p nombre premier $\quad q = p^a \quad a \geq 1 \quad k =$ corps fini à q éléments (1)

Rappel :

Th (TATE) : Soit A ~~une variété~~, B deux variétés abéliennes sur k alors la flèche naturelle :

$$\phi_0 \quad \mathrm{Hom}_k(A,B) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \longrightarrow \mathrm{Hom}_{\mathbb{Z}_\ell[G]}(T_\ell(A), T_\ell(B)) \qquad (G = \mathrm{Gal}(\bar{k}/k))$$

est un isomorphisme

On en avait déduit l'injectivité de l'application

$$\{\text{var abéliennes simples sur } k\}/\sim \xrightarrow{\Psi} \{q\text{-nombres de Weil à conjugaison près}\}$$

$$A \longmapsto \pi_A$$

où $A \sim B$ si A est isogène à B

Th (HONDA-TATE) : L'application précédente est une bijection et si A est une variété abélienne simple sur k

$E = \mathrm{End}_k(A) \otimes \mathbb{Q} = \mathrm{End}_k^0(A)$

$F = \mathbb{Q}[\pi_A] \subset E$

Alors E est une algèbre à division (corps gauche) de centre F et dont les invariants en les places de F sont donnés par :

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

et on a de plus l'égalité suivante :

$$2 \dim A = [E:F]^{\frac{1}{2}} [F:\mathbb{Q}] \quad (2)$$

$\rightarrow$ A est simple donc E est bien un corps gauche

$$\phi : E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \longrightarrow \mathrm{Hom}_{\mathbb{Q}_\ell[G]}(V_\ell(A), V_\ell(A)) = \mathrm{End}_{\mathbb{Q}_\ell[G]}(V_\ell(A))$$

est un isomorphisme d'après Tate.

On identifie $E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ et $F \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ avec leurs images dans $\mathrm{Hom}_{\mathbb{Q}_\ell}(V_\ell(A), V_\ell(B))$. Alors $E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ est le commutant de $\mathbb{Q}_\ell[G]$ ou encore celui de $F \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ ($\mathbb{Q}_\ell[G]$ est topologiquement engendré par π_A) $= \mathbb{Q}_\ell[\pi_A]$

D'après le théorème du bicommutant $F \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ est donc le centre de $E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$

Donc F est le centre de E.

→ ~~Haut~~ Soit f_A le polynôme minimal de π_A dans E (à coefficients dans $\mathbb{Z}$)

χ_{π_A} = polynôme caractéristique de π_A comme élément de $\mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(A)) = f_A^{\,e}$

$$e = \frac{2\dim A}{\deg f_A} = \frac{2\dim A}{[F:\mathbb{Q}]}$$

alors $V_\ell(A)$ est ~~comme~~ un $\mathbb{Q}_\ell[\pi_A]$-module libre de type fini de rang $r = e$

Par ϕ $E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ s'identifie à l'algèbre des endomorphismes de ce module

d'où $E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \simeq M_r(\mathbb{Q}_\ell[\pi_A])$

d'où $[E:F] = [E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell : F \otimes_{\mathbb{Q}} \mathbb{Q}_\ell] = [M_r(\mathbb{Q}_\ell[\pi_A]) : \mathbb{Q}_\ell[\pi_A]]$

$$= r^2 = \frac{(2\dim A)^2}{[F:\mathbb{Q}]^2}$$

D'où la formule (2) -

I - La surjectivité de φ

L'objectif est donc, partant d'un q-nombre de Weil π, de construire une variété A abélienne simple sur k tel que $\mathbb{Q}[\pi_A] \simeq \mathbb{Q}[\pi]$ - On va donc construire des

La construction de variétés abéliennes sur k est difficile - obtenir une v. a. sur un variétés abéliennes sur $\mathbb{C}$ d'un certain type puis par spécialisation nous réduirons la variété modulo un idéal premier ~~..~~ ; procédé corps de nombres, enfin nous réduirons la variété modulo un idéal premier, des variétés abéliennes sur les corps finis -
permettant de construire des variétés abéliennes sur les corps finis -

A) Variété abélienne sur $\mathbb{C}$ et type CM

Df (ici k est un corps quelconque) Soit A une variété abélienne sur k, M un corps de nombres - $g = \dim A$
On dit que A est à multiplication complexe par M si l'on s'est donné une flèche $i : \mathcal{O}_M \to \mathrm{End}_k(A)$ et que $[M:\mathbb{Q}] = 2g$ -

