Corps de division et torsion dans les variétés abéliennes de type C.M. (selon Ribet)

Nicolas Ratazzi

janvier 2005

Dans toute la suite, si k est un corps, $\overline{k}$ dénotera sa cloture séparable.

1 Rappels et motivations

Définition 1.1 Étant donné un corps K, on dit que A/K est une *variété abélienne* si c'est un groupe algébrique sur K (*i.e.* un K-schéma en groupes) connexe, projectif et lisse sur K.

Définition 1.2 Si G_1/K et G_2/K sont deux groupes algébriques connexes. On dit qu'un K-homomorphisme $\varphi : G_1 \to G_2$ est *une isogénie* s'il est surjectif et si G_1 et G_2 sont de même dimension.

Définition 1.3 Soit A/K une variété abélienne simple. On dit que A est *de type C.M.* (pour complex multiplication) si $\mathrm{End}_{\overline{K}}(A) \otimes \mathbb{Q}$ contient un corps commutatif F de degré $[F : \mathbb{Q}] = 2 \dim A$. Une variété abélienne quelconque est dite *de type C.M.* si elle est isogène à un produit de variétés abéliennes simples de type C.M., *i.e.*, si $\mathrm{End}_{\overline{K}}(A) \otimes \mathbb{Q}$ contient un produit de corps commutatif $F_1, \ldots, F_n$ vérifiant $\sum_{i=1}^{n}[F_i : \mathbb{Q}] = 2 \dim A$.

Remarque 1.1

1. Les variétés abéliennes de dimension 1 sont les courbes elliptiques.
2. Si K est un corps de nombres plongé dans $\mathbb{C}$ et si A/K une variété abélienne de dimension $g \geq 1$, la variété analytique complexe associée (correspondant aux points complexes de $A_{\mathbb{C}}$) notée $A(\mathbb{C})$ est juste un tore complexe $\mathbb{C}^g/\Lambda$ où Λ est un réseau, que l'on peut plonger holomorphiquement dans un espace projectif $\mathbb{P}_n(\mathbb{C})$.

Sur les variétés abéliennes, on a un théorème de structure des points rationnels :

Théorème 1.1 (Mordell-Weil) *Soit A/K une variété abélienne sur un corps de nombres K. Le groupe des points K-rationnels est de type fini. Autrement dit, en notant r son rang et $\{P_1, \ldots, P_r\}$ un ensemble de générateurs, on a*

$$A(K) = A(K)_{\mathrm{tors}} \oplus \bigoplus_{i=1}^{r} \mathbb{Z}P_i.$$

Au vu de ce résultat, il y a plusieurs questions naturelles que l'on peut se poser :

1. Comprendre qui est r : c'est le but de la version faible de la conjecture de Birch et Swinnerton-Dyer.
2. Savoir trouver des générateurs de la partie libre du groupe : il y a un algorithme de Manin qui repose sur les conjectures de Birch et Swinerton-Dyer ainsi que sur des conjectures usuelles de prolongement analytique de fonctions L.
3. Mieux comprendre le groupe des points de torsion.

C'est à ce dernier point que nous nous intéresserons dans la suite. Plus précisément, on s'intéressera au problème d'une borne du cardinal des points de torsion.

2 Points de torsion

Concernant le problème de la borne de la torsion sur les variétés abéliennes (ou même simplement sur les courbes elliptiques), il y a essentiellement deux approches très différentes possibles. La première consiste à fixer un corps de nombres K et à chercher une majoration quand on fait varier la variété abélienne A. La seconde approche, consiste à fixer une variété abélienne et à faire varier le corps K.

2.1 Problème de la borne uniforme

Dans tout ce qui suit, K est un corps de nombres.

