

Variétés abéliennes sur les corps finis: théorème de Tate et classification de Honda-Tate

Olivier Wittenberg

5 décembre 2001

Résumé

Le but de cet exposé est de montrer (suivant Tate et Honda) que les classes d'isogénie de variétés abéliennes simples sur \mathbb{F}_q sont en bijection avec les classes de conjugaison de q -nombres de Weil, par l'application qui à une telle variété associe son endomorphisme de Frobenius. On prouvera en détail le théorème de Tate (voir [8]), puis on fera quelques rappels de théorie de la multiplication complexe, pour ensuite terminer la preuve de cette classification.

1 Introduction

Si A et B sont deux variétés abéliennes sur un corps k , on note $\mathrm{Hom}_k(A, B)$ le groupe des k -morphisms de variétés abéliennes de A dans B , et $\mathrm{Hom}_k^0(A, B) = \mathrm{Hom}_k(A, B) \otimes_{\mathbb{Z}} \mathbb{Q}$. Rappelons que toute variété abélienne sur k est isogène à un produit de variétés abéliennes simples. Cela a pour conséquence que la catégorie des variétés abéliennes à isogénie près (dont les ensembles de morphismes sont les $\mathrm{Hom}_k^0(A, B)$) est semi-simple; pour obtenir une classification des variétés abéliennes à isogénie près, il suffit donc de s'intéresser aux variétés abéliennes simples. Ce théorème montre aussi que l'anneau $\mathrm{End}_k^0(A)$ est semi-simple, et que son centre est une \mathbb{Q} -algèbre finie séparable (on suppose connu le fait que $\mathrm{Hom}_k(A, B)$ est un \mathbb{Z} -module libre de type fini).

Supposons maintenant k fini, de cardinal q . Si A est une variété abélienne sur k , on notera π_A son endomorphisme de Frobenius; il s'agit du morphisme de schémas $\pi_A: A \rightarrow A$ qui est l'identité sur l'espace topologique sous-jacent et $f \mapsto f^q$ sur les sections. C'est un élément du centre de $\mathrm{End}_k^0(A)$; en particulier, si A est simple, $\mathbb{Q}(\pi_A)$ est une extension finie de \mathbb{Q} . L'hypothèse de Riemann (prouvée par Weil dans le cas des variétés abéliennes) affirme alors que $\pi_A \in \mathbb{Q}(\pi_A)$ est un q -nombre de Weil, au sens de la définition suivante.

Définition 1.0.1 — Soit K un corps de caractéristique 0. On dit que $x \in K$ est un q -nombre de Weil si x est entier sur \mathbb{Z} et si, pour tout plongement complexe $\sigma: \mathbb{Q}(x) \rightarrow \mathbb{C}$, on a $|\sigma(x)| = q^{\frac{1}{2}}$. On dit que deux q -nombres de Weil $x_1 \in K_1$ et $x_2 \in K_2$ sont conjugués s'ils ont même polynôme minimal sur \mathbb{Q} .

Le théorème que l'on se propose de démontrer est le suivant.

Théorème 1.0.2 (Honda-Tate) — L'application qui à une variété abélienne simple sur k associe son endomorphisme de Frobenius induit une bijection de l'ensemble des classes d'isogénie de variétés abéliennes simples sur k vers l'ensemble des classes de conjugaison de q -nombres de Weil.

Vérifions tout d'abord que cette application est bien définie. Soit une isogénie $f: A \rightarrow B$, de degré N . En factorisant la multiplication par N sur A , on obtient une isogénie $g: B \rightarrow A$ telle que $g \circ f = N$. On a alors $f \circ g \circ f = N \circ f$, mais f est un épimorphisme dans la catégorie des schémas (car c'est un morphisme fidèlement plat), d'où $f \circ g = N$. Ceci permet de vérifier immédiatement que le morphisme d'anneaux

$$\begin{aligned} \mathrm{End}_k^0(A) &\longrightarrow \mathrm{End}_k^0(B) \\ \varphi &\longmapsto \frac{1}{N} f \circ \varphi \circ g \end{aligned}$$

est un isomorphisme qui envoie π_A sur π_B . Les Frobenius sont donc bien conjugués.

La preuve du théorème se fait en deux étapes. L'injectivité de l'application considérée provient du théorème de Tate sur les variétés abéliennes sur les corps finis, auquel on va s'intéresser maintenant ; la surjectivité provient d'arguments de multiplication complexe, que l'on considérera à la troisième section.

2 Le théorème de Tate

Soient A et B deux variétés abéliennes sur un corps k quelconque, et ℓ un nombre premier différent de la caractéristique de k . Fixons une clôture séparable \bar{k} de k , et notons $G = \text{Gal}(\bar{k}/k)$. On dispose d'une flèche

$$\Phi_0 : \text{Hom}_k(A, B) \otimes_{\mathbb{Z}} \mathbb{Z}_{\ell} \longrightarrow \text{Hom}_{\mathbb{Z}_{\ell}[G]}(T_{\ell}(A), T_{\ell}(B))$$

où $T_{\ell}(A) = \varprojlim A[\ell^n](\bar{k})$, en notant $A[f]$ le noyau d'un morphisme f de source A . Il est bien connu que cette flèche est toujours injective.

Théorème 2.0.3 (Tate) — *Si k est fini, cette flèche est un isomorphisme.*

C'est ce théorème que nous allons démontrer dans cette section. Notons que Faltings et Zarhin ont prouvé que cette flèche est un isomorphisme dès que k est un corps de type fini sur son sous-corps premier, ce qui est nettement plus général et d'autant plus difficile.

2.1 Preuve du théorème

Commençons par réduire quelque peu ce qu'il faut prouver.

Lemme 2.1.1 — *Pour prouver que Φ_0 est surjective, on peut supposer que $A = B$. De plus, il suffit de prouver que l'application*

$$\Phi : \text{End}_k(A) \otimes_{\mathbb{Z}} \mathbb{Q}_{\ell} \longrightarrow \text{End}_{\mathbb{Q}_{\ell}[G]}(V_{\ell}(A))$$

est surjective, où $V_{\ell}(A) = T_{\ell}(A) \otimes_{\mathbb{Z}_{\ell}} \mathbb{Q}_{\ell}$.

Démonstration — Commençons par prouver que le conoyau de Φ_0 est un \mathbb{Z}_{ℓ} -module libre. Ce module est évidemment de type fini et \mathbb{Z}_{ℓ} est principal ; la torsion de $\text{Coker}(\Phi_0)$ est donc un sous-module fini, d'ordre ℓ^N pour un certain N , et il suffit de montrer que $N = 0$. Soit $f \in \text{Hom}_{\mathbb{Z}_{\ell}[G]}(T_{\ell}(A), T_{\ell}(B))$ qui soit de torsion dans $\text{Coker}(\Phi_0)$. L'annulateur de f dans $\text{Coker}(\Phi_0)$ est un idéal de \mathbb{Z}_{ℓ} : il est engendré par ℓ^k pour un certain $k \in \mathbb{N}$. Soit $\varphi \in \text{Hom}_k(A, B)$ tel que $T_{\ell}(\varphi) = \ell^k f + \ell^{N+k} g$ pour un certain $g \in \text{Hom}_{\mathbb{Z}_{\ell}[G]}(T_{\ell}(A), T_{\ell}(B))$. Il existe $\varphi' \in \text{Hom}_k(A, B)$ tel que $\varphi = \ell^k \varphi'$ (rappelons qu'un morphisme u tel que $T_{\ell}(u)$ soit divisible par ℓ est lui-même divisible par ℓ). Ainsi, $f + \ell^N g = T_{\ell}(\varphi')$; comme g est nécessairement de torsion dans $\text{Coker}(\Phi_0)$, on en déduit que f est nul dans $\text{Coker}(\Phi_0)$, ce qui est le résultat voulu.

