POINTS DES VARIÉTÉS DE SHIMURA SUR LES CORPS FINIS

Table des matières

Le but de ce chapitre est de donner les outils qui permettent d'étudier, et notamment de dénombrer l'ensemble des points d'une variété de Shimura de type PEL sur un corps fini. L'idée est basique : (1) on regroupe les points en classes d'isogénies, puis (2) on étudie séparément chaque classe d'isogénie.

Première partie 1. **La théorie de Honda-Tate**

Soit k un corps parfait. On a vu précédemment que la catégorie $\mathbf{Ab}_k^0$ des variétés abéliennes sur k à isogénie près est abélienne semi-simple, et que les algèbres d'endomorphismes y sont des $\mathbb{Q}$-algèbres semi-simples de dimension finie. On a donc

$$\mathbf{Ab}_k^0 \simeq \oplus_{[A]\in\mathcal{S}(k)}\mathbf{Mod}_{\mathrm{End}_k^0(A)}$$

où la somme porte sur l'ensemble $\mathcal{S}(k)$ des classes d'isogénies de variétés abéliennes simples sur k, et où $\mathrm{Mod}_{\mathrm{End}_k^0(A)}$ est la catégorie des modules à gauche sur le corps gauche $\mathrm{End}_k^0(A) \overset{\text{déf}}{=} \mathrm{End}_k(A)\otimes\mathbb{Q}$. Lorsque $k=\mathbb{F}_q$ est un corps fini, la théorie de Honda-Tate achève de décrire complètement cette catégorie, en ce sens qu'elle donne une description explicite de l'ensemble $\mathcal{S}(q) \overset{\text{déf}}{=} \mathcal{S}(k)$ et une recette pour déterminer le corps gauche $\mathrm{End}_k^0(A)$ pour toute variété abélienne k-simple A.

1. Le Frobenius

1.1. **Rappels sur les polynômes caractéristiques.** Soit A une variété abélienne sur un corps parfait k. Nous avons vu que la fonction

$$\deg : \mathrm{End}_k(A)\to\mathbb{Z}, \qquad \alpha\mapsto\deg(\alpha)$$

est polynomiale, multiplicative et homogène de degré $2\dim A$. Pour tout anneau commutatif R, on obtient donc une fonction

$$\deg_R : \mathrm{End}_k(A)\otimes R\to R.$$

Definition 1. Le polynôme caractéristique de $\alpha\in\mathrm{End}_k(A)\otimes R$ est

$$P_\alpha = \deg_{R[X]}\left(\alpha\otimes 1_{R[X]} - \mathrm{Id}_A\otimes X\right)\in R[X].$$

C'est donc un polynôme unitaire de degré $2\dim A$, dont la définition est calquée sur celle du polynôme caractéristique de l'endomorphisme d'un R-module libre de rang fini Λ, disons $\beta:\Lambda\to\Lambda$, pour lequel

$$P_\beta = \det_{R[X]}\left(\beta\otimes 1_{R[X]} - \mathrm{Id}_A\otimes X|\Lambda\otimes_R R[X]\right)\in R[X].$$

On sait qu'alors $P_\beta(\beta) = 0$ dans $\mathrm{End}_R(\Lambda)$: c'est le théorème de Cayley-Hamilton, auquel nous allons nous ramener pour établir la proposition suivante.

Proposition 2. *Pour tout $\alpha \in \mathrm{End}_k(A) \otimes R$,*

$$P_\alpha(\alpha) = 0 \quad \textit{dans } \mathrm{End}_k(A) \otimes R.$$

Puisque la formation de $P_\alpha(\alpha)$ commute aux changements de base $R \to R'$, on se ramène facilement pour prouver cette proposition, d'abord au cas où R est une algèbre de polynômes sur $\mathbb{Z}$, puis, en utilisant le fait que $\mathrm{End}_k(A)$ est un $\mathbb{Z}$-module libre, au cas où $R = \mathbb{Z}$, donc $\alpha \in \mathrm{End}_k(A)$. La proposition résulte alors aisément de l'un quelconque des trois énoncés que voici.

Proposition 3. *Soit $\alpha \in \mathrm{End}_k(A)$, P_α son polynôme caractéristique. Alors :*

(1) *Pour tout $k \hookrightarrow \mathbb{C}$, P_α est le polynôme caractéristique du morphisme induit par α sur le $\mathbb{Z}$-module libre $H_1(A(\mathbb{C}), \mathbb{Z})$.*

(2) *Pour tout nombre premier $\ell \neq \mathrm{car}(k)$, P_α est le polynôme caractéristique du morphisme induit par α sur le $\mathbb{Z}_\ell$-module libre $T_\ell(A, \overline{k})$.*

(3) *Pour $\mathrm{car}(k) = p > 0$, P_α est le polynôme caractéristique du morphisme induit par α sur le $W(k)$-module libre $\mathbb{D}(A)$.*

Tous ces polynômes prennent en effet les mêmes valeurs sur $\mathbb{Z}$:

Proposition 4. *Soit $\alpha \in \mathrm{End}_k(A)$.*

(1) *Pour tout $k \hookrightarrow \mathbb{C}$, $\deg(\alpha) = \det_{\mathbb{Z}}\left(\alpha | H_1\left(A(\mathbb{C}), \mathbb{Z}\right)\right)$.*

(2) *Pour tout nombre premier $\ell \neq \mathrm{car}(k)$, $\deg(\alpha) = \det_{\mathbb{Z}_\ell}\left(\alpha | T_\ell(A, \overline{k})\right)$.*

(3) *Pour $\mathrm{car}(k) = p > 0$, $\deg(\alpha) = \det_{W(k)}\left(\alpha | \mathbb{D}(A)\right)$.*

Posons $E = \mathrm{End}_k(A) \otimes K$ avec $K = \mathbb{Q}$, ou $K = \mathbb{Q}_\ell$, ou $K = \mathbb{Q}_p$ selon la formule

$$\left[E \xrightarrow{\deg} K\right] \quad \stackrel{?}{=} \quad \left[E \xrightarrow{\det} K\right]$$

que l'on souhaite démontrer. Ces deux fonctions sont polynomiales, multiplicatives, et homogènes de même rang $2\dim(A)$. Décomposons $E = \prod E_i$ en K-algèbres simples et notons $\mathrm{nr}_i : E_i \to K$ la norme réduite sur E_i. D'après [9, p. 179], il existe des constantes $a_i, b_i \in \mathbb{N}$ telles que pour tout $\alpha = (\alpha_i)$ dans $E = \prod E_i$,

$$\deg(\alpha) = \prod \mathrm{nr}_i(\alpha_i)^{a_i} \quad \text{et} \quad \det(\alpha) = \prod \mathrm{nr}_i(\alpha_i)^{b_i}.$$

Il suffit donc de vérifier que, notant $|-| : K \to \mathbb{R}_{\geq 0}$ la norme usuelle de K,

$$\left[E \xrightarrow{|\deg|} \mathbb{R}_{\geq 0}\right] \quad \stackrel{?}{=} \quad \left[E \xrightarrow{|\det|} \mathbb{R}_{\geq 0}\right].$$

Par homogénéité, il suffit même de tester cette égalité sur $\alpha \in \mathrm{End}_k(A)$. Si α n'est pas une isogénie, $|\deg(\alpha)| = 0 = |\det(\alpha)|$. Supposons donc que α est une isogénie et traitons séparément les différents cas.

1. Pour la première formule, $K = \mathbb{Q}$ et

$$\begin{array}{rcccl} |\deg(\alpha)| & = & +\deg(\alpha) & = & \text{cardinal de } \ker\left(A(\mathbb{C}) \xrightarrow{\alpha} A(\mathbb{C})\right), \\ |\det(\alpha)| & = & \pm\det(\alpha) & = & \text{cardinal de } \mathrm{coker}\left(H_1(A(\mathbb{C}), \mathbb{Z}) \xrightarrow{\alpha} H_1(A(\mathbb{C}), \mathbb{Z})\right). \end{array}$$

Mais si $A(\mathbb{C}) = \mathbb{C}^g/\Lambda$ pour un réseau $\Lambda \simeq \mathbb{Z}^{2g}$, alors $\Lambda \simeq H_1(A(\mathbb{C}), \mathbb{Z})$ et

$$\ker\left(A(\mathbb{C}) \xrightarrow{\alpha} A(\mathbb{C})\right) = \alpha^{-1}\Lambda/\Lambda \simeq \Lambda/\alpha\Lambda \simeq \operatorname{coker}\left(H_1(A(\mathbb{C}), \mathbb{Z}) \xrightarrow{\alpha} H_1(A(\mathbb{C}), \mathbb{Z})\right)$$

donc en effet $\deg(\alpha) = |\det(\alpha)|$.

2. Pour la seconde formule, $K = \mathbb{Q}_\ell$ avec $\ell \neq \operatorname{car}(k)$ et

$$\begin{aligned} |\deg(\alpha)|^{-1} &= \text{rang de } \ker(\alpha)[\ell^\infty] \\ &= \text{cardinal de } \ker\left(A(\overline{k})[\ell^\infty] \xrightarrow{\alpha} A(\overline{k})[\ell^\infty]\right), \\ |\det(\alpha)|^{-1} &= \text{cardinal de } \operatorname{coker}\left(T_\ell(A, \overline{k}) \xrightarrow{\alpha} T_\ell(A, \overline{k})\right). \end{aligned}$$

On conclut grâce au lemme suivant :

Lemma 5. *Si $\alpha : A \to B$ est une isogénie et $\ell \neq \operatorname{car}(k)$ un nombre premier, alors*

$$\operatorname{coker}\left(T_\ell(A, \overline{k}) \xrightarrow{\alpha} T_\ell(B, \overline{k})\right) \simeq \ker\left(A(\overline{k})[\ell^\infty] \xrightarrow{\alpha} B(\overline{k})[\ell^\infty]\right).$$

Démonstration. Soient $\mathcal{A} = A(\overline{k})[\ell^\infty]$, $\mathcal{B} = A(\overline{k})[\ell^\infty]$ et $X = \ker(\mathcal{A} \xrightarrow{\alpha} \mathcal{B})$. Alors

$$\left[T_\ell(A, \overline{k}) \xrightarrow{\alpha} T_\ell(B, \overline{k})\right] \simeq \left[\operatorname{Hom}_{\mathbb{Z}_\ell}(\mathbb{Q}_\ell/\mathbb{Z}_\ell, \mathcal{A}) \xrightarrow{\alpha} \operatorname{Hom}_{\mathbb{Z}_\ell}(\mathbb{Q}_\ell/\mathbb{Z}_\ell, \mathcal{B})\right]$$

Appliquant $\operatorname{Ext}^\bullet_{\mathbb{Z}_\ell}(\mathbb{Q}_\ell/\mathbb{Z}_\ell, -)$ à la suite exacte $0 \to X \to \mathcal{A} \to \mathcal{B} \to 0$, il vient

$$0 \to \operatorname{Hom}_{\mathbb{Z}_\ell}(\mathbb{Q}_\ell/\mathbb{Z}_\ell, \mathcal{A}) \xrightarrow{\alpha} \operatorname{Hom}_{\mathbb{Z}_\ell}(\mathbb{Q}_\ell/\mathbb{Z}_\ell, \mathcal{B}) \to \operatorname{Ext}^1_{\mathbb{Z}_\ell}(\mathbb{Q}_\ell/\mathbb{Z}_\ell, X) \to 0$$

car X est fini et $\mathcal{A}$ injectif (car divisible). Puisque aussi $\operatorname{Ext}^\bullet_{\mathbb{Z}_\ell}(\mathbb{Q}_\ell, X) = 0$,

$$\operatorname{Ext}^1_{\mathbb{Z}_\ell}(\mathbb{Q}_\ell/\mathbb{Z}_\ell, X) \simeq \operatorname{Hom}_{\mathbb{Z}_\ell}(\mathbb{Z}_\ell, X) \simeq X.$$

Donc $\operatorname{coker}\left(T_\ell(A, \overline{k}) \xrightarrow{\alpha} T_\ell(B, \overline{k})\right) \simeq X$, CQFD. □

3. Pour la troisième formule, $K = \mathbb{Q}_p$ et $|\det(\alpha)|^{-1} = p^{v_p(\det(\alpha))}$, avec

$$\begin{aligned} v_p(\det(\alpha)) &= \text{longueur du } W(k)\text{-module } \operatorname{coker}\left(\mathbb{D}(A[p^\infty]) \xrightarrow{\alpha} \mathbb{D}(A[p^\infty])\right) \\ &= \text{longueur du } W(k)\text{-module } \mathbb{D}(\ker\left(A[p^\infty] \xrightarrow{\alpha} A[p^\infty]\right) \\ &= \text{longueur du } W(k)\text{-module } \mathbb{D}(\ker(\alpha)[p^\infty]) \\ &= v_p(\deg(\alpha)) \end{aligned}$$

donc à nouveau $|\deg(\alpha)| = |\det(\alpha)|$.

1.2. **Compléments sur les polynômes caractéristiques.** On peut associer d'autres polynômes dans $\mathbb{Q}[X]$ à un élément α de $E = \operatorname{End}^0_k(A)$:

- $P_{\min,\alpha}$ le polynôme unitaire qui engendre $\{P \in \mathbb{Q}[X] : P(\alpha) = 0 \text{ dans } E\}$.
- $P_{\operatorname{car},\alpha}$ le polynôme caractéristique de α agissant sur E par multiplication à gauche (ou à droite),
- $P_{\operatorname{red},\alpha}$ définit par $P_{\operatorname{red},\alpha}(X) = \operatorname{nr}_{E/\mathbb{Q}}(\alpha - X)$ où $\operatorname{nr}_{E/\mathbb{Q}}$ est la norme réduite de $E/\mathbb{Q}$.

Proposition 6. *P_α, $P_{\min,\alpha}$, $P_{\operatorname{car},\alpha}$ et $P_{\operatorname{red},\alpha}$ ont les mêmes facteurs irréductibles.*

Démonstration. Décomposons $A \sim \oplus A_i^{m_i}$ en composantes isotypiques, donc aussi $E = \prod E_i$ en composantes simples, avec $E_i = M_{m_i}(D_i)$ où $D_i = \mathrm{End}_k^0(A_i)$ est un corps gauche, et $\alpha = (\alpha_i)$. On a alors

$$P_\alpha = \prod P_{\alpha_i}, \quad P_{\min,\alpha} = \mathrm{pgcd}(P_{\min,\alpha_i}), \quad P_{\mathrm{car},\alpha} = \prod P_{\mathrm{car},\alpha_i} \quad \text{et} \quad P_{\mathrm{red},\alpha} = \prod P_{\mathrm{red},\alpha_i}$$

ce qui nous ramène au cas isotypique, i.e. $A \sim A_0^m$ et $E = M_m(D)$ où D est un corps gauche de centre F. Puisque les applications $\deg \alpha$, $\det(\alpha|E)$ et $\mathrm{nr}_{E/\mathbb{Q}}(\alpha)$ sont polynomiales, multiplicatives et homogènes de degré respectivement égal à $2mg_0$, m^2d^2f et mdf où $g_0 = \dim A_0$, $d = [D : F]$ et $f = [F : \mathbb{Q}]$, on en déduit (comme dans la preuve de la proposition 4) que $df \mid 2g_0$ et

$$\deg = \mathrm{nr}_{E/\mathbb{Q}}^{2g_0/df} \quad \text{et} \quad \det(-|E) = \mathrm{nr}_{E/\mathbb{Q}}^{md}$$

donc aussi $P_\alpha = P_{\mathrm{red},\alpha}^{2g_0/df}$ et $P_{\mathrm{car},\alpha} = P_{\mathrm{red},\alpha}^{md}$. Il est enfin bien connu que $P_{\min,\alpha}$ et $P_{\mathrm{car},\alpha}$ ont les mêmes facteurs irréductibles. □

Remark 7. Si A est simple, $E = D$ est un corps, et tous les polynômes ci-dessus sont des puissances de $P_{\min,\alpha}$, qui est irréductible dans $\mathbb{Q}[X]$.

1.3. **Le polynôme caractéristique du Frobenius.** On suppose maintenant que A est une variété abélienne de dimension g sur un corps fini $k = \mathbb{F}_q$. On note $\pi_A \in \mathrm{End}_k(A)$ le Frobenius de A et $P_A \in \mathbb{Z}[X]$ son polynôme caractéristique. On sait déjà que c'est un polynôme unitaire de degré $2g$, de terme constant $q^g = \deg \pi_A$, tel que $P_A(\mathbb{Z}) \subset \mathbb{N}$ et $P_A(\pi_A) = 0$ dans $\mathrm{End}_k(A)$.

Theorem 8. *Si* $P_A(X) = \prod_{i=1}^{2g}(X - \alpha_i)$ *dans* $\overline{\mathbb{Q}}[X]$ *alors*

(1) $|A(\mathbb{F}_{q^n})| = \prod_{i=1}^{2g}(1 - \alpha_i^n)$ *pour tout* $n \geq 1$ *et*

(2) $|\alpha_i| = q^{\frac{1}{2}}$ *pour tout* $i = 1, \ldots, 2g$.

Démonstration. (de (1)) Pour tout $n \geq 1$, on a tout d'abord

$$|A(\mathbb{F}_{q^n})| \overset{(a)}{=} \left|\ker\left(\pi_A^n - \mathrm{Id}_A : A(\overline{\mathbb{F}}_q) \to A(\overline{\mathbb{F}}_q)\right)\right| \overset{(b)}{=} \deg(\pi_A^n - \mathrm{Id}_A) \overset{\text{déf}}{=} P_{\pi_A^n}(1)$$

car (a) π_A agit par Frob_k sur $A(\overline{\mathbb{F}}_q)$ et (b) π_A agit par 0 sur $\mathrm{Lie}A$, donc $\pi_A^n - \mathrm{Id}_A$ est une isogénie étale. D'autre part, choisissons un plongement de $\overline{\mathbb{Q}}$ dans $\mathbb{Q}_\ell$. D'après la proposition 3,

$$P_{\pi_A^n}(X) = \det_{\mathbb{Q}_\ell}\left(\pi_A^n - X \cdot \mathrm{Id}|V_\ell(A, \overline{\mathbb{F}}_q)\right) = \prod_{i=1}^{2g}(X - \alpha_i^n)$$

dans $\overline{\mathbb{Q}}_\ell[X]$, donc aussi dans $\overline{\mathbb{Q}}[X]$, et $|A(\mathbb{F}_{q^n})| = P_{\pi_A^n}(1) = \prod_{i=1}^{2g}(1 - \alpha_i^n)$. □

Example 9. Si A est une courbe elliptique, $g = 1$, et

$$P_A = (X - \alpha_1)(X - \alpha_2) = X^2 - a_q X + q$$

avec $a_q = \alpha_1 + \alpha_2 \in \mathbb{Z}$. La partie déjà démontrée du théorème nous dit que

$$a_q = 1 + q - P_A(1) = \left|\mathbf{P}^1(\mathbb{F}_q)\right| - |A(\mathbb{F}_q)|\,.$$

D'autre part, pour tout $n, d \in \mathbb{Z}$ avec $d \neq 0$,

$$P_A\left(\tfrac{n}{d}\right) = \deg\left(\pi_A - \tfrac{n}{d}\right) = \tfrac{1}{d^2}\deg\left(d\pi_A - n\right) \geqq 0$$

donc le discriminant $\Delta_A = a_q^2 - 4q$ de P_A est inférieur ou égal à 0 :

$$|\alpha_1 + \alpha_2| = |a_q| = \left|\left|\mathbf{P}^1(\mathbb{F}_q)\right| - |A(\mathbb{F}_q)|\right| \leq 2\sqrt{q}$$

Appliquant cette inégalité à A sur $\mathbb{F}_{q^n}$, on obtient

$$|\alpha_1^n + \alpha_2^n| \leq 2q^{n/2}$$

d'où l'on déduit facilement que $|\alpha_1| = |\alpha_2| = q^{1/2}$, ce qui démontre la deuxième partie du théorème lorsque $g = 1$.

Pour le cas général où $g = \dim A > 1$, nous avons besoin du lemme suivant.

Lemma 10. *Soit* $\dagger$ *une involution de Rosati sur* $\mathrm{End}_k^0(A)$. *Alors* $\pi_A^\dagger \circ \pi_A = q$.

Démonstration. Soit $\mathcal{L}$ un faisceau inversible ample sur A, donnant une polarisation $\lambda : A \to A^t$ qui induit $\dagger$ sur $\mathrm{End}_k^0(A)$. Posant $\pi = \pi_A$, on doit montrer que $q = \pi^\dagger \circ \pi = \lambda^{-1} \circ \pi^t \circ \lambda \circ \pi$, ou encore que

$$\left[A \xrightarrow{q\lambda} A^t\right] \quad = \quad \left[A \xrightarrow{\pi} A \xrightarrow{\lambda} A^t \xrightarrow{\pi^t} A^t\right]$$

Soit donc $a \in A$, de sorte que $\lambda(a) = \mathcal{T}_a^*\mathcal{L} \otimes \mathcal{L}^{-1}$ dans $A^t = \mathrm{Pic}^0_{A/k}$ et

$$\pi^t \circ \lambda \circ \pi(a) = [\pi]^*(\mathcal{T}_{\pi(a)}^*\mathcal{L} \otimes \mathcal{L}^{-1}) = \pi^*\mathcal{T}_{\pi(a)}^*\mathcal{L} \otimes \pi^*\mathcal{L}^{-1} = \mathcal{T}_a^*\pi^*\mathcal{L} \otimes \pi^*\mathcal{L}^{-1}.$$

Mais dans $\mathrm{Pic}A$, $\pi^*\mathcal{L} = \mathcal{L}^q$ (exercice!), donc

$$\pi^t \circ \lambda \circ \pi(a) = \mathcal{T}_a^*\mathcal{L}^q \otimes \mathcal{L}^{-q} = (\mathcal{T}_a^*\mathcal{L} \otimes \mathcal{L}^{-1})^q = q\lambda(a),$$

ce qu'il fallait démontrer. □

Montrons maintenant la deuxième partie du théorème.