Conjecture 2.1 *Soit $g \in \mathbb{N}$. Il existe une constante strictement positive $C(K, g)$ telle que pour toute variété abélienne A/K de dimension g on a*

$$|A(K)_{\text{tors}}| \leq C(K, g).$$

On peut se demander s'il est possible de faire en sorte que la dépendance en K n'intervienne qu'à travers son degré. C'est ce qu'on appelle le *problème de la borne uniforme*. Il n'y pour le moment pas de réelles évidences en faveur ou contre ce problème dans le cas général des variétés abéliennes de dimension quelconque. Ceci étant c'est un théorème pour les courbes elliptiques :

Théorème 2.1 (Merel) *Soit d un entier positif. Il existe une constante strictement positive, $C(d)$, telle que pour tout corps de nombres $K/\mathbb{Q}$ de degré d et pour toute courbe elliptique E/K, on a*

$$|E(K)_{\text{tors}}| \leq C(d).$$

En fait dans le cas où $K = \mathbb{Q}$ et $g = 1$, on peut même dire un peu mieux puisque l'on sait décrire exactement quels sont les groupes apparaissant comme groupe de torsion de courbes elliptiques.

Théorème 2.2 (Mazur) *Soit $E/\mathbb{Q}$ une courbe elliptique. Le groupe des points de torsion est l'un des quinze suivants :*

$$\mathbb{Z}/n\mathbb{Z}, \quad 1 \leq n \leq 10 \text{ ou } n = 12 \quad ; \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}, \quad 1 \leq n \leq 4.$$

De plus chacun de ces groupes intervient effectivement comme un $E(\mathbb{Q})_{\text{tors}}$.

Une telle description existe aussi pour les corps quadratiques. Le théorème de Merel a ensuite été rendu effectif par Parent qui obtient pour la constante $C(d)$ quelque chose d'explicite, exponentiel en d. En vu de la suite, notons que dans certains cas on sait dire quelque chose de plus fin :

Théorème 2.3 (Oesterlé-Flexor ; Hindry-Silverman) *Soit d un entier positif. Pour tout corps de nombres $K/\mathbb{Q}$ de degré d et pour toute courbe elliptique E/K ayant potentiellement bonne réduction, on a*

$$|E(K)_{\text{tors}}| \leq 1\,977\,408 \cdot d \log d.$$

Dans le cas des variétés abéliennes, on a le résultat suivant (découlant simplement de ce que la torsion première à p s'injecte dans les points de la réduction modulo p) :

Théorème 2.4 *Pour toute variété abélienne de dimension g ayant potentiellement bonne réduction sur un corps de nombres K de degré d, on a*

$$|A(K)_{\text{tors}}| \leq 6^{gd \cdot 4^{4g^2}}.$$

Comme on le voit en spécialisant pour $g = 1$, ce résultat est très loin d'être optimal. Dans le cas des variétés abélienne de type C.M., Silverberg a montré que l'on peut prendre pour constante $C(d, g)$ quelque chose du type $C_{\text{abs}} d^{2g}$ où C_{abs} est une valeur numérique explicite ne dépendant d'aucun paramètre.

2.2 Borne sur la torsion : seconde approche

Comme indiqué précédemment, il y a une autre approche pour laquelle on sait dire des choses précises sur les variétés abéliennes. Soit A/K une variété abélienne de dimension g sur un corps de nombres K. On note

$$\gamma(A) = \inf \{x > 0 \ / \exists C(A) > 0, \ \ \forall F/K \text{ finie de degré } d, \ \ |A(F)_{\text{tors}}| \leq C(A) d^x\}.$$

Dans le cas général, la meilleure estimation de ce nombre est due à Masser [2] et [1].

Théorème 2.5 (Masser) *On a $\gamma(A) \leq g$.*

Dans le cas des courbes elliptiques de type C.M., le résultat de Masser est optimal. On peut se demander ce qu'il en est en dimension supérieure. Dans le cas des variétés abéliennes simples de type C.M., Ribet a donné une minoration de $\gamma(A)$. Précisément, en notant $\omega(n)$ le nombre de facteurs premiers de l'entier n, Ribet [5] montre que

Théorème 2.6 (Ribet) *Si A/K est une variété abélienne de type C.M., alors, il existe deux constantes strictement positives C_1 et C_2 ne dépendant que de A et K telles que : pour tout entier $n \geq 1$,*

$$C_1^{\omega(n)} \leq \frac{[K(A[n]) : K]}{n^d} \leq C_2^{\omega(n)},$$

où d est la dimension de groupe de Mumford-Tate de A.