Il s'ensuit que la surjectivité de $\Phi_0 \otimes_{\mathbb{Z}_{\ell}} \text{Id}_{\mathbb{Q}_{\ell}}$ implique celle de Φ_0 . Supposons enfin le résultat connu lorsque $A = B$; pour l'obtenir sans cette hypothèse, il suffit de vérifier que l'isomorphisme

$$\text{End}_k(A \times_k B) \otimes_{\mathbb{Z}} \mathbb{Q}_{\ell} \longrightarrow \text{End}_{\mathbb{Q}_{\ell}[G]}(V_{\ell}(A \times_k B))$$

est compatible aux décompositions

$$\text{End}_k^0(A \times_k B) = \text{End}_k^0(A) \times \text{Hom}_k^0(A, B) \times \text{Hom}_k^0(B, A) \times \text{End}_k^0(B)$$

et

$$V_{\ell}(A \times_k B) = V_{\ell}(A) \times V_{\ell}(B).$$

□

Notons E_{ℓ} l'image de Φ et F_{ℓ} la sous-algèbre de $\text{End}_{\mathbb{Q}_{\ell}}(V_{\ell}(A))$ engendrée par l'image de G .

Lemme 2.1.2 — Pour prouver que Φ_0 est surjective, il suffit de prouver que F_ℓ est le commutant de E_ℓ dans $\text{End}_{\mathbb{Q}_\ell}(V_\ell(A))$.

Démonstration — Montrer que Φ est bijective revient à montrer que E_ℓ est le commutant de F_ℓ dans $\text{End}_{\mathbb{Q}_\ell}(V_\ell(A))$. Le lemme est donc une application directe du théorème du bicommutant, puisque E_ℓ est un anneau semi-simple. Rappelons son énoncé : soient k un corps, A une k -algèbre, V un A -module fidèle, semi-simple et de dimension finie sur k ; alors A est égal à son bicommutant dans $\text{End}_k(V)$. \square

Si \mathcal{L} est un faisceau inversible sur A , on note $\varphi_{\mathcal{L}} : A \rightarrow \hat{A}$ le morphisme associé (qui est $x \mapsto t_x^* \mathcal{L} \otimes \mathcal{L}^{-1}$ sur les points à valeurs dans \bar{k}), où \hat{A} est la variété abélienne duale. On note

$$H_0 : T_\ell(A) \times T_\ell(\hat{A}) \rightarrow \mathbb{Z}_\ell(1)$$

l'accouplement de Weil. Si θ est une polarisation, on note $H_0^\theta : T_\ell(A) \times T_\ell(A) \rightarrow \mathbb{Z}_\ell(1)$ l'accouplement déduit de θ (i.e. $H_0^\theta(x, y) = H_0(x, T_\ell(\theta)(y))$), et $H^\theta : V_\ell(A) \times V_\ell(A) \rightarrow \mathbb{Q}_\ell(1)$ celui que l'on obtient par extension des scalaires. Rappelons que ce sont des formes bilinéaires alternées G -équivariantes ; H_0 et H^θ sont non dégénérées, et il en va de même pour H_0^θ si le degré de θ est premier à ℓ . Lorsque $\varphi_{\mathcal{L}}$ est une polarisation (par exemple si \mathcal{L} est très ample), on écrira $H^\mathcal{L}$ (resp. $H_0^\mathcal{L}$) au lieu de $H^{\varphi_{\mathcal{L}}}$ (resp. $H_0^{\varphi_{\mathcal{L}}}$).

Fixons un faisceau très ample \mathcal{L} sur A . Dorénavant, on considérera toujours $V_\ell(A)$ muni de l'accouplement $H^\mathcal{L}$; ainsi, les termes « orthogonal » et « isotrope » seront relatifs à $H^\mathcal{L}$. Notons d^2 le degré de la polarisation $\varphi_{\mathcal{L}}$ et g la dimension de A . Selon la terminologie de Bourbaki, on dira qu'un sous-espace vectoriel de $V_\ell(A)$ est *totalelement isotrope* s'il est inclus dans son orthogonal.

Proposition 2.1.3 — Soit W un sous-espace vectoriel de $V_\ell(A)$ totalelement isotrope maximal, que l'on suppose de plus stable par G . Il existe alors $u \in E_\ell$ tel que $u(V_\ell(A)) = W$.

Démonstration — Notons $T = T_\ell(A)$, $V = V_\ell(A)$ et $X_n = (T \cap W) + \ell^n T$. D'après le théorème de structure des modules sur les anneaux principaux appliqué à T , qui est un \mathbb{Z}_ℓ -module libre de rang $2g$, il existe une \mathbb{Z}_ℓ -base de T (e_1, \dots, e_{2g}) et $\alpha_1, \dots, \alpha_r \in \mathbb{Z}_\ell$ tels que $(\alpha_1 e_1, \dots, \alpha_r e_r)$ soit une \mathbb{Z}_ℓ -base de $T \cap W$. Puisque $(T \cap W) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \approx W$, qui est de dimension g sur \mathbb{Q}_ℓ (étant égal à son orthogonal), on a $r = g$. De plus, $\alpha_i e_i \in T \cap W$ et $e_i \in T$ impliquent que $e_i \in T \cap W$, et donc α_i est inversible : on peut supposer $\alpha_i = 1$. Ainsi l'inclusion $T \cap W \subset T$ est isomorphe à l'inclusion $\mathbb{Z}_\ell^g \times \{0\}^g \subset \mathbb{Z}_\ell^{2g}$, ce qui montre que X_n est d'indice ℓ^{ng} dans T .

Lemme 2.1.4 — Il existe une variété abélienne B_n sur k , et une isogénie $f_n : B_n \rightarrow A$ de degré ℓ^{ng} , telle que $\text{Im}(T_\ell(f_n)) = X_n$.