Démonstration. (de (2)) Soit $\mathbb{Q}[\pi]$ la sous-algèbre engendrée par $\pi = \pi_A$ dans $E = \mathrm{End}_k^0(A)$. C'est une sous-algèbre centrale, puisque π commute avec tous les morphismes de k-schémas, qui est donc réduite, puisque le centre de E est un produit de corps, et qui est donc elle-même un produit de corps. Puisque aussi

$$P_A(\pi) = 0 \quad \text{avec} \quad P_A(0) = \deg(\pi) = q^g \neq 0,$$

le Frobenius π est inversible dans $\mathbb{Q}[\pi]$, et puisque $\pi^\dagger\pi = q$ dans E, $\pi^\dagger = q\pi^{-1}$ est également dans $\mathbb{Q}[\pi]$, qui est donc stable sous l'involution $\dagger$ de E. Admettons le résultat suivant, que l'on a démontré sur $\mathbb{C}$ mais qui reste vrai sur tous les corps. Une preuve basée sur la théorie de l'intersection est dans [9, §21] :

Proposition 11. *L'involution de Rosati* $\dagger$ *est positive, i.e.*

$$\forall 0 \neq x \in E, \qquad \mathrm{tr}(x^\dagger x) > 0.$$

La restriction de cette involution à $\mathbb{Q}[\pi]$ est encore positive, et $\mathbb{Q}[\pi]$ est finalement un produit de corps totalement réels (où $\dagger$ est trivial) et de corps CM (où $\dagger$ est l'involution canonique). Pour tout morphisme de $\mathbb{Q}$-algèbres $\phi : E \to \mathbb{C}$, on a donc

$$q = \phi(q) = \phi(\pi \cdot \pi^\dagger) = \phi(\pi) \cdot \overline{\phi}(\pi), \quad \text{donc } |\phi(\pi)| = q^{1/2}.$$

Mais les $\phi(\pi)$ sont exactement les racines du polynôme minimal $P_{\min,\pi}$ de π, i.e. d'après la proposition 6, les racines du polynôme $P_\pi = P_A$. Les racines de P_A dans $\mathbb{C}$ ont donc toutes la même valeur absolue $q^{1/2}$, ce qu'il fallait démontrer. □

1.4. **La conjecture de Weil pour les variétés abéliennes.** On peut maintenant déterminer la fonction zêta de $A/\mathbb{F}_q$,

$$Z(A,t) = \exp\left(\sum_{n\geq 1} |A(\mathbb{F}_{q^n})|\,\frac{t^n}{n}\right) \in \mathbb{Q}[[t]].$$

En effet, le théorème 8 nous dit que $|A(\mathbb{F}_{q^n})| = F(\alpha_1^n,\ldots,\alpha_{2g}^n)$ où

$$F(X_1,\cdots,X_{2g}) = (1-X_1)\cdots(1-X_{2g}) = \sum_{J\subset\{1,\ldots,2g\}} (-1)^{|J|}\textstyle\prod_{j\in J} X_j.$$

Un petit calcul dans $\mathbb{C}[[t]]$ montre alors que

$$\begin{aligned} Z(A,t) &= \prod_{J\subset\{1,\ldots,2g\}} \left(1-\left(\textstyle\prod_{j\in J}\alpha_j\right)\cdot t\right)^{-(-1)^{|J|}} \\ &= \frac{P_1(t)P_3(t)\cdots P_{2g-1}(t)}{P_0(t)P_2(t)\cdots P_{2g}(t)} \end{aligned}$$

avec $P_0(t) = (1-t)$, $P_{2g}(t) = (1-q^g t)$ et plus généralement

$$\forall j\in\{0,\ldots,2g\}: \qquad P_j(t) = \prod_{J\subset\{1,\cdots,2g\},|J|=j} \left(1-\left(\textstyle\prod_{j\in J}\alpha_j\right)\cdot t\right).$$

On voit donc que $Z(A,t) = \prod_{j=0}^{2g} P_j(t)^{-(-1)^j}$ est dans $\mathbb{Q}(t)$, pour des polynômes $P_j(t)$ dans $\mathbb{Z}[t]$ dont toutes les racines dans $\mathbb{C}$ sont les inverses d'entiers algébriques de modules $q^{j/2}$ (des q-nombres de Weil de poids $-j$), et que $Z(A,t) = Z(A,\frac{1}{q^g t})$.

La conjecture de Weil, démontrée par Deligne [1], étend ces propriétés aux fonctions zêta de toutes les variétés propres et lisses sur $k = \mathbb{F}_q$.

1.5. **Les q-nombres de Weil.**

Definition 12. Un q-nombre de Weil (de poids -1) est un entier algébrique $\pi\in\overline{\mathbb{Q}}$ tel que pour tout plongement $\phi:\mathbb{Q}(\pi)\hookrightarrow\mathbb{C}$, $|\phi(\pi)| = q^{1/2}$. On note $\mathcal{W}(q)$ l'ensemble des q-nombres de Weil.

Si A est une variété abélienne sur $k=\mathbb{F}_q$, π_A son Frobenius et P_A le polynôme caractéristique de π_A, toutes les racines de P_A dans $\overline{\mathbb{Q}}$ sont des q-nombres de Weil d'après le théorème 8 ci-dessus. Si A est simple, $\mathbb{Q}(\pi_A)$ est un corps et P_A est une puissance du polynôme minimal de π_A, qui est irréductible sur $\mathbb{Q}$. Toutes les racines de P_A dans $\overline{\mathbb{Q}}$ sont alors conjuguées sous $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Puisque enfin deux variétés isogènes définissent le même polynôme caractéristique, on obtient une application

$$w:\mathcal{S}(q)\to \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})\backslash\mathcal{W}(q)$$

où $\mathcal{S}(q)$ est l'ensemble des classes d'isogénies de variétés abéliennes simples sur k.

2. Le théorème de Tate ($\ell\neq p$) & Milne-Waterhouse ($\ell = p$)

2.1. **Les énoncés.** Soit k un corps, ℓ un nombre premier. On montre facilement que le foncteur $\mathbf{Ab}_k\otimes\mathbb{Z}_\ell\to\mathbf{BT}_k^\ell$ induit par $A\mapsto A[\ell^\infty]$ est fidèle. Plus précisément :

Lemma 13. *Soient A et B deux variétés abéliennes sur k. Le morphisme*

$$\rho_\ell : \mathrm{Hom}_k(A,B)\otimes\mathbb{Z}_\ell\to\mathrm{Hom}_k(A[\ell^\infty],B[\ell^\infty])$$

est injectif, et son conoyau est sans torsion.

Démonstration. Soit $\alpha_1, \cdots, \alpha_r$ une base du $\mathbb{Z}$-module libre de rang fini $\mathrm{Hom}_k(A,B)$. Considérons d'abord des éléments $\lambda_1, \cdots, \lambda_r$ de $\mathbb{Z}_\ell$ tels que

$$\lambda_1 \rho_\ell(\alpha_1) + \cdots + \lambda_r \rho_\ell(\alpha_r) = 0 \quad \text{dans } \mathrm{Hom}_k\left(A[\ell^\infty], B[\ell^\infty]\right).$$

Pour tout entier $s > 0$, choisissons des entiers $\lambda_{i,s} \in \mathbb{Z}$ tels que

$$\forall i \in \{0, \cdots, r\} \quad \lambda_{i,s} \equiv \lambda_i \quad \text{dans } \mathbb{Z}/\ell^s\mathbb{Z} = \mathbb{Z}_\ell/\ell^s\mathbb{Z}_\ell$$

et posons $f_s = \lambda_{1,s}\alpha_1 + \cdots + \lambda_{r,s}\alpha_r \in \mathrm{Hom}_k(A,B)$. Puisque

$$\rho_\ell(f_s) = (\lambda_{1,s} - \lambda_1)\rho_\ell(\alpha_1) + \cdots + (\lambda_{r,s} - \lambda_r)\rho_\ell(\alpha_r)$$

est divisible par ℓ^s dans $\mathrm{Hom}_k\left(A[\ell^\infty], B[\ell^\infty]\right)$, on voit que $f_s = 0$ sur $A[\ell^s]$. Mais alors f_s est divisible par ℓ^s dans $\mathrm{Hom}_k(A,B)$, donc $\lambda_i \equiv \lambda_{i,s} \equiv 0 \bmod \ell^s$ pour tout i et tout $s > 0$, donc $\lambda_i = 0$ pour tout i. L'application ρ_ℓ est donc injective.

Soit ensuite f un élément de $\mathrm{Hom}_k\left(A[\ell^\infty], B[\ell^\infty]\right)$ pour lequel il existe $s > 0$ et f' dans $\mathrm{Hom}_k\left(A,B\right) \otimes \mathbb{Z}_\ell$ tel que $\ell^s f = \rho_\ell(f')$. Choisissons f'' dans $\mathrm{Hom}_k\left(A,B\right)$ avec $f'' \equiv f' \bmod \ell^s$. Alors $\rho_\ell(f'') = 0 \bmod \ell^s$, d'où l'on déduit comme précédemment que $f'' \equiv 0 \bmod \ell^s$, donc aussi $f' \equiv 0 \bmod \ell^s$, i.e. $f' = \ell^s g$ pour un élément g de $\mathrm{Hom}_k\left(A,B\right) \otimes \mathbb{Z}_\ell$. Mais alors $\ell^s f = \rho_\ell(f') = \ell^s \rho_\ell(g)$, donc $f = \rho_\ell(g)$ car $\mathrm{Hom}_k\left(A[\ell^\infty], B[\ell^\infty]\right)$ est sans torsion. Le conoyau de ρ_ℓ est donc sans torsion. □

Le foncteur $\mathbf{Ab}_k \otimes \mathbb{Z}_\ell \to \mathbf{BT}_k^\ell$ n'est en revanche pas toujours plein, comme on voit par exemple en prenant $k = \mathbb{C}$. C'est néanmoins le cas lorsque

(1) k est un corps de nombres, d'après Faltings [3], ou lorsque

(2) k est un corps de type fini sur $\mathbb{F}_p$, d'après de Jong [2].

Pour un corps fini k, c'est un théorème énoncé pour tout ℓ et démontré pour $\ell \neq p$ par Tate dans [11], et démontré pour $\ell = p$ par Milne et Waterhouse dans [8] :

Theorem 14. *Soient A et B deux variétés abéliennes sur un corps fini k. Alors*

$$\rho_\ell : \mathrm{Hom}_k\left(A,B\right) \otimes \mathbb{Z}_\ell \xrightarrow{\simeq} \mathrm{Hom}_k\left(A[\ell^\infty], B[\ell^\infty]\right).$$

Compte-tenu des équivalences de catégories ***, on peut reformuler ce théorème de la manière suivante, plus utile pour les applications que l'on a en vue.

Theorem 15. *Soient k un corps fini de caractéristique p, $\ell \neq p$ un nombre premier, A et B deux variétés abéliennes sur k. Alors*

$$\begin{array}{rrcl} \rho_\ell : & \mathrm{Hom}_k(A,B) \otimes \mathbb{Z}_\ell & \to & \mathrm{Hom}_{\mathbb{Z}_\ell[\mathrm{Gal}_k]}\left(T_\ell(A), T_\ell(B)\right) \\ \textit{et} \quad \rho_p : & \mathrm{Hom}_k(A,B) \otimes \mathbb{Z}_p & \to & \mathrm{Hom}_{W(k)[F,V]}\left(\mathbb{D}(B), \mathbb{D}(A)\right) \end{array}$$

sont des isomorphismes.

Rappelons que l'anneau de Dieudonné $W(k)[F,V]$ est l'anneau des polynômes en F et V à coefficients dans l'anneau des vecteurs de Witt $W(k)$, avec les relations

$$FV = VF = p, \quad Fx = \sigma(x)F \quad \text{et} \quad xV = V\sigma(x)$$

où σ est l'automorphisme de $W(k)$ qui relève le Frobenius $x \mapsto x^p$ de k. On a

$$W(k)[F,V] \otimes \mathbb{Q}_p = L[F, F^{-1}]$$

où $L = W(k)[\frac{1}{p}]$ est le corps des fractions de $W(k)$. On déduit facilement du lemme 13 que le théorème de Tate est encore équivalent à l'énoncé qui suit.

Theorem 16. *Soient k un corps fini de caractéristique p, $\ell \neq p$ un nombre premier, A et B deux variétés abéliennes sur k. Alors*

$$\begin{array}{rrcl} & \rho_\ell : & \mathrm{Hom}_k(A,B)\otimes\mathbb{Q}_\ell & \to & \mathrm{Hom}_{\mathbb{Q}_\ell[\mathrm{Gal}_k]}\left(V_\ell(A),V_\ell(B)\right) \\ et & \rho_p : & \mathrm{Hom}_k(A,B)\otimes\mathbb{Q}_p & \to & \mathrm{Hom}_{L[F,F^{-1}]}\left(\mathbb{D}(B)\otimes\mathbb{Q}_p,\mathbb{D}(A)\otimes\mathbb{Q}_p\right) \end{array}$$

sont des isomorphismes.

La démonstration de ce théorème est également très instructive.

2.2. **Structure des modules de Tate.** On fixe un corps fini k de caractéristique p et de cardinal $q = p^\nu$. On note $\mathrm{Frob}_k \in \mathrm{Gal}_k$ le Frobenius arithmétique $x \mapsto x^q$. C'est un générateur topologique du groupe profini $\mathrm{Gal}_k \simeq \widehat{\mathbb{Z}}$.

Une représentation ℓ-adique (V,ρ) de Gal_k est un $\mathbb{Q}_\ell$-espace vectoriel V de dimension finie muni d'une action continue $\rho : \mathrm{Gal}_k \to GL_{\mathbb{Q}_\ell}(V)$. La catégorie de ces représentations est équivalente à la catégorie des $\mathbb{Q}_\ell[\Pi,\Pi^{-1}]$-modules de longueur finie, par le foncteur qui à (V,ρ) associe le $\mathbb{Q}_\ell[\Pi,\Pi^{-1}]$-module V où l'indéterminée Π agit par $\rho(\mathrm{Frob}_k)$. Les objets simples de cette catégorie sont donc les modules

$$V(\mathfrak{L}) \overset{\text{déf}}{=} \text{module sous-jacent au corps résiduel } Z(\mathfrak{L}) \overset{\text{déf}}{=} \mathbb{Q}_\ell[\Pi,\Pi^{-1}]/\mathfrak{L}$$

pour les idéaux maximaux $\mathfrak{L}$ de $\mathbb{Q}_\ell[\Pi,\Pi^{-1}]$. On note $\phi_{\mathfrak{L}}(X) \in \mathbb{Q}_\ell[X]$ le polynôme caractéristique de Π agissant sur $V(\mathfrak{L})$. C'est donc un polynôme irréductible unitaire tel que $\phi_{\mathfrak{L}}(\Pi)$ engendre l'idéal $\mathfrak{L}\cap\mathbb{Q}_\ell[\Pi]$ de $\mathbb{Q}_\ell[\Pi]$.

Proposition 17. *Soient A une variété abélienne sur k, $\ell \neq p$ un nombre premier, et $P_A = \prod_{\mathfrak{L}}\phi_{\mathfrak{L}}^{a(\mathfrak{L})}$ la factorisation de P_A dans $\mathbb{Q}_\ell[X]$. Alors*

$$V_\ell(A) \simeq \oplus_{\mathfrak{L}} V(\mathfrak{L})^{a(\mathfrak{L})}.$$

Démonstration. L'algèbre $\mathbb{Q}[\pi_A]$ engendrée par le Frobenius π_A dans $\mathrm{End}_k^0(A)$ est centrale, donc réduite : c'est un produit de corps. Puisque π_A agit sur $V_\ell A$ comme le Frobenius Frob_k de Gal_k, le morphisme $\mathrm{End}_k^0(A)\otimes\mathbb{Q}_\ell \hookrightarrow \mathrm{End}_{\mathbb{Q}_\ell}(V_\ell A)$ identifie $\mathbb{Q}[\pi_A]\otimes\mathbb{Q}_\ell$ à la $\mathbb{Q}_\ell$-algèbre $\mathbb{Q}_\ell[\mathrm{Frob}_k]$ engendrée par l'image de Frob_k (ou de Gal_k) dans $\mathrm{End}_{\mathbb{Q}_\ell}(V_\ell A)$. En particulier, cette $\mathbb{Q}_\ell$-algèbre est semi-simple, et $V_\ell A$ est un donc un Gal_k-module semi-simple : il existe une fonction $\mathfrak{L} \mapsto n(\mathfrak{L})$ à support fini telle que $V_\ell A = \oplus_{\mathfrak{L}} V(\mathfrak{L})^{n(\mathfrak{L})}$. Mais P_A est le polynôme caractéristique de π_A, Frob_k ou Π agissant sur $V_\ell A$ d'après la proposition 3, donc $n(\mathfrak{L}) = a(\mathfrak{L})$ pour tout $\mathfrak{L}$. □

Corollary 18. *Soient A et B deux variétés abéliennes sur k. Alors*

$$\mathrm{Hom}_{\mathbb{Q}_\ell[\mathrm{Gal}_k]}\left(V_\ell A, V_\ell B\right) \simeq \oplus_{\mathfrak{L}} M_{b(\mathfrak{L}),a(\mathfrak{L})}\left(Z(\mathfrak{L})\right)$$

où $P_A = \prod\phi_{\mathfrak{L}}^{a(\mathfrak{L})}$ et $P_B = \prod\phi_{\mathfrak{L}}^{b(\mathfrak{L})}$ dans $\mathbb{Q}_\ell[X]$. En particulier,

$$\mathrm{End}_{\mathbb{Q}_\ell[\mathrm{Gal}_k]}\left(V_\ell A\right) \simeq \prod_{a(\mathfrak{L})\neq 0} M_{a(\mathfrak{L})}\left(Z(\mathfrak{L})\right)$$

est une $\mathbb{Q}_\ell$-algèbre de centre $\mathbb{Q}[\pi_A]\otimes\mathbb{Q}_\ell \simeq \prod_{a(\mathfrak{L})\neq 0} Z(\mathfrak{L})$.

Definition 19. Soient P_A et P_B deux polynômes à coefficients dans un corps K, et $P_A = \prod\phi^{a(\phi)}$ et $P_B = \prod\phi^{b(\phi)}$ leur factorisation en irréductibles. On pose

$$r(P_A,P_B) \overset{\text{déf}}{=} \sum_\phi a(\phi)b(\phi)\deg(\phi) \in \mathbb{N}.$$

C'est invariant par tout changement de base séparable $K \hookrightarrow K'$.

Corollary 20. *Soient A et B deux variétés abéliennes sur k. Alors*

$$\dim_{\mathbb{Q}_\ell} \mathrm{Hom}_{\mathbb{Q}_\ell[\mathrm{Gal}_k]}(V_\ell A, V_\ell B) = r(P_A, P_B)$$

est indépendant du choix de $\ell \nmid p$.

2.3. **Structure des modules de Dieudonné.** On conserve les notations de la section précédente, où k est un corps fini de caractéristique p et de cardinal $q = p^\nu$, mais on travaille maintenant en $\ell = p$, c'est-à-dire que l'on se propose d'étudier la catégorie des modules sur l'algèbre non-commutative $L[F, F^{-1}]$ des polynômes de Laurent $\sum_{|i|\ll\infty} \lambda_i F^i$ à coefficients λ_i dans L, où $L = W(k)[\frac{1}{p}]$. La multiplication dans cette algèbre est caractérisée par $F\lambda = \sigma(\lambda)F$ pour tout $\lambda \in L$, où l'on note σ le relèvement à $W(k)$ (ou L) du Frobenius arithmétique $x \mapsto x^p$, de sorte que

$$\mathrm{Gal}(L/\mathbb{Q}_p) = \langle\sigma\rangle \simeq \mathbb{Z}/\nu\mathbb{Z}.$$

On vérifie facilement que $\mathbb{Q}_p[F^\nu, F^{-\nu}]$ est le centre de $L[F, F^{-1}]$. On pose

$$Z = \mathbb{Q}_p[F^\nu, F^{-\nu}] \quad \text{et} \quad C = L[F, F^{-1}].$$

Montrons tout d'abord que C est une Z-algèbre d'Azumaya de rang ν^2.