Remarque 2.1 Ribet montre également que la dimension d du groupe de Mumford-Tate d'une variété abélienne de type C.M. simple, de dimension g est toujours comprise entre $2 + \log_2(g)$ et $g + 1$.

Comme corollaire du théorème 2.6, on déduit immédiatemment que si A/K est une variété abélienne simple de type C.M., on a $\gamma(A) \geq \frac{2g}{d}$ où d est la dimension du groupe de Mumford-Tate de A. En fait cette minoration reste plus généralement valable pour toute variété abélienne :

Proposition 2.1 [4] *Soit A/K une variété abélienne quelconque de dimension g. On a*

$$\gamma(A) \geq \frac{2g}{d}$$

où d est la dimension du groupe de Mumford-Tate de A.

Avec ces notations, le résultat concernant la borne sur la torsion est le suivant :

Théorème 2.7 [4] *Soit A/K une variété abélienne simple, de type C.M., de dimension g. Le nombre $\gamma(A)$ est un rationnel et on a*

$$\gamma(A) \leq \frac{2g}{2 + \log_2(g)},$$

où l'on a noté $\log_2$ le logarithme en base 2.

Enfin, dans le cas d'une courbe elliptique sans multiplication complexe, on a

Proposition 2.2 [4] *Si E/K est une courbe elliptique sans multiplication complexe, alors*

$$\gamma(E) = \frac{1}{2}.$$

Dans la suite on va essayer de donner une esquisse de preuve du théorème 2.6 de Ribet. La preuve repose essentiellement sur trois choses :

1. Résultats généraux sur les tores algébriques.
2. Connaissance explicite des représentations l-adiques dans le cas C.M.
3. Un peu de théorie du corps de classes.

3 Tores algébriques

3.1 Faits généraux

La théorie des tores algébriques se trouve dans [3]. Soient X un groupe commutatif abstrait et A un anneau. On note $A[X]$ l'algèbre de groupe de X sur A.

Définition 3.1 On appelle *groupe diagonalisable sur* A et on note $D(X)$ (ou $D_A(X)$) le A-schéma Spec $(A[X])$.

Proposition 3.1 *le schéma $D(X)$ est un A-schéma en groupes.*

Démonstration : Pour montrer ceci, il suffit de prouver que le foncteur

$$B \mapsto D(X)(B)$$

allant de la catégorie des A-algèbres dans celle des ensembles, est en fait à valeur dans la catégorie des groupes commutatifs. En effet, $D(X)$ étant affine, il suffit de se restreindre au cas des A-algèbres (schémas affines sur A) plutôt qu'au cas des A-schémas quelconques. On a les isomorphismes

$$D(X)(B) = \mathrm{Hom}_{A-\mathrm{sch}}\left(\mathrm{Spec}\, B, D(X)\right) \simeq \mathrm{Hom}_{A-\mathrm{alg}}\left(A[X], B\right) \simeq \mathrm{Hom}_{\mathrm{gr}}\left(X, B^*\right).$$

Ainsi on obtient naturellement une loi de groupes qui permet de conclure. □

Exemple 3.1 Si on prend $X = \mathbb{Z}$, on a $A[\mathbb{Z}] = A[t, t^{-1}]$, et $D(\mathbb{Z}) = \mathbb{G}_{m,A}$. On appelle ce groupe diagonalisable, le *groupe multiplicatif sur A*.

Proposition 3.2 *Si X et Y sont deux groupes abstraits, on a $D(X \times Y) \simeq D(X) \times_A D(Y)$.*

Démonstration : En effet, on a

$$D(X) \times_A D(Y) = \mathrm{Spec}\, A[X] \times_A \mathrm{Spec}\, A[Y] \simeq \mathrm{Spec}\, \left(A[X] \otimes_A A[Y]\right) \simeq \mathrm{Spec}\, A[X \times Y]. \qquad \square$$

Exemple 3.2 $D(\mathbb{Z}^n) \simeq \mathbb{G}_m^n$.