Démonstration — Soit $\psi_n : T_\ell(A) \rightarrow A[\ell^n](\bar{k})$ la flèche naturelle. On pose $K_n = \psi_n(X_n)$. C'est un sous-groupe fini de $A(\bar{k})$ stable par G , que l'on identifie à un sous- k -schéma en groupes commutatif fini étale de A . Soient $B_n = A/K_n$ et $\pi_n : A \rightarrow B_n$ la projection. Étant donné que K_n est contenu dans $A[\ell^n]$ (en toute rigueur, il faut préciser « en tant que sous-schéma », mais c'est bien sûr équivalent à l'inclusion en tant que partie finie de $A(\bar{k})$ stable par G), il existe un morphisme de variétés abéliennes f_n qui fasse commuter le diagramme suivant :

$$\begin{array}{ccc} A & \xrightarrow{\ell^n} & A \\ & \searrow \pi_n & \nearrow f_n \\ & & B_n \end{array}$$

On a $\psi_n(T_\ell(f_n)(T_\ell(B_n))) = f_n((B_n)[\ell^n](\bar{k})) = (f_n \circ \pi_n)(\{x \in A(\bar{k}) ; \ell^n x \in K_n\}) = K_n$ (les deux dernières égalités proviennent de la surjectivité de π_n et de la multiplication par ℓ^n). En d'autres termes, X_n et $T_\ell(f_n)(T_\ell(B_n))$ sont deux sous-modules de T qui contiennent $\ell^n T$ et qui sont égaux modulo $\ell^n T$. Ils sont donc égaux. L'assertion sur le degré de f_n provient du fait que X_n est d'indice ℓ^{ng} dans T . \square

On aimerait maintenant montrer qu'une infinité de B_n sont isomorphes, à l'aide du théorème suivant.

Théorème 2.1.5 — Soient g et d des entiers, k un corps fini. L'ensemble des classes d'isomorphisme de variétés abéliennes sur k de dimension g sur lesquelles il existe une polarisation de degré d^2 est fini.

Démonstration — La preuve de ce théorème utilise essentiellement trois ingrédients :

- le théorème de Riemann-Roch pour les variétés abéliennes ;
- le fait que si \mathcal{L} est un faisceau ample sur une variété abélienne, \mathcal{L}^3 est très ample ;
- le fait qu'une polarisation sur une variété abélienne sur un corps fini provient toujours d'un faisceau inversible défini sur le corps de base.

Pour plus de détails, voir [4]. □

Il nous reste donc à montrer que B_n possède une polarisation de degré d^2 . Il existe en tout cas une polarisation de degré $\ell^{2ng}d^2$ sur B_n , à savoir $\hat{f}_n \circ \varphi_{\mathcal{L}} \circ f_n = \varphi_{f_n^* \mathcal{L}}$. Comme le degré de la multiplication par ℓ^n est ℓ^{2ng} , il nous suffirait de montrer que l'on peut diviser cette polarisation par ℓ^n . Utilisons pour cela la proposition suivante.

Proposition 2.1.6 — Soit A une variété abélienne sur un corps parfait. Soit θ une polarisation de A , telle que $H_0^\theta : T_\ell(A) \times T_\ell(A) \rightarrow \mathbb{Z}_\ell(1)$ soit à valeurs dans $\ell^n \mathbb{Z}_\ell(1)$. Il existe alors une polarisation θ' de A telle que $\theta = \ell^n \theta'$.

Démonstration — C'est un résultat classique sur les variétés abéliennes. Voir [4]. □

Vérifions que la proposition s'applique. Pour $x, y \in T_\ell(B_n)$, on a

$$H_0^{\hat{f}_n \circ \varphi_{\mathcal{L}} \circ f_n}(x, y) = H_0(T_\ell(f_n)(x), T_\ell(\varphi_{\mathcal{L}}) \circ T_\ell(f_n)(y)) = H_0^{\mathcal{L}}(T_\ell(f_n)(x), T_\ell(f_n)(y))$$

car $T_\ell(\hat{f}_n)$ est l'adjoint à gauche de $T_\ell(f_n)$ pour H_0 . Ainsi, $H_0^{f_n^* \mathcal{L}}$ prend sur $T_\ell(B_n)$ les mêmes valeurs que $H_0^{\mathcal{L}}$ sur $T_\ell(f_n)(T_\ell(B_n)) = X_n = T \cap W + \ell^n T$. Comme W est totalement isotrope, cela montre bien que ces valeurs sont divisibles par ℓ^n , d'où le résultat.

Finalement, une infinité des B_n sont isomorphes. Soit I une partie infinie de \mathbb{N} telle que les B_i pour $i \in I$ soient tous isomorphes. Soit $m = \min I$. On fixe un isomorphisme $v_i : B_m \rightarrow B_i$, pour chaque i . Il existe $g_n : A \rightarrow B_n$ tel que le diagramme suivant commute :

$$\begin{array}{ccc} B_n & \xrightarrow{\deg(f_n)} & B_n \\ & \searrow f_n & \nearrow g_n \\ & & A \end{array}$$

On note $f_n^{-1} = \frac{1}{\deg(f_n)} g_n \in \text{Hom}_k^0(A, B_n)$. Soit u_i l'image, dans $\text{End}_{\mathbb{Q}_\ell}(V_\ell(A))$, de $f_i \circ v_i \circ f_m^{-1} \in \text{End}^0(A)$.

On a

$$u_i(X_m) = u_i(T_\ell(f_m)(T_\ell(B_m))) = T_\ell(f_i) \circ T_\ell(v_i)(T_\ell(B_m)) = T_\ell(f_i)(T_\ell(B_i)) = X_i$$

donc en particulier $u_i(X_m) \subset X_m$ (les X_i sont décroissants), c'est-à-dire $u_i \in \text{End}_{\mathbb{Z}_\ell}(X_m)$. Le \mathbb{Z}_ℓ -module $\text{End}_{\mathbb{Z}_\ell}(X_m)$ est une partie compacte de $\text{End}_{\mathbb{Q}_\ell}(V_\ell(A))$. Quitte à diminuer l'ensemble I , on peut donc supposer que $(u_i)_{i \in I}$ converge vers un certain $u \in \text{End}_{\mathbb{Z}_\ell}(X_m)$ lorsque i tend vers l'infini. Montrons maintenant que $u(X_m) = \bigcap_{i \in I} X_i$. L'inclusion « \subset » est évidente : les X_i sont décroissants. Soit maintenant $x \in \bigcap_{i \in I} X_i$. Il existe $x_i \in X_m$ tel que $x = u_i(x_i)$. Quitte à diminuer encore I , on peut supposer que $(x_i)_{i \in I}$ converge vers un certain $x' \in X_m$; ainsi $x = u_i(x_i) \rightarrow u(x')$ et donc $x \in u(X_m)$: l'autre inclusion est vérifiée. Remarquons enfin que l'on a

$$u(X_m) = \bigcap_{i \in I} X_i = \bigcap_{i \in I} ((T \cap W) + \ell^i T) = T \cap W,$$

la dernière égalité provenant du fait que l'inclusion $T \cap W \subset T$ est isomorphe à l'inclusion $\mathbb{Z}_\ell^g \times \{0\}^g \subset \mathbb{Z}_\ell^{2g}$. Comme E_ℓ est un sous- \mathbb{Q}_ℓ -espace de $\text{End}_{\mathbb{Q}_\ell}(V_\ell(A))$, il est fermé (étant complet). En particulier, $u \in E_\ell$: le résultat est prouvé. □

Proposition 2.1.7 — Si F_ℓ est une \mathbb{Q}_ℓ -algèbre diagonale (i.e. $F_\ell \approx \mathbb{Q}_\ell^s$ pour un $s \in \mathbb{N}$), F_ℓ est bien le commutant de E_ℓ dans $\text{End}_{\mathbb{Q}_\ell}(V_\ell(A))$.

