

# LE PROBLÈME DE LEHMER ABÉLIEN POUR UN MODULE DE DRINFEL'D

SINNOU DAVID ET AMÍLCAR PACHECO

RÉSUMÉ. Soit  $\phi$  un module de DRINFEL'D défini sur une extension finie  $K$  de  $\mathbb{F}_q(T)$ ; nous démontrons une minoration uniforme pour la hauteur canonique d'un point de  $\phi$ , rationnel sur l'extension abélienne maximale de  $K$ , et résolvons ainsi la version dite abélienne du problème de LEHMER dans cette situation. Dans le cadre classique (un point d'ordre infini de  $\mathbb{G}_m(\mathbb{Q}^{\text{ab}})$ ), cette question a été résolue par F. AMOROSO et R. DVORNICICH dans [Am–Dv].

ABSTRACT. **Abelian Lehmer problem for Drinfel'd modules.** Let  $\phi$  be a DRINFEL'D module defined over a finite extension  $K$  of  $\mathbb{F}_q(T)$ ; we establish a uniform lower bound for the canonical height of a point of  $\phi$ , rational over the maximal abelian extension of  $K$ , and thus solve the so called abelian version of the Lehmer problem in this situation. The classical original problem (a non torsion point in  $\mathbb{G}_m(\mathbb{Q}^{\text{ab}})$ ) was solved by F. AMOROSO and R. DVORNICICH in [Am–Dv].

## 1. INTRODUCTION

On note  $h : \overline{\mathbb{Q}} \rightarrow \mathbb{R}^+$  la hauteur de WEIL logarithmique et absolue; soit  $\alpha$  un nombre algébrique; on sait que  $h(\alpha)$  est nul si et seulement si  $\alpha$  est une racine de l'unité. Le problème dit de LEHMER consiste à rechercher une minoration optimale (en fonction de  $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ ) pour  $h(\alpha)$  lorsque  $\alpha$  n'est pas une racine de l'unité. Plus précisément, D. H. LEHMER a demandé en 1932 (*confer* [Leh], § 13, page 476) s'il existe un nombre réel  $c > 0$  tel que pour tout  $\alpha \in \overline{\mathbb{Q}}^*$  qui n'est pas une racine de l'unité,

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

Rappelons que ce problème reste ouvert à ce jour. Toutefois, de nombreuses généralisations ont été proposées (on pourra par exemple se reporter à [Dav] pour plus de détails) et des progrès notables ont été réalisés ces dernières années dans ces directions.

---

*Date:* 2 août 2007.

Ce travail a été entrepris au cours de deux visites successives des auteurs chacun à l'autre en août 2004 à RIO puis en février 2005 à PARIS. Ces missions ont été soutenues par l'accord BRÉSIL–FRANCE en Mathématiques 69.0014/01-5. Amílcar PACHECO a de plus été partiellement soutenu par une bourse de recherche du CNPq numéro 304424/2003-0, et par les programmes Pronex-Rio et CNPq Edital Universal 470099/2003-8. Nous remercions chaleureusement chacune de ces organisations pour leur soutien.

C'est avec plaisir que nous remercions ici le rapporteur dont les remarques sur la première version de ce travail ont contribué à améliorer sensiblement la présentation finale.

Commençons par décrire l'une de ces généralisations. Il s'agit de remplacer le corps  $\mathbb{Q}$  par un sous-corps  $K$  de  $\overline{\mathbb{Q}}$ . Plus précisément, on décompose la question en deux étapes :

- (i) existe-t-il un nombre réel  $c(K) > 0$  tel que pour tout  $\alpha \in \mathbb{G}_m(K) \setminus \mathbb{G}_m(K)_{\text{tor}}$ ,  $h(\alpha) \geq c(K)$  ?
- (ii) si la réponse à (i) est positive, existe-t-il plus généralement un nombre réel  $c'(K) > 0$  tel que pour tout  $\alpha \in \mathbb{G}_m(\overline{K}) \setminus \mathbb{G}_m(\overline{K})_{\text{tor}}$ , on ait

$$h(\alpha) \geq c'(K)/[K(\alpha) : K] ?$$

Bien entendu, si  $K$  est un corps de nombres, la réponse à (i) est positive et découle facilement du théorème de NORTHCOTT, tandis que la question (ii) se ramène essentiellement au problème de LEHMER sur  $\mathbb{Q}$ . Ces généralisations sont autrement plus profondes lorsque  $K$  est une extension infinie de  $\mathbb{Q}$ . Le cas  $K = \mathbb{Q}^{\text{ab}}$  semble être d'une importance particulière. Dans ce cadre, on parle usuellement de problème de LEHMER abélien pour la question (i) dans cette situation et de *problème de Lehmer relatif* pour la question (ii). On notera également que les minoration attendues représentent un renforcement notable par rapport à la conjecture d'origine.

Le problème de LEHMER abélien tel qu'il est formulé ci-dessus a été résolu par F. AMOROSO et R. DVORNICICH (*confer* [Am–Dv, theorem]), qui ont montré que pour tout  $\alpha \in \mathbb{G}_m(\mathbb{Q}^{\text{ab}}) \setminus \mathbb{G}_m(\mathbb{Q}^{\text{ab}})_{\text{tor}}$ ,

$$h(\alpha) \geq \frac{\log(5)}{12} .$$

Quant au problème de LEHMER relatif, un résultat partiel significatif a été obtenu par F. AMOROSO et U. ZANNIER (*confer* [Am–Za, theorem 1.1]) ; plus précisément, pour tout<sup>1</sup>  $\alpha \in \mathbb{G}_m(\overline{\mathbb{Q}^{\text{ab}}}) \setminus \mathbb{G}_m(\overline{\mathbb{Q}^{\text{ab}}})_{\text{tor}}$ , on a

$$h(\alpha) \geq \frac{c'}{D} \left( \frac{\log(2D)}{\log \log(5D)} \right)^{-13} ,$$

où  $D = [\mathbb{Q}^{\text{ab}}(\alpha) : \mathbb{Q}^{\text{ab}}]$  et  $c' > 0$  est un nombre réel  $> 0$ .

Le problème de LEHMER s'étend facilement à d'autres contextes, notamment sur des variétés abéliennes ou des modules de DRINFEL'D. Dans le contexte des variétés abéliennes définies sur un corps de nombres, l'analogie du problème de LEHMER abélien a été obtenu par M. BAKER et J. SILVERMAN : soit  $K$  un corps de nombres,  $\overline{K}$  une clôture algébrique de  $K$  et  $K^{\text{ab}}$  l'extension abélienne maximale de  $K$ . Soit de plus  $A$  une variété abélienne définie sur  $K$  et munie d'un fibré en droites ample et symétrique  $\mathcal{L}$  ; on dispose alors d'une notion de hauteur canonique (ou normalisée) sur  $(A, \mathcal{L})$  :  $\hat{h}_{\mathcal{L}} : A(\overline{K}) \rightarrow \mathbb{R}^+$ . Dans [Ba–Si, theorem 0.1], M. BAKER et J. SILVERMAN prouvent qu'il existe une constante  $c'' = c(A/K, \mathcal{L}) > 0$  ne dépendant que de  $(A/K, \mathcal{L})$ , telle que

$$\hat{h}_{\mathcal{L}}(P) \geq c''$$

pour tout point  $P \in A(K^{\text{ab}}) \setminus A(K^{\text{ab}})_{\text{tor}}$ .

Signalons aussi que le résultat de F. AMOROSO et U. ZANNIER en direction du problème de LEHMER relatif a été étendu au cas d'une courbe elliptique admettant des multiplications complexes par N. RATAZZI (*confer* [Rat]).

---

<sup>1</sup>On notera que  $\mathbb{G}_m(\overline{\mathbb{Q}^{\text{ab}}})_{\text{tor}} = \mathbb{G}_m(\mathbb{Q}^{\text{ab}})_{\text{tor}}$ .

Dans ce texte, nous nous intéressons au cadre des modules de DRINFEL'D<sup>2</sup>. Soit  $p$  un nombre premier et  $n$  un entier  $\geq 1$ , on pose  $q := p^n$ , on désigne par  $\mathbb{F}_q$  le corps fini à  $q$  éléments, et par  $A := \mathbb{F}_q[t] \subset k := \mathbb{F}_q(t)$ . Pour tout  $f/g \in k$ , soit  $|f/g|_\infty := \deg(g) - \deg(f)$  la valeur absolue de  $k$  associée à la place  $(1/t)$ , où  $\deg(f)$  dénote le degré de  $f$  comme polynôme. On désignera par la même notation  $|\cdot|$  une extension de  $|\cdot|_\infty$  à  $\bar{k}$ .

Soit  $\mathcal{C}$  une courbe lisse projective géométriquement connexe définie sur  $\mathbb{F}_q$  où l'on fixe un point  $x$ . Soit  $\mathcal{A}$  l'anneau des fonctions de  $\mathcal{C}$  régulières en tous points à l'exception de  $x$ . Notons que  $\mathcal{A}$  est une  $\mathbb{F}_q$ -algèbre de type fini, en d'autres termes, une extension entière de type fini de  $A = \mathbb{F}_q[t]$  pour un choix quelconque de  $t \in \mathcal{A} \setminus \mathbb{F}_q$ . Un corps  $\mathcal{F}$  est dit un  $\mathcal{A}$ -corps s'il existe un homomorphisme d'anneaux  $\iota : \mathcal{A} \rightarrow \mathcal{F}$ . Si cet homomorphisme est injectif, on dit que  $\mathcal{F}$  a *caractéristique générique*. Sinon, on dit qu'il a *caractéristique finie*  $\wp := \ker(\iota)$ .

Soit  $\mathcal{F}\{\tau\}$  l'anneau des polynômes tordus sur  $\mathcal{F}$ . Pour tout  $f := \sum_{i=0}^n a_i \tau^i \in \mathcal{F}\{\tau\}$ , on définit sa dérivation  $D$  en 0 par  $D(f) := a_0$ . Un homomorphisme de  $\mathbb{F}_q$ -algèbres  $\phi : \mathcal{A} \rightarrow \mathcal{F}\{\tau\}$  est dit un  $\mathcal{A}$ -module de DRINFEL'D défini sur  $\mathcal{F}$  si  $D \circ \phi = \iota$  et s'il existe  $a \in \mathcal{A}$  tel que  $\phi_a \neq \iota(a)\tau^0$ . D'après [Gos, chapter 4, lemma 4.5.1], il existe un entier  $r > 0$  tel que  $\deg(\phi_a) = r \deg(a)$ , pour tout  $a \in \mathcal{A}$ . L'entier  $r$  est appelé le *rang* de  $\phi$ . Si  $\mathcal{F}$  a caractéristique générique, on dit qu'il en est de même pour le module  $\phi$ .

Soient  $K/k$  une extension finie de  $k$ . Le corps  $K$  est considéré comme un  $A$ -corps de caractéristique générique par rapport à l'inclusion  $A \subset K$ . Soit  $\phi : A \rightarrow K\{\tau\}$  un  $A$ -module de DRINFEL'D de rang  $r \geq 1$  défini sur  $K$  de caractéristique générique. Soit  $\bar{K}$  une clôture algébrique de  $K$ ,  $K^s \subset \bar{K}$  une clôture séparable de  $K$  et  $K^{\text{ab}}$  la plus grande extension abélienne de  $K$  dans  $\bar{K}$ . On dispose d'une notion de hauteur de WEIL logarithmique et absolue  $h(\cdot)$  sur  $\bar{K}$  à valeurs dans  $\mathbb{R}^+$ . Par un procédé limite à la TATE, on peut normaliser la hauteur de WEIL pour obtenir une notion de *hauteur canonique associée* à  $\phi$  : soit  $a \in A \setminus \mathbb{F}_q$ , on définit la hauteur canonique  $\hat{h}_\phi : \bar{K} \rightarrow \mathbb{R}$  associée à  $\phi$  par :

$$\hat{h}_\phi(\alpha) := \lim_{n \rightarrow \infty} \frac{h(\phi_{a^n}(\alpha))}{\deg(\phi_{a^n})} ,$$

(confer [Den, théorème 1]). On vérifie (confer *loc. cit.*) que cette limite existe, ne dépend pas du choix de  $a$  et que de plus, pour tout  $\alpha \in \bar{K}$ ,

$$(1.0.1) \quad |\hat{h}_\phi(\alpha) - h(\alpha)| \leq \gamma(\phi) ,$$

où  $\gamma(\phi)$  est un nombre réel ( $\geq 0$ ) ne dépendant que de  $\phi$ .

Les questions (i) et (ii) ci-dessus se transposent naturellement dans le cadre des modules de DRINFEL'D munis de leur hauteur canonique pour tout point de  $\bar{K}$  qui n'est pas de torsion pour  $\phi$ .

Dans ce texte, nous résolvons le problème de LEHMER abélien ; plus précisément, nous obtenons le théorème suivant.

**Théorème 1.1.** *Il existe un nombre réel  $c = c(\phi, K) > 0$  qui ne dépend que de  $\phi$  et  $K$  tel que pour tout  $\alpha \in K^{\text{ab}}$  qui n'est pas de torsion<sup>3</sup> pour  $\phi$ , on ait*

$$\hat{h}_\phi(\alpha) \geq c .$$

<sup>2</sup> Sans aucune restriction sur le rang.

<sup>3</sup> Pour une définition précise, se reporter au début du paragraphe 2.1, ci-dessous.

**Remarque 1.2.** Si  $u : \phi \rightarrow \psi$  est un isomorphisme défini sur  $K$  de  $A$ -modules de DRINFEL'D également définis sur  $K$ , en vertu de la proposition 2 de [Poo], on a  $\hat{h}_\psi(u(\alpha)) = \hat{h}_\phi(\alpha)$ . Donc, si le théorème 1.1 est vrai pour  $\psi$ , la dernière égalité nous montre qu'il est aussi vrai pour  $\phi$ .

Le paragraphe 2 est dédié aux préliminaires. Il y a trois thèmes. D'abord on rappelle les faits généraux sur la torsion de modules de DRINFEL'D (§. 2.1), puis la théorie de la réduction (§. 2.2), et l'on introduit les hauteurs locales (§. 2.3). Au paragraphe 2.4, nous revisitons l'analogie du théorème de KRONECKER-WEBER (théorème 2.5 ci-dessous) pour les corps de fonctions (dû à DRINFEL'D, [Dri, theorem 1, section 8], *confer* aussi [Gos, chapter VII] et [Hay], nous suivons cette dernière exposition). Ce résultat nous permet de prouver une congruence (*confer* le théorème 2.7), qui est l'analogie de celle de AMOROSO et DVORNICICH, [Am-Dv, lemma 2]. Le troisième thème abordé (§. 2.8) est la construction d'un relèvement du morphisme de FROBENIUS dans le cas des modules admettant des multiplications complexes comme on peut le faire sur les variétés abéliennes (*confer* [Sh-Ta]), ce qui ne semblait pas être connu dans le cas d'un module de DRINFEL'D de rang quelconque. Un tel résultat (se reporter à la proposition 2.9) a son intérêt propre. L'existence de ce relèvement est un ingrédient de la preuve du théorème 1.1 dans le cas où  $\phi$  admet des multiplications complexes (pour une caractérisation des modules admettant des multiplications complexes, *confer* la proposition 2.12). Au paragraphe 3, nous prouvons les lemmes auxiliaires nécessaires pour la preuve du théorème 1.1. Finalement, nous démontrons le théorème en plusieurs étapes au paragraphe 4.