Définition 3.2 Un K-schéma en groupes T/K est un *tore algébrique* sur K s'il existe un entier n tel que $T_{\overline{K}} \simeq \mathbb{G}^n_{m,\overline{K}}$. Si T/K est un tore algébrique, on note

$$\widehat{T} = \mathrm{Hom}_{\overline{K}\text{gr-sch}}\left(T_{\overline{K}}, \mathbb{G}_{m,\overline{K}}\right)$$

le *groupe des caractères* de T.

Soit T/K un tore algébrique. Il existe une extension (séparable) finie L/K telle que tout caractère de T soit en fait défini sur L (i.e. provienne d'un L-morphisme $T_L \to \mathbb{G}_{m,L}$). Une telle extension est appelée un *corps de décomposition de T*.

Proposition 3.3 *Soit T/K un tore algébrique de dimension n. En notant L un corps de décomposition, on a l'isomorphisme de L-schémas en groupes*

$$T_L \simeq \mathbb{G}^n_{m,L}.$$

Démonstration : Par définition, on sait qu'il existe un $\overline{K}$-isomorphisme $f_{\overline{K}} : T_{\overline{K}} \to \mathbb{G}^n_{m,\overline{K}}$. Par définition du corps de décomposition, ce morphisme $f_{\overline{K}}$ est en fait défini sur L (i.e., il existe un L-morphisme, $f_L : T_L \to \mathbb{G}^n_{m,L}$ tel que $(f_L)_{\overline{K}} = f_{\overline{K}}$). En effet, $f_{\overline{K}} = (f_1, \ldots, f_n)$ avec les $f_i \in \widehat{T}$. Le morphisme $f_{\overline{K}}$ étant un isomorphisme on en déduit que f_L est également un isomorphisme. Ceci conclut. □

Théorème 3.1 *La correspondance $T \to \widehat{T}$ établit une équivalence de catégorie entre la catégorie des K-tores algébriques et la catégorie des $\mathbb{Z}$-modules libres de type fini munis d'une action continue du groupe de Galois $\mathscr{G} = \mathrm{Gal}(\overline{K}/K)$.*

La preuve se fait un explicitant un adjoint du foncteur “groupe des caractères” :

1. Dans un sens la correspondance, qui à un tore T/K associe son groupe des caractères $\widehat{T}$ muni de son action naturelle du groupe de Galois $\mathscr{G}$.
2. Dans l'autre sens, partant d'un groupe M muni d'une représentation $\rho : \mathscr{G} \to M$, on veut reconstruire le tore T/K correspondant. On peut vérifier que l'algèbre des invariants $\overline{K}[M]^{\mathscr{G}}$ est une K-algèbre de type fini, et que le K-schéma $T = \mathrm{Spec}\,\overline{K}[M]^{\mathscr{G}}$ est le K-schéma en groupes que l'on cherche.

Exemple 3.3 Un exemple particulièrement important de tore algébrique sur K est le *tore associé à une extension finie* L/K : il s'agit de la restriction à la Weil du groupe multiplicatif $\mathbb{G}_{m,L}$. On le définit comme suit : c'est le K-schéma en groupes affine représentant le foncteur $A \mapsto (A \otimes_K L)^*$ allant de la catégorie des K-algèbres dans celle des groupes commutatifs. Il s'agit d'un tore de dimension $[L : K]$.