Démonstration — Nous allons utiliser le lemme suivant.

Lemme 2.1.8 — Soit D le commutant de E_ℓ . Si W est un sous-espace totalement isotrope de V stable par F_ℓ , il est aussi stable par D .

Démonstration du lemme — Procédons par récurrence descendante sur $\dim W$. Le cas où $\dim W = g$ se résout à l'aide de la proposition précédente : il existe $u \in E_\ell$ tel que $u(V) = W$ et on a alors $DW = Du(V) = u(DV) \subset u(V) = W$. Supposons donc que $\dim W < g$ et que le résultat est prouvé en dimension supérieure. La stabilité de W par G et la G -équivariance de $H^\mathcal{L}$ entraînent que W^\perp (l'orthogonal de W pour $H^\mathcal{L}$) est stable par G , donc par F_ℓ . Comme F_ℓ est semi-simple, le sous- F_ℓ -module W de W^\perp admet un supplémentaire semi-simple. On peut décomposer ce supplémentaire comme somme de F_ℓ -modules simples :

$$W^\perp = W \oplus \bigoplus_{i=1}^m L_i$$

où les L_i sont simples sur F_ℓ . Les idéaux bilatères minimaux de F_ℓ sont des anneaux isomorphes à \mathbb{Q}_ℓ ; ainsi, L_i est un \mathbb{Q}_ℓ -espace de dimension 1. Posons maintenant $W_i = W \oplus L_i$, pour $1 \leq i \leq m$. C'est un F_ℓ -module ; vu comme sous-espace de V stable par F_ℓ , il est totalement isotrope puisque $L_i \subset L_i^\perp$ (du fait que L_i est de dimension 1 et que $H^\mathcal{L}$ est alternée) et que $L_i \subset W^\perp$. On peut donc appliquer l'hypothèse de récurrence : W_i est stable par D . Enfin, $\dim W < g$ et $\dim W^\perp + \dim W = 2g$ (la forme est non dégénérée) entraînent que $m \geq 2$, et donc $W = W_1 \cap W_2$, ce qui prouve que W est stable par D . \square

Choisissons une base (e_1, \dots, e_s) de F_ℓ sur \mathbb{Q}_ℓ qui détermine un isomorphisme $F_\ell \approx \mathbb{Q}_\ell^s$ et notons V_i l'image de e_i . Un endomorphisme u de V est dans F_ℓ si et seulement si pour tout i , u stabilise V_i et l'endomorphisme induit $u|_{V_i} \in \text{End}_{\mathbb{Q}_\ell}(V_i)$ est une homothétie. Utilisons cette caractérisation pour prouver que $D \subset F_\ell$. Soit $u \in D$. Si on applique le lemme en prenant pour W la droite engendrée par un $x \in V_i$ (qui est bien totalement isotrope et stable par F_ℓ), on trouve que x est stable par u . En d'autres termes, tout vecteur non nul de V_i est vecteur propre de u : cela montre bien que u stabilise V_i et que $u|_{V_i}$ est une homothétie. Ainsi, $D \subset F_\ell$; l'autre inclusion étant évidente, la proposition est prouvée. \square

À présent, on a montré que si F_ℓ est une \mathbb{Q}_ℓ -algèbre diagonale, l'application Φ est bijective. Remarquons que si l'on prouve la bijectivité de Φ pour un nombre premier ℓ différent de p et que l'on montre que la dimension de $\text{End}_{\mathbb{Q}_\ell[G]}(V_\ell(A))$ sur \mathbb{Q}_ℓ ne dépend pas de ℓ , la bijectivité de Φ pour tout $\ell \neq p$ s'ensuivra (en effet, Φ est toujours injective). C'est ce que nous allons faire.

La \mathbb{Q} -algèbre $\mathbb{Q}[\pi_A]$ étant séparable, on peut l'écrire $\mathbb{Q}[\pi_A] = K_1 \times \dots \times K_n$ où les K_i sont des extensions finies de \mathbb{Q} . Choisissons une extension finie galoisienne K/\mathbb{Q} dans laquelle se plongent tous les K_i . Comme le Frobenius est un générateur topologique de G , on a $F_\ell = \mathbb{Q}[\pi] \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ (remarquons que $T_\ell(\pi_A)$ est égal à l'endomorphisme défini par le Frobenius de G). Pour trouver un ℓ tel que F_ℓ soit une \mathbb{Q}_ℓ -algèbre diagonale, il suffit donc d'en trouver un tel que $K \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ soit une \mathbb{Q}_ℓ -algèbre diagonale (en effet, une sous-algèbre d'une algèbre diagonale est diagonale). Soit $\alpha \in K$ tel que $K = \mathbb{Q}(\alpha)$ et $f \in \mathbb{Z}[X]$, en notant f le polynôme minimal de α sur \mathbb{Q} .

Lemme 2.1.9 — Soit $P \in \mathbb{Z}[X]$ non constant. Il existe une infinité de nombres premiers ℓ tels que P ait une racine dans $\mathbb{Z}/\ell\mathbb{Z}$.

Démonstration — On pose $P = a_n X^n + \dots + a_0$. Si $a_0 = 0$, le résultat est évident. Si $a_0 \neq 0$, on peut supposer $a_0 = 1$ quitte à remplacer X par $a_0 X$. Supposons alors qu'il n'existe qu'un nombre fini de nombres premiers ℓ tels que P ait une racine dans $\mathbb{Z}/\ell\mathbb{Z}$. Soient N le produit de ces entiers ℓ , $x \in \mathbb{N}$ assez grand pour que $|P(Nx)| > 1$ et ℓ un diviseur premier de $P(Nx)$. Par définition, N est un multiple de ℓ ; par ailleurs $P(Nx) = a_n N^n x^n + \dots + a_1 Nx + 1$, d'où une contradiction en regardant modulo ℓ . \square

D'après le lemme, il existe un nombre premier ℓ différent de p et ne divisant pas le discriminant de f et un entier x tels que $f(x) \equiv 0 \pmod{\ell}$. La condition sur le discriminant entraîne que $f'(x) \not\equiv 0 \pmod{\ell}$.

Ainsi, d'après le lemme de Hensel, f a une racine dans \mathbb{Z}_ℓ . En fait, f est même scindé dans \mathbb{Q}_ℓ ; en effet, les conjugués de α s'écrivent comme des polynômes de α (on rappelle que $\mathbb{Q}(\alpha)/\mathbb{Q}$ est une extension galoisienne). La \mathbb{Q}_ℓ -algèbre $K \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ est diagonale : c'est le résultat voulu.

