu)$.*

Démonstration. — Par le point 3 du Lemme 3.10, il existe un élément :

$$\sigma'_\mu \in \mathrm{Gal}(K_\mathfrak{q}(\mathfrak{p}^n)/K_\mathfrak{q})$$

dont l'action sur $\phi[\mathfrak{p}^n]$ est donnée par $\phi(\mu)$. Par le point 3 du Lemme 3.11, l'automorphisme σ'_μ se relève en un unique $\sigma_\mu \in \mathrm{Gal}(K_\mathfrak{q}(I)/K_\mathfrak{q}(J))$. On observe que l'automorphisme σ_μ agit sur $\phi[\mathfrak{p}^n]$ via $\phi(\mu)$, et qu'il agit trivialement sur $\phi[J]$. Il commute donc à tout élément de G. □

5.4. Minoration de la hauteur canonique dans les modules génériques. — On peut désormais donner une minoration absolue de la hauteur canonique sur les corps engendrés par la torsion d'un module de Drinfeld ϕ admettant un premier supersingulier assez grand.

Proposition 5.5. — *Soit $\mathfrak{m}$ un idéal premier de A de degré minimal. On suppose qu'il existe un premier $\mathfrak{p} \neq \mathfrak{m}$ qui est supersingulier pour ϕ et tel que :* $\deg(\mathfrak{p}) \geq \max\{3(c_1(\phi)+1), c_2(\phi)\}$. *Si $\alpha \in K_{\mathrm{tors}} \setminus \phi_{\mathrm{tors}}$, on a :*

$$\hat{h}_\phi(\alpha) \geq \frac{1}{q^{q^{5\deg(\mathfrak{p})}}}.$$

Démonstration. — On note $\mathfrak{m} = (\mu)A$ et on suppose que $\alpha \notin \phi_{\mathrm{tors}}$. Soit :

$$\beta := \sigma_\mu \alpha - \phi(\mu)\cdot\alpha.$$

On remarque d'abord que $\beta \notin \phi_{\mathrm{tors}}$. Si c'était le cas, on aurait en effet :

$$\hat{h}_\phi(\alpha) = \hat{h}_\phi(\sigma_\mu\alpha) = \hat{h}_\phi(\phi(\mu)\cdot\alpha) = q^{2\deg(\mathfrak{m})}\hat{h}_\phi(\alpha),$$

et α serait de torsion. Il est également facile de comparer les hauteurs canoniques de α et β :

$$\hat{h}_\phi(\beta) \leq \hat{h}_\phi(\sigma_\mu\alpha) + \hat{h}_\phi(\phi(\mu)\cdot\alpha) \leq \left(1 + q^{2\deg(\mathfrak{m})}\right)\hat{h}_\phi(\alpha).$$

On peut donc se contenter de minorer la hauteur de β. Comme K_{tors}/K est galoisienne, on a : $\beta \in K(I)$, où $I = \mathfrak{p}^n J$ avec J premier à $\mathfrak{p}$ et $n \geq 0$ minimal. Par la Proposition 5.1, si $n = 0$, on a :

$$\hat{h}_\phi(\alpha) \geq \frac{\hat{h}_\phi(\beta)}{q^{2\deg(\mathfrak{m})}} \geq \frac{1}{2q^{2(\deg(\mathfrak{m})+\deg(\mathfrak{p}))}} \geq \frac{1}{q^{4\deg(\mathfrak{p})}},$$

par minimalité de $\deg(\mathfrak{m})$. Cette minoration est plus forte que celle annoncée. On peut ainsi supposer que $n \geq 1$.