## 2. PRÉLIMINAIRES

**2.1. Torsion de modules de Drinfel'd.** Soit  $\phi : A \rightarrow K\{\tau\}$  un  $A$ -module de DRINFEL'D de rang  $r$ . Pour tout idéal  $\mathfrak{a}$  de  $A$  on considère l'idéal  $I_{\mathfrak{a},\phi}$  engendré par l'ensemble  $\{\phi_a \mid a \in \mathfrak{a}\}$ . L'anneau  $K\{\tau\}$  étant principal à gauche, soit  $\phi_a$  son générateur unitaire, *i. e.*,  $I_{\phi,\mathfrak{a}} = K\{\tau\}\phi_a$ .

Soit  $\phi[\mathfrak{a}] := \{\alpha \in \overline{K} \mid \text{pour tout } a \in \mathfrak{a}, \phi_a(\alpha) = 0\}$  l'ensemble des points de  $\mathfrak{a}$ -torsion de  $\phi$ . On observe que  $\alpha \in \phi[\mathfrak{a}]$  si et seulement si  $\phi_a(\alpha) = 0$ .

Soient  $n \geq 1$  un entier et  $\mathfrak{l}$  un idéal premier de  $A$ ; on note

$$\phi[\mathfrak{l}^n] := \{\alpha \in \overline{K} \mid \text{pour tout } a \in \mathfrak{l}^n, \phi_a(\alpha) = 0\}$$

le sous-module de points de  $\mathfrak{l}^n$ -torsion de  $\phi$ . Observons que puisque le polynôme  $\phi_a \in K\{\tau\}$  est séparable, tout  $\alpha \in \phi[\mathfrak{l}^n]$  appartient à  $K^s$ .

Soient  $A_{\mathfrak{l}}$ , respectivement  $k_{\mathfrak{l}}$  le localisé de  $A$ , respectivement de  $k$ , en  $\mathfrak{l}$ . On définit alors

$$\phi[\mathfrak{l}^\infty] := \varinjlim_n \phi[\mathfrak{l}^n] .$$

Rappelons que le  $\mathfrak{l}$ -module de TATE de  $\phi$  est défini par

$$T_{\mathfrak{l}}(\phi) := \text{Hom}(k_{\mathfrak{l}}/A_{\mathfrak{l}}, \phi[\mathfrak{l}^\infty]) ;$$

$T_{\mathfrak{l}}(\phi)$  est un  $A_{\mathfrak{l}}$ -module libre de rang  $r$  (souvenons que  $r = \text{rang}(\phi)$ ). Le groupe de GALOIS  $G_K := \text{Gal}(K^s/K)$  agit sur chaque  $\phi[\mathfrak{l}^n]$  pour tout  $n \geq 1$ , et agit donc sur  $T_{\mathfrak{l}}(\phi)$  par passage à la limite. On dispose donc d'une représentation galoisienne

$$\rho_{\mathfrak{l}^\infty} : G_K \rightarrow \text{Aut}(T_{\mathfrak{l}}(\phi)) \cong \text{GL}_r(A_{\mathfrak{l}}) .$$

Soit  $\mathfrak{p}$  un idéal premier de la clôture intégrale  $B$  de  $A$  dans  $K$ ; on note  $\kappa_{\mathfrak{p}}$  le corps résiduel  $\kappa_{\mathfrak{p}} := B/\mathfrak{p}$  et l'on désigne par  $q_{\mathfrak{p}} := \#\kappa_{\mathfrak{p}}$  son cardinal. Soit  $F_{\mathfrak{p}}$  l'automorphisme de FROBENIUS de  $\kappa_{\mathfrak{p}}$  défini par  $F_{\mathfrak{p}}(a) := a^{q_{\mathfrak{p}}}$ . On supposera désormais que  $\rho_{l^\infty}$  est non ramifiée en  $\mathfrak{p}$ , et l'on note  $\sigma_{\mathfrak{p}} \in G_K$  l'automorphisme de FROBENIUS associé à  $\mathfrak{p}$ . Soit  $P_{\mathfrak{p}}(x) \in A[x]$  le polynôme caractéristique de  $\rho_{l^\infty}(\sigma_{\mathfrak{p}})$ .

**2.2. Réduction de modules de Drinfel'd.** Soit  $a \in A$  et  $\phi_a$  l'élément de  $K\{\tau\}$  associé :

$$\phi_a = a + c_1(a)\tau + \cdots + c_{r \deg(a)-1}(a)\tau^{r \deg(a)-1} + \Delta(a)\tau^{r \deg(a)} .$$

On dit que le  $A$ -module de DRINFEL'D  $\phi$  est à *coefficients constants en  $\mathfrak{p}$* , si pour tout  $i$  on a  $c_i(a), \Delta(a) \in B_{\mathfrak{p}}$ , où  $B_{\mathfrak{p}}$  est la localisation de  $B$  en  $\mathfrak{p}$ , et si la réduction  $\tilde{\phi}$  de  $\phi$  modulo  $\mathfrak{p}$  est un  $A$ -module de DRINFEL'D défini sur  $\kappa_{\mathfrak{p}}$  de rang  $0 < \tilde{r} \leq r$ . On dit que  $\phi$  est de *réduction stable* en  $\mathfrak{p}$ , s'il existe un  $A$ -module de DRINFEL'D  $\psi$  défini sur  $K$  et  $K$ -isomorphe à  $\phi$  qui est à coefficients constants en  $\mathfrak{p}$ . On dit que  $\phi$  a *bonne réduction en  $\mathfrak{p}$*  si de plus  $\tilde{r} = r$  (*confer* [Gos, 4.10]).

L'analogue du critère de NÉRON-OGG-SHAFAREVICH pour la bonne réduction d'une variété abélienne définie sur un corps des nombres  $L$  sur un idéal premier de la clôture intégrale de  $L$ , existe dans le cadre des modules de DRINFEL'D et est dû à TAKAHASHI (*confer* [Tak], [Gos, theorem 4.10.5]). Il dit que si  $v$  est une place de  $K$  dont la caractéristique résiduelle (*i. e.*, la caractéristique de  $\mathcal{O}_v/\mathcal{M}_v$ ) est différente d'un idéal premier fixé  $\mathfrak{p}$  de  $A$ , le module de DRINFEL'D  $\phi$  a bonne réduction en  $v$  si et seulement si  $\phi[\mathfrak{p}^\infty]$  est non ramifié en  $v$ . Cela veut dire que si  $\bar{v}$  est une extension de  $v$  à  $K^s$  et si  $I_{\bar{v}}$  est le groupe d'inertie associé, alors  $I_{\bar{v}}$  agit trivialement sur  $\phi[\mathfrak{p}^\infty]$ .

De ce résultat, on déduit (*confer* [Gos, corollary 4.10.10]) que si  $l \neq \mathfrak{p}$ , la représentation galoisienne  $\rho_{l^\infty}$  est non ramifiée en  $\mathfrak{p}$  si et seulement si  $\phi$  a bonne réduction en  $\mathfrak{p}$ . Donc, le fait que  $\rho_{l^\infty}$  est non ramifiée en  $\mathfrak{p}$  ne dépend pas du choix de  $l$ , *i. e.*, le même résultat vaut pour n'importe quel autre idéal premier  $l' \neq \mathfrak{p}$ .

Supposons que  $\rho_{l^\infty}$  soit non ramifiée en  $\mathfrak{p}$ . Le polynôme  $P_{\mathfrak{p}}(x) \in A[x]$  coïncide avec le polynôme caractéristique de l'endomorphisme de FROBENIUS (également noté  $F_{\mathfrak{p}}$ ) de  $T_l(\phi)$ . Il suit de [Gos, theorem 4.12.12] que  $P_{\mathfrak{p}}(x)$  ne dépend pas du choix de  $l$ . De plus, par [Gek2, theorem 5.1] toute racine  $\gamma$  de  $P_{\mathfrak{p}}$  est de valeur absolue  $|\gamma| = q_{\mathfrak{p}}^{1/r}$ , où  $|\cdot|$  dénote une extension de la valeur absolue  $|\cdot|_{\infty}$  de  $k$  à  $\bar{K}$ .

**2.3. Hauteurs locales.** Nous allons démontrer le théorème 1.1 en minorant de façon non triviale la hauteur de WEIL locale de  $\alpha$  au-dessus d'un idéal premier  $\mathfrak{p}$  de la clôture intégrale  $B$  de  $A$  dans  $K$  et trivialement pour les autres places. Rappelons quelques normalisations. Soit  $L$  une extension finie de  $K$  et  $\mathfrak{P}$  un premier de la clôture intégrale  $B_L$  de  $B$  dans  $L$ . On notera  $v_{\mathfrak{P}}$  la valuation associée à  $\mathfrak{P}$  normalisée par  $v_{\mathfrak{P}}(L) = \mathbb{Z} \cup \{\infty\}$ , et on pose enfin  $\tilde{v}_{\mathfrak{P}} := \min\{v_{\mathfrak{P}}, 0\}$ .

L'existence d'une bonne décomposition de la hauteur de WEIL  $h$  en somme de hauteurs locales découle immédiatement de sa définition : rappelons que si  $\alpha \in \bar{K}$ , et si  $L$  est une extension finie de  $K$  contenant  $\alpha$ ,

$$h(\alpha) = -\frac{1}{[L:k]} \sum_{\mathfrak{P} \in M_L} \deg(\mathfrak{P}) \tilde{v}_{\mathfrak{P}}(\alpha) .$$

On pose alors

$$(2.3.1) \quad h_{\mathfrak{P}}(\alpha) := -\frac{\deg(\mathfrak{P}) \tilde{v}_{\mathfrak{P}}(\alpha)}{[L:k]} .$$

Il est intéressant de noter que la hauteur canonique de  $\phi$  admet également une bonne décomposition en somme de hauteurs locales positives ou nulles (c'est un théorème de POONEN, *confer* [Poo, §4, proposition 6]); de plus, lorsque  $\phi$  a bonne réduction en  $\mathfrak{P}$  et si  $\phi$  est à coefficients constants (ce qui peut être supposé sans perte de généralité) et  $\Delta(a)$  est une unité modulo  $\mathfrak{P}$  pour tout  $a \in A$ , la hauteur canonique locale coïncide avec la hauteur de WEIL locale (*ibidem*, proposition 4, point (4)). Pour les définitions de bonne réduction, coefficients constants et  $\Delta(a)$  voir le sous-paragraphe 2.2.

#### 2.4. Un analogue du théorème de Kronecker-Weber et une congruence.

Le corps  $K$  est le corps de fonctions  $\mathbb{F}_q(C)$  d'une courbe projective lisse géométriquement connexe  $C$  définie sur  $\mathbb{F}_q$ . Soit  $\infty' \in C$  au-dessus du point à l'infini  $\infty$  (qui correspond donc au zéro de la fonction  $(1/t)$  de  $\mathbb{P}^1(\mathbb{F}_q)$ ). Soit  $\mathfrak{D}$  l'anneau des fonctions de  $C$  qui sont régulières partout à l'exception de  $\infty'$ . Soient  $H'$  le corps de classe de HILBERT de  $\mathfrak{D}$ ,  $K_{\infty'}$  le complété de  $K$  en  $\infty'$ ,  $\mathbb{C}_{\infty'}$  le complété de la clôture algébrique de  $K_{\infty'}$  et  $\mathbb{F}_{\infty'}$  le corps résiduel de  $\infty'$ .

Une *fonction signe* est un homomorphisme  $\text{sgn} : K_{\infty'}^* \rightarrow \mathbb{F}_{\infty'}^*$ , tel que sa restriction à  $\mathbb{F}_{\infty'}^*$  soit l'identité. On définit aussi  $\text{sgn}(0) := 0$ . Pour tout  $\sigma \in \text{Aut}(\mathbb{F}_{\infty'}/\mathbb{F}_q)$ , la composition  $\sigma \circ \text{sgn}$  est appelée une *fonction signe tordue*.

Soit  $F$  une extension finie de  $K$  contenue dans  $\mathbb{C}_{\infty'}$  et  $\varsigma : \mathfrak{D} \rightarrow F\{\tau\}$  un  $\mathfrak{D}$ -module de DRINFEL'D de rang 1. Pour tout  $a \in \mathfrak{D}$  soit  $\mu_{\varsigma}(a)$  le coefficient dominant de  $\varsigma_a$ . On dit que  $\varsigma$  est de *signe normalisé*, si l'application  $\mathfrak{D} \rightarrow F^*$  définie par  $a \mapsto \mu_{\varsigma}(a)$  est la restriction d'une fonction  $\text{sgn}$  signe tordue. Le résultat de HAYES (*confer* [Hay, theorem 12.3]) nous assure que tout  $\mathfrak{D}$ -module de DRINFEL'D de rang 1 défini sur  $\mathbb{C}_{\infty'}$  est isomorphe à un module de signe normalisé. On supposera dorénavant que  $\varsigma$  est de signe normalisé par rapport à  $\text{sgn}$  et on fixera ce module.

Soit  $a \in \mathfrak{D} \setminus \mathbb{F}_q$ . Soit  $H^+$  le sous-corps de  $\mathbb{C}_{\infty}$  engendré sur  $K$  par les coefficients de  $\varsigma_a$ . Ce corps est en réalité indépendant de  $a$  et  $\varsigma$ , et ne dépend que de  $\text{sgn}$ . Il contient  $H'$ , définit une extension galoisienne finie de  $K$  non ramifiée au-dessus de chaque idéal premier de  $\mathfrak{D}$ . De plus, si  $\mathfrak{D}^+$  est la clôture intégrale de  $\mathfrak{D}$  dans  $H^+$ , le  $\mathfrak{D}$ -module  $\varsigma$  de signe normalisé est en réalité défini sur  $\mathfrak{D}^+$ .

Soit  $I$  un idéal de  $\mathfrak{D}$  et  $K(I) := H^+(\varsigma[I])$ . Ce corps est indépendant de  $\varsigma$  et de  $\text{sgn}$ , il ne dépend que de  $I$ . Il définit une extension galoisienne finie de  $H^+$  de groupe de GALOIS isomorphe à  $(\mathfrak{D}/I)^*$ . De plus,  $K(I)/K$  est aussi galoisienne de groupe de GALOIS isomorphe à  $\mathcal{I}(I)/\mathcal{P}_I^+$ , où  $\mathcal{I}(I)$  désigne l'ensemble des idéaux fractionnaires premiers à  $I$  et  $\mathcal{P}_I^+$  le sous-groupe des idéaux principaux engendrés par les éléments positifs  $\alpha \in K$  tels que  $\alpha \equiv 1 \pmod{I}$ . Rappelons qu'un élément  $\alpha$  de  $K$  est dit *positif*, si  $\text{sgn}(\alpha) = 1$ .