Lemma 21. *L'algèbre $L \otimes_{\mathbb{Q}_p} C$ est isomorphe à $M_\nu(L \otimes_{\mathbb{Q}_p} Z)$.*

Démonstration. Considérons C comme un $L \otimes_{\mathbb{Q}_p} C$-module à gauche par

$$\forall \lambda \otimes x \in L \otimes_{\mathbb{Q}_p} C \quad \text{et} \quad y \in C, \qquad (\lambda \otimes x) \cdot y \overset{\text{déf}}{=} xy\lambda.$$

La restriction de ce module au centre $L \otimes_{\mathbb{Q}_p} Z = L[F^\nu, F^{-\nu}]$ de $L \otimes_{\mathbb{Q}_p} C$ est un $L[F^\nu, F^{-\nu}]$-module libre de base $\{1, F, \cdots, F^{\nu-1}\}$: celui que l'on obtient à partir de la multiplication à droite dans $C = L[F, F^{-1}]$ par restriction à la sous-algèbre $L[F^\nu, F^{-\nu}]$. On obtient ainsi un morphisme de $L[F^\nu, F^{-\nu}]$-algèbre

$$L \otimes_{\mathbb{Q}_p} C \longrightarrow \mathrm{End}_{L[F^\nu, F^\nu]}(C) \simeq M_\nu\left(L[F^\nu, F^{-\nu}]\right)$$

qui est explicitement donné par

$$\lambda \otimes \left(\sum F^i \mu_i\right) \mapsto \lambda \left(\sum_{i \equiv a-b \bmod \nu} (F^\nu)^{\frac{i+b-a}{\nu}} \sigma^{-b}(\mu_i) \right)_{a,b \in \{0,\ldots,\nu-1\}}$$

et dont on vérifie facilement que c'est un isomorphisme. □

Pour tout idéal maximal $\mathfrak{P}$ de Z, on note

$$Z(\mathfrak{P}) \overset{\text{déf}}{=} Z/\mathfrak{P} \qquad \text{et} \qquad C(\mathfrak{P}) \overset{\text{déf}}{=} C/\mathfrak{P}C.$$

Corollary 22. *Pour tout $\mathfrak{P}$, $C(\mathfrak{P})$ est une $Z(\mathfrak{P})$-algèbre centrale simple.*

Pour déterminer les invariants de cette algèbre, commençons par remarquer que

$$C \simeq \oplus_{i=0}^{\nu-1} Z_L \cdot \mathcal{F}^i \quad \text{où} \quad Z_L = Z \otimes_{\mathbb{Q}_p} L = L[F^\nu, F^{-\nu}],$$

la multiplication étant donnée par

$$\begin{cases} \mathcal{F} \cdot (z \otimes \ell) = (z \otimes \sigma\ell) \cdot \mathcal{F} & \text{pour } z \in Z \text{ et } \ell \in L, \\ \mathcal{F}^\nu = F^\nu & \text{dans } Z \subset Z_L. \end{cases}$$

On a donc avec les mêmes règles de multiplication

$$C(\mathfrak{P}) = \oplus_{i=0}^{\nu-1} Z(\mathfrak{P})_L \cdot \mathcal{F}^i \quad \text{où} \quad Z(\mathfrak{P})_L = Z(\mathfrak{P}) \otimes_{\mathbb{Q}_p} L$$

avec notamment

$$\mathcal{F}^\nu = \pi_{\mathfrak{P}} \overset{\text{déf}}{=} F^v \bmod \mathfrak{P} \quad \text{dans} \quad Z(\mathfrak{P}) \subset Z(\mathfrak{P})_L.$$

Posons $\mathcal{X}(\mathfrak{P}) = \mathrm{Spec}\,(Z(\mathfrak{P})_L)$, de sorte que

$$Z(\mathfrak{P})_L = \prod_{\mathfrak{Q}\in\mathcal{X}(\mathfrak{P})} L(\mathfrak{Q})$$

où le corps résiduel $L(\mathfrak{Q}) = Z(\mathfrak{P})_L/\mathfrak{Q}$ est une extension non ramifiée de $Z(\mathfrak{P})$. L'action de $\mathrm{Gal}(L/\mathbb{Q}_p) \simeq \langle\sigma\rangle$ sur $\mathcal{X}(\mathfrak{P})$ est transitive, et σ induit des isomorphismes de $Z(\mathfrak{P})$-extensions $\overline{\sigma} : L(\mathfrak{Q}) \to L(\sigma\mathfrak{Q})$. On note r le cardinal de $\mathcal{X}(\mathfrak{P})$ et d celui du sous-groupe d'isotropie. Donc $\nu = rd$ et pour tout $\mathfrak{Q} \in \mathcal{X}(\mathfrak{P})$,

$$\mathrm{Gal}(L(\mathfrak{Q})/Z(\mathfrak{P})) = \{1, \overline{\sigma}^r, \overline{\sigma}^{2r}, \cdots, \overline{\sigma}^{(d-1)r}\}.$$

Revenant à $C(\mathfrak{P})$, on peut donc maintenant écrire

$$C(\mathfrak{P}) = \oplus_{\mathfrak{Q},\nu} L(\mathfrak{Q})\cdot\mathcal{F}^\nu = \oplus_{\mathfrak{Q},i,j}\mathcal{F}^i\cdot L(\mathfrak{Q})\cdot\mathcal{F}^{rj} = \oplus_{\mathfrak{Q}} C(\mathfrak{P},\mathfrak{Q})$$

pour $\mathfrak{Q} \in \mathcal{X}(\mathfrak{P})$, $0 \le i < r$ et $0 \le j < d$, où

$$C(\mathfrak{P},\mathfrak{Q}) = \oplus_{i=0}^{r-1}\mathcal{F}^i\cdot D(\mathfrak{Q}) \qquad \text{avec} \qquad D(\mathfrak{Q}) = \oplus_{j=0}^{d-1} L(\mathfrak{Q})\cdot\mathcal{F}^{rj}.$$

On vérifie alors que $C(\mathfrak{P},\mathfrak{Q})$ est un idéal à gauche de $C(\mathfrak{P})$. Plus précisément, c'est la composante $\mathfrak{Q}$-primaire de $C(\mathfrak{P})$, pour la structure de $Z(\mathfrak{P})_L$-module induite par la multiplication à droite dans $C(\mathfrak{P})$:

$$C(\mathfrak{P},\mathfrak{Q}) = \{x \in C(\mathfrak{P}) : x\cdot y = 0 \text{ pour tout } y \in \mathfrak{Q} \subset Z(\mathfrak{P})_L\}\,.$$

Considérons sur $D(\mathfrak{Q}) = \oplus_{j=0}^{d-1} L(\mathfrak{Q})\cdot\mathcal{F}^{rj}$ la structure de $Z(\mathfrak{P})$-algèbre donnée par

$$\begin{cases} \mathcal{F}^r\cdot\lambda = \overline{\sigma}^r(\lambda)\cdot\mathcal{F}^r & \text{pour } \lambda \in L(\mathfrak{Q}), \text{ et} \\ \mathcal{F}^{rd} = \pi_{\mathfrak{P}} & \text{dans } Z(\mathfrak{P}) \subset L(\mathfrak{Q}). \end{cases}$$

On obtient alors sur $C(\mathfrak{P},\mathfrak{Q}) = \oplus_i \mathcal{F}^i\cdot D(\mathfrak{Q})$ une évidente structure de $D(\mathfrak{Q})$-module à droite, dont on laisse au lecteur le soin de vérifier qu'elle commute à l'action à gauche de $C(\mathfrak{P},\mathfrak{Q})$. Cette action induit donc un morphisme de $Z(\mathfrak{P})$-algèbre

$$C(\mathfrak{P}) \to \mathrm{End}_{D(\mathfrak{Q})}\left(C(\mathfrak{P},\mathfrak{Q})\right) = \mathrm{End}_{D(\mathfrak{Q})}\left(\oplus_i \mathcal{F}^i D(\mathfrak{Q})\right) = M_r\left(D(\mathfrak{Q})\right).$$

Ce morphisme est injectif puisque $C(\mathfrak{P})$ est simple, donc bijectif puisque

$$\dim_{Z(\mathfrak{P})} C(\mathfrak{P}) = \nu^2 = r^2d^2 = \dim_{Z(\mathfrak{P})} M_r\left(D(\mathfrak{Q})\right).$$

En particulier, $[C(\mathfrak{P})] = [D(\mathfrak{Q})]$ dans le groupe de Brauer $\mathrm{Br}(Z(\mathfrak{P}))$. Or $D(\mathfrak{Q})$ est presque donné sous la forme standard des $Z(\mathfrak{P})$-algèbres centrales simples cycliques, à ceci près que le générateur $\overline{\sigma}^r$ de $\mathrm{Gal}\left(L(\mathfrak{Q})/Z(\mathfrak{P})\right)$ n'est pas nécéssairement le Frobenius arithmétique de cette extension non-ramifiée.

Soit $Z_0(\mathfrak{P})$ la plus grande sous-extension de $Z(\mathfrak{P})/\mathbb{Q}_p$ qui se plonge dans L. C'est donc une extension non-ramifiée de $\mathbb{Q}_p$ dont le degré est égal au plus grand diviseur commun des degrés ν et $f_{\mathfrak{P}}$ des corps résiduels de L et $Z(\mathfrak{P})$. On a alors

$$Z(\mathfrak{P})_L = Z(\mathfrak{P})\otimes_{Z_0(\mathfrak{P})}\left(Z_0(\mathfrak{P})\otimes_{\mathbb{Q}_p} L\right) = \prod_{\iota\in\mathcal{I}(\mathfrak{P})} L(\iota)$$

où $\mathcal{I}(\mathfrak{P}) = \mathrm{Hom}_{\mathbb{Q}_p}(Z_0(\mathfrak{P}), L)$ et $L(\iota) = Z(\mathfrak{P})\otimes_{Z_0(\mathfrak{P}),\iota} L$ est un corps, puisque $Z(\mathfrak{P})$ et L sont linéairement disjointes sur $Z_0(\mathfrak{P})$. Il y a donc une bijection $\iota \mapsto \mathfrak{Q}$ de $\mathcal{I}(\mathfrak{P})$ sur $\mathcal{X}(\mathfrak{P})$, telle que $L(\iota) = L(\mathfrak{Q})$ comme quotient de $Z(\mathfrak{P})_L$. En particulier,

$$r = |\mathcal{X}(\mathfrak{P})| = |\mathcal{I}(\mathfrak{P})| = [Z_0(\mathfrak{P}) : \mathbb{Q}_p] = \mathrm{pgcd}(\nu, f_{\mathfrak{P}}).$$

Par construction, $\overline{\sigma}^r = \mathrm{Id} \otimes \sigma^r$ sur $L(\iota) = Z(\mathfrak{P}) \otimes_{Z_0(\mathfrak{P}),\iota} L$, qui agit donc sur le corps résiduel par l'élément $\mathrm{Id} \otimes (x \mapsto x^{p^r}) = (\mathrm{Id}, \mathrm{Frob}^r)$ du groupe de Galois

$$\mathrm{Gal}\left(\mathbb{F}_{p^{f_\mathfrak{P}}} \otimes_{\mathbb{F}_{p^r},\iota} \mathbb{F}_{p^\nu}/\mathbb{F}_{p^r}\right) \simeq \mathrm{Gal}\left(\mathbb{F}_{p^{f_\mathfrak{P}}}/\mathbb{F}_{p^r}\right) \times \mathrm{Gal}\left(\mathbb{F}_{p^\nu}/\mathbb{F}_{p^r}\right) \simeq \mathbb{Z}/s\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z}$$

où $f_\mathfrak{P} = rs$ et $\nu = rd$, de sorte que $\mathrm{pgcd}(s,d) = 1$. Le Frobenius arithmétique $\phi_\mathfrak{P}$ de $L(\iota)/Z(\mathfrak{P})$ agit quant à lui par $(x \mapsto x^{p^{f_\mathfrak{P}}}) = (\mathrm{Id}, \mathrm{Frob}^{f_\mathfrak{P}})$, donc $\phi_\mathfrak{P} = (\overline{\sigma}^r)^s = \overline{\sigma}^{f_\mathfrak{P}}$. Puisque s est inversible dans $\mathbb{Z}/d\mathbb{Z}$, on peut alors réécrire

$$\mathcal{D}(\mathfrak{Q}) = \oplus_{i=0}^{d-1} L(\iota) \cdot \mathcal{F}^{f_\mathfrak{P} i} \qquad \text{avec} \qquad \mathcal{F}^{f_\mathfrak{P}} = (\mathcal{F}^r)^s$$

où la structure multiplicative est maintenant donnée par

$$\begin{cases} \mathcal{F}^{f_\mathfrak{P}} \cdot \lambda = \phi_\mathfrak{P}(\lambda) \cdot \mathcal{F}^{f_\mathfrak{P}} & \text{pour } \lambda \in L(\iota), \text{ et} \\ \mathcal{F}^{f_\mathfrak{P} d} = \pi_\mathfrak{P}^s & \text{dans } Z(\mathfrak{P}) \subset L(\mathfrak{Q}). \end{cases}$$

D'après (***), l'invariant de $D(\mathfrak{Q})$ est donc donné par la formule

$$\mathrm{inv}_{Z(\mathfrak{P})}\left[D(\mathfrak{Q})\right] = \frac{v(\pi_\mathfrak{P}^s)}{d} = \frac{s v(\pi_\mathfrak{P})}{d} \in \mathbb{Q}/\mathbb{Z}$$

où il faut prendre pour v la valuation normalisée de $Z(\mathfrak{P})$, i.e. celle pour laquelle $v(p)$ est l'indice de ramification absolu $e_\mathfrak{P}$ de $Z(\mathfrak{P})$. Puisque alors

$$\frac{s}{d} = \frac{sr}{dr} = \frac{f_\mathfrak{P}}{\nu} = \frac{f_\mathfrak{P} e_\mathfrak{P}}{\nu e_\mathfrak{P}} = \frac{[Z(\mathfrak{P}) : \mathbb{Q}_p]}{v(q)}$$

on obtient finalement la formule suivante pour l'invariant de $C(\mathfrak{P})$, formule dans laquelle il n'est plus besoin de supposer que la valuation v est normalisée.

Proposition 23. *Pour tout $\mathfrak{P}$, l'invariant de $[C(\mathfrak{P})] \in \mathrm{Br}(Z(\mathfrak{P}))$ est égal à*

$$\mathrm{inv}_{Z(\mathfrak{P})}\left[C(\mathfrak{P})\right] = [Z(\mathfrak{P}) : \mathbb{Q}_p] \cdot \lambda(\mathfrak{P}) \in \mathbb{Q}/\mathbb{Z} \quad \textit{avec} \quad \lambda(\mathfrak{P}) = \frac{v(\pi_\mathfrak{P})}{v(q)} \in \mathbb{Q}$$

où $\pi_\mathfrak{P}$ est l'image de F^ν dans $Z(\mathfrak{P})$.

Definition 24. On note $S(\mathfrak{P}) \neq 0$ un $C(\mathfrak{P})$-module simple,

$$D(\mathfrak{P}) = \mathrm{End}_{C(\mathfrak{P})}\left(S(\mathfrak{P})\right)^{\mathrm{opp}}, \quad r_\mathfrak{P} = [S(\mathfrak{P}) : D(\mathfrak{P})] \quad \text{et} \quad d_\mathfrak{P}^2 = [D(\mathfrak{P}) : Z(\mathfrak{P})].$$

On a donc $C(\mathfrak{P}) \simeq M_{r_\mathfrak{P}}(D(\mathfrak{P}))$, $S(\mathfrak{P}) \simeq D(\mathfrak{P})^{r_\mathfrak{P}}$. On sait aussi que

$$\nu = r_\mathfrak{P} d_\mathfrak{P} \quad \text{et} \quad d_\mathfrak{P} = \text{ordre de } [Z(\mathfrak{P}) : \mathbb{Q}_p] \cdot \lambda(\mathfrak{P}) \text{ dans } \mathbb{Q}/\mathbb{Z}$$

où $\lambda(\mathfrak{P}) = v(\pi_\mathfrak{P})/v(q)$ pour toute valuation v de $Z(\mathfrak{P})$.

Remark 25. Nous verrons plus loin que $\lambda(\mathfrak{P})$ est la pente du module de Dieudonné déduit de $S(\mathfrak{P})$ par passage à une clôture algébrique de $k = \mathbb{F}_q$.

Lemma 26. *Tout C-module simple est isomorphe à un unique $S(\mathfrak{P})$.*

Démonstration. Soit $M \neq 0$ un C-module simple. Alors $M = C \cdot m$ pour tout $m \neq 0$ dans M, donc M est un Z-module de type fini puisque C l'est. Soit $I \subsetneq Z$ l'annulateur du Z-module M, et $I \subset J \neq Z$ un idéal. Alors JM est un sous-C-module de M, et $JM \subsetneq M$ d'après Nakayama, donc $JM = 0$ par simplicité du C-module M, et finalement $I = J$. Donc $I = \mathfrak{P}$ est un idéal maximal de Z, et M un $C(\mathfrak{P})$-module simple, i.e. $M \simeq S(\mathfrak{P})$. □

Corollary 27. *Soit M un C-module. Alors*

$$M \text{ est } C\text{-semi-simple} \iff M \text{ est } Z\text{-semi-simple.}$$

Démonstration. Si M est Z-semi-simple, alors $M = \oplus_{\mathfrak{P}} M[\mathfrak{P}]$ où chacun des

$$M[\mathfrak{P}] = \{m \in M : \mathfrak{P}m = 0\}$$

est un $C(\mathfrak{P})$-module, donc un C-module semi-simple puisque tous les $C(\mathfrak{P})$-modules le sont. Inversement, si M est C-semi-simple, c'est une somme directe de C-modules simples $S(\mathfrak{P})$, et chacun de ces modules est évidemment Z-semi-simple. □

Corollary 28. *Pour tout C-module M, les conditions suivantes sont équivalentes :*

(1) *M est de longueur finie,*
(2) *M est de $\mathbb{Q}_p$-dimension finie,*
(3) *M est de L-dimension finie,*
(4) *M est un Z-module de torsion et de type fini.*

Démonstration. C'est immédiat. □

Definition 29. Le polynôme caractéristique d'un tel C-module M est

$$P_M(X) = \det_L\left(X \cdot \mathrm{Id} - F^\nu | M\right).$$

Ce polynôme est bien défini car M est de L-dimension finie et l'action de $F^\nu \in Z$ sur M est L-linéaire. C'est un polynôme unitaire, dont les coefficients sont à priori dans L, et c'est aussi le produit des polynômes caractéristiques des facteurs d'une filtration de Jordan-Hölder de M. On note $P_{\mathfrak{P}}$ le polynôme caractéristique de $S(\mathfrak{P})$. Pour le calculer, notons que :

(1) $C(\mathfrak{P}) \simeq S(\mathfrak{P})^{r_{\mathfrak{P}}}$ comme $C(\mathfrak{P})$-module, et
(2) $C(\mathfrak{P}) = Z(\mathfrak{P})^\nu_L$ comme $Z(\mathfrak{P})_L = Z(\mathfrak{P}) \otimes_{\mathbb{Q}_p} L$-module.

On en déduit que

$$P_{\mathfrak{P}}^{r_{\mathfrak{P}}} = \det_L\left(X \cdot \mathrm{Id} - F^\nu | Z(\mathfrak{P})_L\right)^\nu = \det_{\mathbb{Q}_p}\left(X \cdot \mathrm{Id} - F^\nu | Z(\mathfrak{P})\right)^\nu$$

Soit $\phi_{\mathfrak{P}} \in \mathbb{Q}_p[X]$ le polynôme irréductible unitaire tel que $\phi_{\mathfrak{P}}(F^\nu)$ engendre $\mathfrak{P}$ dans $Z = \mathbb{Q}_p[F^\nu, F^{-\nu}]$. On a donc $\deg \phi_{\mathfrak{P}} = [Z(\mathfrak{P}) : \mathbb{Q}_p]$. Puisque $\nu = d_{\mathfrak{P}} r_{\mathfrak{P}}$, on obtient

$$P_{\mathfrak{P}} = \phi_{\mathfrak{P}}^{d_{\mathfrak{P}}} \in \mathbb{Q}_p[X].$$

En particulier, $P_M \in \mathbb{Q}_p[X]$ pour tout C-module M de longeur finie.

Proposition 30. *Soit A une variété abélienne sur k, $P_A = \prod_{\mathfrak{P}} \phi_{\mathfrak{P}}^{a(\mathfrak{P})}$ la décomposition de P_A dans $\mathbb{Q}_p[X]$. Alors $d_{\mathfrak{P}} \mid a(\mathfrak{P})$ pour tout $\mathfrak{P}$ et*

$$\mathbb{D}(A) \otimes \mathbb{Q}_p \simeq \oplus_{\mathfrak{P}} S(\mathfrak{P})^{a(\mathfrak{P})/d_{\mathfrak{P}}}.$$

Démonstration. On sait que π_A agit comme F^ν sur $M_A = \mathbb{D}(A) \otimes \mathbb{Q}_p$. On en déduit comme dans la proposition 17 que M_A est un module semi-simple sur le centre $Z = \mathbb{Q}_p[F^\nu, F^{-\nu}]$ de C, donc aussi un C-module semi-simple d'après le corollaire 27. On peut donc écrire $M_A \simeq \oplus_{\mathfrak{P}} S(\mathfrak{P})^{n(\mathfrak{P})}$ pour une fonction $\mathfrak{P} \mapsto n(\mathfrak{P})$ à support fini. Mais la proposition 3 montre que $P_A = P_{M_A}$ dans $\mathbb{Q}_p[X]$, i.e.

$$\prod_{\mathfrak{P}} \phi_{\mathfrak{P}}^{a(\mathfrak{P})} = P_A = P_{M_A} = \prod_{\mathfrak{P}} P_{\mathfrak{P}}^{n(\mathfrak{P})} = \prod_{\mathfrak{P}} \phi_{\mathfrak{P}}^{d_{\mathfrak{P}} n(\mathfrak{P})}$$

donc $a(\mathfrak{P}) = d_{\mathfrak{P}} n(\mathfrak{P})$ pour tout $\mathfrak{P}$. □

Corollary 31. *Soient A et B deux variétés abéliennes sur k. Alors*

$$\mathrm{Hom}_C\left(\mathbb{D}(B)\otimes\mathbb{Q}_p, \mathbb{D}(A)\otimes\mathbb{Q}_p\right) \simeq \oplus_{\mathfrak{P}} M_{\frac{a(\mathfrak{P})}{d_{\mathfrak{P}}}, \frac{b(\mathfrak{P})}{d_{\mathfrak{P}}}}\left(D(\mathfrak{P})^{\mathrm{opp}}\right)$$

où $P_A = \prod_{\mathfrak{P}} \phi_{\mathfrak{P}}^{a(\mathfrak{P})}$ et $P_B = \prod_{\mathfrak{P}} \phi_{\mathfrak{P}}^{b(\mathfrak{P})}$ dans $\mathbb{Q}_p[X]$. En particulier,

$$\mathrm{End}_C\left(\mathbb{D}(A)\otimes\mathbb{Q}_p\right)^{\mathrm{opp}} \simeq \prod_{a(\mathfrak{P})\neq 0} M_{\frac{a(\mathfrak{P})}{d_{\mathfrak{P}}}}\left(D(\mathfrak{P})\right)$$

est une $\mathbb{Q}_p$-algèbre de centre $\mathbb{Q}[\pi_A]\otimes\mathbb{Q}_p \simeq \prod_{a(\mathfrak{P})\neq 0} Z(\mathfrak{P})$.