Rappelons qu'une variété abélienne sur $\mathbb{C}$, n'est rien d'autre qu'un tore complexe ($= \mathbb{C}^g/\Lambda$ $\Lambda = \mathbb{Z}$-réseau de $\mathbb{C}^g$) polarisable, i.e. tel qu'il existe une forme antisymétrique $\mathbb{R}$ bilinéaire

$$E \quad \mathbb{C}^g \times \mathbb{C}^g \to \mathbb{R}$$

tq $E(iv, iw) = E(v,w)$ et, $E(\Lambda \times \Lambda) \subset \mathbb{Z}$

et $E(iv, v) > 0$ $\forall v, w \in \mathbb{C}^g \setminus \{0\}$

②

~~[illegible]~~ Soit $A \simeq \mathbb{C}^g/\Lambda$ une variété abélienne sur $\mathbb{C}$ à multiplication complexe par M

l'isomorphisme $A \simeq \mathbb{C}^g/\Lambda$ induit deux flèches:

~~[illegible]~~ $\mathrm{End}_{\mathbb{C}}(A) \to M_g(\mathbb{C})$ (en considérant l'application induite sur le revêtement universel)

et $\mathrm{End}_{\mathbb{C}}(A) \to M_{2g}(\mathbb{Z})$ (en considérant l'application induite sur Λ)

D'où l'on déduit deux représentations:

$$\rho_{\mathbb{C}} : \mathrm{End}^0_{\mathbb{C}}(A) \to M_g(\mathbb{C})$$

$$\mathrm{End}^0_{\mathbb{C}}(A) \to M_{2g}(\mathbb{Q}) \subset M_{2g}(\mathbb{C})$$

et $\rho_{\mathbb{Q}}$

Il n'est pas bien difficile de voir que $\rho_{\mathbb{Q}} = \rho_{\mathbb{C}} \oplus \overline{\rho}_{\mathbb{C}}$

de la flèche $O_M \to \mathrm{End}_{\mathbb{C}}(A)$, on déduit une flèche $M \to \mathrm{End}^0_{\mathbb{C}}(A)$ alors

~~[illegible]~~ Soit $x \in M$ de degré $2g = [M:\mathbb{Q}]$ avec $2g$ valeurs propres 2 à 2 distinctes

$\rho_{\mathbb{Q}|M}(x)$ est diagonalisable ($\rho_{\mathbb{Q}}$ est clairement injective)

tout les plongements $M \to \mathbb{C}$

Donc si on note $\varphi_1, \dots, \varphi_{2g}$

$$\rho_{\mathbb{Q}|M} \simeq \bigoplus_{1 \le i \le 2g} \varphi_i$$

Et par conséquent:

$$\rho_{\mathbb{C}|M} \simeq \bigoplus_{i \in I} \varphi_i \qquad \overline{\varphi}_{\mathbb{C}|M} \simeq \bigoplus_{i \notin I} \varphi_i \qquad |I| = g$$

On doit avoir $\overline{\{\varphi_i \mid i \in I\}} = \{\varphi_i \mid i \notin I\}$

on note $\Phi = \{\varphi_i \mid i \in I\}$ et on dit que A est de type (M, Φ)

Déf : 1/ On appelle type CM tout couple (M, ϕ) où M est un corps de nombres, ϕ un ensemble de plongements complexes $M \hookrightarrow \mathbb{C}$ tel qu'il existe une variété abélienne A sur $\mathbb{C}$ de type (M, ϕ)

Déf 2/ Un corps CM est un corps de nombres M vérifiant l'une des deux assertions équivalentes suivantes :

i) M est totalement imaginaire, extension quadratique d'un corps totalement réel

ii) Si on voit M comme un sous-corps de $\mathbb{C}$ alors ρ (la conjugaison complexe) induit un automorphisme de M non trivial et ρ commute à toutes les injections $M \hookrightarrow \mathbb{C}$

Th Soit M un corps de nombres, ϕ un ensemble de n plongements $M \hookrightarrow \mathbb{C}$ $[M:\mathbb{Q}] = 2n$

Alors (M, ϕ) est un type CM si et seulement si M contient un corps CM K tq $\forall \varphi_1, \varphi_2 \in \phi \quad \rho \circ \varphi_1|_K \neq \rho \circ \varphi_2|_K$