Le groupe  $\text{Gal}(K(I)/K)$  contient un sous-groupe  $G_{\infty}$  isomorphe à  $\mathbb{F}_{\infty}^*$ . On notera que le groupe  $G_{\infty}$  est simultanément le groupe de décomposition et d'inertie de  $\infty$  dans  $\text{Gal}(K(I)/K)$ . L'extension  $K(I)/K$  est modérément ramifiée sur  $\infty$ . Soit  $K(I)^+$  le sous-corps de  $K(I)$  fixé par  $G_{\infty}$ . Donc,  $K(I)^+/K$  est totalement décomposée en  $\infty$ . De plus,  $K(I)^+$  est  $K$ -isomorphe au corps de fonctions du schéma  $M_I^1$  qui paramétrise les  $\mathfrak{D}$ -modules de DRINFEL'D de rang 1 avec structure de niveau  $I$ .

Soit

$$K_{\infty'}^+ := \prod_I K(I)^+ ,$$

le compositum de tous ces corps. Soit  $\infty''$  un autre point de  $C$  distinct de  $\infty'$ . On définit similairement  $K_{\infty''}^+$  par rapport à l'anneau  $\mathfrak{D}'$  des fonctions régulières hors de  $\infty''$ .

**Théorème 2.5** (analogue du théorème de KRONECKER-WEBER). [Gos, remark 7.5.12 (3)] *La plus grande extension abélienne  $K^{\text{ab}}$  de  $K$  est le compositum  $K_{\infty'}^+ \cdot K_{\infty''}^+$ .*

Pour fixer les notations, soient  $\zeta'$  un  $\mathfrak{D}'$ -module de DRINFEL'D de signe normalisé par rapport une fonction signe  $\text{sgn}'$ ,  $H'^+$  le corps engendré par  $K$  et les coefficients de  $\zeta'_a$  pour un  $a \in \mathfrak{D}' \setminus \mathbb{F}_q$ , et  $\mathfrak{D}'^+$  la clôture intégrale de  $\mathfrak{D}$  dans  $H'^+$ .

Soit  $I \subset \mathfrak{D}$  un idéal. Il suit du fait que  $\zeta$  est de rang 1 que  $\zeta[I] \cong \mathfrak{D}/I$  est un  $\mathfrak{D}$ -module cyclique, disons engendré par  $\lambda_I$ . De façon similaire, soit  $I' \subset \mathfrak{D}'$  un idéal et  $\lambda_{I'}$  un générateur de  $\zeta'[I']$  comme  $\mathfrak{D}'$ -module. Observons que la clôture intégrale de  $\mathfrak{D}$  dans le compositum  $H^+(\lambda_I) \cdot H'^+(\lambda_{I'}) = H^+ \cdot H'^+(\lambda_I, \lambda_{I'})$  est l'anneau  $\mathfrak{D}^+ \cdot \mathfrak{D}'^+[\lambda_I, \lambda_{I'}]$ . Soit  $\mathcal{Q}$  un idéal premier de  $\mathfrak{D}$  divisant  $I$ . De plus, supposons que  $s \geq 1$  soit un entier tel que  $\mathcal{Q}^s$  divise  $I$ .

**Proposition 2.6.** *Soit  $\eta \neq \text{id} \in \text{Gal}(H^+ \cdot H'^+(\lambda_I, \lambda_{I'})/H^+ \cdot H'^+(\lambda_{I/\mathcal{Q}^s}, \lambda_{I'}))$ . Pour tout  $\alpha \in \mathfrak{D}^+ \cdot \mathfrak{D}'^+[\lambda_I, \lambda_{I'}]$  on a*

$$(\eta(\alpha))^{q^s \deg(\mathcal{Q})} - \alpha^{q^s \deg(\mathcal{Q})} \in \mathcal{Q}\mathfrak{D}^+ \cdot \mathfrak{D}'^+[\lambda_I, \lambda_{I'}] .$$

*Démonstration.* Soit  $\alpha = f(\lambda_I, \lambda_{I'}) = \sum_{i,j} a_{ij} \lambda_I^i \lambda_{I'}^j$ , avec  $a_{ij} \in \mathfrak{D}^+ \cdot \mathfrak{D}'^+$  pour tout  $i$  et  $j$ . Donc,  $\eta(\alpha) = f(\eta(\lambda_I), \lambda_{I'})$ .

Pour tout  $m \in \mathcal{Q}^s$  on a  $\zeta_m(\lambda_I) \in \zeta[I/\mathcal{Q}^s]$ . D'où,  $\zeta_m(\eta(\lambda_I)) = \eta(\zeta_m(\lambda_I)) = \zeta_m(\lambda_I)$ . En particulier, il existe  $\omega \in \zeta[\mathcal{Q}^s]$  tel que  $\eta(\lambda_I) - \lambda_I = \omega$ . Donc,

$$\eta(\alpha) = f(\lambda_I + \omega, \lambda_{I'}) = \sum_{i,j} a_{ij} (\lambda_I + \omega)^i \lambda_{I'}^j .$$

Ainsi,

$$\eta(\alpha) - \alpha = \sum_{i,j} a_{ij} \sum_{1 \leq k \leq i} \binom{i}{k} \lambda_I^{i-k} \omega^k \lambda_{I'}^j = \omega \beta ,$$

où  $\beta \in \mathfrak{D}^+ \cdot \mathfrak{D}'^+[\lambda_I, \lambda_{I'}]$ , car  $\omega \in \mathfrak{D}^+[\lambda_{\mathcal{Q}^s}] \subset \mathfrak{D}^+[\lambda_I] \subset \mathfrak{D}^+ \cdot \mathfrak{D}'^+[\lambda_I, \lambda_{I'}]$ .

Comme on l'a déjà observé au paragraphe 2.1, le fait que  $\omega \in \zeta[\mathcal{Q}^s]$  équivaut à  $\zeta_{\mathcal{Q}^s}(\omega) = 0$ . Rappelons que l'extension  $H^+/K$  est non ramifiée au-dessus de  $\mathcal{Q}$  et que  $\zeta$  est défini sur  $\mathfrak{D}^+$ . Donc, par [Hay, proposition 11.4], le polynôme  $\zeta_{\mathcal{Q}^s}$  est un produit des polynômes d'EISENSTEIN en  $\mathcal{Q}$ . *A fortiori*, tous les coefficients, sauf le coefficient dominant, appartiennent à  $\mathcal{Q}$ . Disons,

$$\zeta_{\mathcal{Q}^s}(\tau) = \tau^{s \deg(\mathcal{Q})} + c_{s \deg(\mathcal{Q})-1} \tau^{s \deg(\mathcal{Q})-1} + \dots + c_0 \tau^0 .$$

Finalement,

$$\begin{aligned} (\eta(\alpha) - \alpha)^{q^s \deg(\mathcal{Q})} &= \omega^{q^s \deg(\mathcal{Q})} \beta^{q^s \deg(\mathcal{Q})} = \\ &- (c_{s \deg(\mathcal{Q})-1} \omega^{q^s \deg(\mathcal{Q})-1} + \dots + c_0 \omega) \beta^{q^s \deg(\mathcal{Q})} \in \mathcal{Q}\mathfrak{D}^+ \cdot \mathfrak{D}'^+[\lambda_I, \lambda_{I'}]. \end{aligned}$$

□

De cette proposition, on déduit l'analogie de la congruence de F. AMOROSO et R. DVORNICICH :

**Théorème 2.7.** *Soit  $L/K$  une extension abélienne finie ramifiée au-dessus d'un idéal premier  $\mathfrak{p}$  de la clôture intégrale  $B$  de  $A$  dans  $K$ . Soit  $\mathfrak{P}$  un premier de la clôture intégrale  $B_L$  de  $L$  au-dessus de  $\mathfrak{p}$ . Il existe  $\eta \neq \text{id}$  dans l'inertie de  $\mathfrak{P}$  sur  $\mathfrak{p}$  tel que pour tout  $\alpha \in B_L$  on ait*

$$(\eta(\alpha))^{q^{\deg(\mathfrak{p})}} - \alpha^{q^{\deg(\mathfrak{p})}} \in \mathfrak{p}B_L .$$

*Démonstration.* Il suit du théorème 2.5 qu'il existe des idéaux  $I \subset \mathfrak{D}$  et  $I' \subset \mathfrak{D}'$  tels que  $L \subset K(I)^+ \cdot K(I')^+ \subset H^+(\zeta[I]) \cdot H'^+(\zeta'[I'])$ . Observons que par le choix du point  $\infty'$  de  $C$  (dont  $K$  est le corps de fonctions) on a  $\mathfrak{D} \subset B$ . Soit  $\mathcal{Q} := \mathfrak{p} \cap \mathfrak{D}$ .

Par hypothèse,  $\mathcal{Q}$  divise  $I$ , sinon  $L/K$  serait non ramifiée au-dessus de  $\mathfrak{p}$ . Donc, par la proposition 2.6 on a

$$(2.7.1) \quad (\eta(\alpha))^{q^{\deg(\mathcal{Q})}} - \alpha^{q^{\deg(\mathcal{Q})}} \in \mathcal{Q}\mathfrak{D}^+ \cdot \mathfrak{D}'^+[\lambda_I, \lambda_{I'}],$$

pour  $\eta \neq \text{id} \in \text{Gal}(H^+ \cdot H'^+(\lambda_I, \lambda_{I'})/H^+ \cdot H'^+(\lambda_{I/\mathcal{Q}}, \lambda_{I'}))$ . Notons que la restriction de  $\eta$  à  $\text{Gal}(L/K)$  appartient à l'inertie de  $\mathfrak{P}|\mathfrak{p}$ . Il suit de la relation (2.7.1) que  $(\eta(\alpha))^{q^{\deg(\mathcal{Q})}} - \alpha^{q^{\deg(\mathcal{Q})}} \in \mathcal{Q}B_L \subset \mathfrak{p}B_L$ . *A fortiori*,  $(\eta(\alpha))^{q^{\deg(\mathfrak{p})}} - \alpha^{q^{\deg(\mathfrak{p})}} \in \mathfrak{p}B_L$ .  $\square$

**2.8. Relèvement du Frobenius.** Nous retournons à la situation de l'introduction. Soit  $\phi : A \rightarrow K\{\tau\}$  un module de DRINFEL'D défini sur une extension finie  $K$  de  $k = \mathbb{F}_q(t)$ , donc de caractéristique générique et de rang  $r$ .

Soit  $\text{End}(\phi)$  l'anneau des endomorphismes de  $\phi$  sur  $\overline{K}$ . On peut voir  $A$  comme un sous-anneau de  $\text{End}(\phi)$ , puisque pour tout  $a \in A$ ,  $\phi_a$  commute avec  $\phi_b$  pour chaque  $b \in A$ . Pour simplifier la terminologie, on dira que le module  $\phi$  est à *multiplications complexes* par  $\mathcal{O} := \text{End}(\phi)$ , si  $A \subsetneq \mathcal{O}$  et si  $\mathcal{O} \otimes_A k$  est une extension de  $k$  de degré égal à  $r = \text{rang}(\phi)$ . Sinon (par exemple si  $A = \text{End}(\phi)$  et  $r > 1$ ), on dit que  $\phi$  est *sans multiplications complexes*<sup>4</sup>.

Nous supposons dans ce paragraphe que  $\phi$  est un module de rang  $r$  admettant des multiplications complexes par  $\mathcal{O}$ . Dans ce cas, on peut considérer  $\phi$  comme un  $\mathcal{O}$ -module de DRINFEL'D de rang 1 et on peut appliquer la théorie de corps de classes (*confer* [Hay]) pour produire un relèvement du FROBENIUS.

Soit  $\mathcal{F} := \text{Frac}(\mathcal{O})$  le corps de fractions de  $\mathcal{O}$  que l'on suppose contenu dans  $K$  et soit  $B$  la clôture intégrale de  $A$  dans  $K$ .

Soit  $\mathfrak{p} \subset B$  un idéal premier tel que  $\phi$  ait bonne réduction en  $\mathfrak{p}$ , et  $\mathfrak{m} := \mathfrak{p} \cap \mathcal{O}$ .

Soit enfin  $H$  le corps de classes de HILBERT de  $\mathcal{O}$ . Supposons de plus que  $H \subset K$ . On notera  $\mathcal{O}'$  la clôture intégrale de  $\mathcal{O}$  dans  $H$ ; comme  $\mathcal{O}$  est entier sur  $A$ , on remarque que  $\mathcal{O}' \subset B$ .

Comme  $\phi$  est un  $\mathcal{O}$ -module de rang 1, il existe un  $\mathcal{O}$ -module  $\psi$  de rang 1, défini sur  $H$  et isomorphe à  $\phi$  sur  $K$ , *i. e.*,  $\phi \cong \psi \times_H K$ . En d'autres termes, il existe un élément  $z \in K^*$  tel que  $\phi = z\psi z^{-1}$ . En particulier, on obtient un isomorphisme entre les anneaux  $\mathcal{O} = \text{End}(\phi) \rightarrow \text{End}(\psi)$  défini par  $f \mapsto z^{-1}fz$ .

On considère l'idéal  $I_{\psi, \mathfrak{m}}$  de  $H\{\tau\}$  engendré par l'ensemble  $\{\psi_m \mid m \in \mathfrak{m}\}$ . L'anneau  $H\{\tau\}$  étant principal à gauche, soit  $\psi_{\mathfrak{m}}$  son générateur unitaire, *i. e.*,  $I_{\psi, \mathfrak{m}} = H\{\tau\}\psi_{\mathfrak{m}}$ . Observons que  $I_{\psi, \mathfrak{m}}$  est stable par multiplication à droite par  $\psi_x$  pour  $x \in \mathcal{O}$ . *A fortiori*, pour tout  $x \in \mathcal{O}$  il existe un seul  $\psi'_x \in H\{\tau\}$  tel que  $\psi_{\mathfrak{m}}\psi_x = \psi'_x\psi_{\mathfrak{m}}$ . Cela définit une fonction  $\psi' : \mathcal{O} \rightarrow H\{\tau\}$  qui est en fait également

<sup>4</sup>On notera que notre définition (qui provient de [Li, deuxième paragraphe de la page 154]) permet à un module  $\phi$  sans multiplications complexes d'avoir un endomorphisme qui n'appartient pas à  $A$ . Cela arrive d'ailleurs dès que le rang  $r$  est un nombre composé. Elle est présentée de cette manière pour garantir la validité de la proposition 2.12.

un  $\mathcal{O}$ -module de DRINFEL'D, que l'on notera  $\mathfrak{m} * \psi$  suivant HAYES. Observons que cette construction est également valable pour des modules de DRINFEL'D de rang arbitraire (*confer* [Hay, §4]). Mais ici, comme  $\phi$  et  $\psi$  sont de rang 1, le module  $\mathfrak{m} * \phi$  l'est aussi.