Corollary 32. *Soient A et B deux variétés abéliennes sur k. Alors*

$$\dim_{\mathbb{Q}_p} \mathrm{Hom}_C\left(\mathbb{D}(B)\otimes\mathbb{Q}_p, \mathbb{D}(A)\otimes\mathbb{Q}_p\right) = r(P_A, P_B).$$

2.4. **Preuve du théorème 16.** On sait déjà que les applications (pour $\ell \neq p$)

$$\begin{array}{rccc} \rho_\ell : & \mathrm{Hom}_k(A,B)\otimes\mathbb{Q}_\ell & \to & \mathrm{Hom}_{\mathbb{Q}_\ell[\mathrm{Gal}_k]}\left(V_\ell(A), V_\ell(B)\right) \\ \text{et} \quad \rho_p : & \mathrm{Hom}_k(A,B)\otimes\mathbb{Q}_p & \to & \mathrm{Hom}_{L[F,F^{-1}]}\left(\mathbb{D}(B)\otimes\mathbb{Q}_p, \mathbb{D}(A)\otimes\mathbb{Q}_p\right) \end{array}$$

sont injectives, et il résulte des corollaires 20 et 32 que

$$\begin{array}{rcl} r(P_A,P_B) & = & \dim_{\mathbb{Q}_\ell}\left(\mathrm{Hom}_{\mathbb{Q}_\ell[\mathrm{Gal}_k]}\left(V_\ell(A), V_\ell(B)\right)\right), \\ \text{et} \quad r(P_A,P_B) & = & \dim_{\mathbb{Q}_p}\left(\mathrm{Hom}_{L[F,F^{-1}]}\left(\mathbb{D}(B)\otimes\mathbb{Q}_p, \mathbb{D}(A)\otimes\mathbb{Q}_p\right)\right). \end{array}$$

Il suffit donc de démontrer le théorème de Tate pour un unique $\ell \neq p$! En outre, on peut toujours supposer que $A = B$, puisque pour $C = A \times B$, le morphisme

$$\rho_\ell : \mathrm{End}_k^0(C)\otimes\mathbb{Q}_\ell \to \mathrm{End}_{\mathbb{Q}_\ell[\mathrm{Gal}_k]}\left(V_\ell C, V_\ell C\right)$$

s'identifie évidemment à

$$\begin{pmatrix} \mathrm{End}_k^0(A) & \mathrm{Hom}_k^0(B,A) \\ \mathrm{Hom}_k^0(A,B) & \mathrm{End}_k^0(B) \end{pmatrix}\otimes\mathbb{Q}_\ell \to \begin{pmatrix} \mathrm{End}_{\mathbb{Q}_\ell[\mathrm{Gal}_k]}(V_\ell A) & \mathrm{Hom}_{\mathbb{Q}_\ell[\mathrm{Gal}_k]}(V_\ell B, V_\ell A) \\ \mathrm{Hom}_{\mathbb{Q}_\ell[\mathrm{Gal}_k]}(V_\ell A, V_\ell B) & \mathrm{End}_{\mathbb{Q}_\ell[\mathrm{Gal}_k]}(V_\ell B) \end{pmatrix}$$

Soit donc A une variété abélienne sur k, $\pi = \pi_A$ son Frobenius. On pose $F = \mathbb{Q}[\pi]$ qui est centrale dans $E = \mathrm{End}_k(A)$. Pour tout $\ell \neq p$, on note $V_\ell = V_\ell A$ et

$$F_\ell \overset{\text{déf}}{=} F\otimes\mathbb{Q}_\ell \subset E_\ell \overset{\text{déf}}{=} E\otimes\mathbb{Q}_\ell \subset D_\ell \overset{\text{déf}}{=} \mathrm{End}_{F_\ell}(V_\ell) \subset M_\ell \overset{\text{déf}}{=} \mathrm{End}_{\mathbb{Q}_\ell}(V_\ell).$$

On veut montrer que $E_\ell = D_\ell$ (pour un choix convenable de ℓ), i.e. que E_ℓ est le commutant de F_ℓ dans M_ℓ, ou encore que F_ℓ est le commutant de E_ℓ dans M_ℓ. Notons $C_\ell = \mathrm{End}_{E_\ell}(V_\ell)$ ce commutant, de sorte que $F_\ell \subset C_\ell$ et on veut montrer que $F_\ell = C_\ell$ (pour un choix convenable de ℓ).

Décomposons $F = \prod F_i$ en produit de corps et choisissons pour ℓ un nombre premier qui se décompose totalement dans tous les F_i (il en existe une infinité). On a alors $F_\ell \simeq \mathbb{Q}_\ell^r$, et $V_\ell = \oplus_{i=1}^r V_\ell^i$ se décompose de même en espaces propres pour l'action de F_ℓ, où F_ℓ agit sur V_ℓ^i par la i-ème projection $F_\ell \to \mathbb{Q}_\ell$. Ces sous-espaces sont stables sous C_ℓ, puisque F_ℓ est centrale dans C_ℓ. Pour voir que $F_\ell = C_\ell$, il suffit donc de démontrer que l'action de C_ℓ y est scalaire, ou encore que

Claim 33. Toute $\mathbb{Q}_\ell$-droite $W \subset V_\ell$ qui est stable sous F_ℓ (c'est à dire contenue dans l'un des V_ℓ^i), est également stable sous C_ℓ.

Choisissons sur A une polarisation $\lambda : A \to A^t$, disons de degré d^2 et soit $\psi_\ell : V_\ell A \times V_\ell A \to V_\ell\mu$ la forme symplectique qu'elle induit sur V_ℓ. Il suffit alors de démontrer que

Claim 34. Tout sous-espace totalement isotrope maximal W de (V_ℓ, ψ_ℓ) qui est stable sous F_ℓ, est également stable sous C_ℓ.

Cette hypothèse implique en effet que tout sous-espace totalement isotrope (mais pas forcément maximal) W de (V_ℓ, ψ_ℓ) qui est stable sous F_ℓ (par exemple une $\mathbb{Q}_\ell$-droite stable sous F_ℓ) est encore stable sous C_ℓ. On le montre par récurrence descendante sur la dimension de W, le cas initial où $\dim_{\mathbb{Q}_\ell} W = g$ étant précisément notre hypothèse. Soit donc W un tel sous-espace, avec $\dim_{\mathbb{Q}_\ell} W = g - s$, pour un $s > 0$. Puisque F est stable sous l'involution de Rosati $\dagger$ induite par λ, F_ℓ est stable sous l'involution $\dagger$ induite par ψ_ℓ, donc l'orthogonal $W^\perp$ de W dans (V_ℓ, ψ_ℓ) est encore F_ℓ-stable, donc de la forme $W^\perp = W \oplus \oplus_{i=1}^{2s} D_i$ pour des $\mathbb{Q}_\ell$-droites D_i qui sont F_ℓ-stables ; alors $W_1 = W \oplus D_1$ et $W_2 = W \oplus D_2$ sont deux sous-espaces totalement isotropes et F_ℓ-stables de V_ℓ, ils sont stables sous C_ℓ d'après l'hypothèse de récurrence, et leur intersection W est donc également stable sous V_ℓ.

Le théorème de Tate résulte alors de la proposition suivante, dans laquelle il n'est plus nécessaire de supposer que $F_\ell \simeq \mathbb{Q}_\ell^r$, mais où l'on demande en revanche que $\ell \nmid pd$ (concrètement, il faut donc choisir d'abord λ d'un degré d^2 arbitraire, puis ensuite $\ell \nmid pd$ décomposant E).

Proposition 35. *Pour tout sous-espace totalement isotrope maximal W de (V_ℓ, ψ_ℓ) qui est stable sous F_ℓ, il existe un élément $e \in E_\ell$ tel que $e \cdot V_\ell = W$. En particulier, W est stable sous le commutant C_ℓ de E_ℓ dans M_ℓ.*

Démonstration. Dire que W est F_ℓ-stable revient à dire que c'est un sous-$\mathbb{Q}_\ell[\mathrm{Gal}_k]$-module. Pour tout $n \geq 0$, on pose $X_n = (T_\ell A \cap W) + \ell^n T_\ell A \subset T_\ell A$. C'est donc un $\mathbb{Z}_\ell$-sous-réseau d'indice ℓ^{ng} dans $T_\ell A$ qui est stable sous Gal_k. Soit $\alpha_n : A_n \to A$ l'isogénie (de degré ℓ^{ng}) telle que $\alpha_n(T_\ell A_n) = X_n$ dans $T_\ell A$. Pour tout $x, y \in T_\ell A_n$, on a donc

$$\langle x, (\alpha_n^* \lambda)(y) \rangle_\ell^{A_n} = \langle x, y \rangle_\ell^{\alpha_n^* \lambda} = \langle \alpha_n(x), \alpha_n(y) \rangle_\ell^{\lambda} \subset \ell^n T_\ell(\mu)$$

puisque $W \subset V_\ell A$ est totalement isotrope, donc $(\alpha_n^* \lambda)(T_\ell A_n) \subset \ell^n T_\ell A_n^t$, i.e.

$$\alpha_n^* \lambda = \alpha_n^t \circ \lambda \circ \alpha_n : A_n \to A_n^t \text{ est triviale sur } A_n[\ell^n].$$

Soit $\lambda_n : A_n \to A_n^t$ telle que $\ell^n \lambda_n = \alpha_n^* \lambda$. C'est encore une polarisation de A_n, et

$$(\ell^n)^{2g} \deg(\lambda_n) = \deg(\ell^n \lambda_n) = \deg(\alpha_n^* \lambda) = (\ell^{ng})^2 \deg(\lambda)$$

puisque $\deg \alpha_n = \deg \alpha_n^t = \ell^{ng}$. Donc $\deg \lambda_n = \deg \lambda$. D'après le lemme ci-dessous, il y a un ensemble infini $I \subset \mathbb{N}$ tel que $(A_i, \lambda_i) \simeq (A_j, \lambda_j)$ pour tout $i, j \in I$. Soit n le plus petit élément de I, et pour tout $i \in I$, choisissons arbitrairement un isomorphisme $\theta_i : A_n \to A_i$. Alors $e_i = \alpha_i \circ \theta_i \circ \alpha_n^{-1} \in E$ induit sur $V_\ell A$ un morphisme tel que $e_i(X_n) = X_i \subset X_n$. Vus dans E_ℓ, ces morphismes restent donc dans le compact $E_\ell \cap \mathrm{End}_{\mathbb{Z}_\ell}(X_n)$. On peut donc extraire de (e_i) une sous-suite $(e_{\phi(i)})$ qui converge vers un élément e de E_ℓ. On montre facilement que

$$e(X_n) = \cap X_i = T_\ell A \cap W,$$

puis que $e(V_\ell A) = W$. □

Lemma 36. *L'ensemble $\mathbf{M}_{d,1}^g(k)$ des classes d'isomorphismes de paires (B, ν) où B est une variété abélienne de dimension g sur k et $\nu : B \to B^t$ est une polarisation de degré d^2 est fini.*

Démonstration. Ce serait trivial si l'on savait qu'il s'agit là des k-points d'un schéma de type fini sur $\mathrm{Spec}(\mathbb{Z})$ (ou $\mathbb{F}_p$). Malheureusement, $\mathbf{M}_{d,1}^g$ n'est pas représentable. On peut rajouter une structure de niveau $N \geq 3$ premier à p : si B est une variété

abélienne de dimension g sur k, le noyau de $\mathrm{Gal}_k \to \mathrm{Aut}(B[N](\overline{k}))$ est d'indice majoré par le cardinal de $\mathrm{Aut}(B[N](\overline{k})) \simeq GL_{2g}(\mathbb{Z}/N\mathbb{Z})$, donc il existe une extension finie K de k telle que toute variété abélienne B sur k de dimension g admet une structure de niveau N sur K. Puisque $\mathbf{M}^g_{d,N}(K)$ est fini, on en déduit que l'ensemble $\mathbf{M}^g_{d,1}(k)$ est d'image finie dans $\mathbf{M}^g_{d,1}(K)$, mais il resterait alors à vérifier que les fibres de $\mathbf{M}^g_{d,1}(k) \to \mathbf{M}^g_{d,1}(K)$ sont finies (ce qui n'est pas très difficile). On peut aussi rajouter une rigidification : puisque k est un corps, $\mathbf{RM}^g_{d,1}(k) \to \mathbf{M}^g_{d,1}(k)$ est surjective : on conclut alors directement, puisqu'on a vu que $\mathbf{RM}^g_{d,N}$ est représentable (sans restriction sur N) par un schéma de type fini sur $\mathrm{Spec}(\mathbb{Z})$. □

2.5. **Conséquences, I.** Nous avons vu que le polynôme caractéristique du Frobénius détermine la structure des modules de Tate et du module de Dieudonné. Le théorème de Tate implique tout d'abord que ce polynôme détermine aussi la classe d'isogénie.

Proposition 37. *Pour deux variétés abéliennes A et B sur k, les conditions suivantes sont équivalentes :*

(1) *A est un sous-quotient de B dans $\mathbf{Ab}^0_k$,*
(2) *$V_\ell A$ est un sous-quotient de $V_\ell B$ dans $\mathbf{Mod}_{\mathbb{Q}_\ell[\mathrm{Gal}_k]}$ pour un $\ell \neq p$,*
(3) *$V_\ell A$ est un sous-quotient de $V_\ell B$ dans $\mathbf{Mod}_{\mathbb{Q}_\ell[\mathrm{Gal}_k]}$ pour tout $\ell \neq p$,*
(4) *$\mathbb{D}(A) \otimes \mathbb{Q}_p$ est un sous-quotient de $\mathbb{D}(B) \otimes \mathbb{Q}_p$ dans $\mathbf{Mod}_{W(k)[\frac{1}{p}][F,F^{-1}]}$,*
(5) *$P_A \mid P_B$ dans $\mathbb{Z}[\Pi]$.*

De plus, les sous-quotients de $(1-4)$ sont alors des facteurs directs.

Démonstration. La dernière remarque résulte de la semi-simplicité de la catégorie $\mathbf{Ab}^0_k$, et de la semi-simplicité des objets $V_\ell B$ et $\mathbb{D}(B) \otimes \mathbb{Q}_p$. Les implications $(1) \Rightarrow (2-4)$ sont évidentes, et les équivalences $(2-4) \iff (5)$ résultent des propositions 17 et 30. Pour $(2) \Rightarrow (1)$, soit $f : V_\ell A \hookrightarrow V_\ell B$ une injection Gal_k-équivariante. On peut d'après le théorème 15 approcher f par un élément $\rho_\ell(f') \in \rho_\ell(\mathrm{Hom}^0_k(A,B))$, et si $\rho_\ell(f')$ est suffisamment proche de f, alors $\rho_\ell(f')$ sera encore injective, donc $f' : A \hookrightarrow B$ dans $\mathbf{Ab}^0_k$. Le même argument démontre aussi que $(4) \Rightarrow (1)$. □

Corollary 38. *Les conditions suivantes sont équivalentes :*

(1) *A et B sont isogènes sur k, i.e. isomorphes dans $\mathbf{Ab}^0_k$,*
(2) *$V_\ell A \simeq V_\ell B$ comme $\mathbb{Q}_\ell[\mathrm{Gal}_k]$-module pour un $\ell \neq p$,*
(3) *$V_\ell A \simeq V_\ell B$ comme $\mathbb{Q}_\ell[\mathrm{Gal}_k]$-module pour tout $\ell \neq p$,*
(4) *$\mathbb{D}(A) \otimes \mathbb{Q}_p \simeq \mathbb{D}(B) \otimes \mathbb{Q}_p$ comme $W(k)[\frac{1}{p}][F,F^{-1}]$-module,*
(5) *$P_A = P_B$ dans $\mathbb{Z}[\Pi]$.*

Remark 39. Il en résulte que deux variétés abéliennes A et B sur k qui sont isogènes sur k ont le même nombre de points sur toutes les extensions finies de k, et donc aussi la même fonction Zêta (ce qui n'est à priori pas du tout évident). D'ailleurs, cette condition caractérise aussi le fait que A et B soient isogènes !

Corollary 40. *L'application $w : \mathcal{S}(q) \to \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})\backslash\mathcal{W}(q)$ est injective.*

Démonstration. Ce n'est pas complètement tautologique. Si A et B sont simples et $w(A) = w(B)$, les polynômes *minimaux* de π_A et π_B sont égaux donc $P^a_A = P^b_B$ pour des entiers a et b convenables, donc $A^a \sim B^b$ dans $\mathbf{Ab}^0_k$ puis $A \sim B$ car A et B sont simples (donc aussi $P_A = P_B$ et $a = b$). □

2.6. **Conséquences, II.** On peut ensuite utiliser les résultats qui précèdent pour déterminer entièrement les anneaux d'endomorphismes dans la catégorie $\mathbf{Ab}_k^0$.

Proposition 41. *Pour tout $A \in \mathbf{Ab}_k^0$, le centre de $\mathrm{End}_k^0(A)$ est égal à $\mathbb{Q}[\pi_A]$.*

Démonstration. Cela résulte du théorème de Tate et du corollaire 18 (ou 31). □

Proposition 42. *Soient A une variété abélienne simple sur k, π son Frobenius, $D = \mathrm{End}_k^0(A)$ et $F = \mathbb{Q}(\pi)$ le centre de D. Alors*

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

et pour toute place v de F, l'invariant de D en v est donné par

$$\mathrm{inv}_v D = \begin{cases} 0 & \text{si } v \nmid p\infty \\ \frac{1}{2} & \text{si } v \text{ est réelle} \\ \frac{v(\pi)}{v(q)}[F_v:\mathbb{Q}_p] & \text{si } v \mid p \end{cases} \qquad \text{dans } \mathbb{Q}/\mathbb{Z}.$$

Démonstration. Cela résulte à nouveau du théorème de Tate, des corollaire 18 et 31, et de la proposition 23 - sauf pour la valeur de l'invariant aux places réelles, s'il y en a. Mais si F a une place réelle, alors $\pi = \pm\sqrt{q} = \pm p^{\nu/2}$, ce qui limite beaucoup les cas à considérer !

Si ν est pair, disons $\nu = 2\nu'$ avec $\nu' \neq 0 \in \mathbb{N}$, alors $\pi = \pm p^{\nu'}$ et $F = \mathbb{Q}$. L'invariant de D en v est trivial si $v \nmid p\infty$, égal à $\frac{1}{2}$ si $v = p$, donc aussi égal à $\frac{1}{2}$ en $v = \infty$ puisque la somme des invariants doit être nulle. Donc D est le corps de quaternion $B_{p,\infty}$ sur $\mathbb{Q}$ tel que $\mathrm{Ram}(B_{p,\infty}) = \{p, \infty\}$, et A est une courbe elliptique supersingulière.

Si ν est impair, disons $\nu = 2\nu' + 1$ avec $\nu' \in \mathbb{N}$, alors $\pi = \pm p^{\nu'}\sqrt{p}$ et $F = \mathbb{Q}(\sqrt{p})$. Les invariants de D sont triviaux à toutes les places finies de F, ce qui ne laisse à priori que deux possibilités pour les invariants de D aux places archimédiennes ∞_1 et ∞_2 de F, à savoir $(0,0)$ ou $(\frac{1}{2},\frac{1}{2})$. Dans le premier cas, $D = F = \mathbb{Q}(\sqrt{p})$, donc $\dim A = 1$, i.e. A est une courbe elliptique ; mais puisque $\pi^2 = q$ est le Frobenius de $A \times_{\mathbb{F}_q} \mathbb{F}_{q^2}$, l'extension quadratique réelle F de $\mathbb{Q}$ devrait alors se plonger dans le corps de quaternion $B_{p,\infty}$ sur $\mathbb{Q}$, une contradiction. Donc D est le corps de quaternion B_{∞_1,∞_2} sur F tel que $\mathrm{Ram}(B_{\infty_1,\infty_2}) = \{\infty_1, \infty_2\}$, et A est une surface abélienne – simple sur $\mathbb{F}_q$, mais qui devient isogène au produit de deux courbes elliptiques supersingulières sur l'extension quadratique $\mathbb{F}_{q^2}$ de $\mathbb{F}_q$. □

Remark 43. Concrètement, supposons connu le polynôme caractéristique $P_A \in \mathbb{Z}[\Pi]$ d'une variété abélienne A sur un corps fini k. Les facteurs irréductibles Q_i de P_A correspondent alors bijectivement aux facteurs simples A_i de A. Le centre F_i du corps gauche $D_i = \mathrm{End}_k^0(A_i)$ est canoniquement isomorphe à $\mathbb{Q}[\Pi]/Q_i$, par l'application $\Pi \mapsto \pi_{A_i}$. C'est une extension de degré $f_i = \deg(Q_i)$ de $\mathbb{Q}$. La classe de D_i dans le groupe de Brauer de F_i est entièrement déterminée par la proposition ci-dessus. L'ordre de cette classe est égal à $d_i = [D_i : F_i]^{\frac{1}{2}}$. Le polynôme caractéristique de A_i est donc $P_{A_i} = Q_i^{d_i}$, et $P_A = \prod Q_i^{d_i r_i}$ si $A \sim \oplus A_i^{r_i}$. La multiplicité r_i de A_i dans A est ainsi donnée par la formule $r_i d_i = \mathrm{ord}_{Q_i}(P_A)$. On retrouve donc bien

$$\deg(P_A) = \sum \deg(Q_i^{d_i r_i}) = \sum r_i \cdot f_i d_i = \sum r_i \cdot 2\dim(A_i) = 2\dim(A).$$

Enfin, $\mathrm{End}_k^0(A) \simeq \prod M_{r_i}(D_i)$.