3.2 Réduction modulo l^n

On se donne un tore algébrique T sur $\mathbb{Q}$ (dans notre utilisation, ce tore sera le tore associé à une extension finie de $\mathbb{Q}$). On se donne également un nombre premier l et un entier positif n. On introduit deux notations supplémentaires

$$T\left(1 + l^n \mathbb{Z}_l\right) = \left\{ t \in T(\mathbb{Q}_l) \;/\; \forall \chi \in \widehat{T_{\mathbb{Q}_l}}, \quad \chi(t) = 1 \bmod l^n \right\}$$

et,

$$T\left(\mathbb{Z}/l^n\mathbb{Z}\right) = T(\mathbb{Z}_l)/T\left(1 + l^n\mathbb{Z}_l\right).$$

Dans le cas où le tore a bonne réduction en l, (*i.e.* s'il existe un modèle lisse de $T_{\mathbb{Q}_l}$ sur $\mathrm{Spec}\,\mathbb{Z}_l$) il s'agit juste des points $\mathbb{Z}/l^n\mathbb{Z}$-rationnels du modèle $T_{\mathbb{Z}_l}$. Dans le cas encore plus spécifique où l'on suppose de plus $n = 1$, il s'agit juste des points $\mathbb{F}_l$-rationnels de T_l, où T_l est la réduction modulo l du tore T.

Étant donné un homomorphisme de tores algébriques $\lambda : T \to T'$ sur $\mathbb{Q}$, on en déduit un homomorphisme λ_l sur $\mathbb{Q}_l$ par extension des scalaires, puis on en déduit un homorphisme

$$\lambda_{l,n} : T\left(\mathbb{Z}/l^n\mathbb{Z}\right) \to T'\left(\mathbb{Z}/l^n\mathbb{Z}\right).$$

3.3 Un théorème de Ribet

On peut maintenant énoncer le résultat dû à Ribet [5] dont nous aurons besoin sur les tores.

Théorème 3.2 *Soit $\lambda : T \to T'$ un homomorphisme sur $\mathbb{Q}$ entre deux $\mathbb{Q}$-tores algébriques. Il existe deux constantes $C, C' > 0$ telles que, pour tout entier n et pour tout premier l, on a*

$$C \leq \frac{\mathrm{Card}\ \mathrm{Im}(\lambda_{l,n})}{l^{n\nu}} \leq C',$$

où $\nu = \dim \mathrm{Im}\lambda$.

On admettra ce résultat dans la suite.

4 Théorie de Shimura-Taniyama, Serre-Tate

Pour ce paragraphe les deux références sont [6] et [7]. On rappelle dans ce paragraphe deux résultats concernant les variétés abéliennes. On commence par un critère de Néron-Ogg-Shafarevitch généralisé, caractérisant la bonne réduction. Ensuite, on indique, en donnant les énoncés de Serre-Tate, la théorie de Shimura-Taniyama donnant une description "explicite" des représentations l-adiques des variétés abéliennes de type C.M.

Théorème 4.1 *Soient K un corps, v une valuation discrète de corps résiduel k supposé parfait et A/K une variété abélienne. Les propriétés suivantes sont équivalentes*

1. *la variété abélienne A a bonne réduction en v.*
2. *l'extension $K(A[n])/K$ est non-ramifiée en v pour tout entier n premier à* $\mathrm{char}(k)$*.*

On suppose désormais (au moins dans la suite de ce paragraphe) que K est un corps de nombres et A/K une variété abélienne simple à multiplication complexe par F. Quitte à augmenter un peu K, on suppose que F est inclus dans K et que tous les endomorphismes de $A_{\overline{K}}$ sont définis sur K. Par ailleurs, on fait l'hypothèse simplificatrice suivante :

$$\mathscr{O}_F \subset \mathrm{End}(A).$$

Soit l un nombre premier, on introduit le module de Tate

$$T_l(A) = \varprojlim A[l^n] \quad \text{et} \quad V_l(A) = T_l(A) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l.$$

Enfin on introduit la représentation l-adique

$$\rho_l : \mathscr{G}_K = \mathrm{Gal}(\overline{K}/K) \longrightarrow \mathrm{Aut}(T_l(A)).$$

Proposition 4.1 *La représentation ρ_l est à valeures dans $(\mathscr{O}_F \otimes \mathbb{Z}_l)^\times$. En particulier son image est un groupe commutatif.*