Soit  $(\mathfrak{m}, H/\mathcal{F})$  le symbole d'ARTIN de l'extension  $H/\mathcal{F}$  en  $\mathfrak{m}$ . D'après un résultat de HAYES (*confer* [Hay, theorem 10.8]) on dispose d'un isomorphisme de  $\mathcal{O}$ -modules de DRINFEL'D

$$(\mathfrak{m}, H/\mathcal{F})(\psi) \cong \mathfrak{m} * \psi .$$

Par le théorème de ČEBOTAREV (*confer* [Fr-Ja, theorem 6.3.1], et, pour la version effective [Fr-Ja, proposition 6.4.8]) on peut choisir  $\mathfrak{m}$  tel que  $(\mathfrak{m}, H/\mathcal{F}) = 1$ . Par conséquent,  $\psi \cong \mathfrak{m} * \psi$ , *i. e.*, il existe un élément  $u$  de  $H^*$  tel que  $\mathfrak{m} * \psi = u\psi u^{-1}$ . Il en suit que  $\lambda_{\mathfrak{m}} := u^{-1}\psi_{\mathfrak{m}}$  appartient à  $\text{End}(\psi)$ .

Un résultat dû à TAKAHASHI (*confer* [Tak], et [Hay, theorem 15.8]) nous assure qu'il existe un  $\mathcal{O}$ -module de DRINFEL'D  $\hat{\psi}$  défini sur  $\mathcal{O}'$  tel que  $\psi \cong \hat{\psi} \times_{\mathcal{O}'} H$ . Donc, pour tout  $x \in \mathcal{O}$  on a  $\hat{\psi}_x \in \mathcal{O}'\{\tau\}$  et le coefficient dominant de  $\hat{\psi}_x$  est une unité de  $\mathcal{O}'$ . Il n'y a pas de restriction à travailler avec  $\hat{\psi}$  en lieu et place de  $\psi$ ; nous supposons donc par la suite que  $\psi = \hat{\psi}$  et garderons la notation  $\psi$  pour alléger.

Soit  $\mathfrak{n}$  un idéal premier de  $\mathcal{O}'$  au-dessus de  $\mathfrak{m}$ . On en conclut que  $\phi$  a bonne réduction en  $\mathfrak{p}$  si et seulement si  $\psi$  a bonne réduction en  $\mathfrak{n}$ . Dans ce cas-là, on déduit que  $z$  est une unité en  $\mathfrak{p}$ . De plus, comme on a une isogénie  $\psi \rightarrow \mathfrak{m} * \psi$  définie par  $\psi_{\mathfrak{m}}$ , on en déduit que  $\mathfrak{m} * \psi$  a également bonne réduction en  $\mathfrak{n}$  (*confer* [Tag]), ce qui implique que  $u$  est une unité en  $\mathfrak{n}$ .

Soient  $\tilde{\psi}$  la réduction de  $\psi$  modulo  $\mathfrak{n}$  et  $\kappa_{\mathfrak{n}} := \mathcal{O}'/\mathfrak{n}$  le corps résiduel en  $\mathfrak{n}$ . Le module  $\tilde{\psi}$  est de caractéristique  $\mathfrak{n} = \mathfrak{m} \cap \mathcal{O}$ . Soit  $I_{\tilde{\psi}, \mathfrak{m}}$  l'idéal de  $\kappa_{\mathfrak{n}}\{\tau\}$  engendré par  $\{\tilde{\psi}_m \mid m \in \mathfrak{m}\}$ . Soit  $\tilde{\psi}_m$  son générateur unitaire, *i. e.*,  $I_{\tilde{\psi}, \mathfrak{m}} = \kappa_{\mathfrak{n}}\{\tau\}\tilde{\psi}_m$ . Par [Hay, proposition 5.9] on a  $\tilde{\psi}_m = \tau^{\deg(\mathfrak{m})}$ , et  $\tau^{\deg(\mathfrak{m})}$  coïncide avec l'endomorphisme de FROBENIUS  $\text{Frob}_{\mathfrak{n}}$  de  $\psi$ , car l'hypothèse  $(\mathfrak{m}, H/\mathcal{F}) = 1$  implique  $\deg(\mathfrak{m}) = \deg(\mathfrak{n})$ .

Il suit de [Hay, proposition 11.4] que  $\psi_{\mathfrak{m}}$  est un polynôme d'EISENSTEIN en  $\mathfrak{n}$ . En particulier,  $\psi_{\mathfrak{m}} \in \mathcal{O}'_{\mathfrak{n}}\{\tau\}$ . D'après le résultat de TAKAHASHI on peut considérer l'idéal  $I'_{\psi, \mathfrak{m}}$  de  $\mathcal{O}'_{\mathfrak{n}}\{\tau\}$  engendré par  $\{\psi_m \mid m \in \mathfrak{m}\}$ . Observons que  $I'_{\psi, \mathfrak{m}} \subset I_{\psi, \mathfrak{m}}$ , où ce dernier est l'idéal de  $H\{\tau\}$  engendré par  $\{\psi_m \mid m \in \mathfrak{m}\}$ . Par la minimalité du degré,  $\psi_{\mathfrak{m}}$  engendre simultanément les idéaux  $I_{\psi, \mathfrak{m}}$  et  $I'_{\psi, \mathfrak{m}}$ . De plus, on a un homomorphisme surjectif  $I'_{\psi, \mathfrak{m}} \twoheadrightarrow I_{\tilde{\psi}, \mathfrak{m}}$  de réduction modulo  $\mathfrak{n}$ . Donc, par minimalité des degrés des générateurs, on en conclut que

$$(2.8.1) \quad \deg(\mathfrak{m}) = \deg(\tilde{\psi}_m) = \deg(\psi_m) .$$

D'autre part, la proposition [Hay, proposition 11.4] nous donne des informations supplémentaires. Pour chaque entier  $i \geq 1$ , le polynôme  $\psi_{\mathfrak{m}^{i+1}}$  divise  $\psi_{\mathfrak{m}^i}$  dans  $\mathcal{O}'_{\mathfrak{n}}\{\tau\}$  et le quotient est un polynôme d'EISENSTEIN en  $\mathfrak{n}$ . Donc, si  $\nu := \frac{\deg(\mathfrak{p})}{\deg(\mathfrak{m})}$ , on a

$$\widetilde{\psi_{\mathfrak{m}^{\nu}}} = \tau^{\deg(\mathfrak{p})} = \text{Frob}_{\mathfrak{p}} .$$

Soit  $c \in \mathcal{O}^*$  dont la réduction  $\tilde{c}$  modulo  $\mathfrak{m}$  (donc modulo  $\mathfrak{n}$ ) est égale à  $\tilde{u}$  (on rappelle que  $u$  est une unité locale en  $\mathfrak{n}$ ). Soit  $\lambda_{\mathfrak{m}^{\nu}} := u^{-1}\psi_{\mathfrak{m}^{\nu}}$ . On prend maintenant  $\vartheta_{\mathfrak{m}^{\nu}} := c\lambda_{\mathfrak{m}^{\nu}}$  et on obtient que  $\vartheta_{\mathfrak{m}^{\nu}} \in \text{End}(\psi)$  et  $\widetilde{\vartheta_{\mathfrak{m}^{\nu}}} = \tau^{\deg(\mathfrak{p})} = \text{Frob}_{\mathfrak{p}}$ . Finalement, en prenant l'isomorphisme inverse  $\text{End}(\psi) \rightarrow \mathcal{O} = \text{End}(\phi)$ , on voit que  $F_{\mathfrak{p}} := z\vartheta_{\mathfrak{m}^{\nu}}z^{-1}$  est un relèvement de l'endomorphisme de FROBENIUS  $\text{Frob}_{\mathfrak{p}}$  de  $\tilde{\phi}$  à  $\mathcal{O} = \text{End}(\phi)$ , d'où la proposition suivante.

**Proposition 2.9.** *Il existe  $F_{\mathfrak{p}} := z\vartheta_{\mathfrak{m}^\nu}z^{-1} \in \mathcal{O}$  qui relève l'endomorphisme de FROBENIUS  $\text{Frob}_{\mathfrak{p}}$  de  $\tilde{\mathcal{O}} := \text{End}(\tilde{\phi})$ .*

**Remarque 2.10.** Soit  $\phi[F_{\mathfrak{p}}] := \{\alpha \in \overline{K} \mid F_{\mathfrak{p}}(\alpha) = 0\}$ . Notons que  $\alpha \in \phi[F_{\mathfrak{p}}]$  si et seulement si  $\alpha$  est un zéro de  $\vartheta_{\mathfrak{m}^\nu}$ , i. e., de  $\psi_{\mathfrak{m}^\nu}$ . Mais,  $\psi_{\mathfrak{m}^\nu}$  engendre l'idéal  $I_{\psi, \mathfrak{m}^\nu}$ , donc cette dernière condition équivaut à  $\alpha \in \psi[\mathfrak{m}^\nu]$ . De plus, comme  $\phi$  est  $K$ -isomorphe à  $\psi$ , on a  $\alpha \in \psi[\mathfrak{m}^\nu]$  si et seulement si  $\alpha \in \phi[\mathfrak{m}^\nu]$ . D'où,

$$(2.10.1) \quad \phi[F_{\mathfrak{p}}] = \phi[\mathfrak{m}^\nu] \cong \psi[\mathfrak{m}^\nu] \cong \mathcal{O}/\mathfrak{m}^\nu$$

est un  $\mathcal{O}$ -module de cardinal  $q_{\mathfrak{p}} = q^{\deg(\mathfrak{p})}$ . On aura besoin du deuxième isomorphisme dans la preuve de la proposition 3.11.

**2.11. Multiplication complexe et torsion.** On note  $\phi_{\text{tor}}$  l'ensemble des *points de torsion* pour  $\phi$  :

$$\phi_{\text{tor}} := \{\alpha \in \overline{K} \mid \text{il existe } a \in A \setminus \{0\} \text{ tel que } \phi_a(\alpha) = 0\}$$

et enfin,  $\phi_{\text{tor}}(K^{\text{ab}}) := \phi_{\text{tor}} \cap K^{\text{ab}}$ .

Rappelons le résultat suivant dû à A. LI qui permet de caractériser les  $A$ -modules de DRINFEL'D qui admettent des multiplications complexes. Cette caractérisation jouera un rôle non négligeable dans la preuve du théorème 1.1.

**Proposition 2.12.** [Li, main theorem] *Le  $A$ -module de Drinfel'd  $\phi$  admet des multiplications complexes si et seulement si  $\phi(K^{\text{ab}})_{\text{tor}}$  est infini.*

### 3. LEMMES AUXILIAIRES

**3.1. Cas non CM et non ramifié.** Soit  $a \in A$ ,  $\sigma$  un élément de  $G_K$  et  $\alpha \in K^s$ . On conviendra pour la suite que  $a\sigma(\alpha) := \phi_a(\sigma(\alpha))$ . On étend par linéarité cette action à tout l'anneau de groupe  $A[G_K]$  par

$$\left( \sum_{\sigma \in G_K} a_\sigma \sigma \right) (\alpha) := \sum_{\sigma \in G_K} \phi_{a_\sigma}(\sigma(\alpha)) .$$

Soit  $B^s$  la clôture entière de  $B$  dans  $K^s$  et  $\mathfrak{p}^s \subset B^s$  un idéal premier tel que  $\mathfrak{p}^s \cap B = \mathfrak{p}$ . On notera  $(\mathfrak{p}^s, K^s/K)$  la classe de conjugation de l'élément de FROBENIUS de  $\mathfrak{p}^s$  dans  $G_K$ .

On dispose alors du lemme suivant :

**Lemme 3.2.** *Supposons que le  $A$ -module de Drinfel'd  $\phi$  ait bonne réduction en  $\mathfrak{p}$  et soit  $\sigma \in (\mathfrak{p}^s, K^s/K)$ . On a alors les propriétés suivantes :*

- (i) *Pour tout  $\alpha \in K^s$  entier en  $\mathfrak{p}^s$  on a  $P_{\mathfrak{p}}(\sigma)(\alpha) \equiv 0 \pmod{\mathfrak{p}^s}$ . Cette congruence a lieu dans le localisé  $B_{\mathfrak{p}^s}^s$  de  $B^s$  en  $\mathfrak{p}^s$ .*
- (ii) *Si  $\alpha \in K^s$  est tel que  $P_{\mathfrak{p}}(\sigma)(\alpha) = 0$ , alors  $\alpha$  est un élément de torsion pour  $\phi$ .*

*Démonstration.* Montrons (i). Par hypothèse sur  $\sigma$ , l'automorphisme  $\sigma$  agit sur  $\tilde{\phi}$  comme  $\text{Frob}_{\mathfrak{p}} \in \text{End}(\tilde{\phi})$ , et comme  $P_{\mathfrak{p}}(x)$  est le polynôme caractéristique de  $\text{Frob}_{\mathfrak{p}}$  sur  $T_1(\tilde{\phi})$ , on en déduit que  $P_{\mathfrak{p}}(\text{Frob}_{\mathfrak{p}})$  annule  $T_1(\tilde{\phi})$ .

Par ailleurs, il suit du fait que  $\tilde{\phi}$  est aussi un  $A$ -module de DRINFEL'D qu'on a un homomorphisme bijectif  $\varepsilon' : \text{End}(\tilde{\phi}) \otimes A_{\mathfrak{l}} \rightarrow \text{End}_{A_{\mathfrak{l}}[G_{\kappa_{\mathfrak{p}}}]}(T_1(\tilde{\phi}))$ , où  $G_{\kappa_{\mathfrak{p}}} := \text{Gal}(\overline{\kappa}_{\mathfrak{p}}/\kappa_{\mathfrak{p}})$ , (confer [Gos, proposition 4.12.12]). En particulier,  $P_{\mathfrak{p}}(\text{Frob}_{\mathfrak{p}}) = 0$  en tant qu'élément de  $\text{End}(\tilde{\phi})$ . Mais, pour les éléments  $\mathfrak{p}^s$ -entiers dans  $K^s$ , la réduction

modulo  $\mathfrak{p}^s$  commute avec l'action de GALOIS. On en déduit que pour tout  $\alpha \in K^s$  qui est  $\mathfrak{p}^s$ -entier, l'élément  $P_{\mathfrak{p}}(\sigma)(\alpha)$  appartient à  $\mathfrak{p}^s B_{\mathfrak{p}^s}$ .