3. Le théorème de Honda

Disons qu'un q-nombre de Weil $\pi \in \mathcal{W}(q)$ est effectif si et seulement si il est conjugué au Frobenius d'une variété abélienne simple A sur $\mathbb{F}_q$. Le théorème de Honda dit tout simplement que

Theorem 44. [4, 12] *Tous les nombres de Weil sont effectifs.*

Corollary 45. *L'application* $w : \mathcal{S}(q) \to \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})\backslash\mathcal{W}(q)$ *est bijective.*

3.1. Préliminaires.

Lemma 46. *Soit* $\pi \in \mathcal{W}(q)$ *et* $n \geq 1$. *Alors* $\pi^n \in \mathcal{W}(q^n)$ *et*

$$\pi \text{ est effectif } \iff \pi^n \text{ est effectif.}$$

Démonstration. Soient $k = \mathbb{F}_q$ et $k' = \mathbb{F}_{q^n}$. Si π est effectif, il existe une variété abélienne A sur k telle que $P_A(\pi) = 0$. Alors $P_{A'}(\pi^n) = 0$ où $A' = A \times_k k'$, donc π^n est effectif. Si inversement π^n est effectif, il existe une variété abélienne A' sur k' telle que $P_{A'}(\pi^n) = 0$. La restriction de Weil $A = \mathrm{Res}_k^{k'} A'$ est une variété abélienne sur k avec $P_A(X) = P_{A'}(X^n)$, donc $P_A(\pi) = P_{A'}(\pi^n) = 0$ et π est effectif. □

Pour montrer qu'un q-nombre de Weil π est effectif, il nous faut construire une variété abélienne simple A sur $k = \mathbb{F}_q$ dont le Frobenius soit conjugué à π. On sait déjà ce que doit être l'anneau des endomorphismes $\mathrm{End}_k^0(A)$ d'une telle variété abélienne : un corps gauche $D = D(\pi)$ de centre $F = \mathbb{Q}(\pi)$ dont les invariants sont décrits dans la proposition 42. Nous reconstruirons ci-dessous ce corps ex-nihilo, puis nous choisirons dans D un corps CM E, et sur E un type CM Φ, puis une variété abélienne de type CM (E, Φ) sur un corps de nombres suffisamment large, ayant bonne réduction en une place convenable de ce corps de nombres, dont le corps résiduel soit une extension $k' = \mathbb{F}_{q^n}$ de k, et telle que le Frobenius de la réduction de cette variété abélienne soit précisément égal à π^n. Alors A sera, d'après la preuve du lemme ci-dessus, l'un des facteurs simples de la restriction à la Weil (de k' vers k) de la réduction de cette variété abélienne CM.

On fixe pour tout la suite de cette section un q-nombre de Weil π. On note $P \in \mathbb{Z}[X]$ son polynôme minimal (unitaire, irréductible).

3.2. Le corps $F = \mathbb{Q}(\pi)$.

On pose $F = \mathbb{Q}(\pi)$. Pour tout plongement $\phi : F \hookrightarrow \mathbb{C}$,

$$\overline{\phi(\pi)} = \frac{\phi(\pi) \cdot \overline{\phi(\pi)}}{\phi(\pi)} = \frac{q}{\phi(\pi)} = \phi\left(\frac{q}{\pi}\right)$$

donc

$$0 = \overline{\phi}(P(\pi)) = P\left(\overline{\phi}(\pi)\right) = P\left(\phi\left(\frac{q}{\pi}\right)\right) = \phi\left(P\left(\frac{q}{\pi}\right)\right)$$

de sorte que $\frac{q}{\pi}$ est encore une racine de P. Soit $\star$ l'automorphisme de F qui envoie π sur $\frac{q}{\pi}$. C'est évidemment une involution de F, et puisque $\overline{\phi(\pi)} = \phi(\pi^\star)$ pour tout plongement $\phi : F \hookrightarrow \mathbb{C}$, on trouve l'une des deux possibilités suivantes :

(1) $\star \neq \mathrm{Id}$ sur F, donc F est un corps CM.

(2) $\star = \mathrm{Id}$ sur F, i.e. $\pi^2 = q$ donc $\pi = \pm\sqrt{q}$. Si $q = p^{2a}$, on obtient deux orbites galoisiennes triviales distinctes, à savoir celles de $\pi = \pm p^a$, pour lesquelles $F = \mathbb{Q}$ et $P = X \pm p^a$. Si $q = p^{2a+1}$, on obtient une seule orbite galoisienne non-triviale, $\pi \in \{\pm p^a\sqrt{p}\}$, pour laquelle $F = \mathbb{Q}(\sqrt{p})$.

3.3. **Le corps gauche $D = D(\pi)$.** Pour toute place v de $F = \mathbb{Q}(\pi)$ on note

$$\|-\|_v : F_v \to \mathbb{R}_{\geq}$$

la valuation normalisée en v et on définit $i_v(\pi) \in \mathbb{R}$ par $\|\pi\|_v = q^{-i_v(\pi)}$. Puisque $\|\pi\|_v = q^{\frac{[F_v:\mathbb{R}]}{2}}$ pour $v \mid \infty$, la formule du produit $\prod \|-\|_v = 1$ montre que

$$i_v(\pi) \neq 0 \iff \|\pi\|_v \neq 1 \Longrightarrow v \mid p\infty.$$

On a d'autre part $i_v(\pi) = -\frac{[F_v:\mathbb{R}]}{2}$ pour $v \mid \infty$, et

$$i_v(\pi) = \frac{v(\pi)}{v(q)} \cdot [F_v : \mathbb{Q}_p] \in \mathbb{Q} \quad \text{pour } v \mid p.$$

On note $D(\pi)$ un corps gauche de centre F tel que

$$\forall v \text{ de } F : \qquad \mathrm{inv}_v D(\pi) = i_v(\pi) \quad \text{dans } \mathbb{Q}/\mathbb{Z}.$$

Vérifions qu'un tel corps existe bien. Si $F = \mathbb{Q}$, donc $\pi = \pm p^a$ et $q = p^{2a}$, on a $i_v(\pi) = \frac{1}{2} \bmod \mathbb{Z}$ pour $v \mid p\infty$ et 0 sinon : $D(\pi)$ est alors le corps de quaternion $B_{p,\infty}$ sur $\mathbb{Q}$ tel que $\mathrm{Ram}(B_{p,\infty}) = \{p, \infty\}$. Si $F = \mathbb{Q}(\sqrt{p})$, donc $\pi = \pm p^a\sqrt{p}$ et $q = p^{2a+1}$, on a $i_v(\pi) = \frac{1}{2} \bmod \mathbb{Z}$ pour $v \mid \infty$ et 0 sinon : $D(\pi)$ est alors le corps de quaternion B_{∞_1,∞_2} sur $\mathbb{Q}(\sqrt{p})$ tel que $\mathrm{Ram}(B_{\infty_1,\infty_2}) = \{\infty_1, \infty_2\}$. Dans tous les autres cas, F est un corps CM (donc sans place réelle), et il faut voir que

$$\sum_{v|p} \frac{v(\pi)}{v(q)} \cdot [F_v : \mathbb{Q}_p] = \sum_{v \neq v^\star} \frac{v(\pi) + v^\star(\pi)}{v(q)} \cdot [F_v : \mathbb{Q}_p] + \sum_{v = v^\star} \frac{v(\pi)}{v(q)} \cdot [F_v : \mathbb{Q}_p] \in \mathbb{Z}.$$

Or $v(\pi) + v(\pi^\star) = v(\pi\pi^\star) = v(q)$ dans tous les cas, et si $v = v^\star$, alors $2 \mid [F_v : \mathbb{Q}_p]$: la somme ci-dessus est donc bien dans $\mathbb{Z}$.

3.4. **Un corps CM $E \subset D(\pi)$.** On note $D = D(\pi)$, $i_v = i_v(\pi)$ et $d^2 = [D : F]$, de sorte que d est le plus petit multiple commun des dénominateurs des i_v.

Lemma 47. *Il existe des corps CM $F \subset E \subset D$ avec $[E : F] = d$.*

Démonstration. On traite à nouveau séparément les cas où F n'est pas CM, qui sont faciles. Si F est CM de sous-corps totalement réel F_0, on choisit une extension E_0 de F_0 qui est (1) de degré d, (2) totalement réelle, et (3) telle que pour toute place $v \neq v^\star$ de F sur p, pour toute place w de E_0 au-dessus de $v|F_0$, $[E_{0,w} : F_{0,v}] \cdot i_v \in \mathbb{Z}$. Alors $E = E_0 \cdot F$ est un corps CM de degré d, et pour toute place $w \mid p$ de E au dessus de $v = w|F$,

$$\mathrm{inv}_w(D \otimes_F E) = \mathrm{inv}_w(D_v \otimes_{F_v} E_w) = [E_w : F_v] \cdot i_v \in \mathbb{Z},$$

car $i_v = 0$ si $v = v^\star$ tandis que $[E_w : F_v] = [E_{0,w} : F_{0,v}]$ si $v \neq v^\star$. Donc E décompose D, et puisque $[D : F] = d^2 = [E : F]^2$, E se plonge dans D. □

Remark 48. On peut aussi d'abord montrer que $D(\pi)$ admet une involution positive, puis choisir dans $D(\pi)$ un sous-corps commutatif maximal et stable par cette involution : un tel corps est automatiquement CM.

3.5. **Un type CM Φ sur E.** On fixe un plongement $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$. On a alors :

$$\mathrm{Hom}_{\mathbb{Q}-alg}(E, \mathbb{C}) = \mathrm{Hom}_{\mathbb{Q}_p-alg}(E \otimes \mathbb{Q}_p, \overline{\mathbb{Q}}_p) = \coprod_{w|p} H(w)$$

où w décrit les places de E au-dessus de p, donc $E \otimes \mathbb{Q}_p = \prod_{w|p} E_w$, avec

$$H(w) = \mathrm{Hom}_{\mathbb{Q}_p-alg}(E_w, \overline{\mathbb{Q}}_p).$$

Lemma 49. *Il existe un type CM Φ sur E tel que pour tout $w \mid p$,*

$$\frac{w(\pi)}{w(q)} = \frac{|H(w) \cap \Phi|}{|H(w)|}.$$

Démonstration. On veut que pour tout $w \mid p$ de E sur v de F,

$$|H(w) \cap \Phi| = |H(w)| \cdot \frac{w(\pi)}{w(q)} = [E_w : \mathbb{Q}_p] \cdot \frac{v(\pi)}{v(q)} = [E_w : F_v] \cdot i_v.$$

Si $w^\star = w$, $v^\star = v$ et $[E_w : F_v] \cdot i_v = \frac{1}{2}[E_w : \mathbb{Q}_p] = \frac{1}{2}|H(w)|$: on choisit pour $\Phi \cap H(w)$ un système de représentants (quelconque) des orbites de $\star$ dans $H(w)$. Si $w^\star \neq w$, on a

$$[E_w : F_v] \cdot i_v + [E_{w^\star} : F_{v^\star}] \cdot i_{v^\star} = [E_w : \mathbb{Q}_p] = |H(w)| = |H(w^\star)|.$$

On choisit alors pour $\Phi \cap (H(w) \coprod H(w^\star))$ un système de représentant des orbites de $\star$ tel que $\Phi \cap H(w)$ contienne $[E_w : F_v] \cdot i_v$ éléments, et alors $\Phi \cap H(w^\star)$ en contient bien $[E_{w^\star} : F_{v^\star}] \cdot i_{v^\star}$éléments. □

3.6. **Conclusion.** Soit (E, Φ) comme ci-dessus, $k \subset \overline{\mathbb{Q}}$ une extension finie de $\mathbb{Q}$ telle que $\phi(E) \subset k$ pour tout $\phi \in \Phi$. Quitte à agrandir k, on peut supposer que (1) il existe sur k une variété abélienne A de type CM (E, Φ) à multiplication complexe par $\mathcal{O}_E$, que (2) A a bonne réduction en la place P de $\mathcal{O}_k$ déterminée par le plongement $\overline{\mathbb{Q}} \hookrightarrow \mathbb{Q}_p$ fixé plus haut, et que (3) $\mathcal{O}_k/P = \mathbb{F}_{q^n}$. D'après la formule de Shimura-Tanyiama, le Frobenius de la réduction de A en P est un élément π_1 de $\mathcal{O}_E$ tel que pour tout $w \mid p$ de E,

$$\frac{w(\pi_1)}{w(q^n)} = \frac{|H(w) \cap \Phi|}{|H(w)|} = \frac{w(\pi^n)}{w(q^n)}.$$

Les idéaux engendrés dans $\mathcal{O}_E$ par $\pi_1 \in \mathcal{O}_E$ et $\pi^n \in \mathcal{O}_F \subset \mathcal{O}_E$ sont alors égaux, donc $\pi_1 = u\pi^n$ pour une unité u de $\mathcal{O}_E^\times$. Puisque π_1 et π^n sont des q^n-nombres de Weil, u est un $q^0 = 1$-nombre de Weil, c'est-à-dire une racine de l'unité. Donc pour un entier m convenable, $\pi_1^m = \pi^{nm}$. Puisque enfin π_1^m est effectif, π l'est également.

4. Exemples sur un corps fini

Dans les exemples qui suivent, on note typiquement A une variété abélienne, le plus souvent simple, sur un corps fini k de cardinal $q = p^\nu$, π son Frobenius, $F = \mathbb{Q}(\pi)$ le centre du corps gauche $D = \mathrm{End}_k^0(A)$, g la dimension de A, $f = [F : \mathbb{Q}]$ et $d = [D : F]^{1/2}$, de sorte que $2g = df$.

4.1. **Cas où F est totalement réel.** Ce cas regroupe deux situations différentes.

4.1.1. *Le cas pair.* Si $q = p^{2a}$ pour un entier $a \geq 1$, alors

$$\pi = +p^a \text{ ou } -p^a, \quad F = \mathbb{Q}, \quad D = B_{p,\infty} \quad \text{et} \quad g = 1,$$

où $B_{p,\infty}$ est le corps de quaternions ramifié en $\{p, \infty\}$. C'est donc le cas où A est une courbe elliptique supersingulière dont tous les endomorphismes sont définis sur $k = \mathbb{F}_q$. On peut construire toutes ces courbes de la manière suivante.

Soit H l'extension abélienne partout non-ramifiée maximale de $K = \mathbb{Q}(\sqrt{-p})$, $\mathcal{O}_K$ et $\mathcal{O}_H$ les anneaux d'entiers de K et H, P_K l'unique idéal maximal de $\mathcal{O}_K$ au-dessus de p, et P_H un idéal maximal de $\mathcal{O}_H$ au dessus de P_K. Puisque $P_K = \mathcal{O}_K\sqrt{-p}$ est un idéal principal de corps résiduel $\mathbb{F}_p$, cet idéal est totalement décomposé dans $\mathcal{O}_H$, et le corps résiduel de P_H est encore $\mathbb{F}_p$. La théorie de la multiplication complexe montre que la courbe elliptique $\mathbb{C}/\mathcal{O}_K$ admet un modèle E sur H qui a partout bonne réduction. On note E_0 la fibre spéciale en P_H du modèle de Néron de E sur $\mathcal{O}_H$. C'est donc une courbe elliptique sur $\mathbb{F}_p$, munie d'une action de $\mathcal{O}_K$. La formule de Shimura-Tanyiama décrit l'idéal engendré par son Frobenius π_0 dans $\mathcal{O}_K$: c'est $\mathcal{O}_K\pi_0 = P_K$, d'où l'on déduit que $\pi_0 = \mu\sqrt{-p}$ pour une unité $\mu \in \mathcal{O}_K^\times$. Si $p \neq 3$, on a donc $\mu \in \{\pm 1\}$. Si $p = 3$, on peut aussi supposer que cette condition est satisfaite – quitte à remplacer E_0 par un twist convenable. On a alors, et dans tous les cas, $\pi_0^{2a} = (-p)^a$.

La classe d'isogénie déterminée par le q-nombre de Weil $(-p)^a$ est donc celle de $E_0 \times_{\mathbb{F}_p} \mathbb{F}_{p^{2a}}$. L'autre classe d'isogénie, qui correspond au q-nombre de Weil $-(-p)^a$, est d'après la preuve du lemme 46 celle du noyau du morphisme trace

$$\mathrm{Res}^{\mathbb{F}_{p^{4a}}}_{\mathbb{F}_{p^{2a}}}\left(E_0 \times_{\mathbb{F}_p} \mathbb{F}_{p^{4a}}\right) \twoheadrightarrow E_0 \times_{\mathbb{F}_p} \mathbb{F}_{p^{2a}}.$$

Si $a = 2^m a'$ avec $2 \nmid a'$ et $m \geq 0$, on note que ce morphisme s'identifie à

$$\left[\mathrm{Res}^{\mathbb{F}_{p^{2^{m+2}}}}_{\mathbb{F}_{p^{2^{m+1}}}}\left(E_0 \times_{\mathbb{F}_p} \mathbb{F}_{p^{2^{m+2}}}\right) \twoheadrightarrow E_0 \times_{\mathbb{F}_p} \mathbb{F}_{p^{2^{m+1}}}\right] \times_{\mathbb{F}_{p^{2^{m+1}}}} \mathbb{F}_{p^{2a}}.$$

Notant E_{m+1} la courbe elliptique sur $\mathbb{F}_{p^{2^{m+1}}}$ qui est le noyau du morphisme trace ci-dessus entre crochet, on voit donc que les $\{E_m, m \in \mathbb{N}\}$ recouvrent toutes les classes d'isogénies ici considérées. Plus précisément :

Fact 50. *Les deux classes d'isogénies de courbes elliptiques supersingulières sur $\mathbb{F}_q$ ayant tous leurs endomorphismes définis sur $\mathbb{F}_q$ sont représentées par*

$$E_0 \times_{\mathbb{F}_p} \mathbb{F}_q \quad \textit{pour } \pi = (-p)^a \quad \textit{et} \quad E_{m+1} \times_{\mathbb{F}_{p^{2^{m+1}}}} \mathbb{F}_q \quad \textit{pour } \pi = -(-p)^a$$

où $q = p^{2a}$ et $a = 2^m a'$ avec $2 \nmid a'$. Chacune de ces deux classes fusionne avec la classe d'isogénie où $\pi = q$ après le changement de base quadratique $\mathbb{F}_q \to \mathbb{F}_{q^2}$.

4.1.2. *Le cas impair.* Si $q = p^{2a+1}$ pour un entier $a \geq 0$, alors

$$\pi \in \{\pm p^a\sqrt{p}\}, \quad F = \mathbb{Q}(\sqrt{p}), \quad D = B_{\infty_1,\infty_2} \quad \text{et} \quad g = 2,$$

où B_{∞_1,∞_2} est le corps de quaternions ramifié en $\{\infty_1, \infty_2\}$. Avec les notations ci-dessus, cette classe d'isogénie est représentée par la surface abélienne simple

$$\mathrm{Res}^{\mathbb{F}_{q^2}}_{\mathbb{F}_q}\left(E_1 \times_{\mathbb{F}_{p^2}} \mathbb{F}_{q^2}\right) = \mathrm{Res}^{\mathbb{F}_{p^2}}_{\mathbb{F}_p}(E_1) \times_{\mathbb{F}_p} \mathbb{F}_q.$$

Cette surface abélienne n'est pas absolument simple : elle devient isogène au carré de $E_1 \times_{\mathbb{F}_{p^2}} \mathbb{F}_{q^2}$ sur l'extension quadratique $\mathbb{F}_{q^2}$ de $\mathbb{F}_q$.

4.2. **Les courbes elliptiques.** Si A est une courbe elliptique, alors

$$[D : F]^{\frac{1}{2}}[F : \mathbb{Q}] = 2$$

donc (1) D est un corps de quaternions sur $F = \mathbb{Q}$, ou bien (2) $D = F$ est une extension quadratique de $\mathbb{Q}$. Le premier cas a déjà été traité ci-dessus : il n'existe que pour $q = p^{2a}$, et correspond aux deux classes d'isogénies de courbes elliptiques supersingulières dont tous les endomorphismes sont définis sur $k = \mathbb{F}_q$.

Dans le second cas, auquel on se restreint désormais, l'extension quadratique F est forcément imaginaire, le cas d'une extension réelle étant exclu par la discussion précédente. Si p est inerte ou ramifié dans F, une puissance convenable de π est dans $\mathbb{Q}$, donc A est une courbe elliptique supersingulière, mais qui n'acquiert tous ces endomorphismes qu'après une extension non-triviale du corps de base k. Si au contraire p est décomposé dans F, alors F ne se plonge pas dans $B_{p,\infty}$, et A n'est pas supersingulière : on dit que la courbe elliptique A est ordinaire.