On note $t_{A/K}$ l'espace tangent de A en l'origine. C'est un K-espace vectoriel de dimension g. Il est naturellement muni d'une structure de F-espace vectoriel compatible à l'action de K. Autrement dit, on peut voir $t_{A/K}$ comme un (F, K)-bimodule sur $\mathbb{Q}$. Soit $u \in K$. On note $\det(u)$ le déterminant de la multiplication par u sur $t_{A/K}$ vu comme F-espace vectoriel. Si u est inversible, $\det(u)$ l'est également. Autrement dit, on obtient ainsi un morphisme

$$\psi_0 : K^* \longrightarrow F^*.$$

Plus généralement, si Λ est une $\mathbb{Q}$-algèbre commutative, l'espace $t_{A/K} \otimes_{\mathbb{Q}} \Lambda$ est un $(F \otimes \Lambda, K \otimes \Lambda)$-bimodule sur Λ. Soit maintenant $u \in K \otimes \Lambda$. On note $\det(u)$ le déterminant de la multiplication par u sur $t_{A/K} \otimes \Lambda$ vu comme $F \otimes \Lambda$-module. Si u est inversible, $\det(u)$ l'est également. Autrement dit, on obtient ainsi pour toute $\mathbb{Q}$-algèbre Λ, un morphisme

$$\psi_\Lambda : (K \otimes_{\mathbb{Q}} \Lambda)^* \longrightarrow (F \otimes_{\mathbb{Q}} \Lambda)^*,$$

fonctoriel en Λ. Une autre manière de dire ceci est la suivante : on a un morphisme de tores algébriques sur $\mathbb{Q}$,

$$\psi : T_K \to T_F$$

entre le tore $T_K/\mathbb{Q}$ associé à l'extension $K/\mathbb{Q}$ et le tore $T_F/\mathbb{Q}$ associé à l'extension $F/\mathbb{Q}$. On note en particulier, ψ_l le morphisme obtenu avec $\Lambda = \mathbb{Q}_l$ pour l premier.

On rappelle la notion d'*idèles I_K d'un corps de nombres K* : c'est le sous-groupe du produit des K_v^*, v décrivant l'ensemble des places de K (archimédiennes et ultramétriques), défini par la condition

$$x = (x_v) \in I_K \;\text{ si pour presque toute place } v \quad x_v \in (\mathscr{O}_{K_v})^\times.$$

Ceci étant on peut maintenant donner une proposition issue de la théorie du corps de classes :

Proposition 4.2 *Il existe un homomorphisme surjectif*

$$I_K \longrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K).$$

De plus le produit sur les places finie $\prod_v \mathscr{O}_{K_v}$ est d'image d'indice fini par ce morphisme.

Ceci nous permet d'interpréter la représentation l-adique ρ_l comme étant un homomorphisme

$$\rho_l : I_K \longrightarrow (\mathscr{O}_F \otimes \mathbb{Z}_l)^\times.$$

On peut maintenant passer à la description explicite des représentations l-adiques pour les variétés abéliennes de type C.M.

Théorème 4.2 *Pour tout premier l et pour tout $a \in I_K$, on a avec les notations précédentes*

$$\rho_l(a) = \varepsilon(a)\psi_l(a_l^{-1}), \quad \text{où} \quad a_l \in K_l^* = \prod_{v|l} K_v^*,$$

et où ε est un morphisme tel que pour tout place v de bonne réduction

$$\forall a_v \in (\mathscr{O}_{K_v})^\times, \quad \varepsilon(a_v) = 1.$$

5 Preuve du théorème 2.6

On commmence par une petite réduction : quitte à augmenter un peu K, on peut :

1. supposer que $F \subset \mathrm{End}_{\overline{K}}(A) \otimes \mathbb{Q} \subset K$,
2. remplacer K par son corps de classes de Hilbert,
3. supposer que A/K a bonne réduction en toutes places.