Passons maintenant à la preuve du point (ii). Soit  $L/K$  une extension galoisienne de degré  $m$  telle que  $\alpha \in L$ ; on notera encore  $\sigma$  la restriction de  $\sigma$  à  $L$ . Par définition de  $m$ ,  $\sigma^m = 1$  dans  $\text{Gal}(L/K)$ , et *a fortiori*  $\sigma^m(\alpha) = \alpha$ . Soit

$$\mathcal{R} := \text{Res}(P_{\mathfrak{p}}(x), x^m - 1) \in A$$

le résultant des deux polynômes  $P_{\mathfrak{p}}(x)$  et  $x^m - 1$ . Comme les coefficients de plus haut degré de  $P_{\mathfrak{p}}(x)$  et  $x^m - 1$  sont égaux à 1, on en conclut qu'il existe des éléments  $a(x), b(x)$  de  $A[x]$  tels que  $a(x)P_{\mathfrak{p}}(x) + b(x)(x^m - 1) = \mathcal{R}$ . De plus, comme les racines de  $P_{\mathfrak{p}}(x)$  sont de valeurs absolues  $q_{\mathfrak{p}}^{1/r}$ , on en déduit que  $\mathcal{R} \neq 0$ .

En particulier,  $\mathcal{R} = a(\sigma)P_{\mathfrak{p}}(\sigma) + b(\sigma)(\sigma^m - 1)$ , d'où par définition de l'action sur  $A[G_K]$ ,

$$\phi_{\mathcal{R}}(\alpha) = a(\sigma)P_{\mathfrak{p}}(\sigma)(\alpha) + b(\sigma)(\sigma^m - 1)(\alpha) = 0 .$$

Le point  $\alpha$  est donc de  $\mathcal{R}$ -torsion pour  $\phi$ , ce qui montre le point (ii) et conclut la preuve du lemme 3.2.  $\square$

### 3.3. Cas non CM et ramifié.

**Lemme 3.4.** *Soit  $\mathfrak{p}$  un premier de  $B$  tel que  $\phi$  ait bonne réduction en  $\mathfrak{p}$ . Soit  $L/K$  une extension abélienne finie ramifiée au dessus de  $\mathfrak{p}$ . Soit  $\mathfrak{P}$  un premier de  $B_L$  au dessus de  $\mathfrak{p}$ . Soit  $\eta \neq \text{id} \in \text{Gal}(L/K)$  dans l'inertie de  $\mathfrak{P}|\mathfrak{p}$  comme dans le théorème 2.7. Soit  $b \in A$  un générateur unitaire de l'idéal premier  $\mathfrak{q} = \mathfrak{p} \cap A$ . Alors, pour tout entier,  $l \geq 1$ , il existe un élément  $g_l(\tau) \in B_{\mathfrak{p}}\{\tau\}$  tel que*

$$(3.4.1) \quad \phi_{b^l}(\tau) \equiv g_l(\tau)\tau^l \pmod{(bB_{\mathfrak{p}}\{\tau\})} .$$

*En particulier, pour tout  $\alpha \in \mathcal{O}_{\mathfrak{P}}$  on a  $\eta(\alpha) - \alpha \in \mathfrak{P}$  et*

$$(3.4.2) \quad \phi_{b^{\deg(\mathfrak{p})}}(\eta(\alpha) - \alpha) \in \mathfrak{p}\mathcal{O}_{\mathfrak{P}} .$$

*Démonstration.* On observe que  $\phi_b(\tau) - b \in B_{\mathfrak{p}}\{\tau\}\tau$  et par récurrence pour tout entier  $l \geq 1$  on a  $\phi_{b^l}(\tau) \equiv g_l(\tau)\tau^l \pmod{(bB_{\mathfrak{p}}\{\tau\})}$ , où  $g_l(\tau) \in B_{\mathfrak{p}}\{\tau\}$ , d'où le point (i). On remarque aussi que si  $\alpha \in \mathcal{O}_{\mathfrak{P}}$ , on a  $\eta(\alpha) - \alpha \in \mathfrak{P}$ , parce que  $\sigma$  fixe tout modulo  $\mathfrak{P}$ . D'autre part, comme  $\eta(\alpha) - \alpha \in \mathfrak{P} \subset \mathcal{O}_{\mathfrak{P}}$  et que  $bB_{\mathfrak{p}} \subset \mathfrak{p}B_{\mathfrak{p}}$ , on obtient (en faisant  $l = \deg(\mathfrak{p})$ )

$$\phi_{b^{\deg(\mathfrak{p})}}(\eta(\alpha) - \alpha) \equiv g_{\deg(\mathfrak{p})}(\eta(\alpha) - \alpha) \left( (\eta(\alpha) - \alpha)^{q^{\deg(\mathfrak{p})}} \right) \pmod{(\mathfrak{p}\mathcal{O}_{\mathfrak{P}})} .$$

Le point (ii) et donc le lemme suit du théorème 2.7 (on notera que la proposition 2.6 reste vraie après localisation, et donc également le théorème 2.7).  $\square$

### 3.5. Cas CM et non ramifié.

**Lemme 3.6.** *Soit  $L/K$  une extension abélienne finie non-ramifiée au-dessus d'un premier  $\mathfrak{p} \subset B$  où  $\phi$  admet bonne réduction et tel que  $\mathfrak{p}$  soit non ramifié au-dessus de  $\mathfrak{q} = \mathfrak{p} \cap A$ . Soit  $\alpha \in L$  un élément qui n'est pas de torsion pour  $\phi$ . Alors,*

- (i) *pour tout  $\sigma \in \text{Gal}(L/K)$ , on a  $F_{\mathfrak{p}}(\alpha) - \sigma(\alpha) \neq 0$ ;*
- (ii) *pour toute place  $\mathfrak{P}$  de  $L$  au-dessus de  $\mathfrak{p}$ , si  $\sigma \in (\mathfrak{P}, L/K)$  la classe de conjugaison de l'élément de Frobenius en  $\mathfrak{P}$  et  $\alpha \in \mathcal{O}_{\mathfrak{P}}$ , on a  $F_{\mathfrak{p}}(\alpha) - \sigma(\alpha) \in \mathfrak{P}$ .*

*Démonstration.* Pour la première partie, si  $F_{\mathfrak{p}}(\alpha) = \sigma(\alpha)$ , on a  $F_{\mathfrak{p}}^k(\alpha) = \sigma^k(\alpha)$  pour tout  $k \geq 1$ . Soit  $m$  l'ordre de  $\sigma$  dans  $\text{Gal}(L/K)$ . D'où,  $(F_{\mathfrak{p}}^m - 1)(\alpha) = 0$ . Donc, pour tout  $a \in A$  on a  $\phi_a((F_{\mathfrak{p}}^m - 1)(\alpha)) = 0$ . Mais,  $\phi_a((F_{\mathfrak{p}}^m - 1)) = (F_{\mathfrak{p}}^m - 1)(\phi_a)$ , donc  $\phi_a(\alpha) \in \ker(F_{\mathfrak{p}}^m - 1) = \phi[F_{\mathfrak{p}}^m - 1]$  qui est fini. Mais, cela contredit le fait que  $\alpha$  n'est pas un élément de torsion pour  $\phi$ . La deuxième partie, suit de la définition de  $\sigma$  et de la construction de  $F_{\mathfrak{p}}$ .  $\square$

### 3.7. Cas CM et ramifié.

**Lemme 3.8.** *Soit  $H$  le corps de classes de Hilbert de  $\mathcal{O}$ . Soit  $\mathfrak{n}$  une place de  $H$  et on suppose que  $H$  est non ramifié au dessus de  $\mathfrak{q} = \mathfrak{n} \cap A$  (en particulier sur  $\mathfrak{m} = \mathfrak{n} \cap \mathcal{O}$ ). On suppose de plus que  $(\mathfrak{m}, H/\mathcal{F}) = 1$  et  $H \subset K$ . Alors,*

- (i) *pour tout  $e \geq 0$  on a  $H(\psi[\mathfrak{m}^{\nu e}]) \subsetneq H(\psi[\mathfrak{m}^{\nu(e+1)}])$  et l'extension est totalement ramifiée au-dessus du seul idéal  $\mathfrak{n}_{\nu e}$  de  $H(\psi[\mathfrak{m}^{\nu e}])$  au-dessus de l'idéal  $\mathfrak{n}$  correspondant de  $H$  ;*
- (ii) *soit  $e$  un entier,  $e \geq 0$ , et  $\eta \neq \text{id} \in \text{Gal}(H(\psi[\mathfrak{m}^{\nu(e+1)}])/H(\psi[\mathfrak{m}^{\nu e}]))$ , on notera par la même lettre une extension de  $\eta$  à  $\text{Gal}(H(\psi[\mathfrak{m}^{\nu(e+1)}])/H(\psi[\mathfrak{m}^{\nu e}]))$  ; alors, l'application naturelle*

$$\frac{\psi[\mathfrak{m}^{\nu(e+1)}]}{\psi[\mathfrak{m}^{\nu e}]} \longrightarrow \psi[\mathfrak{m}^{\nu}] \text{ définie par } x \longmapsto \eta(x) - x$$

*induit un isomorphisme de  $\mathcal{O}$ -modules.*

*Démonstration.* Pour l'affirmation (i), on observe que par [Hay, proposition 1.14] pour tout  $i \geq 1$  chaque polynôme  $\frac{\psi_{\mathfrak{m}^i}}{\psi_{\mathfrak{m}^{i-1}}}$  est un polynôme d'EISENSTEIN<sup>5</sup> en  $\mathfrak{n}$ . Donc, l'extension  $H(\psi[\mathfrak{m}^i])/H$  est totalement ramifiée au-dessus  $\mathfrak{n}$  pour chaque  $i \geq 1$ . Par un argument d'induction sur  $i$ , on en conclut aussi que chaque extension  $H(\psi[\mathfrak{m}^i]) \subsetneq H(\psi[\mathfrak{m}^{i+1}])$  est totalement ramifiée au-dessus du premier  $\mathfrak{n}_i$  au-dessus de  $\mathfrak{n}$ . *A fortiori*, l'extension  $H(\psi[\mathfrak{m}^{\nu e}]) \subsetneq H(\psi[\mathfrak{m}^{\nu(e+1)}])$  est totalement ramifiée au-dessus de  $\mathfrak{n}_{\nu e}$ .

Pour l'affirmation (ii), définissons premièrement l'application  $\mu : \psi[\mathfrak{m}^{\nu(e+1)}] \rightarrow \psi[\mathfrak{m}^{\nu}]$  par  $\mu(x) := \eta(x) - x$ . Observons d'abord que l'image de  $\mu$  est en réalité dans  $\psi[\mathfrak{m}^{\nu}]$ . En effet, soit  $x \in \psi[\mathfrak{m}^{\nu(e+1)}]$ . Rappelons que  $\lambda_{\mathfrak{m}^{\nu}} = u^{-1}\psi_{\mathfrak{m}^{\nu}} \in \text{End}(\psi)$ . On a  $\lambda_{\mathfrak{m}^{\nu}}(x) \in \psi[\mathfrak{m}^{\nu e}]$ . Pour voir cela, notons que comme  $\lambda_{\mathfrak{m}^{\nu}} \in I_{\psi, \mathfrak{m}^{\nu}}$ , on a

$$\lambda_{\mathfrak{m}^{\nu}} = \sum_{m_i \in \mathfrak{m}^{\nu}} f_i \psi_{m_i} ,$$

avec  $f_i \in H\{\tau\}$ . D'où, pour  $n \in \mathfrak{m}^{\nu e}$  on a

$$\psi_n(\lambda_{\mathfrak{m}^{\nu}}(x)) = \lambda_{\mathfrak{m}^{\nu}}(\psi_n(x)) = \left( \sum_{m_i \in \mathfrak{m}^{\nu}} f_i \psi_{m_i} \right) (\psi_n(x)) = \sum_{m_i \in \mathfrak{m}^{\nu}} f_i \psi_{m_i n}(x) = 0 ,$$

parce que  $m_i n \in \mathfrak{m}^{\nu(e+1)}$ . On en déduit que  $\lambda_{\mathfrak{m}^{\nu}}(x) = \eta(\lambda_{\mathfrak{m}^{\nu}}(x)) = \lambda_{\mathfrak{m}^{\nu}}(\eta(x))$ , donc  $\lambda_{\mathfrak{m}^{\nu}}(\mu(x)) = 0$ . De plus,  $\mu$  se factorise par un homomorphisme

$$\bar{\mu} : \psi[\mathfrak{m}^{\nu(e+1)}]/\psi[\mathfrak{m}^{\nu e}] \rightarrow \psi[\mathfrak{m}^{\nu}] .$$

Le même raisonnement montre que  $\mu$  respecte les filtrations

$$E_0 := \psi[\mathfrak{m}^{\nu e}] \subsetneq E_1 := \psi[\mathfrak{m}^{\nu e+1}] \subsetneq \dots \subsetneq E_{\nu} := \psi[\mathfrak{m}^{\nu(e+1)}]$$

<sup>5</sup>Avec la convention que  $\psi_{\mathfrak{m}^0} := 1$ .

de  $\psi[\mathfrak{m}^{\nu(e+1)}]$  et

$$F_0 := \{0\} = \psi[\mathfrak{m}^0] \subsetneq F_1 := \psi[\mathfrak{m}^1] \subsetneq \cdots \subsetneq F_\nu := \psi[\mathfrak{m}^\nu] ,$$

de  $\psi[\mathfrak{m}^\nu]$ . La restriction  $\mu_j$  de  $\mu$  à  $E_j$  induit donc un morphisme  $\bar{\mu}_j : E_j/E_{j-1} \longrightarrow F_j/F_{j-1}$  pour tout  $j$  compris entre 1 et  $\nu$ . Mais les deux côtés sont isomorphes à  $\mathcal{O}/\mathfrak{m}$  qui est un corps. Donc, les applications  $\bar{\mu}_j$  sont soit nulles soit des isomorphismes. On notera que par hypothèse sur  $\eta$ ,  $\mu_1$  et donc  $\bar{\mu}_1$  est non nulle. Enfin, on peut remarquer que  $\bar{\mu}_j \circ \lambda_{\mathfrak{m}} = \bar{\mu}_{j-1}$ . Par suite, comme  $\bar{\mu}_1 \neq 0$ , il en est de même de tous les  $\bar{\mu}_j$ , pour  $1 \leq j \leq \nu$ . Par recollement,  $\bar{\mu}$  est également un isomorphisme. Le lemme 3.8 est donc entièrement établi.  $\square$

**Remarque 3.9.** D'après la relation (2.10.1) le point (ii) du lemme se réécrit comme l'isomorphisme suivant de  $\mathcal{O}$ -modules

$$\frac{\phi[\mathfrak{m}^{\nu(e+1)}]}{\phi[\mathfrak{m}^{\nu e}]} \rightarrow \phi[F_{\mathfrak{p}}] .$$

**Remarque 3.10.** Comme on l'a déjà observé, une fois le théorème 1.1 prouvé pour un  $A$ -module de DRINFEL'D il est aussi vrai pour tout autre  $A$ -module de DRINFEL'D  $K$ -isomorphe à  $\phi$ . Donc, pour le lemme suivant on peut supposer que  $\phi$  comme  $\mathcal{O}$ -module soit de signe normalisé. Dans ce cas-là (avec les notations du paragraphe 2.4 ci-dessus)  $H^+$  est un corps de définition pour  $\phi$ . Par conséquent, en choisissant un entier  $e \geq 0$  comme dans le lemme ci-dessus, avec les notations du théorème 2.7,  $K' := K(\phi[\mathfrak{m}^{\nu(e-1)}]) \subset H^+(\phi[I/\mathfrak{m}])$ . Donc, on peut vraiment choisir un élément  $\eta \neq \text{id} \in \text{Gal}(L/K')$  appartenant à l'inertie de  $\mathfrak{P}|\mathfrak{p}$  comme dans le théorème 2.7. Et on peut le faire en imposant en sus que  $\eta$  agisse non trivialement sur  $\phi[\mathfrak{m}^{\nu(e-1)+1}]$ .