Considérons d'abord le cas supersingulier, où p est inerte ou ramifié dans F. Si $\nu = 2a$, alors $\pi = \mu p^a$ pour une racine de l'unité $\mu \neq \pm 1$ dans $F = \mathbb{Q}(\pi)$, donc $F = \mathbb{Q}(i)$ et $\mu \in \{\pm i\}$, ou bien $F = \mathbb{Q}(\rho)$ et $\mu \in \{\pm\rho, \pm\rho^2\}$. Si au contraire $\nu = 2a+1$, il faut que p soit ramifié dans F puisque π y engendre un idéal de norme $q = p^\nu$. Donc $(p) = \mathfrak{P}^2$ et $(\pi) = \mathfrak{P}^\nu$ pour l'unique idéal $\mathfrak{P}$ de $\mathcal{O}_F$ au-dessus de p, qui doit être principal puisque ν est impair. Si $F \neq \mathbb{Q}(i), \mathbb{Q}(\rho)$, il faut donc que $F = \mathbb{Q}(\sqrt{-p})$ avec $\pi \in \{\pm p^a\sqrt{-p}\}$. Il reste enfin les cas pathologiques : $F = \mathbb{Q}(i)$ avec $p = 2$, et $F = \mathbb{Q}(\rho) = \mathbb{Q}(\sqrt{-3})$ avec $p = 3$: ils sont décrits dans le tableau suivant, qui liste toutes les classes d'isogénie de courbes elliptiques supersingulières A dont l'anneau des endomorphismes $\mathrm{End}^0_k(A) \simeq F$ est commutatif, c'est-à-dire strictement contenu dans $\mathrm{End}^0_{\bar{k}}(A) \simeq B_{p,\infty}$. On y donne aussi l'entier r qui est le degré de la plus petite extension k' de $k = \mathbb{F}_q$ telle que $\mathrm{End}^0_{k'}(A) \simeq B_{p,\infty}$.

q	F	π	r
p^{2a} avec $p = 2$ ou $p \equiv 3 \bmod 4$	$\mathbb{Q}(i)$	ip^a	2
p^{2a} avec $p = 3$ ou $p \equiv 2 \bmod 3$	$\mathbb{Q}(\rho)$	ρp^a, $\rho^2 p^a$	3
2^{2a+1}	$\mathbb{Q}(i)$	$2^a(i+1)$, $2^a(i-1)$	4
3^{2a+1}	$\mathbb{Q}(\rho)$	$3^a(1+\rho)$, $3^a(-1-\rho)$	6
p^{2a+1}	$\mathbb{Q}(\sqrt{-p})$	$p^a\sqrt{-p}$	2

Passant au cas ordinaire, notons $\mathfrak{P}_1 \neq \mathfrak{P}_2$ les idéaux premiers de $\mathcal{O}_F$ au-dessus de p. Si $(\pi) = \mathfrak{P}_1^{\nu_1}\mathfrak{P}_2^{\nu_2}$ et $q = p^\nu$, on sait que

$$\nu_1 + \nu_2 = \nu \quad \text{et} \quad \frac{\nu_1}{\nu} \equiv \frac{\nu_2}{\nu} \equiv 0 \text{ dans } \mathbb{Q}/\mathbb{Z}.$$

Donc $(\nu_1, \nu_2) = (\nu, 0)$ ou $(0, \nu)$. Inversement, soit F un corps quadratique imaginaire où p est décomposé, $\mathfrak{P}$ l'un des deux idéaux de $\mathcal{O}_F$ au-dessus de p, et $\nu_p(F)$ l'ordre de la classe de $\mathfrak{P}$ dans $\mathrm{Pic}(\mathcal{O}_F)$. Alors pour tout entier ν divsible par $\nu_p(F)$, chaque générateur π de $\mathfrak{P}^\nu$ est un $q = p^\nu$-nombre de Weil qui correspond à une classe d'isogénie de courbes elliptiques ordinaires sur $k = \mathbb{F}_q$. Pour $F \neq \mathbb{Q}(i), \mathbb{Q}(\rho)$, on obtient ainsi exactement deux classes d'isogénie associées à F. On en obtient évidemment 4 pour $F = \mathbb{Q}(i)$ et 6 pour $F = \mathbb{Q}(\rho)$.

4.3. **Les surfaces abéliennes.** Lorsque A est (simple) et de dimension 2, on a

$$4 = [D : F]^{1/2}[F : \mathbb{Q}].$$

Le seul cas où F est totalement réel est celui de $\pi = \pm p^a\sqrt{p}$ pour $q = p^{2a+1}$, qui correspond à une surface abélienne simple sur $\mathbb{F}_q$ qui devient isogène au produit de deux courbes elliptiques supersingulières de Frobenius $\pi^2 = p^{2a+1}$ sur $\mathbb{F}_{q^2}$. On peut donc supposer que F est un corps CM, ce qui nous donne deux cas.

4.3.1. F est une extension quadratique imaginaire de $\mathbb{Q}$ et D est un corps de quaternion sur F. Puisque D ne peut être ramifié qu'aux places de F qui divisent p et que D est effectivement ramifié en un nombre strictement positif et pair de places de F, on voit donc que $(p) = \mathfrak{P}_1\cdot\mathfrak{P}_2$ est décomposé dans F, et $\mathrm{Ram}(D) = \{\mathfrak{P}_1, \mathfrak{P}_2\}$. Si $(\pi) = \mathfrak{P}_1^{\nu_1}\mathfrak{P}_2^{\nu_2}$, il faut alors que

$$\frac{\nu_1}{\nu} \equiv \frac{\nu_2}{\nu} \equiv \frac{1}{2} \in \mathbb{Q}/\mathbb{Z} \quad \text{avec } \nu_1 + \nu_2 = \nu$$

donc $\nu = 2a$ est pair, $\nu_1 = \nu_2 = a$, et $\pi = \mu p^a$ pour une racine de l'unité $\mu \neq \pm 1$ dans $F = \mathbb{Q}(\pi)$. On trouve donc $F = \mathbb{Q}(i)$ avec $p \equiv 1 \bmod 4$ et $\pi \in \{\pm ip^a\}$, ou bien $F = \mathbb{Q}(\rho)$ avec $p \equiv 1 \bmod 3$, et $\pi \in \{\rho p^a, -\rho^2 p^a\}$ ou $\pi \in \{\rho^2 p^a, -\rho p^a\}$. Dans ces trois cas, la surface abélienne devient isogène au produit de deux copies d'une même courbe elliptique supersingulière après une extension de degré 2 ou 3 du corps de base $k = \mathbb{F}_q$.

4.3.2. $F = D$ est une extension CM de degré 4 de $\mathbb{Q}$. Si $(\pi) = (\overline{\pi})$, alors $(\pi^2) = (q)$, donc $\pi^2 = \mu q$ pour une racine de l'unité dans F, et A devient isogène au produit de deux copies d'une même courbe elliptique supersingulière après une extension finie du corps de base. Si $(\pi) \neq (\overline{\pi})$, il y a au moins un idéal premier $\mathfrak{P} \mid p$ de F tel que $\mathfrak{P} \neq \overline{\mathfrak{P}}$, donc au moins un idéal $\mathfrak{p} \mid p$ du sous-corps totalement réel $L = \mathbb{Q}(\pi + \overline{\pi})$ de $F = \mathbb{Q}(\pi)$ qui se décompose dans F, avec $\mathfrak{p}\mathcal{O}_F = \mathfrak{P}\cdot\overline{\mathfrak{P}}$. Il y a alors différents cas selon la décomposition de p dans F. Le cas le plus notable est celui où la variété A n'est pas ordinaire : cela arrive uniquement lorsque p est déployé dans L mais pas totalement déployé dans F (i.e. $p\mathcal{O}_L = \mathfrak{p}\cdot\mathfrak{p}'$ avec $\mathfrak{p}'$ inerte ou ramifié dans L). Dans ce cas, l'extension $F/\mathbb{Q}$ n'est pas galoisienne, A est géométriquement simple, et son groupe p-divisible a trois pentes : 0 et 1 avec multiplicité 1, et $\frac{1}{2}$ avec multiplicité 2. Pour les détails, voir [5, Thm 3.6, 3.7].

4.4. **Classe d'isogénie unique de la fibre spéciale d'une courbe de Shimura.** Soit A une surface abélienne sur $k = \mathbb{F}_q$ munie de l'action $\iota : B \hookrightarrow \mathrm{End}_k^0(A)$ d'un corps de quaternions B sur $\mathbb{Q}$ qui est indéfini (i.e. déployé à l'infini) mais ramifié en p. Nous allons montrer que A devient isogène au carré d'une courbe elliptique supersingulière sur $\overline{k}$. C'est évidemment le cas si A est simple d'après la discussion ci-dessus, puisque la non-commutativité de B implique celle de $D = \mathrm{End}_k^0(A)$. Le même argument implique que $A \times_k \overline{k}$ ne saurait être le produit de deux courbes elliptiques non-isogènes. Enfin si E est une extension quadratique imaginaire de $\mathbb{Q}$ où p est décomposé, il n'y a pas de plongement de B dans $M_2(E)$, car B_p ne se plonge pas dans $M_2(E_p) \simeq M_2(\mathbb{Q}_p) \times M_2(\mathbb{Q}_p)$. Il ne reste donc qu'une possibilité pour $A \times_k \overline{k}$: c'est le carré d'une courbe elliptique supersingulière.

5. La catégorie $\mathbf{Ab}^0_{\mathbb{F}}$ pour $\mathbb{F} = \overline{\mathbb{F}}_p$

Soit $\mathbb{F} = \overline{\mathbb{F}}_p$ une cloture algébrique de $\mathbb{F}_p$. On note $(\mathcal{I}, \subset)$ l'ensemble réticulé des sous-corps finis k de $\mathbb{F}$, ordonné par l'inclusion. L'application $k \mapsto [k : \mathbb{F}_p]$ est donc une bijection croissante de $(\mathcal{I}, \subset)$ sur l'ensemble réticulé des entiers $n \geq 1$ ordonné par la relation de divisibilité. Puisque $\mathbb{F} = \cup_{k\in\mathcal{I}} k$, la théorie de la descente

et les résultats de [6, IV.8] permettent de ramener l'étude de la catégorie (abélienne semi-simple) des variétés abéliennes à isogénie près sur $\mathbb{F}$ à celle des catégories (abéliennes semi-simples) des variétés abéliennes à isogénie près sur les sous-corps finis k de $\mathbb{F}$, c'est-à-dire essentiellement, à la théorie de Honda-Tate.

5.1. **Les germes.** Si $(M, \times)$ est un monoïde (ou même seulement un magma), on note $\mathcal{G}(M)$ la limite inductive du foncteur $(\mathcal{I}, \subset) \to \mathbf{Ens}$ qui envoit k sur M et l'inclusion $k \subset k'$ sur l'application $x \mapsto x^{[k':k]}$. C'est aussi le quotient de l'ensemble des couples (x, k) avec $x \in M$ et $k \in \mathcal{I}$ pour la relation d'équivalence définie par $(x, k) \sim (x', k')$ si et seulement si il existe $k'' \in \mathcal{I}$ contenant k et k' tel que $x^{[k'':k]} = x'^{[k'':k']}$ dans M. On dit des éléments de $\mathcal{G}(M)$ que ce sont les germes d'éléments de M. Lorsque $(M, \times)$ est le monoïde multiplicatif $(R, \times)$ d'un anneau $(R, +, \times)$, on note simplement $\mathcal{G}(R) = \mathcal{G}(M)$. Si de plus R est une $\mathbb{Q}$-algèbre et $\alpha \in \mathcal{G}(R)$, on note $\mathbb{Q}[\alpha]$ la sous-algèbre de R qui est l'intersection des sous-algèbres $\mathbb{Q}[x]$ engendrées dans R par les éléments x des représentants (x, k) de α. Si l'on fixe un tel représentant, on a donc $\mathbb{Q}[\alpha] = \cap_{n>0}\mathbb{Q}[x^n]$. En particulier si R est de dimension finie sur $\mathbb{Q}$, $\mathbb{Q}[\alpha] = \mathbb{Q}[x^n]$ pour tout n assez grand. Si enfin v est une place de $\mathbb{Q}[\alpha]$ au dessus de p, le nombre rationnel $v(x)/v(|k|)$ est indépendant du choix du représentant (x, k) de α tel que $\mathbb{Q}[\alpha] = \mathbb{Q}[x]$. C'est la pente de α en v, que l'on note $\lambda_v(\alpha)$.

5.2. **Le Frobenius.** Soit maintenant A une variété abélienne sur $\mathbb{F}$. Un modèle de A sur un sous-corps fini k de $\mathbb{F}$ est une variété abélienne A_k sur k munie d'un isomorphisme $A_k \times_k \mathbb{F} \simeq A$. Puisque $\mathbb{F} = \cup_{k \in \mathcal{I}} k$, on sait que de tels modèles existent sur les sous-corps finis suffisament gros k de $\mathbb{F}$. De plus, si A_1 et A_2 sont des modèles de A définis respectivement sur des sous-corps finis k_1 et k_2 de $\mathbb{F}$, il existe un sous-corps fini k de $\mathbb{F}$ contenant k_1 et k_2 au-dessus duquel les modèles $A_1 \times_{k_1} k$ et $A_2 \times_{k_2} k$ sont isomorphes. Si π_1 et π_2 sont les images dans $\mathrm{End}_{\mathbb{F}}(A)$ des Frobenius $\pi_{A_1} \in \mathrm{End}_{k_1}(A_1)$ et $\pi_{A_2} \in \mathrm{End}_{k_2}(A_2)$, on a donc $\pi_1^{[k:k_1]} = \pi_2^{[k:k_2]}$, ce qui signifie encore que (π_1, k_1) et (π_2, k_2) définissent le même germe dans $\mathcal{G}(\mathrm{End}_{\mathbb{F}}(A))$.

Definition 51. Le Frobenius de A est le germe ainsi défini :

$$\pi_A = [\pi_1, k_1] \in \mathcal{G}\left(\mathrm{End}_{\mathbb{F}}(A)\right) \subset \mathcal{G}\left(\mathrm{End}^0_{\mathbb{F}}(A)\right).$$

Remark 52. Si $\alpha : A \to B$ est un morphisme de variétés abéliennes sur $\mathbb{F}$, alors $\alpha \circ \pi_A = \pi_B \circ \alpha$. De même, si $\dagger$ est une involution de Rosati sur $\mathrm{End}^0_{\mathbb{F}}(A)$, alors $\pi_A^\dagger \circ \pi_A = [p]$ dans $\mathcal{G}\left(\mathrm{End}^0_{\mathbb{F}}(A)\right)$, où $[p]$ est le germe réprésenté par $(|k|, k)$ pour tout $k \in \mathcal{I}$. On laisse au lecteur le soin de préciser le sens de ces deux assertions.

Proposition 53. *Pour toute place $v \mid p$ de $\mathbb{Q}[\pi_A] \subset \mathrm{End}^0_{\mathbb{F}}(A)$, le groupe v-divisible $A[v^\infty]$ de A est isocline de pente $\lambda_v(\pi_A) \in \mathbb{Q} \cap [0, 1]$.*

Démonstration. Cela résulte immédiatement de ***. □

5.3. **Les morphismes.** Soient A_1 et A_2 des variétés abéliennes sur $\mathbb{F}$, $A_{1,k}$ et $A_{2,k}$ des modèles de ces variétés sur un sous-corps fini k de $\mathbb{F}$, $\mathcal{I}(k)$ l'ensemble cofinal dans $\mathcal{I}$ des extensions finies de k dans $\mathbb{F}$. Pour $k' \in \mathcal{I}(k)$, on note $A_{1,k'} = A_{1,k} \times_k k'$ et $A_{2,k'} = A_{2,k} \times_k k'$ les modèles sur k' déduit de $A_{1,k}$ et $A_{2,k}$.

Lemma 54. *Pour $k' \in \mathcal{I}(k)$ et $k' \subset k'' \subset \mathbb{F}$, le morphisme de changement de base*

$$\alpha_{k'}^{k''} : \mathrm{Hom}_{k'}\left(A_{1,k'}, A_{2,k'}\right) \to \mathrm{Hom}_{k''}\left(A_{1,k''}, A_{2,k''}\right)$$

est injectif et son conoyau est sans torsion, nul si k' est suffisament gros.

Démonstration. La démonstration de la trivialité du noyau et de la torsion du conoyau est élementaire. D'autre part, il résulte de [6, Théorème 8.8.2] que les morphismes de changement de base $\alpha_{k'}^{\mathbb{F}}$ induisent un isomorphisme

$$\varinjlim \mathrm{Hom}_{k'}\left(A_{1,k'}, A_{2,k'}\right) \to \mathrm{Hom}_{\mathbb{F}}\left(A_1, A_2\right)$$

Puisque le second de ces deux groupes est un $\mathbb{Z}$-module de type fini d'après ***, on en déduit que $\alpha_{k'}^{\mathbb{F}}$ est un isomorphisme pour tout k' suffisament gros. □

Proposition 55. *La sous-algèbre $F = \mathbb{Q}[\pi_A]$ est le centre de $D = \mathrm{End}_{\mathbb{F}}^0(A)$. Si A est simple, D est un corps gauche de centre F et pour toute place v de F,*

$$\mathrm{inv}_v D = \begin{cases} 0 & \text{si } v \nmid p\infty \\ \frac{1}{2} & \text{si } v \text{ est réelle} \\ \lambda_v(\pi_A) \cdot [F_v : \mathbb{Q}_p] & \text{si } v \mid p \end{cases} \qquad \text{dans } \mathbb{Q}/\mathbb{Z}.$$

Démonstration. Le lemme précédent nous ramène immédiatement au cas des corps fini, c'est-à-dire aux propositions 41 et 42. □

5.4. **Les groupes ℓ-divisibles.** Pour tout nombre premier ℓ, on vérifie facilement que le morphisme de changement de base

$$\alpha_{k'}^{k''} : \mathrm{Hom}_{k'}\left(A_{1,k'}[\ell^\infty], A_{2,k'}[\ell^\infty]\right) \to \mathrm{Hom}_{k''}\left(A_{1,k''}[\ell^\infty], A_{2,k''}[\ell^\infty]\right)$$

est encore injectif avec un conoyau sans torsion, mais le conoyau de

$$\alpha_{k'}^{\mathbb{F}} : \mathrm{Hom}_{k'}\left(A_{1,k'}[\ell^\infty], A_{2,k'}[\ell^\infty]\right) \hookrightarrow \mathrm{Hom}_{\mathbb{F}}\left(A_1[\ell^\infty], A_2[\ell^\infty]\right)$$

peut être non-nul pour tout $k' \in \mathcal{I}(k)$: s'il est encore vrai que pour tout $n \geq 1$,

$$\varinjlim_{k'} \mathrm{Hom}_{k'}\left(A_{1,k'}[\ell^n], A_{2,k'}[\ell^n]\right) = \mathrm{Hom}_{\mathbb{F}}\left(A_1[\ell^n], A_2[\ell^n]\right)$$

d'après [6, Théorème 8.8.2], ces limites ne commutent généralement pas à celles de

$$\varprojlim_n \mathrm{Hom}_{\mathbb{F}}\left(A_1[\ell^n], A_2[\ell^n]\right) = \mathrm{Hom}_{\mathbb{F}}\left(A_1[\ell^\infty], A_2[\ell^\infty]\right).$$

On peut cependant décrire l'image

$$\mathrm{Hom}_{\mathbb{F}}^{alg}\left(A_1[\ell^\infty], A_2[\ell^\infty]\right) \subset \mathrm{Hom}_{\mathbb{F}}\left(A_1[\ell^\infty], A_2[\ell^\infty]\right)$$

du morphisme injectif de $\mathbb{Z}_\ell$-module

$$\varinjlim_{k'}(\alpha_{k'}^{\mathbb{F}}) : \varinjlim_{k'} \mathrm{Hom}_{k'}\left(A_{1,k'}[\ell^\infty], A_{2,k'}[\ell^\infty]\right) \hookrightarrow \mathrm{Hom}_{\mathbb{F}}\left(A_1[\ell^\infty], A_2[\ell^\infty]\right).$$

Tout d'abord, les isomorphismes du théorème de Tate

$$\rho_\ell : \mathrm{Hom}_{k'}\left(A_{1,k'}, A_{2,k'}\right) \otimes \mathbb{Z}_\ell \xrightarrow{\simeq} \mathrm{Hom}_{k'}\left(A_{1,k'}[\ell^\infty], A_{2,k'}[\ell^\infty]\right)$$

donnent par passage à la limite un isomorphisme

$$\rho_\ell : \mathrm{Hom}_{\mathbb{F}}\left(A_1, A_2\right) \otimes \mathbb{Z}_\ell \xrightarrow{\simeq} \mathrm{Hom}_{\mathbb{F}}^{alg}\left(A_1[\ell^\infty], A_2[\ell^\infty]\right).$$

En particulier, pour tout $k' \in \mathcal{I}(k)$ tel que

$$\alpha_{k'}^{\mathbb{F}} : \mathrm{Hom}_{k'}\left(A_{1,k'}, A_{2,k'}\right) \otimes \mathbb{Z}_\ell \xrightarrow{\simeq} \mathrm{Hom}_{\mathbb{F}}\left(A_1, A_2\right) \otimes \mathbb{Z}_\ell$$

on a aussi pour les groupes ℓ-divisibles

$$\alpha_{k'}^{\mathbb{F}} : \mathrm{Hom}_{k'}\left(A_{1,k'}[\ell^\infty], A_{2,k'}[\ell^\infty]\right) \xrightarrow{\simeq} \mathrm{Hom}_{\mathbb{F}}^{alg}\left(A_1[\ell^\infty], A_2[\ell^\infty]\right).$$

Pour $k' \in \mathcal{I}(k)$ et $i \in \{1, 2\}$, on note $\pi_{i,k'} = \alpha_{k'}^{\mathbb{F}}(\pi_{A_{i,k'}})$ l'image du Frobenius.

Lemma 56. *Pour tout morphisme $f \in \mathrm{Hom}_{\mathbb{F}}\left(A_1[\ell^\infty], A_2[\ell^\infty]\right)$, les conditions suivantes sont équivalentes :*

(1) *Il existe* $k' \in \mathcal{I}(k)$ *tel que* $f \circ \pi_{1,k'} = \pi_{2,k'} \circ f$,

(2) *Pour tout* $k' \in \mathcal{I}(k)$ *suffisament gros,* $f \circ \pi_{1,k'} = \pi_{2,k'} \circ f$,

(3) f *appartient à* $\mathrm{Hom}_{\mathbb{F}}^{alg}(A_1[\ell^\infty], A_2[\ell^\infty])$,

(4) f *appartient à* $\rho_\ell(\mathrm{Hom}_{\mathbb{F}}(A_1, A_2) \otimes \mathbb{Z}_\ell)$.