Pour alléger les notations, on note pour tout N entier, $K_N := K(A[N])$. Par le théorème 4.1, le point 3. entraîne que K_N/K est (éventuellement) ramifiée uniquement en les premiers l divisant N. Par le point 2., si N et M sont premiers entre eux, alors $K_N \cap K_M = K$. Ainsi, la fonction $N \mapsto [K_N : K]$ est multiplicative (au sens arithmétique usuel). Pour prouver le théorème, il suffit donc d'obtenir les inégalités

$$\forall l, n \;\; C_1 \leq \frac{[K_{l^n} : K]}{l^{n\nu}} \leq C_2. \tag{1}$$

On suppose désormais A/K simple pour alléger les notations. On rappelle qu'au paragraphe précédent on a introduit un morphisme $\psi : T_K \to T_F$ entre les deux $\mathbb{Q}$-tores algébriques associés aux extensions K et F. On va prouver les inégalités (1) avec $\nu = \dim \mathrm{Im}\psi$.

On a vu que la théorie du corps de classe nous permet d'interpréter ρ_l comme un morphisme de I_K dans $(\mathscr{O}_F \otimes \mathbb{Z}_l)^\times$. De plus la proposition 4.2 nous permet, ce qui ne modifiera que les constantes, de remplacer I_K par le produit $\prod_v (\mathscr{O}_{K_v})^\times$. Enfin par le théorème 4.2, on constate que ρ_l est triviale sur les $(\mathscr{O}_{K_v})^\times$ avec v ne divisant pas l. On peut finalement voir la représentation ρ_l comme

$$\rho_l : \prod_{v/l} (\mathscr{O}_{K_v})^\times \to (\mathscr{O}_F \otimes \mathbb{Z}_l)^\times,$$

c'est à dire comme un homorphisme $T_K(\mathbb{Z}_l) \to T_F(\mathbb{Z}_l)$ entre le points $\mathbb{Z}_l$-rationels de T_K et T_F. De plus, toujours par le théorème 4.2, cet homorphisme n'est autre que l'application sur les $\mathbb{Z}_l$-points induite par $\lambda : x \mapsto \lambda(x^{-1})$. En notant $\overline{\rho}_{l^n}$ la réduction modulo l^n de ρ_l, on a

$$\overline{\rho}_{l^n} : T_K(\mathbb{Z}_l) \to T_F\left(\mathbb{Z}/l^n\mathbb{Z}\right).$$

Le diagramme suivant est clairement commutatif

$$\begin{tikzcd}
T_K(\mathbb{Z}_l) \arrow[r, "\rho_l"] \arrow[d] & T_E(\mathbb{Z}_l) \arrow[d] \\
T_K(\mathbb{Z}/l^n\mathbb{Z}) \arrow[r, "\lambda_{l,n}"'] & T_F(\mathbb{Z}/l^n\mathbb{Z})
\end{tikzcd}$$

On en déduit

$$G_{l,n} := \rho_{l^n}(G_K) = \mathrm{Im}\lambda_{l,n}.$$

Le corollaire 3.2 énoncé au paragraphe précédent sur les tores permet alors de conclure. Il reste pour conclure à voir que ν est bien la dimension du groupe de Mumford-Tate, mais ceci découle de l'interprétation que l'on a du groupe de Mumford-Tate dans le cas C.M. : c'est le groupe de Galois motivique associé aux représentations l-adiques. Ceci conclut.

Références

[1] D. Masser. Lettre à Daniel Bertrand du 10 novembre 1986.

[2] D. Masser. Small values of the quadratic part of the Néron-Tate height. In *Progr. Math.*, volume 12, pages 213–222. Birkhäuser, 1981.

[3] T. Ono. Arithmetic of algebraic tori. *Ann. Math.*, 74, n. 1 :101–139, 1961.

[4] N. Ratazzi. Borne sur la torsion dans les variétés abéliennes C.M. prépublication à venir.

[5] K. A. Ribet. Division fields of abelian varieties with complex multiplication. *Mémoires de la S.M.F*, 2 :75–94, 1980.

[6] J.-P. Serre and J. Tate. Good reduction of abelian varieties. *Ann. Math.*, 88 :492–517, 1968.

[7] G. Shimura and Y. Taniyama. *Complex multiplication of abelian varieties and its applications to number theory*, volume 6 of *Publications of the Mathematical Society of Japan.* The Mathematical Society of Japan, Tokyo, 1961.