Preuve Seule l'existence d'une variété abélienne A de type (M, ϕ) nous servira. Nous construisons alors lorsque M est un corps CM nous servira. Nous construisons alors A de la façon suivante :

Soit $\phi = \{\varphi_1, \dots, \varphi_n\}$

alors $\mathrm{Hom}(M, \mathbb{C}) = \{\varphi_1, \dots, \varphi_n, \rho\varphi_1, \dots, \rho\varphi_n\}$

Soit $\Phi : \mathcal{O}_M \longrightarrow \mathbb{C}^n$

$\alpha \longmapsto \begin{pmatrix} \varphi_1 \alpha \\ | \\ \varphi_n \alpha \end{pmatrix}$ alors $\Phi(\mathcal{O}_M)$ est un $\mathbb{Z}$-module libre de rang $2n$

Soit $\{\alpha_1, \dots, \alpha_{2n}\}$ une $\mathbb{Z}$-base de $\mathcal{O}_M$

il faut vérifier que $(\Phi(\alpha_1), \dots, \Phi(\alpha_{2n}))$ est $\mathbb{R}$-libre

or la matrice
$$\begin{pmatrix} \varphi_1\alpha_1 & \cdots & \varphi_n\alpha_1 & \rho\varphi_1\alpha_1 & \cdots & \rho\varphi_n\alpha_1 \\ | & & | & | & & | \\ \varphi_1\alpha_{2n} & \cdots & \varphi_n\alpha_{2n} & \rho\varphi_1\alpha_{2n} & \cdots & \rho\varphi_n\alpha_{2n} \end{pmatrix}$$
est inversible (indépendance des caractères)

Donc $\Phi(\mathcal{O}_M)$ est un $\mathbb{Z}$-réseau de $\mathbb{C}^n$

Posons $A = \mathbb{C}^n / \Phi(\mathcal{O}_M)$

Construisons une forme de Riemann pour A

Soit M^+ le ~~corps~~ sous-corps totalement réel maximal de M

$M = M^+[\xi]$ pour un certain $\xi \in M$ tq $-\xi^2$ soit totalement réel positif

Par le théorème d'approximation on peut trouver $\alpha \in M^+$ tq

$\forall i = 1, \dots, n \quad \varphi_i \alpha \; \mathrm{Im}(\varphi_i \xi) > 0$

quitte à remplacer ξ par $\alpha\xi$, on peut supposer que

$\forall i \quad \mathrm{Im}(\varphi_i \xi) > 0$ et que $\xi \in \mathcal{O}_M$

Posons alors $\forall z, w \in \mathbb{C}^n \quad E(z,w) = \sum_{j=1}^{n} (\varphi_j \xi)(\bar{z}_j w_j - z_j \bar{w}_j)$

E est clairement une forme bilinéaire réelle antisymétrique et $E(iz, iw) = E(z, w)$

$$E(iz, z) = \sum_{j=1}^{n} -i(\varphi_j \xi)\,|z_j|^2 = \sum_{j=1}^{n} \mathrm{Im}(\varphi_j \xi)\,|z_j|^2 > 0$$

dès que $z \neq 0$

et $\forall\ \Phi(\alpha) \in \Phi(\mathcal{O}_M)$, $\Phi(\beta)$

$$E(\Phi(\alpha), \Phi(\beta)) = \sum_{j=1}^{n} (\varphi_j \xi)\left(\rho\varphi_j(\alpha)\,\varphi_j(\beta) - \varphi_j(\alpha)\,\rho\varphi_j(\beta)\right)$$

$$= \cancel{\sum_{\varphi \in \mathrm{Hom}(M,\mathbb{C})}} \mathrm{Tr}_{M/\mathbb{Q}}(\bar{\alpha}\xi\beta) \in \mathbb{Z}$$

Donc A est une variété abélienne sur $\mathbb{C}$

L'application $\beta \mapsto \begin{pmatrix} \varphi_1\beta & & 0 \\ & \ddots & \\ 0 & & \varphi_n\beta \end{pmatrix}$ induit une flèche

$i : \mathcal{O}_M \hookrightarrow \mathrm{End}_{\mathbb{C}}(A)$ d'où le résultat ∎