Le Corollaire 4.8 et la minimalité de n nous montrent qu'il existe $\sigma \in G$ tel que $\sigma(\beta) \notin K_{\mathfrak{q}}(I/\mathfrak{p})$. On pose : $\alpha' = \sigma\alpha$ et : $\beta' = \sigma\beta = \sigma_\mu\alpha' - \phi(\mu)\cdot\alpha'$ (puisque σ_μ commute à σ). Il existe donc $\psi \in H_v$ tel que : $\psi(\beta') \neq \beta'$. Si :

$$t := \psi(\beta') - \beta' \notin \phi[\mathfrak{p}^\infty],$$

le Lemme 5.2 donne :

$$\hat{h}_\phi(\alpha) \geq \frac{\hat{h}_\phi(\beta)}{q^{2\deg(\mathfrak{p})}} = \frac{\hat{h}_\phi(\beta')}{q^{2\deg(\mathfrak{p})}} \geq \frac{1}{q^{5\deg(\mathfrak{p})q_{\mathfrak{q}}^2}} \geq \frac{1}{q^{q^{5\deg(\mathfrak{p})}}},$$

où on a utilisé dans la dernière inégalité que : $\deg(\mathfrak{p}) \geq 3$.

Il reste donc à envisager l'éventualité que $t \in \phi[\mathfrak{p}^\infty]$. Notons que $t \neq 0$ par construction. En utilisant la construction kummerienne, on va obtenir une contradiction. Soit $v := \psi(\alpha') - \alpha'$. Comme σ_μ commute à ψ, on constate que :

$$t = \sigma_\mu v - \phi(\mu)\cdot v.$$

Puisque t est de torsion, on a : $\hat{h}_\phi(\sigma_\mu v) = \hat{h}_\phi(\phi(\mu)\cdot v)$, et on en déduit que v est de torsion. On décompose l'idéal d'annulation de v pour trouver $\lambda \in A \setminus \mathfrak{p}$ tel que

$\phi(\lambda)\cdot v \in \phi[\mathfrak{p}^\infty]$. Comme il s'agit d'un élément de $K(I)$, le Lemme 5.3 montre que $\phi(\lambda)\cdot v \in \phi[\mathfrak{p}^n]$. Il suit :

$$\phi(\lambda)\cdot t = \phi(\lambda)\cdot\big(\sigma_\mu v - \phi(\mu)\cdot v\big) = \sigma_\mu(\phi(\lambda)\cdot v) - \phi(\mu)\cdot(\phi(\lambda)\cdot v) = 0.$$

Comme on a aussi : $\phi(\pi^n)\cdot t = 0$, le lemme de Bezout appliqué à λ et à π^n montre que $t = 0$, ce qui est absurde. □

Références

[1] F. Amoroso et S. David, *Le problème de Lehmer en dimension supérieure*, J. reine angew. Math **513** (1999), 145-179.

[2] F. Amoroso, S. David et U. Zannier, *On fields with Property (B)*, Proc. Amer. Math. Soc. **142** (2014), 1893-1910.

[3] F. Amoroso et R. Dvornicich, *A lower bound for the height in abelian extensions*, J. Number Theory **80** (2000), 260-272.

[4] F. Amoroso et D. Masser, *Lower bounds for the height in galois extensions*, Prépublication (2016).

[5] F. Amoroso et U. Zannier, *A relative Dobrowolski's lower bound over abelian extensions*, Ann. Sc. Norm. Super. Pisa Cl. Sci. **29** (2000), 711-727.

[6] S. Bae, *Drinfeld modules with bad reduction over complete local rings*, Bull. Korean Math. Soc. **32** (1995), 2, 349-357.

[7] M. Baker et J. Silverman, *A lower bound for the canonical height on abelian varieties over abelian extensions*, Math. Res. Lett. **11** (2004), 377-396.

[8] H. Bauchère, *Minoration de la hauteur canonique pour les modules de Drinfeld à multiplications complexes*, J. Number Theory **157** (2015), 291-328.

[9] E. Bombieri et U. Zannier *A note on heights in certain infinite extensions of* $\mathbb{Q}$, Rend. Mat. Acc. Lincei **12** (2001), 5-14.

[10] M. Brown, *Singular moduli and supersingular moduli of Drinfeld modules*, Invent. Math. **110** (1992), 419-439.