Il ne reste plus qu'à montrer que la dimension de $\text{End}_{\mathbb{Q}_\ell[G]}(V_\ell(A))$ sur \mathbb{Q}_ℓ est indépendante de ℓ . Notons cette dimension d_ℓ . Notons aussi π_ℓ l'endomorphisme de $V_\ell(A)$ induit par π_A . Il est semi-simple, puisque π_A est séparable sur \mathbb{Q} et que Φ est injective. Par conséquent $V_\ell(A)$ est un $\mathbb{Q}_\ell[\pi_\ell]$ -module semi-simple : on peut écrire $V_\ell(A) = V_1^{n_1} \oplus \dots \oplus V_m^{n_m}$ où les V_i sont des $\mathbb{Q}_\ell[\pi_\ell]$ -modules simples non nuls deux à deux non isomorphes. On a alors $d_\ell = \dim \text{End}_{\mathbb{Q}_\ell[\pi_\ell]}(V_\ell(A)) = \sum n_i^2 \dim \text{End}_{\mathbb{Q}_\ell[\pi_\ell]}(V_i) = \sum n_i^2 \dim V_i$, du fait que V_i est un sous-espace cyclique pour π_ℓ . Notons $P_{\ell,i}$ le polynôme minimal sur \mathbb{Q}_ℓ de l'endomorphisme de V_i induit par π_ℓ (qui est aussi son polynôme caractéristique) et $P \in \mathbb{Q}[X]$ le polynôme caractéristique de π_A (voir [4] pour la définition). Il est bien connu que P est aussi le polynôme caractéristique de π_ℓ ; ainsi, $P = \prod_i P_{\ell,i}^{n_i}$ et $\dim V_i = \deg P_{\ell,i}$, de sorte que

$$d_\ell = \sum v_Q(P)^2 \deg Q,$$

où la somme porte sur les $Q \in \mathbb{Q}_\ell[X]$ irréductibles unitaires et où $v_Q(P)$ dénote la Q -valuation de P . Une vérification facile montre que cette somme reste inchangée si on la fait porter sur les $Q \in \mathbb{Q}[X]$ irréductibles unitaires (écrire la décomposition d'un polynôme irréductible unitaire de $\mathbb{Q}[X]$ dans $\mathbb{Q}_\ell[X]$, sans oublier qu'il est séparable). Il est maintenant évident que d_ℓ ne dépend pas de ℓ . Le théorème de Tate est prouvé.

2.2 Quelques corollaires

On garde les notations précédentes; k est un corps fini.

Corollaire 2.2.1 — *Soient A et B des variétés abéliennes sur k . Il y a équivalence entre :*

- B est isogène à une sous-variété abélienne de A ;
- $V_\ell(B)$ se plonge dans $V_\ell(A)$ comme $\mathbb{Q}_\ell[G]$ -module;
- le polynôme caractéristique de π_B divise celui de π_A .

En particulier, le polynôme caractéristique du Frobenius d'une variété abélienne sur k détermine uniquement sa classe d'isogénie.

Démonstration — L'équivalence des deux dernières conditions est une conséquence du fait que l'action du Frobenius sur le module de Tate est semi-simple. La seule chose à montrer est que s'il existe une injection $\mathbb{Q}_\ell[G]$ -linéaire $F: V_\ell(B) \rightarrow V_\ell(A)$, B est isogène à une sous-variété abélienne de A . D'après le théorème de Tate, il existe $f: B \rightarrow A$ tel que $V_\ell(f)$ soit arbitrairement proche de F (topologie ℓ -adique). Si $V_\ell(f)$ est suffisamment proche de F , $V_\ell(f)$ sera injectif lui aussi (il faut vérifier la non annulation d'un certain nombre de mineurs), ce qui implique que la restriction de f à son image est une isogénie. \square

Soit A une variété abélienne sur k . Notons $E = \text{End}_k^0(A)$ et $F = \mathbb{Q}[\pi_A]$. Le théorème de Tate affirme que $F \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ est le centre de $E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$; on en déduit que F est le centre de E .

Proposition 2.2.2 — *Supposons A simple. Alors E est un corps gauche de centre F . Soit v une place de F . Alors,*

$$\text{inv}_v(E) = \begin{cases} 1/2 & \text{si } v \text{ est réelle,} \\ \frac{\text{ord}_v(\pi_A)}{\text{ord}_v(q)} [F_v : \mathbb{Q}_p] & \text{si } v \mid p, \\ 0 & \text{sinon,} \end{cases}$$

où ord_v désigne la valuation normalisée associée à une place finie, et inv_v est la composée des flèches canoniques $\text{Br}(F) \rightarrow \text{Br}(F_v)$ et $\text{Br}(F_v) \rightarrow \mathbb{Q}/\mathbb{Z}$ (cette dernière étant un isomorphisme lorsque v est finie), et l'égalité suivante est vérifiée :

$$2 \dim A = [E : F]^{1/2} [F : \mathbb{Q}]$$

Démonstration — Le calcul de l'invariant en une place divisant p n'est pas un corollaire de ce qui précède; voir [9]. Le reste est facile et nous ne le détaillerons pas. \square

3 Rappels sur la multiplication complexe

Les références pour cette section sont [6] et [3]. Soient k un corps, M un corps de nombres et A une variété abélienne sur k . Notons $g = \dim A$. On dit que A est à *multiplication complexe* par M si l'on s'est donné une flèche $i: \mathcal{O}_M \rightarrow \text{End}_k(A)$ et que $[M: \mathbb{Q}] = 2g$.

Proposition 3.0.3 — *Soit (A, i) une variété abélienne sur k à multiplication complexe par M . Alors :*

1. M est totalement imaginaire,
2. M est égal à son commutant dans $\text{End}_k^0(A)$,
3. A est isogène à B^d où B est une variété abélienne simple sur k et $d \in \mathbb{N}$.

Démonstration — Fixons ℓ premier différent de la caractéristique de k , et une clôture algébrique $\overline{\mathbb{Q}_\ell}$ de \mathbb{Q}_ℓ . Nous allons utiliser un lemme d'approximation bien connu.

Lemme 3.0.4 — *Soit K un corps. Soient $|\cdot|_1, \dots, |\cdot|_n$ des valeurs absolues sur K deux à deux non équivalentes, avec $n \in \mathbb{N}^*$. On munit K^n de la topologie produit des topologies déduites des $|\cdot|_i$. Alors, l'image de l'application diagonale $K \rightarrow K^n$ est dense dans K^n .*

Supposons que M possède une place réelle v . D'après le lemme, il existe $x \in M$ tel que x soit arbitrairement proche de 1 en toute place archimédienne de M autre que v , et tel que x soit négatif de valeur absolue arbitrairement grande, en v . Ainsi, on peut choisir $x \in \mathcal{O}_M$ de sorte que $N_{M/\mathbb{Q}}(x) < 0$. Par ailleurs, $N_{M/\mathbb{Q}}(x)$ est le coefficient constant du polynôme caractéristique de l'endomorphisme de $T_\ell(A)$ induit par x , du fait que M est de degré $2g$, et c'est donc aussi le degré de l'endomorphisme de A induit par x , qui est un entier positif : contradiction.