Démonstration. L'équivalence de (3) et (4) est démontrée ci-dessus, celle de (1) et (2) est immédiate, de même que l'implication (3) $\Rightarrow$ (1). Il reste à démontrer que (1) $\Rightarrow$ (3), supposons donc que $f \circ \pi_{1,k'} = \pi_{2,k'} \circ f$ pour un corps fini $k' \in \mathcal{I}(k)$, et montrons qu'alors $f = \alpha_{k'}^{\mathbb{F}}(f_1)$ pour un morphisme $f_1 : A_{1,k'}[\ell^\infty] \to A_{2,k'}[\ell^\infty]$. On peut supposer que $k' = k$. Si $\ell \neq p$, il s'agit de vérifier que le morphisme induit par f sur les modules de Tate commute à l'action de $\mathrm{Gal}(\mathbb{F}/k)$, ce qui résulte facilement de l'hypothèse. Si $\ell = p$, on note $\mathbb{D}_i = \mathbb{D}(A_{i,k})$ le module de Dieudonné de $A_{i,k}$, un $W(k)$-module libre avec un Frobenius F_i et un Verschiebung V_i. Le morphisme de groupes p-divisibles $f : A_1[p^\infty] \to A_2[p^\infty]$ induit un morphisme $W(\mathbb{F})$-linéaire

$$\mathbb{D}(f) : \mathbb{D}_2 \otimes_{W(k)} W(\mathbb{F}) \to \mathbb{D}_1 \otimes_{W(k)} W(\mathbb{F})$$

qui commute avec les Frobenius et les Verschiebung respectifs, i.e.

$$\begin{aligned} \mathbb{D}(f) \circ (F_2 \otimes \sigma) &= (F_1 \otimes \sigma) \circ \mathbb{D}(f) \\ \mathbb{D}(f) \circ \left(V_2 \otimes \sigma^{-1}\right) &= \left(V_1 \otimes \sigma^{-1}\right) \circ \mathbb{D}(f) \end{aligned}$$

où σ est le Frobenius arithmétique de $W(\mathbb{F})$. Notre hypothèse implique aussi que

$$\mathbb{D}(f) \circ \left(F_2^{[k:\mathbb{F}_p]} \otimes \mathrm{Id}\right) = \left(F_1^{[k:\mathbb{F}_p]} \otimes \mathrm{Id}\right) \circ \mathbb{D}(f).$$

On en déduit que $\mathbb{D}(f)$ commute aussi à $\mathrm{Id} \otimes \sigma^{[k:\mathbb{F}_p]}$, puisque

$$\begin{aligned} &\left(F_1^{[k:\mathbb{F}_p]} \otimes \mathrm{Id}\right) \left[\mathbb{D}(f) \circ \left(\mathrm{Id} \otimes \sigma^{[k:\mathbb{F}_p]}\right) - \left(\mathrm{Id} \otimes \sigma^{[k:\mathbb{F}_p]}\right) \circ \mathbb{D}(f)\right] \\ &\quad = \mathbb{D}(f) \circ (F_2 \otimes \sigma)^{[k:\mathbb{F}_p]} - (F_1 \otimes \sigma)^{[k:\mathbb{F}_p]} \circ \mathbb{D}(f) = 0 \end{aligned}$$

avec $F_1^{[k:\mathbb{F}_p]} \otimes \mathrm{Id}$ injectif. Mais alors $\mathbb{D}(f)$ provient par extension des scalaires de $W(k)$ à $W(\mathbb{F})$ d'un morphisme $\mathbb{D}(f_1) : \mathbb{D}_2 \to \mathbb{D}_1$, pour un morphisme de groupes p-divisibles $f_1 : A_{1,k}[p^\infty] \to A_{2,k}[p^\infty]$ tel que $\alpha_k^{\mathbb{F}}(f_1) = f$. □

Example 57. Si E est une courbe elliptique ordinaire sur $\mathbb{F}$ et $\ell \neq p$,

$$\mathrm{End}_{\mathbb{F}}(E) \otimes \mathbb{Z}_\ell \simeq \mathrm{End}_{\mathbb{F}}^{alg}(E[\ell^\infty]) \subsetneq \mathrm{End}_{\mathbb{F}}(E[\ell^\infty]) \simeq M_2(\mathbb{Z}_\ell).$$

5.5. **Les classes d'isogénie de variétés abéliennes simples.** Pour $k \subset k'$ dans $\mathcal{I}$, l'application $x \mapsto x^{[k':k]}$ de $\overline{\mathbb{Z}}$ envoie $\mathcal{W}(k)$ sur $\mathcal{W}(k')$. On pose

$$\mathcal{W}(\mathbb{F}) = \varinjlim_{k \in \mathcal{I}} \mathcal{W}(k) \subset \mathcal{G}\left(\overline{\mathbb{Z}}\right) \subset \mathcal{G}\left(\overline{\mathbb{Q}}\right).$$

Ce sont les germes de $[p]$-nombres de Weil (de poids -1). L'action de $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ sur chacun des $\mathcal{W}(k)$ induit une action de $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ sur $\mathcal{W}(\mathbb{F})$ et

$$\varinjlim_{k \in \mathcal{I}} \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \backslash \mathcal{W}(k) \simeq \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \backslash \mathcal{W}(\mathbb{F}).$$

Si A est une variété abélienne simple sur $\mathbb{F}$, si A_k est un modèle de A sur $k \in \mathcal{I}$, et si π est un élément de $\mathcal{W}(k)$ qui est conjugué au Frobenius de A_k, l'image de π dans $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right) \backslash \mathcal{W}(\mathbb{F})$ ne dépend que de la classe d'isogénie de A sur $\mathbb{F}$. En effet, si A' est isogène à A, si $A'_{k'}$ est un modèle de A sur $k' \in \mathcal{I}$, et si π' est un élément de $\mathcal{W}(k')$ qui est conjugué au Frobenius de $A'_{k'}$, il existe d'après le lemme 54 une

extension finie k'' de k et k' telle que les variétés abéliennes $A_k \times_k k''$ et $A'_{k'} \times_{k'} k''$ sont isogènes sur k''. Leurs Frobenius sont donc conjugués, i.e. $\pi^{[k'':k]} = \pi'^{[k'':k']}$ dans $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)\backslash\mathcal{W}(k'')$. On obtient ainsi une application bien définie

$$w : \mathcal{S}(\mathbb{F}) \to \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)\backslash\mathcal{W}(\mathbb{F})$$

où l'on rappelle que $\mathcal{S}(\mathbb{F})$ est l'ensemble des classes d'isogénie de variétés abéliennes simples sur $\mathbb{F}$, ou encore l'ensemble des classes d'isomorphismes d'objets simples dans la catégorie abélienne semi-simple $\mathbf{Ab}^0_{\mathbb{F}}$.

Proposition 58. *L'application $w : \mathcal{S}(\mathbb{F}) \to \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)\backslash\mathcal{W}(\mathbb{F})$ est bijective.*

Démonstration. La surjectivité résulte du théorème 44 (de Honda). Pour l'injectivité, considérons deux variétés abéliennes A_1 et A_2 simples sur $\mathbb{F}$ telles que $w(A_1) = w(A_2)$ dans $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)\backslash\mathcal{W}(\mathbb{F})$. Soient $A_{1,k}$ et $A_{2,k}$ des modèles de A_1 et A_2 définis sur $k \in \mathcal{I}$, et soient π_1 et π_2 des éléments de $\mathcal{W}(k)$ conjugués au Frobenius de ces modèles. Puisque $w(A_1) = w(A_2)$, il existe $k' \in \mathcal{I}(k)$ tel que $\pi_1^{[k':k]}$ et $\pi_2^{[k':k]}$ sont conjugués dans $\mathcal{W}(k')$. Mais alors $A_{1,k} \times_k k'$ et $A_{2,k} \times_k k'$ sont isogènes sur k' d'après le théorème de Tate, donc A_1 et A_2 sont isogènes sur $\mathbb{F}$. □

5.6. **Une autre description de $\mathcal{W}(\mathbb{F})$.** On considére les couples $(F, (\lambda_v))$ qui sont formés d'un corps de nombres $F \subset \overline{\mathbb{Q}}$ et de la donnée, pour chaque place $v \mid p$ de F, d'une pente $\lambda_v \in \mathbb{Q} \cap [0,1]$. On note $\mathcal{C}(\mathbb{F})$ ceux de ces couples pour lesquels (1) $F = \mathbb{Q}$ et $\lambda_p = \frac{1}{2}$, ou bien (2) F est un corps CM et $\lambda_{v^\star} + \lambda_v = 1$ pour tout $v \mid p$, où $\star$ est l'involution canonique de F. Le groupe $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$ agit sur $\mathcal{C}(\mathbb{F})$ par $\sigma \cdot (F, (\lambda_v)) = (\sigma F, (\lambda_{\sigma^{-1}v}))$. Nous allons ici décrire deux applications $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-équivariantes

$$c : \mathcal{W}(\mathbb{F}) \to \mathcal{C}(\mathbb{F}) \quad \text{et} \quad \varpi : \mathcal{C}(\mathbb{F}) \to \mathcal{W}(\mathbb{F})$$

telles que $\varpi \circ c = \mathrm{Id}_{\mathcal{W}(\mathbb{F})}$.

Pour $\pi \in \mathcal{W}(\mathbb{F})$, on pose $c(\pi) = (F, (\lambda_v))$ où $F = \mathbb{Q}[\pi]$ et $\lambda_v = \lambda_v(\pi)$. Choisissons un représentant (π_k, k) de $\pi \in \mathcal{W}(\mathbb{F})$ avec $k \in \mathcal{I}$, $\pi_k \in \mathcal{W}(k)$, et $F = \mathbb{Q}[\pi_k]$. Soit $\star$ l'unique involution de de F telle que $\pi_k^\star = |k|/\pi_k$, cf. ***. Si $\star = \mathrm{Id}$, alors $\pi_k = \pm\sqrt{|k|}$, donc $F = \mathbb{Q}[\pi_k^2] = \mathbb{Q}$ et $\lambda_p = \frac{1}{2}$. Sinon, F est un corps CM dont $\star$ est l'involution canonique. Puisque $\lambda_v = v(\pi_k)/v(|k|)$ par définition de $\lambda_v(\pi)$, on a bien $\lambda_v \in \mathbb{Q} \cap [0,1]$ et $\lambda_v + \lambda_{v^\star} = 1$ pour tout $v \mid p$, donc $c(\pi) \in \mathcal{C}(\mathbb{F})$. On vérifie facilement que l'application c ainsi définie est $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-équivariante.

Dans l'autre sens, on définit d'abord $\varpi(\mathbb{Q}, \frac{1}{2})$ comme le germe qui correspond à la classe d'isogénie des courbes elliptiques supersingulières, c'est-à-dire celui qui est représenté par $(|k|^{1/2}, k)$ pour tout $k \in \mathcal{I}$. Soit ensuite $(F, (\lambda_v)) \neq (\mathbb{Q}, \frac{1}{2})$ un autre élément de $\mathcal{C}(\mathbb{F})$. On note $\star$ l'involution canonique de F, F_0 le sous-corps totalement réel de F fixé par $\star$, $\mathfrak{P}_v$ l'idéal maximal de $\mathcal{O}_F$ qui correspond à $v \mid p$, et e_v l'indice de ramification de F_v sur $\mathbb{Q}_p$, de sorte que $(p) = \prod_{v|p} \mathfrak{P}_v^{e_v}$. On note également

(1) $a \geq 1$ le plus petit dénominateur commun des $e_v\lambda_v$ pour $v \mid p$,

(2) $b \geq 1$ l'ordre de l'idéal $I = \prod_{v|p} \mathfrak{P}_v^{ae_v\lambda_v}$ dans $\mathrm{Pic}(\mathcal{O}_F)$,

(3) $c \geq 1$ l'indice de $\mathcal{O}_{F_0}^\times$ dans $\mathcal{O}_F^\times$, et

(4) $k \in \mathcal{I}$ le corps de cardinal $q = p^{2abc}$.

Par construction, $I \cdot I^\star = (p^a)$ et $I^b = (x)$ pour un x dans $\mathcal{O}_F$, donc $xx^\star = up^{ab}$ pour une unité u dans $\mathcal{O}_{F_0}^\times$. Alors $\pi_x = u^{-1}x^2$ est un p^{2ab}-nombre de Weil puisque $\pi_x \in \mathcal{O}_F$ et $\pi_x\pi_x^\star = p^{2ab}$, et $\lambda_v = v(\pi_x)/v(p^{2ab})$ pour tout $v \mid p$ puisque

$$(\pi_x) = I^{2b} = \textstyle\prod_{v|p} \mathfrak{P}_v^{2abe_v\lambda_v} \quad \text{et} \quad (p^{2ab}) = \prod_{v|p} \mathfrak{P}_v^{2abe_v}.$$

Si $I^b = (y)$, alors $y = vx$ pour une unité v de $\mathcal{O}_F$, donc $\pi_y = \frac{v}{v^\star}\pi_x$ et $\pi_y^c = \pi_x^c$ puisque $v^c \in \mathcal{O}_{F_0}^\times$. Donc $\pi_k = \pi_x^c$ est un q-nombre de Weil qui est indépendant du choix du générateur x de I^b. On note $\varpi(F, (\lambda_v))$ la classe de (π_k, k) dans $\mathcal{W}(\mathbb{F})$.

On laisse au lecteur le soin de vérifier que l'application $\varpi : \mathcal{C}(\mathbb{F}) \to \mathcal{W}(\mathbb{F})$ ainsi définie est $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-equivariante. Par ailleurs, avec les notations précédentes, il est clair que $c \circ \varpi(F, (\lambda_v)) = (F, (\lambda_v))$ si et seulement si $F = \mathbb{Q}[\pi_k^n]$ pour tout $n \geq 1$. Inversement, supposons que $(F, (\lambda_v)) = c(\varpi)$ pour un germe $\varpi \in \mathcal{W}(\mathbb{F})$ représenté par $(\varpi_{k'}, k')$ avec $k' \in \mathcal{I}$, $\varpi_{k'} \in \mathcal{W}(k')$ et $F = \mathbb{Q}[\varpi_{k'}]$. Alors

$$(\varpi_{k'}) = \textstyle\prod_{v|p} \mathfrak{P}_v^{[k':\mathbb{F}_p]e_v\lambda_v} \quad \text{puisque} \quad (|k'|) = \prod_{v|p} \mathfrak{P}_v^{[k':\mathbb{F}_p]e_v}$$

donc $[k' : \mathbb{F}_p] = abd$ pour un entier $d \geq 1$, puis $(\varpi_{k'}) = I^{bd} = (x^d)$ et donc $\varpi_{k'}^2 = \nu\pi_x^d$ pour une unité $\nu \in \mathcal{O}_F^\times$ qui est un 1-nombre de Weil, c'est-à-dire une racine de l'unité. On en déduit immédiatement que $\varpi(F, (\lambda_v)) = \varpi$, i.e. $\varpi \circ c = \mathrm{Id}$.

5.7. **Les variétés abéliennes ordinaires.** Une variété abélienne A sur un corps de caractéristique p est dite ordinaire si et seulement si toutes les pentes de son polygone de Newton sont entières, i.e. égales à 0 ou 1. C'est donc une notion géométrique, qui se lit sur le groupe p-divisible de A, et qui est stable par isogénie. De plus, si $A \sim \prod A_i$ alors A est ordinaire si et seulement si tous les A_i le sont.

Soit A une variété abélienne simple sur $\mathbb{F}$, π_A son Frobenius, $F = \mathbb{Q}[\pi_A]$ le centre de $D = \mathrm{End}_{\mathbb{F}}^0(A)$, $\star$ l'involution canonique de F, et $\lambda_v = \lambda_v(A)$ pour toute place $v \mid p$ de F. Alors A est ordinaire si et seulement si $\lambda_v \in \{0, 1\}$ pour tout $v \mid p$. Dans ce cas, $\mathrm{inv}_v(D) = 0$ pour toute place finie v de F, donc $D = F$ est un corps CM et $2 \dim A = [F : \mathbb{Q}]$. De plus, $v \neq v^\star$ pour tout $v \mid p$ puisque $\lambda_v + \lambda_{v^\star} = 1$.

Inversement : soit $F \subset \overline{\mathbb{Q}}$ un corps CM, F_0 le sous-corps totalement réel de F qui est fixé par l'involution canonique $\star$ de F. Supposons que toutes les places $v_0 \mid p$ de F_0 sont décomposés dans F. Choisissons dans l'ensemble des places $v \mid p$ de F un système de représentants $\mathcal{V}$ des orbites de F, et définissons $\lambda_v = 1$ si $v \in \mathcal{V}$ et $\lambda_v = 0$ sinon. Alors $\varpi(F, (\lambda_v)) \in \mathcal{W}(\mathbb{F})$ est un germe ordinaire, i.e. la classe d'isogénie de variétés abéliennes simples qui est déterminée par ce germe est ordinaire.

5.8. **Les variétés abéliennes supersingulières.** Une variété abélienne A sur un corps de caractéristique p est dite supersingulière si et seulement son polygone de Newton est isocline, i.e. de pente $\frac{1}{2}$. C'est donc à nouveau une notion géométrique, qui se lit sur le groupe p-divisible de A, et qui est stable par isogénie. Si $A \sim \prod A_i$, alors A est supersingulière si et seulement si tous les A_i le sont, mais on a maintenant beaucoup mieux.

Theorem. [10] *Soit A une variété abélienne de dimension g sur un corps k de caractéristique p. Alors A est supersingulière si et seulement si $A \times_k \overline{k}$ est isogène à E^g, où $\overline{k}$ est une cloture algébrique de k et E une courbe elliptique supersingulière.*

Démonstration. Le lemme 4.5 de [10] ramène la démonstration de ce théorème au cas des corps finis, qui résulte facilement de la théorie de Honda-Tate. Soit en effet A une variété abélienne simple sur $\mathbb{F}$, π_A son Frobenius, $F = \mathbb{Q}[\pi_A]$ et (π_k, k) un

représentant de π_A avec $k \in \mathcal{I}$ et $F = \mathbb{Q}[\pi_k]$. Alors A est supersingulière si et seulement si $\lambda_v(\pi_A) = v(\pi_k)/v(|k|) = \frac{1}{2}$ pour tout $v \mid p$. Dans ce cas, $\mathcal{O}_F \pi_k^2 = \mathcal{O}_F |k|$, donc $\pi_k^2 = u|k|$ pour une unité u de $\mathcal{O}_F$ qui est aussi un 1-nombre de Weil, c'est-à-dire une racine de l'unité. Mais alors $\pi_k^{2n} = |k|^n$ pour $n \gg 0$, donc $F = \mathbb{Q}$, $\lambda_p = \frac{1}{2}$, et A est une courbe elliptique supersingulière. □

5.9. **La conjecture de Manin.** Puisque toute variété abélienne A admet une polarisation, elle est en particulier isogène à son dual A^t. Si A est une variété abélienne sur un corps parfait k de caractéristique p, les modules de Dieudonné de A et A^t sont donc isogènes. En particulier, ils ont le même polygone de Newton. Puisque la dualité échange les pentes μ et $1-\mu$, on en déduit que ce polygone est symétrique. Inversement, Manin a conjecturé dans [7] que tout polygone de Newton symétrique provenait d'une variété abélienne. La théorie de Honda-Tate fournit une démonstration très élémentaire de cette conjecture.

On sait déjà comment obtenir les segments de pentes $\frac{1}{2}$: avec des courbes elliptiques supersingulières. Pour le reste, il suffit de construire, pour tout couple d'entier $(r,s) \neq (0,0)$ avec $r < s$ et $\mathrm{pgcd}(r,s) = 1$, une variété abélienne simple A sur $\mathbb{F}$, de dimension $r+s$ et de pentes $\{\frac{r}{r+s}, \frac{s}{r+s}\}$. On peut imposer au centre de $D = \mathrm{End}^0_{\mathbb{F}}(A)$ d'être une extension quadratique imaginaire donnée F de $\mathbb{Q}$, à condition que p soit décomposé dans F (puisqu'il nous faut deux pentes). Il suffit alors de choisir A dans la classe d'isogénie qui est déterminée par $\omega(F, (\lambda_v))$ où

$$\{\lambda_v : v \mid p\} = \left\{\frac{r}{r+s}, \frac{s}{r+s}\right\} = \{\mathrm{inv}_v(D) : v \mid p\}\,.$$

Puisque $\mathrm{pgcd}(r,s) = 1$, on a bien $r+s = [D:F]^{1/2} = \dim(A)$.

On peut aussi se donner un nombre de Weil π qui a les bonnes pentes, en spécifiant son polynôme minimal P. Soit par exemple π une racine de

$$P = X^2 + p^r X + p^{r+s} \in \mathbb{Z}[X].$$

Alors π est un p^{r+s}-nombre de Weil qui engendre une extension quadratique imaginaire $F = \mathbb{Q}[\pi]$ de $\mathbb{Q}$. Le polygone de Newton du polynôme $P \in \mathbb{Z}_p[X]$ a pour pentes r et $s > r$, donc p est décomposé dans F et

$$\left\{\frac{v(\pi)}{v(p^{r+s})} : v \mid p\right\} = \left\{\frac{r}{r+s}, \frac{s}{r+s}\right\}.$$

On conclut comme ci-dessus que toute variété abélienne A sur $\mathbb{F}_{p^{r+s}}$ de Frobenius conjugué à π est de dimension $r+s$, avec les pentes recherchées.