**Lemme 3.11.** Soient  $L/K$  une extension abélienne finie de  $K$ , que l'on supposera ramifiée au-dessus d'une place  $\mathfrak{p}$  de  $K$  et soit  $\mathfrak{P}$  une place de  $L$  au-dessus de  $\mathfrak{p}$ . Supposons que  $K$  soit non ramifié au-dessus de  $\mathfrak{q} = \mathfrak{p} \cap A$ . Soit de plus  $e$  le plus grand entier  $\geq 0$  tel que  $L \supset K(\phi[\mathfrak{m}^{\nu e}])$ , et posons<sup>6</sup>  $K' := K(\phi[\mathfrak{m}^{\nu(e-1)}])$ . Soit  $\eta \neq \text{id}$  un élément de  $\text{Gal}(L/K')$  comme dans le théorème 2.7 (donc un élément de l'inertie de  $\mathfrak{P}|\mathfrak{p}$ ) et qui de plus agit non trivialement sur  $\phi[\mathfrak{m}^{\nu(e-1)+1}]$ . Supposons que  $\alpha \in L$  ne soit pas de un élément de torsion pour  $\phi$ . Posons  $\alpha' := F_{\mathfrak{p}}(\eta(\alpha)) - F_{\mathfrak{p}}(\alpha)$ . On a alors les propriétés suivantes :

- (i)  $F_{\mathfrak{p}} \equiv z^{1-q^{\deg(\mathfrak{p})}} cu^{-1} \tau^{\deg(\mathfrak{p})} \pmod{(\mathfrak{p}B_{\mathfrak{p}}\{\tau\})}$ , et en particulier,  $\alpha' \in \mathfrak{p}B_{L,\mathfrak{P}}$  si  $\alpha'$  est entier en  $\mathfrak{P}$ .
- (ii) Si  $\alpha' = 0$ , alors il existe un point de torsion  $\delta \in \phi[\mathfrak{m}^{\nu e}]$  tel que  $\alpha + \delta$  soit fixé par  $\eta$ .

*Démonstration.* Rappelons tout d'abord que  $F_{\mathfrak{p}} = z(cu^{-1}\psi_{\mathfrak{m}^\nu})z^{-1}$ , où  $\psi_{\mathfrak{m}^\nu}$  est un produit de polynômes d'EISENSTEIN à coefficients dans  $\mathcal{O}'_{\mathfrak{n}} \subset B_{\mathfrak{p}}$  et que de plus chaque coefficient (sauf le coefficient dominant) appartient à  $\mathfrak{n} \subset \mathfrak{p}$ . La constante  $z \in K$  est une unité en  $\mathfrak{p}$ , les constantes  $c$  et  $u$  dans  $H$  sont des unités en  $\mathfrak{n}$ . D'où on conclut que  $F_{\mathfrak{p}} \equiv z(cu^{-1}\tau^{\deg(\mathfrak{p})})z^{-1} \pmod{(\mathfrak{p}B_{\mathfrak{p}}\{\tau\})} \equiv z^{1-q^{\deg(\mathfrak{p})}} cu^{-1} \tau^{\deg(\mathfrak{p})} \pmod{(\mathfrak{p}B_{\mathfrak{p}}\{\tau\})}$ . La congruence fonctionnelle en découle.

<sup>6</sup>On conviendra que  $\phi[\mathfrak{m}^0] = \emptyset$ , et que  $K(\emptyset) = K$ ; on notera de plus que comme l'extension de  $K$  engendrée par la torsion première à  $\mathfrak{m}$  est non ramifiée au dessus de  $\mathfrak{m}$  (donc de  $\mathfrak{p}$ ), on a nécessairement  $e \geq 1$  et donc  $e - 1 \geq 0$ .

Par conséquent,  $F_{\mathfrak{p}}((\eta - 1)(\alpha)) \equiv z^{1-q^{\deg(\mathfrak{p})}} cu^{-1}((\eta - 1)(\alpha))^{q^{\deg(\mathfrak{p})}} \pmod{(\mathfrak{p}B_L, \mathfrak{q})}$ .  
la première partie du lemme suit maintenant du théorème 2.7, en observant que la preuve de la proposition 2.6 reste vraie si on localise tous les anneaux.

Passons à (ii) et supposons donc que  $\alpha' = 0$ , *i. e.*,

$$\beta := \eta(\alpha) - \alpha \in \phi[F_{\mathfrak{p}}] .$$

Observons que

$$\begin{aligned} & \text{Gal}(K(\phi[\mathfrak{m}^{\nu e}])/K(\phi[\mathfrak{m}^{\nu(e-1)}])) \\ & \cong \text{Gal}(H(\phi[\mathfrak{m}^{\nu e}])/(H(\psi[\mathfrak{m}^{\nu(e-1)}]) \cap K(\phi[\mathfrak{m}^{\nu(e-1)}])) \\ & \subset \text{Gal}(H(\psi[\mathfrak{m}^{\nu e}])/H(\psi[\mathfrak{m}^{\nu(e-1)}])). \end{aligned}$$

Donc, on identifie  $\eta$  à un élément du dernier groupe de Galois et on peut appliquer le lemme 3.8. Par la remarque 3.9, il existe un élément  $\epsilon \in \phi[\mathfrak{m}^{\nu e}]$  tel que  $\eta(\epsilon) - \epsilon = \beta$ . Dans ces conditions,

$$\eta(\alpha - \epsilon) = (\alpha + \beta) - (\epsilon + \beta) = \alpha - \epsilon .$$

Finalement, notons que par construction,  $\delta := -\epsilon$  est un point de  $\mathfrak{m}^{\nu e}$ -torsion pour  $\phi$ . Le lemme 3.11 est donc entièrement établi.  $\square$

#### 4. DÉMONSTRATION DU THÉORÈME 1.1

Nous commençons par choisir un bon premier de  $B$ . Plus précisément, nous pouvons toujours choisir un premier  $\mathfrak{p}$  de  $B$  avec  $\mathfrak{q} = \mathfrak{p} \cap A$  tel que les hypothèses (i)-(iv) sont satisfaites si  $\phi$  est sans multiplications complexes ; dans le cas contraire, on remplace (i) par (v) et on ajoute (vi) :

- (i)  $\phi(K^{\text{ab}})[\mathfrak{q}] = \{\alpha \in K^{\text{ab}} \mid \text{pour tout } a \in \mathfrak{q}, \text{ on a } \phi_a(\alpha) = 0\} = \{0\}$ .
- (ii)  $\phi$  ait bonne réduction en  $\mathfrak{p}$ .
- (iii)  $\mathfrak{q}$  soit non ramifié sur  $K$ .
- (iv)  $\deg(\mathfrak{p}) \geq 8[K : k](\gamma(\phi) + 1)$ , où  $\gamma(\phi)$  est introduite à la formule (1.0.1).
- (v) le corps de classes de HILBERT  $H$  de l'anneau des endomorphismes  $\mathcal{O}$  de  $\phi$  est inclu dans  $K$  ;
- (vi) en posant  $\mathfrak{m} = \mathfrak{p} \cap \mathcal{O}$ , le symbole d'ARTIN  $(\mathfrak{m}, H/\mathcal{F})$  est égal à 1, où  $\mathcal{F} = \text{Frac}(\mathcal{O})$ .

Les points (ii) et (iii) sont toujours satisfaits, sauf pour un nombre fini d'idéaux premiers de  $B$  qu'on exclut ; quant au point (i), la proposition 2.12 montre qu'il est également satisfait sauf pour au plus un nombre fini de premiers que l'on peut également exclure. La condition (v) impose de se placer sur une extension de  $K$  de degré relatif borné. Comme l'on a déjà observé on peut choisir  $\mathfrak{p}$  tel que la condition (vi) soit satisfaite grâce au théorème de ČEBOTAREV, *confer* [Fr-Ja, theorem 6.3.1 et proposition 6.4.8]. Cette condition ne dépend que de la paire  $(\phi, K)$ . De plus, on notera que le théorème 1.1 est vrai pour  $K$  s'il est vrai pour une extension  $K'$  de  $K$  puisque  $K^{\text{ab}} \subset (K')^{\text{ab}}$ . Enfin, la condition (iv) ne dépend également que de la paire  $(\phi, K)$ .

On notera que l'ensemble de mauvais premiers exclus ne dépend que de  $(\phi, K)$  ; le minimum des normes des premiers vérifiant ces propriétés est donc une constante ne dépendant que de  $(\phi, K)$ . Dans toute la suite, on supposera que  $\mathfrak{p}$  est choisi au hasard parmi les bons premiers de norme minimale.

**4.1. Cas non entier.** Nous montrons ici le théorème 1.1 dans le cas où  $\alpha$  possède un gros dénominateur. Le cas non entier est classiquement le cas facile pour le problème de LEHMER (où l'on peut supposer que le point étudié est une unité), mais nous recherchons ici une minoration *indépendante* du degré, et la minoration recherchée est également non triviale dans ce cas. On notera également que dans le cas classique du groupe multiplicatif, le nombre de  $\mathbb{Q}^{\text{ab}}$  ayant la plus petite hauteur connue n'est pas un entier algébrique (*confer* [Am–Dv]).

Soit  $\mathcal{P}$  l'ensemble des premiers de  $L$  divisant  $\mathfrak{p}$ , soit  $b \in A$  un élément irréductible, unitaire tel<sup>7</sup> que  $\mathfrak{q} = (b)$ . Soit enfin  $\alpha$  dans  $L$  comme dans le théorème 1.1 ; on définit :

$$\mathcal{P}_\infty := \begin{cases} \left\{ \mathfrak{P} \mid \mathfrak{p} \text{ tels que } v_{\mathfrak{P}}(\alpha) < 0 \right\} & \text{si } e_{\mathfrak{p}}(L/K) = 1 \\ \left\{ \mathfrak{P} \mid \mathfrak{p} \text{ tels que } v_{\mathfrak{P}}(\alpha) < -\frac{v_{\mathfrak{P}}(b)}{4q^{r \deg(\mathfrak{p})^2}} \right\} & \text{si } e_{\mathfrak{p}}(L/K) > 1 . \end{cases}$$

On introduit enfin  $p(\mathcal{P}_\infty) := \frac{\text{Card}(\mathcal{P}_\infty)}{\text{Card}(\mathcal{P})}$ . Avec ces notations, on dispose de la :

**Proposition 4.2.** *Il existe une constante  $c = c(\phi, K)$  ne dépendant que de la paire  $(\phi, K)$  telle que si  $p(\mathcal{P}_\infty) \geq \frac{1}{2}$ , on ait :*

$$\hat{h}_\phi(\alpha) \geq c(\phi, K) .$$

*Démonstration.* Par définition de la hauteur locale (voir formule (2.3.1)), pour tout  $\mathfrak{P} \in \mathcal{P}_\infty$ , on a :

$$h_{\mathfrak{P}}(\alpha) \geq \frac{\deg(\mathfrak{P})}{[L : k]} v_{\mathfrak{P}}(b) = \frac{\deg(\mathfrak{P})}{[L : k]} ,$$

si l'extension  $L/K$  est non ramifiée au dessus de  $\mathfrak{p}$  et

$$h_{\mathfrak{P}}(\alpha) \geq \frac{\deg(\mathfrak{P})}{4q^{r \deg(\mathfrak{p})^2} \cdot [L : k]} v_{\mathfrak{P}}(b)$$

sinon. Dans tous les cas, on a donc :

$$\sum_{\mathfrak{P} \in \mathcal{P}_\infty} h_{\mathfrak{P}}(\alpha) \geq \sum_{\mathfrak{P} \in \mathcal{P}_\infty} \frac{\deg(\mathfrak{P}) v_{\mathfrak{P}}(b)}{4q^{r \deg(\mathfrak{p})^2} \cdot [L : k]} \geq \frac{\deg(\mathfrak{p})}{8q^{r \deg(\mathfrak{p})^2} \cdot [K : k]}$$

par hypothèse sur  $\mathcal{P}_\infty$ .

Par le choix de  $\mathfrak{p}$  (hypothèse (iii)), et comme l'on peut sans perte de généralité supposer que  $\phi$  est à coefficients constants et que le terme de plus haut degré de  $\phi$  est une unité en  $\mathfrak{p}$  pour tout  $a \in A$ , la proposition 6 de B. POONEN (*confer* [Poo, §4]) nous assure que la hauteur normalisée locale  $\hat{h}_{\phi, \mathfrak{P}}(\cdot)$  coïncide avec la hauteur de WEIL locale en  $\mathfrak{P}$  pour tout  $\mathfrak{P}$  divisant  $\mathfrak{p}$  (voir §. 2.3). Comme par ailleurs toutes les hauteurs locales normalisées sont positives ou nulles, on en déduit que (condition (iv) ci-dessus) :

$$\hat{h}_\phi(\alpha) \geq \frac{\deg(\mathfrak{p})}{8q^{r \deg(\mathfrak{p})^2} \cdot [K : k]} \geq \frac{(\gamma(\phi) + 1)}{q^{r \deg(\mathfrak{p})^2}} \geq \frac{1}{q^{r \deg(\mathfrak{p})^2}} .$$

D'où la proposition<sup>8</sup>. □

<sup>7</sup>On rappelle que  $\mathfrak{q} = \mathfrak{p} \cap A$ .

<sup>8</sup>On notera que comme la dernière minoration comporte un facteur exponentiel en le degré de  $\mathfrak{p}$  au dénominateur, il est important de calculer directement la hauteur normalisée de  $\alpha$ . Un argument *via* la hauteur de WEIL serait ici insuffisant, même en prenant le degré de  $\mathfrak{p}$  assez grand en raison de la constante de comparaison  $\gamma(\phi)$ .