Pour montrer la seconde assertion, il suffit de voir que $M \otimes_{\mathbb{Q}} \overline{\mathbb{Q}_\ell}$ est égal à son commutant dans $\text{End}_{\overline{\mathbb{Q}_\ell}}(V_\ell(A) \otimes_{\mathbb{Q}_\ell} \overline{\mathbb{Q}_\ell})$, puisque $\text{End}_k(A) \otimes_{\mathbb{Z}} \overline{\mathbb{Q}_\ell} \rightarrow \text{End}_{\overline{\mathbb{Q}_\ell}}(V_\ell(A) \otimes_{\mathbb{Q}_\ell} \overline{\mathbb{Q}_\ell})$ est une injection. Soit x dans M tel que $M = \mathbb{Q}(x)$; comme x est de degré la dimension de $V_\ell(A)$, l'endomorphisme de $V_\ell(A) \otimes_{\mathbb{Q}_\ell} \overline{\mathbb{Q}_\ell}$ qu'il induit est diagonalisable et ses valeurs propres sont toutes distinctes, d'où le résultat (une matrice D diagonale à coefficients diagonaux deux à deux distincts ne commute qu'avec les matrices diagonales, qui sont toutes des polynômes en D).

La troisième assertion n'est pas plus difficile à démontrer mais elle ne nous servira pas. Voir [6], p. 36. \square

Rappelons maintenant la notion de type de multiplication complexe (en abrégé, type CM). Soit A une variété abélienne sur \mathbb{C} de dimension g , à multiplication complexe par M (cela sous-entend que M est de degré $2g$, d'après notre définition). Il existe un réseau $\Lambda \subset \mathbb{C}^g$ et un isomorphisme de groupes analytiques $A \approx \mathbb{C}^g/\Lambda$. Cet isomorphisme détermine alors de deux flèches naturelles $\text{End}_{\mathbb{C}}(A) \rightarrow \mathcal{M}_g(\mathbb{C})$ (passage à l'application tangente en 0) et $\text{End}_{\mathbb{C}}(A) \rightarrow \mathcal{M}_{2g}(\mathbb{Z})$ (endomorphisme induit sur Λ), quitte à choisir une \mathbb{Z} -base de Λ (ce choix est inutile mais facilite l'exposition). On en déduit des flèches

$$\begin{aligned} \rho_{\mathbb{C}}: \text{End}_{\mathbb{C}}^0(A) &\longrightarrow \mathcal{M}_g(\mathbb{C}) \\ \rho_{\mathbb{Q}}: \text{End}_{\mathbb{C}}^0(A) &\longrightarrow \mathcal{M}_{2g}(\mathbb{C}) \end{aligned}$$

où $\rho_{\mathbb{Q}}$ se factorise par $\mathcal{M}_{2g}(\mathbb{Q}) \subset \mathcal{M}_{2g}(\mathbb{C})$. Ce sont respectivement la *représentation analytique* et la *représentation rationnelle*. Il est bien connu que $\rho_{\mathbb{Q}}$ est isomorphe à $\rho_{\mathbb{C}} \oplus \overline{\rho_{\mathbb{C}}}$. Notons $\varphi_1, \dots, \varphi_{2g}$ tous les plongements $M \rightarrow \mathbb{C}$, et $\rho_{\mathbb{Q}}|_M, \rho_{\mathbb{C}}|_M$ les représentations restreintes à M . En considérant un élément $x \in M$ de degré $2g$ sur \mathbb{Q} , et en remarquant que $\rho_{\mathbb{Q}}(x)$ est diagonalisable et que ses valeurs propres sont deux à deux distinctes, on voit tout de suite qu'il existe un isomorphisme de représentations

$$\rho_{\mathbb{Q}}|_M \approx \bigoplus_{1 \leq i \leq 2g} \varphi_i,$$

et que l'on a donc

$$\rho_{\mathbb{C}}|_M \approx \bigoplus_{i \in I} \varphi_i \quad ; \quad \overline{\rho_{\mathbb{C}}}|_M \approx \bigoplus_{i \notin I} \varphi_i$$

pour une certaine partie $I \subset \{1, \dots, 2g\}$ avec $\text{Card } I = g$. On dit alors que A est de type $(M, \{\varphi_i; i \in I\})$.

Définition 3.0.5 — On appelle type CM tout couple (M, Φ) où M est un corps de nombres et Φ un ensemble de plongements complexes $M \rightarrow \mathbb{C}$, tel qu'il existe une variété abélienne A sur \mathbb{C} de type (M, Φ) (i.e. $\dim A = [M : \mathbb{Q}]/2$, il existe $i : \mathcal{O}_M \rightarrow \text{End}_{\mathbb{C}}(A)$ et $\rho_{\mathbb{C}}|_M \approx \bigoplus_{\varphi \in \Phi} \varphi$).

Définition 3.0.6 — On appelle corps CM un corps de nombres totalement imaginaire, extension quadratique d'un corps de nombres totalement réel.

Théorème 3.0.7 — Soit M un corps de nombres de degré $2n$, où $n \in \mathbb{N}^*$, et Φ un ensemble de n plongements $M \rightarrow \mathbb{C}$. Alors (M, Φ) est un type CM si et seulement si M contient un corps CM K tel que pour tous $\varphi_1, \varphi_2 \in \Phi$, $\varphi_1|_K \neq \overline{\varphi_2}|_K$.

Démonstration — Ce théorème se trouve dans [6], chapitre II. Notons que seul le cas où M est un corps CM nous servira. \square

Si k est un sous-corps de \mathbb{C} , A une variété abélienne sur k , M un corps de nombres, et Φ un ensemble de plongements de M dans \mathbb{C} , on dira que A est de type (M, Φ) si A est à multiplication complexe par M et que $A \times_k \mathbb{C}$ est de type (M, Φ) . En d'autres termes, une variété abélienne sur k de type (M, Φ) est une variété abélienne sur \mathbb{C} de type (M, Φ) , définie sur k , et telle que les endomorphismes de A induits par les éléments de M soient eux aussi définis sur k .

Théorème 3.0.8 — Soit (M, Φ) un type CM et A une variété abélienne sur \mathbb{C} à multiplication complexe par M , de ce type. Alors A provient par extension des scalaires d'une variété abélienne de type (M, Φ) sur un corps de nombres.

Démonstration — C'est la proposition 1.1 du chapitre 5 de [3]. \square

Théorème 3.0.9 (décomposition du Frobenius en idéaux premiers) — Soient K un corps de nombres, (M, Φ) un type CM, A une variété abélienne sur K de type (M, Φ) . On suppose que K contient une clôture galoisienne de M , et l'on convient donc que les $\varphi \in \Phi$ sont des plongements $\varphi : M \rightarrow K$. Soit \mathfrak{p} une place finie de K de bonne réduction pour A . Soit $\pi_0 \in M$ qui induise le Frobenius sur la réduction de A modulo \mathfrak{p} . Alors :

$$\pi_0 \mathcal{O}_F = \prod_{\varphi \in \Phi} \varphi^{-1}(\mathcal{N}_{K/\varphi(F)} \mathfrak{p})$$

Démonstration — Voir [6], chapitre III, théorème 13.1, ou [3], chapitre 3, théorème 3.3. \square

Théorème 3.0.10 (Serre, Tate, Néron, Ogg, Shafarevitch) — Soient K et M des corps de nombres. Soit A une variété abélienne sur K , à multiplication complexe par M . Alors A a potentiellement bonne réduction partout (autrement dit, après une extension finie des scalaires, A a bonne réduction partout).