Deuxième partie 2. Les relèvements CM

6. Le théorème de Zink

6.1. **Enoncé.**

6.2. **Construction d'un corps CM.**

6.2.1. *Préliminaires.* Soit $(B, \star)$ une $\mathbb{Q}$-algèbre semi-simple à involution positive. On note $\mathcal{E} = \mathcal{E}(B, \star)$ l'ensemble des sous-algèbres de B qui sont commutatives et stables sous $\star$. Tout élément E de $\mathcal{E}$ est une $\mathbb{Q}$-algèbre commutative de dimension finie qui admet une involution positive, c'est donc un produit de corps totalement réels et de corps CM. On note $\mathcal{E}^{CM}$ l'ensemble des éléments de $\mathcal{E}$ qui sont des

$\mathbb{Q}$-algèbres CM, i.e. ceux qui n'ont aucune composante totalement réelle. On note $\mathcal{E}_{max} \neq \emptyset$ l'ensemble des élements maximaux de $\mathcal{E}$, et $\mathcal{E}^{CM}_{max} = \mathcal{E}^{CM} \cap \mathcal{E}_{max}$. Pour tout $E \in \mathcal{E}$, le commutant E' de E dans B est encore stable sous $\star$. Si x appartient à l'un des sous-espaces propres $E'_{\pm}$ de $\star$ agissant sur E', l'algèbre $E(x)$ engendré par E et x dans B est commutative et stable sous $\star$, donc $E(x) \in \mathcal{E}$. Si $E \in \mathcal{E}_{max}$, on a donc $E(x) = E$ pour tout $x \in E'_{\pm}$, donc $E' = E'_+ \oplus E'_- \subset E$, et $E' = E$ est une sous-algèbre commutative maximale de B. Si $(B, \star) = \prod(B_i, \star_i)$, l'application

$$\prod \mathcal{E}(B_i, \star_i) \to \mathcal{E}(B, \star) \qquad (E_i) \mapsto \prod E_i$$

n'est en général pas surjective, mais elle induit des bijections

$$\prod \mathcal{E}_{max}(B_i, \star_i) \simeq \mathcal{E}_{max}(B, \star) \qquad \text{et} \qquad \prod \mathcal{E}^{CM}_{max}(B_i, \star_i) \simeq \mathcal{E}^{CM}_{max}(B, \star).$$

Supposons donc que $(B, \star)$ est simple de centre F. Si l'involution est de seconde espèce, F est un corps CM qui est contenu dans chaque élément de $\mathcal{E}_{max}$, donc $\mathcal{E}_{max} = \mathcal{E}^{CM}_{max} \neq \emptyset$. Examinons les autres cas, où F est totalement réel :

C1. $(B, \star) \simeq (\mathrm{End}_F(V), \star_\varphi)$ avec $0 \neq (V, \varphi) \in \mathcal{Q}_{\gg}(F)$. Si $E \in \mathcal{E}^{CM}_{max}$, alors $E = \prod E_i$ où chacun des E_i est une extension CM de F, donc

$$\dim_F V = [E : F] = \sum [E_i : F] \equiv 0 \bmod 2.$$

Inversement, supposons que $2 \mid \dim_F V$ et écomposons arbitrairement (V, φ) en somme directe orthogonale de F-plans : $(V, \varphi) = \perp(V_i, \varphi_i)$ où $\dim_F V_i = 2$. On sait alors que (V_i, φ_i) est le F-espace quadratique sous-jacent d'une E_i-droite hermitienne (W_i, ψ_i) (essentiellement unique), où $E_i = F(\sqrt{\delta_i})$ est l'extension quadratique de F déterminée par le discriminant $\delta_i \in F^\times/(F^\times)^2$ de (V_i, φ_i). Puisque $(V_i, \varphi_i) \gg 0$, $\delta_i \ll 0$ et E_i est une extension CM de F. De plus, $E_i \subset \mathrm{End}_F(V_i)$ est stable sous l'involution $\star_{\varphi_i}$, donc $E = \prod E_i$ appartient à $\mathcal{E}^{CM}_{max}$. On a ainsi démontré que $\mathcal{E}^{CM}_{max} \neq \emptyset$ si et seulement si $2 \mid \dim_F V$.

C2. $(B, \star) \simeq (\mathrm{End}_D(V), \star_\varphi)$ avec $0 \neq (V, \varphi) \in \mathcal{A}_{\gg}(D)$ pour un corps de quaternion totalement indéfini D sur F. Décomposons arbitrairement $(V, \varphi) = \perp(V_i, \varphi_i)$ en somme directe orthogonale de D-droites. Alors $(V_i, \varphi_i) \simeq (D, \overline{x} d_i y)$ avec $d_i \in D^\times$, $\mathrm{tr}(d_i) = 0$ et $\mathrm{nr}(d_i) \gg 0$. Donc $E_i = F(d_i) \subset D = \mathrm{End}_D(V_i)$ est une extension CM de F qui est stable sous $\star_{\varphi_i}$, et $E = \prod E_i$ appartient à $\mathcal{E}^{CM}_{max} \neq \emptyset$.

C3. $(B, \star) \simeq (\mathrm{End}_D(V), \star_\varphi)$ avec $0 \neq (V, \varphi) \in \mathcal{Q}_{\gg}(D)$ pour un corps de quaternion totalement défini D sur F. Si $E \in \mathcal{E}_{max}$, alors $E = \prod E_i$ où chacun des E_i est une extension de F qui décompose D et n'admet donc pas de plongement réel. Par conséquent $\mathcal{E}^{CM}_{max} = \mathcal{E}_{max} \neq \emptyset$.

6.2.2. *Multiplication complexe.* Soient (A, λ) une variété abélienne polarisée sur k, $(C, \star) = (\mathrm{End}^0 A, \star_\lambda)$ l'algèbre à involution qui s'en déduit, $(B, \star) \subset (C, \star)$ une sous-algèbre semi-simple stable, et $(B', \star) \subset (C, \star)$ le commutant de B dans C, i.e. $B' = \mathrm{End}^0_B(A)$, muni de l'involution positive induite par celle de C. On note $\mathcal{E} = \mathcal{E}(B', \star)$, et l'on cherche à déterminer les conditions qui garantissent que $\mathcal{E}^{CM}_{max} \neq \emptyset$.

Example 59. Donnons d'abord quelques contre-exemples.

(1) Soit A une courbe elliptique supersingulière sur $k = \mathbb{F}_{p^{2n}}$. Alors C est le corps de quaternion sur $\mathbb{Q}$ tel que $\mathrm{Ram}(C) = \{p, \infty\}$. Si $B = C$, on a $B' = \mathbb{Q}$ et $\mathcal{E} = \{\mathbb{Q}\}$ ne contient pas de $\mathbb{Q}$-algèbre CM.

(2) Soient $A = A_+ \times A_-$ le produit de deux courbes elliptiques supersingulières non-isogènes sur $k = \mathbb{F}_{p^{2n}}$. Alors $C = D \times D$ où D est le corps de quaternion sur $\mathbb{Q}$ décrit précédemment. Si $B = D$ plongé diagonalement, alors $B' = \mathbb{Q} \times \mathbb{Q}$ avec l'involution triviale, et $\mathcal{E}_{max} = \{\mathbb{Q} \times \mathbb{Q}\}$ ne contient pas de $\mathbb{Q}$-algèbre CM. Mais si l'on passe à une extension quadratique k' de k sans changer B, les deux courbes deviennent isogènes, C s'agrandit en $M_2(D)$, et B' en $M_2(\mathbb{Q})$, dans lequel on peut plonger *toutes* les $\mathbb{Q}$-algèbres semi-simples de dimension 2, et en particulier *tous* les corps quadratiques imaginaires.

(3) Soit A une surface elliptique supersingulière sur $k = \mathbb{F}_{p^n}$ avec n impair. Alors C est le corps de quaternion sur $\mathbb{Q}(\sqrt{p})$ tel que $\mathrm{Ram}(C) = \{\infty_1, \infty_2\}$. Soit B une algèbre de quaternion sur $\mathbb{Q}$ telle que $B \otimes \mathbb{Q}(\sqrt{p}) \simeq C$, et $(B, \star) \subset (C, \star)$ le plongement déduit du choix d'un tel isomorphisme. Alors $B' = \mathbb{Q}(\sqrt{p})$, et $\mathcal{E}_{max} = \{\mathbb{Q}(\sqrt{p})\}$ ne contient pas de $\mathbb{Q}$-algèbre CM. Mais si l'on passe à une extension quadratique k' de k sans changer B, A se décompose en produit de deux courbes elliptiques isogènes, C s'agrandit en $M_2(D)$ où D est maintenant le corps de quaternion sur $\mathbb{Q}$ décrit en (1), et B' devient l'algèbre de quaternion telle que $B \otimes D \simeq M_2(B')$, qui à nouveau contient de nombreux corps CM.

Revenons maintenant à notre question de départ, en supposant pour commencer que B est simple de centre F. Puisque tout élément de $\mathcal{E}_{max}$ contient F, on peut tout de suite supposer que F est un corps totalement réel, donc $B \simeq M_b(B_0)$ avec (C1) $B_0 = F$, ou (C2) B_0 est un corps de quaternion totalement indéfini sur F, ou (C3) B_0 est un corps de quaternion totalement défini sur F.

Décomposons $(C, \star) = \prod (C_i, \star_i)$ en composantes simples, ce qui revient à décomposer $A \sim \prod A_i$ en composantes isotypiques, i.e. $A_i \sim A_{i,0}^{c_i}$ où les $A_{i,0}$ sont des variétés abéliennes simples sur k qui sont deux à deux non-isogènes. On a donc $C_i \simeq M_{c_i}(C_{i,0})$ où $C_{i,0} = \mathrm{End}_k^0(A_{i,0})$, et $(B', \star) = \prod (B_i', \star_i)$ où B_i' est le commutant de l'image de B dans C_i. En particulier,

$$\mathcal{E}_{max}^{CM}(B', \star) \neq \emptyset \iff \forall i : \qquad \mathcal{E}_{max}^{CM}(B_i', \star_i) \neq \emptyset.$$

Si le centre $F_i = Z(C_i) = Z(C_{i,0})$ est un corps CM, $\mathcal{E}_{max}^{CM}(B_i') = \mathcal{E}_{max}(B_i') \neq \emptyset$. Si en revanche F_i est un corps totalement réel, la classification des variétés abéliennes simples sur $k = \mathbb{F}_{p^n}$ impose de sévères restrictions :

- Si $n \equiv 0 \bmod 2$, $A_{i,0}$ est une courbe elliptique supersingulière, et $C_{i,0}$ est le corps de quaternion C_1 sur $F_i = \mathbb{Q}$ tel que $\mathrm{Ram}(\mathrm{C}_1) = \{p, \infty\}$,
- Si $n \equiv 1 \bmod 2$, $A_{i,0}$ est une surface elliptique supersingulière, et $C_{i,0}$ est le corps de quaternion C_2 sur $F_i = \mathbb{Q}(\sqrt{p})$ tel que $\mathrm{Ram}(\mathrm{C}_2) = \{\infty_1, \infty_2\}$.

Le cas pair. Supposons d'abord que $n \equiv 0 \bmod 2$. Alors

$$B \otimes C_i^{opp} \simeq M_{bc_i}(B_0 \otimes \mathrm{C}_1) \simeq M_{bc_i d_i}(D_i) \quad \text{où} \quad B_0 \otimes \mathrm{C}_1 \simeq M_{d_i}(D_i)$$

pour un corps D_i de centre F. Si $C_i \simeq (D_i^{bc_i d_i})^{e_i}$ comme $B \otimes C_i^{opp}$-module,

$$B_i' = \mathrm{End}_{B \otimes C_i^{opp}}(C_i) \simeq M_{e_i}(D_i).$$

Dans les cas $(C1)$ et $(C2)$ pour B_0, on vérifie facilement que D_i est un corps de quaternion totalement défini sur F, donc $\mathcal{E}_{max}^{CM}(B_i') = \mathcal{E}_{max}(B_i') \neq \emptyset$. Dans le cas $(C3)$ pour B_0, il convient de distinguer encore deux situations. Si B_0 n'est pas isomorphe à $\mathrm{C}_1 \otimes F$, D_i est un corps de quaternion totalement indéfini sur F,

et l'on sait à nouveau qu'alors $\mathcal{E}_{max}(B_i') \neq \emptyset$. Si en revanche B_0 est isomorphe à $\mathrm{C}_1 \otimes F$, alors $d_i = 4$, $D_i \simeq F$ et $\mathcal{E}_{max}^{CM}(B_i') \neq \emptyset$ si et seulement si $2 \mid e_i$. Puisque

$$4c_i^2 = [C_i : \mathbb{Q}] = 4bc_ie_i[F : \mathbb{Q}]$$

on voit que $2 \mid e_i$ si et seulement si $2b[F : \mathbb{Q}]$ divise $c_i = \dim A_i$.

Supposons donc que $B \simeq M_b(\mathrm{C}_1 \otimes F)$, et soit $I = \{i : C_{i,0} \simeq \mathrm{C}_1\}$ l'ensemble des indices problématiques, i.e. ceux qui correspondent à des classes d'isogénies de courbes elliptiques supersingulières $A_{i,0}$ (donc $|I| = 0, 1$ ou 2). Pour $i \notin I$, on vient de voir que $\mathcal{E}_{max}^{CM}(B_i', \star_i) \neq \emptyset$. Choisissons donc $E_i \in \mathcal{E}_{max}^{CM}(B_i', \star_i)$, et fixons également $E \in \mathcal{E}_{max}(B)$. Alors $E \otimes_F E_i$ est une sous-algèbre commutative maximale de $C_i = \mathrm{End}^0(A_i)$ d'après ***, donc $[E \otimes_F E_i : \mathbb{Q}] = 2 \dim A_i$ d'après ***. Mais $[E \otimes_F E_i : \mathbb{Q}] = [E : \mathbb{Q}][E_i : F]$ avec $[E : \mathbb{Q}] = 2b[F : \mathbb{Q}]$ et $2 \mid [E_i : F]$ (puisque E_i est une $\mathbb{Q}$-algèbre CM), donc $2b[F : \mathbb{Q}]$ divise $\dim A_i$. Si l'on sait donc à priori que $2b[F : \mathbb{Q}]$ divise $\dim A$, alors $2b[F : \mathbb{Q}]$ divise aussi $\sum_{i \in I} c_i$. Si $|I| = 0$ ou 1, on a donc bien $\mathcal{E}_{max}^{CM}(B') \neq \emptyset$. Si en revanche $I = \{i_1, i_2\}$, comme dans le contre-exemple *** ci-dessus, $\mathcal{E}_{max}^{CM}(B') \neq \emptyset$. Mais en passant à l'extension quadratique $k' = \mathbb{F}_{p^{2n}}$ de $k = \mathbb{F}_{p^n}$, les deux courbes elliptiques $A_{i_1,0}$ et $A_{i_2,0}$ deviennent isogènes, et aparaissent dans $A \times_k k'$ avec une multiplicité $c = c_{i_1} + c_{i_2}$ que divise $2b[F : \mathbb{Q}]$. Pour le commutant $B" \supset B'$ de B dans $\mathrm{End}_{k'}^0(A \times_k k')$, on a donc bien $\mathcal{E}_{max}^{CM}(B") \neq \emptyset$.

Le cas impair. Supposons maintenant que $n \equiv 0 \bmod 2$, et concentrons nous à nouveau sur un indice i (il y en a maintenant au plus un) pour lequel $A_{i,0}$ est une surface elliptique supersingulière, et $C_{i,0} \simeq \mathrm{C}_2$ sur $F_i = \mathbb{Q}(\sqrt{p})$. Pour les applications que l'on a en vu, où B et F sont non ramifiés en p, on peut supposer que $\sqrt{p} \notin F$. On a alors

$$B \otimes C_i^{opp} \simeq M_{bc_i}(B_0 \otimes \mathrm{C}_2) \simeq M_{bc_id_i}(D_i) \quad \text{où} \quad B_0 \otimes \mathrm{C}_2 \simeq M_{d_i}(D_i)$$

pour un corps D_i de centre $F' = F(\sqrt{p})$. Si $C_i = (D_i^{bc_id_i})^{e_i}$ comme $B \otimes C_i^{opp}$-module, alors

$$B_i' = \mathrm{End}_{B \otimes C_i^{opp}}(C_i) \simeq M_{e_i}(D_i).$$

Comme précédement, le seul cas qui pose problème est celui où $D_i = F'$ (où $d_i = 4$), c'est à dire lorsque $B_0 \otimes_F F' \simeq \mathrm{C}_2 \otimes_{\mathbb{Q}(\sqrt{p})} F'$. Puisque

$$8c_i^2 = [C_i : \mathbb{Q}] = 8bc_ie_i[F : \mathbb{Q}]$$

on voit que $\mathcal{E}_{max}^{CM}(B_i') \neq \emptyset$ si et seulement si $2b[F : \mathbb{Q}]$ divise c_i. Si l'on sait à priori que $2b[F : \mathbb{Q}]$ divise $\dim A$, le même argument que ci-dessus montre seulement que $2b[F : \mathbb{Q}]$ divise $\dim A_i = 2c_i$, et l'on peut rencontre des cas d'égalité, comme dans le contre-exemple *** ci-dessus. Mais en passant à l'extension quadratique $k' = \mathbb{F}_{p^{2n}}$ de $k = \mathbb{F}_{p^n}$, la variété abélienne A_i devient isogène au produit de $2c_i$ copies d'une meme courbe elliptique supersingulière, donc $\mathcal{E}_{max}^{CM}(B") \neq \emptyset$ pour le commutant $B" \supset B'$ de B dans $\mathrm{End}_{k'}^0(A \times_k k')$.

Nous avons donc démontré le résultat suivant...

6.2.3. *Preuve.*

6.3. **Construction d'un type CM.**

Proposition 60. *Il existe un type CM* $\Phi \coprod \Phi\iota = \mathrm{Hom}_{\mathbb{Q}}(E, \overline{\mathbb{Q}})$ *tel que*

$$\forall w, \rho : \qquad |\Phi_w| = \dim A[w] \quad \textit{et} \quad |\Phi_\rho| = n_\rho.$$

Soit $\mathcal{H} = \mathrm{Hom}_{\mathbb{Q}-alg}(E, \overline{\mathbb{Q}})$. On note $\mathcal{H}_{w,\rho}$ l'ensemble des éléments $E \to \overline{\mathbb{Q}}$ de $\mathcal{H}$ qui induisent la place w de E et le plongement ρ de F. Cet ensemble est non-vide si et seulement si w et ρ induisent la même place v de F, et alors $|\mathcal{H}_{w,\rho}| = [E_w : F_v]$. Soit $\mathcal{I}$ l'ensemble de ces indices (w, ρ). Pour tout type CM $\Phi \subset \mathcal{H}$ vérifiant les conditions de l'énoncé, les entiers $n_{w,\rho} = |\Phi \cap \mathcal{H}_{w,\rho}|$ vérifient donc les relations suivantes : pour $(w, \rho) \in \mathcal{I}$ sur v,

$$n_{w,\rho} + n_{\overline{w},\overline{\rho}} = [E_w : F_v], \quad \sum_{\rho|v} n_{w,\rho} = \dim A[w] \quad \text{et} \quad \sum_{w|v} n_{w,\rho} = n_\rho.$$

Inversement, supposons donné une telle collection d'entiers. Choisissons dans $\mathcal{I}$ un ensemble $\mathcal{J}$ de représentants des orbites de l'involution $(w, \rho) \mapsto (\overline{w}, \overline{\rho})$, et choisissons également pour chaque (w, ρ) dans $\mathcal{J}$ un sous-ensemble $\Phi_{w,\rho}$ de $\mathcal{H}_{w,\rho}$ tel que $|\Phi_{w,\rho}| = n_{w,\rho}$. Pour $(w, \rho) \notin \mathcal{I} - \mathcal{J}$, on pose $\Phi_{w,\rho} = \mathcal{H}_{w,\rho} - \Phi_{\overline{w},\overline{\rho}} \circ \iota$, de sorte qu'à nouveau $|\Phi_{w,\rho}| = n_{w,\rho}$. Alors $\Phi = \coprod_{\mathcal{I}} \Phi_{w,\rho}$ est un type CM qui vérifie évidemment les conditions de l'énoncé.

Il reste à construire une solution du système d'équation ***. Soit M_w le module de Dieudonné de $A[w]$. C'est un $W(k)$-module libre de rang $2 \dim A[w] = [E_w : \mathbb{Q}_p]$ sur lequel $\mathcal{O}_{E,w}$ agit. Quitte à élargir k, on peut découper M_w en sous-espaces caractéristiques pour la restriction de cette action à $\mathcal{O}_{F,v}$: $M_w = \oplus_{\rho|v} M_{w,\rho}$ où

$$M_{w,\rho} = \{m \in M_w | \forall x \in \mathcal{O}_{F,v} : \quad x \cdot m = \rho(x) \cdot m\}.$$

On a alors $F : M_{w,\rho} \leftrightarrow M_{w,\sigma\rho} : V$. On en déduit facilement que chacun des $M_{w,\rho}$ est libre de rang $[E_w : F_v]$ sur $W(k)$, et d'autre part que

$$M_w / V M_w = \oplus_{\rho|v} M_{w,\rho} / V M_{w,\sigma\rho}.$$

On pose $n_{w,\rho} = \dim_k M_{w,\rho} / V M_{w,\sigma\rho}$. On a donc par construction

$$\sum_{\rho|v} n_{w,\rho} = \dim_k M_w / V M_w = \dim A[w] \quad \text{et} \quad \sum_{w|v} n_{w,\rho} = n_\rho$$

D'autre part la dualité entre $A[w]$ et $A[\overline{w}]$ induit un accouplement parfait

$$\langle \cdot, \cdot \rangle_w : M_w \times M_{\overline{w}} \to W(k)$$

tel que $\psi(Fx, Fy) = p\sigma\psi(x, y)$. On en déduit un accouplement parfait induit

$$\langle \cdot, \cdot \rangle_{w,\rho} : M_{w,\rho} \times M_{\overline{w},\overline{\rho}} \to W(k).$$

Puisque $\sigma\psi(Vx, y) = \psi(x, Fy)$, on obtient encore un accouplement parfait

$$\langle \cdot, \cdot \rangle_{w,\rho} : M_{w,\rho} / V M_{w,\sigma\rho} \times p^{-1} V M_{\overline{w},\sigma\overline{\rho}} / M_{\overline{w},\overline{\rho}} \to k$$

d'où l'on tire immédiatement que $n_{w,\rho} + n_{\overline{w},\overline{\rho}} = [E_w : F_v]$, ce qu'il fallait démontrer.

6.4. **Conclusion.**

7. Suite

[Pour la suite, il faut savoir ce que l'on veut faire, et il faut avoir des notations stabilisés pour le problème de module...]

Références

[1] Deligne, Conjecture de Weil.

[2] de Jong, A. J. Homomorphisms of Barsotti-Tate groups and crystals in positive characteristic. Invent. Math. 134 (1998), no. 2, 301–333.

[3] Faltings

[4] Honda, ***, J. Math. Soc. Japan **20**, 1968.

[5] Gonzalez, On the pp-rank of an abelian variety and its endomorphism algebra.

[6] Grothendieck, EGA IV

[7] Manin, the theory of Commutative Formal Groups

[8] J.S. Milne et W.C. Waterhouse, Abelian Varieties over Finite Fields.

[9] D. Mumford, *Abelian Varieties*.

[10] Oort, 1974

[11] J. Tate, Endomorphisms of Abelian Varieties over Finite Fields, Inventiones n°**2**.

[12] J. Tate, ***, Séminaire Bourbaki n°**352**, 1968-1969.