Nous terminons ce paragraphe par une estimation métrique (on notera que cette dernière est plus faible que celle donnée par le théorème 2.7 si l'extension  $L/K$  est non ramifiée au dessus de  $\mathfrak{p}$ ) et qui nous sera utile dans les paragraphes suivants :

**Lemme 4.3.** *Soit  $\alpha$  comme dans le théorème 1.1, et  $\mathfrak{P}$  un premier divisant  $\mathfrak{p}$  n'appartenant pas à  $\mathcal{P}_\infty$  ; soit enfin  $\eta$  un élément du groupe d'inertie de  $\mathfrak{P}$  sur  $\mathfrak{p}$  comme dans le théorème 2.7. Alors,*

$$v_{\mathfrak{P}} \left( \eta(\alpha)^{q^{\deg(\mathfrak{p})}} - \alpha^{q^{\deg(\mathfrak{p})}} \right) \geq \frac{v_{\mathfrak{P}}(b)}{2} .$$

En particulier,

(i) si  $\phi$  n'admet pas de multiplications complexes,

$$v_{\mathfrak{P}} \left( \phi_{b^{\deg(\mathfrak{p})}}(\eta(\alpha)) - \phi_{b^{\deg(\mathfrak{p})}}(\alpha) \right) \geq \frac{v_{\mathfrak{P}}(b)}{4} ;$$

(ii) si  $\phi$  admet des multiplications complexes,

$$v_{\mathfrak{P}}(F_{\mathfrak{p}}(\eta(\alpha)) - F_{\mathfrak{p}}(\alpha)) \geq \frac{v_{\mathfrak{P}}(b)}{2} .$$

*Démonstration.* Écrivons  $\alpha$  sous la forme  $\alpha_1/\alpha_2$ , avec  $\alpha_1, \alpha_2$  dans le localisé  $\mathcal{O}_{L, \mathfrak{P}}$  en  $\mathfrak{P}$  de l'anneau des entiers de  $L$ . L'anneau  $\mathcal{O}_{L, \mathfrak{P}}$  étant de valuation discrète, on peut supposer que  $\min(v_{\mathfrak{P}}(\alpha_1), v_{\mathfrak{P}}(\alpha_2)) = 0$ . Soit  $\eta$  dans le groupe d'inertie de  $\mathfrak{P}$  sur  $\mathfrak{p}$  comme dans le théorème 2.7. On a :

$$\eta(\alpha)^{q^{\deg(\mathfrak{p})}} - \alpha^{q^{\deg(\mathfrak{p})}} = \frac{\eta \left( \alpha_1^{q^{\deg(\mathfrak{p})}} \right)}{\eta \left( \alpha_2^{q^{\deg(\mathfrak{p})}} \right)} - \frac{\left( \alpha_1^{q^{\deg(\mathfrak{p})}} \right)}{\eta \left( \alpha_2^{q^{\deg(\mathfrak{p})}} \right)} + \frac{\left( \alpha_1^{q^{\deg(\mathfrak{p})}} \right)}{\eta \left( \alpha_2^{q^{\deg(\mathfrak{p})}} \right)} - \frac{\left( \alpha_1^{q^{\deg(\mathfrak{p})}} \right)}{\left( \alpha_2^{q^{\deg(\mathfrak{p})}} \right)} .$$

En tenant compte du théorème 2.7, qui demeure valable après des localisations, on a

$$v_{\mathfrak{P}} \left( \eta(\alpha_2)^{q^{\deg(\mathfrak{p})}} - \alpha_2^{q^{\deg(\mathfrak{p})}} \right) \geq v_{\mathfrak{P}}(b) ,$$

d'où par additivité des valuations<sup>9</sup> (on rappelle que  $v_{\mathfrak{P}}(\eta(\alpha_2)) = v_{\mathfrak{P}}(\alpha_2)$ , parce que  $\eta$  est dans l'inertie de  $\mathfrak{P}$  sur  $\mathfrak{p}$ ),

$$\begin{aligned} v_{\mathfrak{P}} \left( \frac{\left( \alpha_1^{q^{\deg(\mathfrak{p})}} \right)}{\eta \left( \alpha_2^{q^{\deg(\mathfrak{p})}} \right)} - \frac{\left( \alpha_1^{q^{\deg(\mathfrak{p})}} \right)}{\left( \alpha_2^{q^{\deg(\mathfrak{p})}} \right)} \right) &\geq q^{\deg(\mathfrak{p})} v_{\mathfrak{P}}(\alpha_1) + v_{\mathfrak{P}}(b) \\ &\quad + 2q^{\deg(\mathfrak{p})} \min(-v_{\mathfrak{P}}(\eta(\alpha_2)), -v_{\mathfrak{P}}(\alpha_2)) \\ &\geq q^{\deg(\mathfrak{p})} v_{\mathfrak{P}}(\alpha) + v_{\mathfrak{P}}(b) - q^{\deg(\mathfrak{p})} v_{\mathfrak{P}}(\alpha_2) \geq \frac{v_{\mathfrak{P}}(b)}{2} . \end{aligned}$$

De même, en tenant compte du théorème 2.7,

$$v_{\mathfrak{P}} \left( \frac{\eta \left( \alpha_1^{q^{\deg(\mathfrak{p})}} \right)}{\eta \left( \alpha_2^{q^{\deg(\mathfrak{p})}} \right)} - \frac{\left( \alpha_1^{q^{\deg(\mathfrak{p})}} \right)}{\eta \left( \alpha_2^{q^{\deg(\mathfrak{p})}} \right)} \right) \geq v_{\mathfrak{P}}(b) - q^{\deg(\mathfrak{p})} v_{\mathfrak{P}}(\eta(\alpha_2)) \geq \frac{3v_{\mathfrak{P}}(b)}{4} ,$$

et donc, au total,

$$v_{\mathfrak{P}} \left( \eta(\alpha)^{q^{\deg(\mathfrak{p})}} - \alpha^{q^{\deg(\mathfrak{p})}} \right) \geq \min \left( \frac{3v_{\mathfrak{P}}(b)}{4}, \frac{v_{\mathfrak{P}}(b)}{2} \right) = \frac{v_{\mathfrak{P}}(b)}{2}$$

d'où la première partie du lemme 4.3.

<sup>9</sup>Pour la dernière inégalité, on note simplement que  $r$  et  $\deg(b)$  sont  $\geq 1$ .

Passons au point (i) de la deuxième partie. En tenant compte du point (i) du lemme 3.4, on peut écrire  $\phi_{b^{\deg(\mathfrak{p})}}$  sous la forme  $\phi_{b^{\deg(\mathfrak{p})}}(\tau) = g(\tau) \cdot \tau^{q^{\deg(\mathfrak{p})}} + bh(\tau)$ , où  $g(\tau), h(\tau) \in B_{\mathfrak{p}}\{\tau\}$ . En tenant compte de l'inégalité ultramétrique et de la première partie du lemme, on en déduit donc

$$v_{\mathfrak{P}}(\phi_{b^{\deg(\mathfrak{p})}}(\eta(\alpha)) - \phi_{b^{\deg(\mathfrak{p})}}(\alpha)) \geq \min \left\{ v_{\mathfrak{P}}(g(\eta(\alpha) - \alpha)) + \frac{v_{\mathfrak{P}}(b)}{2}, v_{\mathfrak{P}}(b) + v_{\mathfrak{P}}(h(\eta(\alpha) - \alpha)) \right\} .$$

Par ailleurs, comme  $\phi_{b^{\deg(\mathfrak{p})}}(\tau)$  est un polynôme en  $\tau$  de degré  $r \deg(b) \deg(\mathfrak{p}) = r \deg(\mathfrak{p})^2$ , et comme  $\eta$  est dans l'inertie de  $\mathfrak{P}$  sur  $\mathfrak{p}$ ,

$$v_{\mathfrak{P}}(h(\eta(\alpha) - \alpha)) \geq q^{r \deg(\mathfrak{p})^2} \frac{-v_{\mathfrak{P}}(b)}{4q^{r \deg(\mathfrak{p})^2}} = \frac{-v_{\mathfrak{P}}(b)}{4} .$$

Similairement, on a  $v_{\mathfrak{P}}(g(\eta(\alpha) - \alpha)) \geq \frac{-v_{\mathfrak{P}}(b)}{4}$ , d'où le point (i).

Pour (ii), on procède de même, en notant que le point (i) du lemme 3.11 permet d'écrire  $F_{\mathfrak{p}}$  sous la forme

$$F_{\mathfrak{p}} = z^{1-q^{\deg(\mathfrak{p})}} cu^{-1} \tau^{\deg(\mathfrak{p})} + l(\tau) ,$$

où  $l(\tau) = al_1(\tau) \in \mathfrak{p}B_{\mathfrak{p}}\{\tau\}$  est un polynôme en  $\tau$  de degré au plus  $\deg(\mathfrak{p})$  et  $a \in \mathfrak{p}$ . En appliquant la première partie du lemme, on obtient donc de même :

$$\begin{aligned} v_{\mathfrak{P}}(F_{\mathfrak{p}}(\eta(\alpha)) - F_{\mathfrak{p}}(\alpha)) &\geq \min \left( \frac{v_{\mathfrak{P}}(b)}{2}, v_{\mathfrak{P}}(b) + v_{\mathfrak{P}}(l_1(\eta(\alpha) - \alpha)) \right) \\ &\geq \min \left( \frac{v_{\mathfrak{P}}(b)}{2}, v_{\mathfrak{P}}(b) - \frac{q^{\deg(\mathfrak{p})} v_{\mathfrak{P}}(b)}{4q^{r \deg(\mathfrak{p})^2}} \right) \\ &\geq \frac{v_{\mathfrak{P}}(b)}{2} . \end{aligned}$$

Le lemme 4.3 est donc entièrement établi.  $\square$

**4.4. Cas non CM et non ramifié.** Soit  $\alpha \in K^{\text{ab}}$  et  $L = K(\alpha)$ . Nous allons procéder par récurrence sur l'indice de ramification  $e_{\mathfrak{p}}(L/K)$  de  $L/K$  en  $\mathfrak{p}$ . Dans ce paragraphe, nous traiterons le cas où  $L/K$  est non ramifiée en  $\mathfrak{p}$  (i. e.  $e_{\mathfrak{p}}(L/K) = 1$ ), la récurrence proprement dite étant pour sa part effectuée au paragraphe 4.6.

Comme  $L/K$  est non ramifiée en  $\mathfrak{p}$ , on a  $\mathfrak{p}B_L = \mathfrak{P}_1 \cdots \mathfrak{P}_g$ , où les idéaux premiers  $\mathfrak{P}_j$  de  $B_L$  satisfont  $\mathfrak{P}_j \cap B = \mathfrak{p}$ . Par ailleurs, comme  $L/K$  est abélienne, les automorphismes de FROBENIUS en les idéaux  $\mathfrak{P}_j$  sont tous égaux ; nous noterons cet automorphisme  $\sigma := (\mathfrak{P}_j, L/K) \in \text{Gal}(L/K)$ . Nous noterons encore  $\sigma$  un relèvement de  $\sigma$  à  $G_K$  et nous désignerons par  $P_{\mathfrak{p}}(x) \in A[x]$  le polynôme caractéristique de l'automorphisme de Frobenius  $F_{\mathfrak{p}}$  sur le module de Tate  $l$ -adique  $T_l(\tilde{\phi})$  de  $\tilde{\phi}$  par rapport au corps résiduel  $\kappa_{\mathfrak{p}}$ .

Le lemme 3.2 point (ii) nous assure que si  $\alpha$  n'est pas un élément de torsion pour  $\phi$ , alors  $P_{\mathfrak{p}}(\sigma)(\alpha) \neq 0$ . Soit  $\beta := (P_{\mathfrak{p}}(\sigma)(\alpha))^{-1}$ .

Supposons maintenant<sup>10</sup> que  $p(\mathcal{P}_{\infty}) \leq \frac{1}{2}$ , et soit  $1 \leq j \leq g$  un entier tel que  $\mathfrak{P}_j \notin \mathcal{P}_{\infty}$  (i. e.,  $\alpha$  est  $\mathfrak{P}_j$ -entier) ; d'après le lemme 3.2, point (i),  $\beta^{-1} \in \mathfrak{P}_j$ , et en particulier  $-v_{\mathfrak{P}_j}(\beta) = v_{\mathfrak{P}_j}(\beta^{-1}) > 0$ . Donc,  $\tilde{v}_{\mathfrak{P}_j}(\beta) = v_{\mathfrak{P}_j}(\beta)$ .

<sup>10</sup>Le cas où  $p(\mathcal{P}_{\infty}) \geq \frac{1}{2}$  a déjà été traité ci-dessus.

D'après la relation (2.3.1), on a donc :

$$h_{\mathfrak{P}_j}(\beta) = -\frac{\deg(\mathfrak{P}_j)}{[L : k]} v_{\mathfrak{P}_j}(\beta) .$$

Comme l'extension  $L$  est non ramifiée en  $\mathfrak{p}$  et  $K$  est non ramifiée en  $\mathfrak{q}$ , on a en particulier :

$$h_{\mathfrak{P}_j}(\beta) \geq \frac{\deg(\mathfrak{P}_j)}{[L : k]} v_{\mathfrak{P}_j}(b) = \frac{\deg(\mathfrak{P}_j)}{[L : k]} .$$

Il en suit,

$$\sum_{\mathfrak{P} \notin \mathcal{P}_\infty} h_{\mathfrak{P}}(\beta) \geq \sum_{\mathfrak{P} \notin \mathcal{P}_\infty} \frac{\deg(\mathfrak{P})}{[L : k]} \geq \frac{\deg(\mathfrak{p})}{2[K : k]} .$$

Finalement, en utilisant la décomposition de la hauteur de WEIL en somme de hauteurs locales et le fait que les hauteurs locales sont toutes positives ou nulles, on obtient :

$$h(\beta) = \sum_{\mathfrak{P} \in M_L} h_{\mathfrak{P}}(\beta) \geq \sum_{\mathfrak{P} \notin \mathcal{P}_\infty} h_{\mathfrak{P}}(\beta) \geq \frac{\deg(\mathfrak{p})}{2[K : k]} .$$

Par ailleurs, rappelons (relation (1.0.1)) qu'il existe une constante réelle  $\gamma(\phi) > 0$  ne dépendant que de  $\phi$  telle que pour tout  $x \in \overline{K}$  on ait

$$|\hat{h}_\phi(x) - h(x)| \leq \gamma(\phi) .$$

*A fortiori*, comme  $h(\beta) = h(P_{\mathfrak{p}}(\alpha))$ , on obtient

$$\hat{h}_\phi(P_{\mathfrak{p}}(\alpha)) \geq h(\beta) - \gamma(\phi) \geq \frac{\deg(\mathfrak{p})}{2[K : k]} - \gamma(\phi) .$$

Comme nous avons supposé (condition (iv) au début de ce paragraphe) que  $\deg(\mathfrak{p}) \geq 8[K : k](\gamma(\phi) + 1)$ , on obtient

$$\hat{h}_\phi(P_{\mathfrak{p}}(\alpha)) > 1 .$$

Il reste à en déduire une minoration pour la hauteur de  $\alpha$  ; pour ce faire, écrivons explicitement

$$P_{\mathfrak{p}}(x) = x^r + d_1 x^{r-1} + \cdots + d_{r-1} x + u d_r ,$$

où  $u \in \mathbb{F}_{\mathfrak{q}}^*$  et  $d_r \in \mathfrak{p}$  (on rappelle que les racines de  $P_{\mathfrak{p}}$  sont toutes de module  $q_{\mathfrak{p}}^{1/r}$ ).