Démonstration — Ce théorème provient du critère de Néron-Ogg-Shafarevitch, qui est une conséquence de la théorie des modèles de Néron. Voir [5]. \square

4 Preuve du théorème de Honda-Tate

Il s'agit de prouver le théorème 1.0.2. Montrons d'abord l'injectivité de l'application considérée. Soient A et B deux variétés abéliennes simples sur k , non isogènes, dont les Frobenius sont des q -nombres de Weil conjugués. Soit $C = A \times_k B$. On a la décomposition $\text{End}_k^0(C) = \text{End}_k^0(A) \times \text{End}_k^0(B)$, puisque A et B ne sont pas isogènes. En passant aux centres, on obtient, d'après le théorème de Tate, $\mathbb{Q}[\pi_C] = \mathbb{Q}[\pi_A] \times \mathbb{Q}[\pi_B]$. Ceci signifie que la \mathbb{Q} -algèbre $\mathbb{Q}[\pi_A] \times \mathbb{Q}[\pi_B]$ est engendrée par (π_A, π_B) . En notant P le polynôme minimal de π_A sur \mathbb{Q} , qui est aussi celui de π_B , on en déduit que la \mathbb{Q} -algèbre $\mathbb{Q}[X]/(P) \times \mathbb{Q}[X]/(P)$ doit être engendrée par (X, X) , ce qui n'est pas ; π_A et π_B ne sont donc pas conjugués.

Reste à prouver l'existence d'une variété abélienne sur k de Frobenius donné. Soit π un q -nombre de Weil. On pose $F = \mathbb{Q}(\pi)$. Soit E le corps gauche de centre F dont les invariants aux places v de F sont

$$\text{inv}_v(E) = \begin{cases} 1/2 & \text{si } v \text{ est réelle,} \\ \frac{\text{ord}_v(\pi)}{\text{ord}_v(q)} [F_v : \mathbb{Q}_p] & \text{si } v \mid p, \\ 0 & \text{sinon,} \end{cases}$$

(La nullité dans \mathbb{Q}/\mathbb{Z} de la somme de ces quantités provient de la formule du produit pour le corps F .)

Lemme 4.0.11 — *Il existe un corps CM L contenant F qui décompose E , c'est-à-dire tel que $L \otimes_F E$ soit L -isomorphe à $\mathcal{M}_n(L)$ pour un $n \in \mathbb{N}$.*

Démonstration — Ce lemme est élémentaire. Voir [7] pour la démonstration. \square

Fixons une clôture algébrique $\overline{\mathbb{Q}_p}$ de \mathbb{Q}_p et un isomorphisme $\overline{\mathbb{Q}_p} \approx \mathbb{C}$. Nous allons introduire une notation. Soit $\Phi \subset \text{Hom}_{\mathbb{Q}}(L, \mathbb{C})$. Si w est une place de L divisant p , on dispose d'une application injective

$$\text{Hom}_{\mathbb{Q}_p}(L_w, \overline{\mathbb{Q}_p}) \longrightarrow \text{Hom}_{\mathbb{Q}}(L, \overline{\mathbb{Q}_p}) = \text{Hom}_{\mathbb{Q}}(L, \mathbb{C}),$$

c'est la composition par $L \rightarrow L_w$. Notons H_w son image, et $\Phi_w = \Phi \cap H_w$. Si $\varphi \in \Phi$, $\varphi: L \rightarrow \mathbb{C} \approx \overline{\mathbb{Q}_p}$ induit un \mathbb{Q}_p -morphisme $\prod_{w \mid p} L_w \approx L \otimes_{\mathbb{Q}} \mathbb{Q}_p \rightarrow \overline{\mathbb{Q}_p}$, d'où un plongement $L_w \rightarrow \overline{\mathbb{Q}_p}$ pour une certaine place w divisant p . On a alors $\varphi \in \Phi_w$. Il est maintenant clair que les Φ_w forment une partition de Φ .

Lemme 4.0.12 — *Il existe $\Phi \subset \text{Hom}_{\mathbb{Q}}(L, \mathbb{C})$ tel que, pour toute place w de L divisant p ,*

$$\frac{\text{ord}_w(\pi)}{\text{ord}_w(q)} = \frac{\text{Card } \Phi_w}{\text{Card } H_w}$$

et tel que $\{\Phi, \overline{\Phi}\}$ forme une partition de $\text{Hom}_{\mathbb{Q}}(L, \mathbb{C})$.

Démonstration — Posons $n_w = \frac{\text{ord}_w(\pi)}{\text{ord}_w(q)} \text{Card } H_w$ pour w place de L divisant p . D'après l'expression de l'invariant local de E en la place de F en-dessous de w , on voit tout de suite que l'image de n_w dans \mathbb{Q}/\mathbb{Z} est $\text{inv}_w(L \otimes_F E)$, qui est nul puisque $L \otimes_F E$ est L -isomorphe à $\mathcal{M}_n(L)$ pour un $n \in \mathbb{N}$. Ainsi, $n_w \in \mathbb{Z}$, et donc évidemment $n_w \in \mathbb{N}$. Si w est une place de L divisant p , correspondant à un idéal maximal \mathfrak{m} de \mathcal{O}_L , on notera \overline{w} la place de L correspondant à l'idéal $\rho(\mathfrak{m})$, où ρ est l'unique automorphisme non trivial de L induisant l'identité sur son sous-corps totalement réel maximal. Pour chaque w telle que $\overline{w} = w$, on choisit une partie $\Phi_w \subset H_w$ telle que $\Phi_w \cup \overline{\Phi_w} = H_w$ et $\Phi_w \cap \overline{\Phi_w} = \emptyset$. Ensuite, on choisit un w tel que Φ_w n'ait pas encore été défini, puis on choisit une partie de H_w de cardinal n_w , que l'on note Φ_w ; on pose alors $\overline{\Phi_w} = H_w \setminus \Phi_w$ (par hypothèse on a $w \neq \overline{w}$). On recommence, de manière à définir Φ_w pour toute place w de L divisant p . On vérifie tout de suite que les Φ_w conviennent, i.e. vérifient $n_w = \text{Card } \Phi_w$, à l'aide de la relation $n_w + n_{\overline{w}} = \text{Card } H_w$. \square