[11] S. Checcoli, *Fields of algebraic numbers with bounded local degrees and their properties*, Trans. Amer. Math. Soc. **365** (2013), 2223-2240.

[12] C. David, *Supersingular reduction of Drinfeld modules*, Duke Math. J. **78** (1995), 399-411.

[13] S. David et A. Pacheco, *Le problème de Lehmer abélien pour un module de Drinfeld*, Int. J. Number Theory **4** (2008), 1043-1067.

[14] L. Denis, *Hauteurs canoniques et modules de Drinfeld*, Math. Ann. **294** (1992), 213-223.

[15] L. Denis, *Problèmes diophantiens sur les t-modules*, J. Théor. Nombres Bordeaux **7** (1995), 1, 97-110.

[16] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*, Acta Arith. **34** (1979), 391-401.

[17] M.D. Fried et M. Jarden, *Field arithmetic*, Springer-Verlag, 2005.

[18] A. Galateau et V. Mahé, *Some consequences of Masser's counting theorem on elliptic curves*, Math. Z. (2016), doi :10.1007/s00209-016-1728-4.

[19] E.-U. Gekeler, *Frobenius distributions of Drinfeld modules of finite characteristics*, Trans. Amer. Math. Soc. **360** (2008), 1695-1721.

[20] E.-U. Gekeler, *Zur Arithmetik von Drinfeld-Moduln*, Math. Ann. **262** (1983), 167-182.

[21] D. R. Hayes, *A brief introduction to Drinfeld modules*, The Arithmetic of Function Fields. Ohio State Univ. Math. Res. Inst. Publ. **2** (1992), 1-32.

[22] D. Ghioca *The local Lehmer inequality for Drinfeld modules*, J. Number Theory **123** (2007), 426-455.

[23] D. Goss, *Basic Structures of Function Field Arithmetic*, Springer-Verlag, 1996.

[24] P. Habegger, *Small height and infinite non-abelian extensions*, Duke Math. J. **162** (2013), 11, 2027-2076.

[25] P. Ingram, *A lower bound for the canonical height associated to a Drinfeld module*, Int. Math. Res. Not. IMRN **17** (2014), 4879-4916.

[26] D. H. Lehmer, *Factorization of certain cyclotomic functions*, Ann. of Math. **34** (1933), 461-479.

[27] D. Lombardo, *Bounds for Serre's open image theorem for elliptic curves over number fields*, Algebra Number Theory, **9** (2015), 10, 2347–2395.

[28] J. Neukirch, *Algebraic Number Theory*, Springer-Verlag, 1999.

[29] R. Pink, *The Mumford-Tate conjecture for Drinfeld modules*, Publ. Res. Inst. Math. Sci. **33** (1997), 3, 393-425.

[30] R. Pink, *The Galois representations associated to Drinfeld modules in Special Characteristic, I : Zariski density*, J. Number Theory **116** (2006), 2, 324-347.

[31] R. Pink et E. Rütsche, *Adelic Openness for Drinfeld modules in general characteristic*, J. Number Theory **129** (2009), 4, 866-881.

[32] B. Poonen, *Drinfeld modules with no supersingular primes*, Int. Mat. Res. Not. IMRN **3** (1998), 151-159.

[33] M. Rosen, *Formal Drinfeld modules*, J. Number Theory **103** (2003), 234-256.

[34] A. Schinzel, *On the product of the conjugates outside the unit circle of an algebraic number*, Acta Arith. 24 (1973), 385-399.

[35] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259-331.

[36] T. Takahashi, *Good reduction of elliptic modules*, J. Math. Soc. Japan **34** (1982), 3, 475-487.

Aurélien Galateau, Université de Franche-Comté • *E-mail :* agalatea@univ-fcomte.fr

Amílcar Pacheco, Universidade Federal do Rio de Janeiro, Departamento de Matemática
E-mail : amilcar@acd.ufrj.br