Par [Den, Théorème 1] et en tenant compte de l'invariance de la hauteur globale par rapport à l'action du groupe de GALOIS, on a :

$$\begin{aligned} \hat{h}_\phi(P_{\mathfrak{p}}(\sigma)(\alpha)) &= \hat{h}_\phi\left(\sigma^r(\alpha) + \phi_{d_1}(\sigma^{r-1}(\alpha)) + \cdots + \phi_{d_{r-1}}(\sigma(\alpha)) + \phi_{u d_r}(\alpha)\right) \\ &\leq \hat{h}_\phi(\sigma^r(\alpha)) + \hat{h}_\phi(\phi_{d_1}(\sigma^{r-1}(\alpha))) + \cdots + \hat{h}_\phi(\phi_{d_{r-1}}(\sigma(\alpha))) + \hat{h}_\phi(\phi_{u d_r}(\alpha)) \\ &= \hat{h}_\phi(\sigma^r(\alpha)) + |d_1|^r \hat{h}_\phi(\sigma^{r-1}(\alpha)) + \cdots + |d_{r-1}|^r \hat{h}_\phi(\sigma(\alpha)) + |d_r|^r \hat{h}_\phi(\alpha) \\ &= \hat{h}_\phi(\alpha)(1 + |d_1|^r + \cdots + |d_{r-1}|^r + |d_r|^r) \\ &\leq \hat{h}_\phi(\alpha)(1 + q_{\mathfrak{p}} + \cdots + q_{\mathfrak{p}}^r) , \end{aligned}$$

car  $|d_i| \leq q_{\mathfrak{p}}^{i/r}$  pour  $i = 1, \dots, r$ , puisque ce sont des fonctions symétriques des racines de  $P_{\mathfrak{p}}$ . Par conséquent,

$$\hat{h}_\phi(\alpha) > \frac{1}{1 + q_{\mathfrak{p}} + \cdots + q_{\mathfrak{p}}^r} .$$

En vertu du choix de  $\mathfrak{p}$ , cette borne inférieure est une fonction  $c(\phi, K) > 0$ .

4.5. **Cas CM et non ramifié.** On suppose toujours  $p(\mathcal{P}_\infty) \leq \frac{1}{2}$ ; le même type d'argument que ci-dessus, en utilisant le lemme 3.6, point (ii) en lieu et place du lemme 3.2, point (i) conduit à

$$h_{\mathfrak{P}}((F_{\mathfrak{p}}(\alpha) - \sigma(\alpha))^{-1}) \geq \frac{\deg(\mathfrak{P})}{[L : k]} ,$$

si  $\mathfrak{P}$  divise  $\mathfrak{p}$  et si  $\alpha$  est  $\mathfrak{P}$ -entier et, *a fortiori*, à la minoration

$$h((F_{\mathfrak{p}}(\alpha) - \sigma(\alpha))^{-1}) \geq \sum_{\mathfrak{P} \notin \mathcal{P}_\infty} \frac{\deg(\mathfrak{P})}{[L : k]} \geq \frac{\deg(\mathfrak{p})}{2[K : k]} .$$

On obtient aussi

$$\hat{h}_\phi(F_{\mathfrak{p}}(\alpha) - \sigma(\alpha)) \geq h((F_{\mathfrak{p}}(\alpha) - \sigma(\alpha))) - \gamma(\phi) > 1 .$$

D'autre part,

$$\hat{h}_\phi(F_{\mathfrak{p}}(\alpha) - \sigma(\alpha)) \leq \hat{h}_\phi(F_{\mathfrak{p}}(\alpha)) + \hat{h}_\phi(\sigma(\alpha)) = (q_{\mathfrak{p}} + 1)\hat{h}_\phi(\alpha) .$$

D'où,

$$\hat{h}_\phi(\alpha) > \frac{1}{q_{\mathfrak{p}} + 1} .$$

Ce qui donne la minoration voulue dans ce cas.

4.6. **Cas non CM et ramifié.** Nous supposons par récurrence le théorème 1.1 démontré pour toute extension abélienne  $L'$  de  $K$  telle que  $e_{\mathfrak{p}}(L'/K) < e_{\mathfrak{p}}(L/K)$  (le cas non ramifié ayant été établi au paragraphe 4.4 ci-dessus).

Nous allons appliquer le lemme 4.3; pour ce faire, considérons l'élément

$$\alpha' := \phi_{b^{\deg(\mathfrak{p})}}((\eta - 1)(\alpha)) .$$

Supposons  $\alpha' \neq 0$ , et posons  $\beta := (\alpha')^{-1}$ . Soit  $\mathfrak{P} \subset B_L$  un idéal premier tel que  $\mathfrak{P} \cap B = \mathfrak{p}$ . Supposons que  $\mathfrak{P}$  n'appartienne pas  $\mathcal{P}_\infty$ . Il suit de la relation (2.3.1) et du lemme 4.3, point (i) réunis que

$$h_{\mathfrak{P}}(\beta) = -\frac{\deg(\mathfrak{P})}{[L : k]} v_{\mathfrak{P}}(\beta) \geq \frac{\deg(\mathfrak{P})}{4[L : k]} v_{\mathfrak{P}}(b) = \frac{\deg(\mathfrak{P})}{4[L : k]} e_{\mathfrak{P}|\mathfrak{p}} ,$$

où  $e_{\mathfrak{P}|\mathfrak{p}}$  est l'indice de ramification de  $\mathfrak{P}$  sur  $\mathfrak{p}$ . Par conséquent, en tenant compte de l'hypothèse sur  $\mathcal{P}_\infty$ ,

$$\sum_{\mathfrak{P} \notin \mathcal{P}_\infty} h_{\mathfrak{P}}(\beta) \geq \sum_{\mathfrak{P} \notin \mathcal{P}_\infty} \frac{\deg(\mathfrak{P})}{4[L : k]} e_{\mathfrak{P}|\mathfrak{p}} \geq \frac{\deg(\mathfrak{p})}{8[K : k]} .$$

Là encore, la positivité des hauteurs locales nous assure au total que :

$$h(\beta) = \sum_{\mathfrak{P} \in M_L} h_{\mathfrak{P}}(\beta) \geq \sum_{\mathfrak{P} \notin \mathcal{P}_\infty} h_{\mathfrak{P}}(\beta) \geq \frac{\deg(\mathfrak{p})}{8[K : k]} .$$

Par ailleurs, comme par hypothèse  $\deg(\mathfrak{p}) \geq 8[K : k](\gamma(\phi) + 1)$ , on en conclut

$$\hat{h}_\phi(\alpha') \geq \frac{\deg(\mathfrak{p})}{8[K : k]} - \gamma(\phi) > 1 .$$

D'autre part, par [Den, théorème 1] et par l'invariance de la hauteur globale par l'action du groupe de GALOIS on obtient comme précédemment :

$$\begin{aligned} \hat{h}_\phi(\phi_{b^{\deg(\mathfrak{p})}}((\eta-1)(\alpha))) &= |b|^{r \deg(\mathfrak{p})} \hat{h}_\phi((\eta-1)(\alpha)) = N(\mathfrak{q})^{r \deg(\mathfrak{p})} \hat{h}_\phi(\eta(\alpha) - \alpha) \\ &\leq N(\mathfrak{q})^{r \deg(\mathfrak{p})} (\hat{h}_\phi(\eta(\alpha)) + \hat{h}_\phi(\alpha)) = 2N(\mathfrak{q})^{r \deg(\mathfrak{p})} \hat{h}_\phi(\alpha) , \end{aligned}$$

car  $|b| = \#(A/(b)) = N(\mathfrak{q})$ . On en conclut

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

Supposons donc que  $\alpha' = 0$ , *i. e.*,  $\phi_{b^{\deg(\mathfrak{p})}}(\sigma(\alpha) - \alpha) = 0$ . Par hypothèse  $\phi(K^{\text{ab}})[\mathfrak{q}] = \{0\}$  (c'est notre hypothèse (i) du début de ce paragraphe conduisant au choix de  $\mathfrak{p}$ ), donc  $\sigma(\alpha) = \alpha$ , *i. e.*,  $\alpha \in L^\sigma$ , le sous-corps strict de  $L$  fixé par  $\sigma$  (car  $\sigma \neq 1$ ). Notons que nécessairement  $e_{\mathfrak{p}}(L^\sigma/K) < e_{\mathfrak{p}}(L/K)$ .

Par hypothèse de récurrence, on en conclut  $\hat{h}_\phi(\alpha) \geq c(\phi, K)$ , où  $c(\phi, K)$  est une constante qui ne dépend que du  $A$ -module  $\phi$  et de  $K$ . Ceci termine la récurrence dans le cas non CM.

**4.7. Cas CM et ramifié.** Nous supposons par récurrence que le théorème 1.1 soit démontré pour toute extension abélienne  $L'$  de  $K$  telle que  $e_{\mathfrak{p}}(L'/K) < e_{\mathfrak{p}}(L/K)$  (le cas non ramifié ayant été établi au paragraphe 4.5 ci-dessus).

Supposons maintenant que  $L/K$  soit ramifiée au-dessus de  $\mathfrak{p}$ . On reprend les notations et hypothèses des lemmes 3.11 et 4.3, et l'on suppose tout d'abord que le point  $\alpha' = F_{\mathfrak{p}}(\eta(\alpha) - \alpha) \neq 0$ . Par le lemme 4.3, point (ii), si  $\mathfrak{P}$  n'appartient pas à  $\mathcal{P}_\infty$ ,

$$h_{\mathfrak{P}}((\alpha')^{-1}) \geq \frac{\deg(\mathfrak{P})}{2[L:k]} e_{\mathfrak{P}|\mathfrak{p}} .$$

Ceci conduit comme ci-dessus à

$$h((\alpha')^{-1}) \geq \frac{\deg(\mathfrak{p})}{4[K:k]}, \text{ et donc } \hat{h}_\phi(\alpha') > 1 .$$

D'autre part,

$$\begin{aligned} \hat{h}_\phi(\alpha') &= \hat{h}_\phi(\eta(F_{\mathfrak{p}}(\alpha)) - F_{\mathfrak{p}}(\alpha)) \\ &\leq \hat{h}_\phi(\eta(F_{\mathfrak{p}}(\alpha))) + \hat{h}_\phi(F_{\mathfrak{p}}(\alpha)) = 2\hat{h}_\phi(F_{\mathfrak{p}}(\alpha)) = 2q_{\mathfrak{p}} \hat{h}_\phi(\alpha) . \end{aligned}$$

D'où,

$$\hat{h}_\phi(\alpha) > \frac{1}{2q_{\mathfrak{p}}} .$$

Si  $\alpha' \neq 0$ , le théorème suit donc de l'argument ci-dessus.

On peut donc supposer que  $\alpha' = 0$ .

Le point (ii) du lemme 3.11 nous assure l'existence d'un élément de torsion  $\delta \in \phi[\mathfrak{m}^{\nu e}] \subset L$  pour  $\phi$  tel que  $\alpha + \delta$  soit fixé par  $\eta$ . Soit  $L'$  le sous-corps de  $L$  fixé par  $\eta$ . Par le choix de  $\eta$  on a  $f_{\mathfrak{p}}(L'/K) < f_{\mathfrak{p}}(L/K)$ , où  $f_{\mathfrak{p}}(L/K)$  dénote le conducteur local, et donc, par hypothèse de récurrence, le théorème 1.1 est vrai pour  $\alpha + \delta$ . Mais,

$$\hat{h}_\phi(\alpha) = \hat{h}_\phi(\alpha + \delta) ,$$

puisque  $\delta$  est de torsion, et le théorème 1.1 est entièrement établi.  $\square$

## RÉFÉRENCES

- [Am–Dv] F. Amoroso, R. Dvornicich, *A lower bound for the height in abelian extensions*, J. Number Theory **80** (2000), pages 260–272.
- [Am–Za] F. Amoroso, U. Zannier, *A relative Dobrowolski lower bound over abelian extensions*, Ann. Scuola Norm. Sup. Pisa **29** (2000), pages 711–727.
- [Ba–Si] M. Baker, J. Silverman, *A lower bound for the canonical height on abelian varieties over abelian extensions*, Mathematical Research Letters **11** (2004), pages 377–396.
- [Dav] S. David, *On the height of subvarieties of group varieties*, The Ramanujan Journal of Math., à paraître.
- [Den] L. Denis, *Hauteurs canoniques et modules de Drinfel’d*, Math. Ann. **294** (1992), pages 213–223.
- [Dri] V. Drinfel’d, *Elliptic modules*, Math USSR Sbornik **23** (1976), pages 561–592.
- [Fr–Ja] M. D. Fried, M. Jarden, *Field Arithmetic*, Springer-Verlag, 2005, 2nd edition.
- [Gek] E.-U. Gekeler, *Zur Arithmetik von Drinfel’d-Moduln*, Math. Ann **262** (1983), pages 167–182.
- [Gek2] E.-U. Gekeler, *On finite Drinfel’d modules*, J. Algebra **141**, pages 187–203 (1991).
- [Gos] D. Goss, *Basic Structures of Function Field Arithmetic*, Springer-Verlag 1996.
- [Hay] D. Hayes, *A brief introduction to Drinfel’d modules*, in The Arithmetic of Function Fields, Ohio State Univ. Math. Res. Inst. Pub. **2**, pages 1–32, 1992.
- [Lan] S. Lang, *Elliptic Functions*, Springer-Verlag, 1986.
- [Leh] D. H. Lehmer, *Factorisation of some cyclotomic functions*, Annals of Math., **34**, (2) (1933), pages 461–479.
- [Li] A. Li, *On the torsion points of Drinfel’d modules in abelian extensions*, J. Pure and Applied Algebra **176** (2002), pages 153–159.
- [Poo] B. Poonen, *Local height functions and the Mordell-Weil theorem for Drinfel’d modules*, Compositio Math. **97** (1995), pages 349–368.
- [Rat] N. Rattazi, *Le théorème de Dobrowolski–Laurent pour les extensions abéliennes sur une courbe elliptique à multiplications complexe*, International Math. Research Notices, **45** (2004), pages 3121–3152.
- [Sh–Ta] G. Shimura, Y. Taniyama, *Complex Multiplication Abelian Varieties and applications to number theory*, Pub. Japan Math. Soc. **6**, 1961.
- [Tag] Y. Taguchi, *Semi-simplicity of Galois representations attached to Drinfel’d modules*, J. Number Th. **44** (3) (1993), pages 292–314.
- [Tak] T. Takahashi, *Good reduction of elliptic modules*, J. Math. Soc. Japan **34** (1982), pages 475–487.

UNIVERSITÉ PARIS VI (PIERE ET MARIE CURIE), UMR 7586 ET UFR 929, THÉORIE DES NOMBRES, INSTITUT DE MATHÉMATIQUES DE JUSSIEU, 4, PLACE JUSSIEU, F-75005 PARIS, FRANCE  
*E-mail address:* david@math.jussieu.fr

UNIVERSIDADE FEDERAL DO RIO DE JANEIRO, INSTITUTO DE MATEMÁTICA, RUA GUAIÁQUIL 83, CACHAMBI, 20785-050 RIO DE JANEIRO, RJ, BRASIL  
*E-mail address:* amilcar@acd.ufrj.br