Comme L est un corps CM et $\{\Phi, \overline{\Phi}\}$ est une partition de $\text{Hom}_{\mathbb{Q}}(L, \mathbb{C})$, le couple (L, Φ) est un type CM (d'après le théorème 3.0.7). Il existe donc une variété abélienne A sur \mathbb{C} de type (L, Φ) . D'après le théorème 3.0.8, on peut supposer que (A, i) est définie sur un corps de nombres K . D'après le théorème 3.0.10, quitte à agrandir le corps K , on peut supposer que A a bonne réduction partout. Enfin, on peut supposer que K contient une clôture galoisienne de L . Choisissons une place finie \mathfrak{p} de K divisant p . Notons A_0 la réduction de A modulo \mathfrak{p} , k_0 le corps résiduel de K en \mathfrak{p} et q_0 le cardinal de k_0 . On a une flèche $\mathcal{O}_L \rightarrow \text{End}_K(A) \rightarrow \text{End}_{k_0}(A_0)$; comme A_0 et A ont même dimension, A_0 est naturellement à multiplication complexe par L . On a vu que cela implique que L est égal à son commutant dans $\text{End}_{k_0}(A_0)$; en particulier, il existe un $\pi_0 \in L$ qui induise le Frobenius sur A_0 . On peut maintenant appliquer le théorème de décomposition du Frobenius en idéaux premiers; il affirme, dans une formulation légèrement différente, que l'on a, pour toute place w de L divisant p ,

$$\frac{\text{ord}_w(\pi_0)}{\text{ord}_w(q_0)} = \frac{\text{Card } \Phi_w}{\text{Card } H_w}.$$

Ainsi, pour $w \mid p$,

$$\frac{\text{ord}_w(\pi_0)}{\text{ord}_w(q_0)} = \frac{\text{ord}_w(\pi)}{\text{ord}_w(q)}.$$

Quitte à remplacer (K, \mathfrak{p}) par (K', \mathfrak{p}') où K' est une extension de K non ramifiée en \mathfrak{p}' , de degré résiduel N_0 en \mathfrak{p}' et où \mathfrak{p}' est au-dessus de \mathfrak{p} , on peut remplacer q_0 par $q_0^{N_0}$ et π_0 par $\pi_0^{N_0}$, de sorte que l'on peut supposer qu'il existe un entier $N \in \mathbb{N}^*$ tel que $q_0 = q^N$. On a alors $|\pi_0/\pi^N|_w = 1$ pour toute place w de L divisant p . De plus, pour toute place finie w de L ne divisant pas p , on a aussi $|\pi_0/\pi^N|_w = 1$ puisque π et π_0 divisent des puissances de p (en effet, $\pi\bar{\pi} = q$). Enfin, pour toute place archimédienne w de L , $|\pi_0/\pi^N|_w = 1$ puisque $|\pi_0|_w = q_0^{1/2}$ et $|\pi^N|_w = q^{N/2}$. Ainsi, π_0/π^N est de valeur absolue 1 en toute place de L ; on en déduit que c'est une racine de l'unité (en effet, la condition sur les places finies implique que le polynôme minimal de cet élément est à coefficients entiers, et l'on sait que les racines d'un polynôme unitaire de $\mathbb{Z}[X]$ dont toutes les racines sont de module 1 sont des racines de l'unité). Quitte à remplacer encore π_0 par une puissance, et N par un multiple, on peut donc supposer que $\pi_0 = \pi^N$. Le théorème sera donc montré si l'on prouve le lemme suivant.

Lemme 4.0.13 — *Soit $j \in \mathbb{N}^*$ tel que π^j soit conjugué au Frobenius d'une variété abélienne simple A sur k_j , où k_j est l'extension de k de degré j contenue dans \bar{k} . Alors π est conjugué au Frobenius d'une variété abélienne simple sur k .*

Démonstration — Soit A' la variété abélienne sur k obtenue par restriction des scalaires à la Weil de k_j à k à partir de A (voir par exemple [1] pour une introduction à la restriction des scalaires à la Weil). Les k -morphisms $\text{Spec } \bar{k} \rightarrow A'$ correspondent bijectivement aux k_j -morphisms $\text{Spec } (\bar{k} \otimes_k k_j) \rightarrow A$, qui correspondent bijectivement aux j -uplets de k_j -morphisms $\text{Spec } k_j \rightarrow A$. Ainsi, $V_\ell(A')$ est canoniquement isomorphe à $V_\ell(A)^j$ comme $\mathbb{Q}_\ell[\text{Gal}(\bar{k}/k_j)]$ -module, et l'action du Frobenius relatif à k sur $V_\ell(A')$ se traduit par une permutation d'ordre j sur les facteurs de $V_\ell(A)^j$. Dans de bonnes bases de $V_\ell(A')$ et de $V_\ell(A)$, si l'on note M la matrice de π_A agissant sur $V_\ell(A)$ et M' la matrice de $\pi_{A'}$ agissant sur $V_\ell(A')$, on a :

$$M' = \begin{pmatrix} 0 & \cdots & \cdots & 0 & M \\ M & 0 & & \vdots & 0 \\ & M & \ddots & \vdots & \\ & & \ddots & 0 & \\ 0 & & & M & 0 \end{pmatrix}$$

Par conséquent, M'^j est diagonale par blocs, de blocs diagonaux M^j , ce qui montre que $\chi_{M'^j} = (\chi_{M^j})^j$ (les χ désignent les polynômes caractéristiques). On vérifie facilement que si λ est une valeur propre de M' et ζ une racine j -ème de l'unité, alors $\lambda\zeta$ est encore une valeur propre de M' . Ainsi, on a même $\chi_{M'} = \chi_M(X^j)$. En particulier, π est une racine du polynôme caractéristique de $\pi_{A'}$; il est donc conjugué au Frobenius d'un facteur simple de A . \square

Bibliographie

- [1] BOSCH, S., LÜTKEBOHMERT, W., RAYNAUD, M., Néron models, *Ergebnisse der Mathematik und ihrer Grenzgebiete (3)*, 21, Springer-Verlag, Berlin, 1990.
- [2] HONDA, T., Isogeny classes of abelian varieties over finite fields, *J. Math. Soc. Japan* **20** (1968), 83–95.
- [3] LANG, S., Complex multiplication, *Grundlehren der Mathematischen Wissenschaften*, 255, Springer-Verlag, New York, 1983.
- [4] MILNE, J. S., Abelian varieties, *Arithmetic geometry (Storrs, Conn., 1984)*, 103–150, Springer, New York, 1986.
- [5] SERRE, J.-P., TATE, J., Good reduction of abelian varieties, *Ann. of Math. (2)* **88** (1968) 492–517.

- [6] SHIMURA, G., Abelian varieties with complex multiplication and modular functions, *Princeton Mathematical Series*, 46, Princeton University Press, Princeton, NJ, 1998.
- [7] TATE, J., Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda), *Sém. Bourbaki*, 1968/69, exposé 352.
- [8] TATE, J., Endomorphisms of abelian varieties over finite fields, *Inv. Math.* **2** (1966), 134.
- [9] WATERHOUSE, W. C., MILNE, J. S., Abelian varieties over finite fields, *1969 Number Theory Institute (Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, N.Y., 1969)*, 53–64, Amer. Math. Soc., Providence, R.I., 1971.