B) Réduction des variétés abéliennes

Soit R un anneau de valuation discrète (AVD) et $K = \mathrm{Frac}\, A$

$\mathfrak{M}$ = idéal maximal de R $\quad k = R/\mathfrak{M}$ = corps résiduel

A une variété abélienne sur K

Déf : On dit que A a bonne réduction sur R s'il existe un schéma abélien $\mathcal{A}$ sur R tq la fibre générique $\mathcal{A}_K = \mathcal{A} \times_R K$ soit isomorphe à A

↳ = R-schéma en groupe propre lisse à fibre connexe.

exemple : Soit E une courbe elliptique, alors E a bonne réduction si et seulement si on peut trouver une équation de Weierstrass de E de discriminant $\Delta \not\equiv 0 \bmod \mathfrak{M}$

Par la théorie des modèles de Néron, on a un foncteur

$A \longmapsto N(A)$ tq A a bonne réduction ssi $N(A)$

$Var ab/_K \longmapsto Sch/R$ est propre sur R

et alors $N(A)$ est un modèle pour A.

Si A a bonne réduction alors on a un morphisme (par fonctorialité)

$$\mathrm{End}_K(A) \longrightarrow \mathrm{End}_k(N(A) \times_R k) \quad (*)$$

Prop : Si $K = K_0(t)$ ~~donc~~ et A est une variété abélienne sur K alors A a bonne réduction presque partout i.e. en toute place de K (K_0 étant considéré comme le corps des constantes) sauf un nombre fini.

Preuve : $\alpha \in K^*$ est une unité pour presque toute place de K. Il suffit de prendre les places pour lesquels les équations définissant A, la multiplication, l'inverse soient à coefficients unitaires dans R.

Conséquence : Soit $A/_{\mathbb{C}}$ une variété abélienne ~~à coefficients~~ sur $\mathbb{C}$ à multiplication complexe par (H, Φ) alors A est définie sur un corps de type $\overline{\mathbb{Q}}(x_1, \dots, x_d)$ par la proposition précédente et par réduction successive et par $(*)$ on obtient une variété abélienne sur ~~k~~ un corps de nombres à multiplication complexe ~~par~~ de type (H, Φ).

Th (Serre, Tate, Néron, Ogg, Shafarevitch) Soient K et H des corps de nombres. Soit A une variété abélienne sur K, à multiplication complexe par H, alors après une extension finie des scalaires, A a bonne réduction partout.

Th (Décomposition du Frobenius en idéaux premiers).

K = corps de nombres A/K var abélienne de type (H, Φ)

on suppose que $H^{gal} \subset K$ et on considère les $\varphi \in \Phi$ comme des plongements $\varphi : H \hookrightarrow K$

Soit $\mathfrak{p}$ une place finie de bonne réduction pour A.

Σ

$\pi_0 \in M$ qui induise le frobenius sur la réduction de Amodulop -

Alors :
$$\pi_0 \mathcal{O}_M = \prod_{\varphi \in \Phi} \varphi^{-1}(N_{K/\varphi(M)} \mathfrak{P})$$

c) Surjectivité

Prop : Soient K et K' deux corps de nombres CM alors :

i) leur composé est CM

ii) K^{gal} est CM

Preuve : évident par la caractérisation :

K est CM $\Leftrightarrow$ ρ induit un automorphisme de K non trivial qui commute à tout les plongements $K \hookrightarrow \mathbb{C}$

Si K est un corps de nombres tq $K/\mathbb{Q}$ extension galoisienne, on notera respectivement e_K et f_K le degré de ramification, et le degré d'inertie de l'extension en p-

Prop : Soit π un q-nombre de Weil, il existe une extension finie L de $\mathbb{Q}[\pi]$ normale telle que $\forall w | p$ place de L
$$\frac{w(\pi)}{w(q)} e_L f_L \in \mathbb{Z}$$
et telle que L soit CM

Preuve : Deux cas : soit π est totalement réel ($\pi^2 = q$) soit $\rho(\pi) \neq \pi$

Dans les deux cas $\mathbb{Q}[\pi]$ est contenu dans un corps CM (dans le premier cas $\mathbb{Q}[\pi]$ est totalement réel, dans le deuxième $\mathbb{Q}[\pi]$ est déjà un corps CM)

Si w est un place quelconque $| p$ d'une extension de $\mathbb{Q}[\pi] = F$, il existe $v | p$ place de F tq $\frac{w(\pi)}{w(q)} = \frac{v(\pi)}{v(q)}$, il suffit donc de trouver L corps CM (contenant F) tel que $N | e_L f_L$ pour un certain N

or $\forall \zeta$ racine primitive n-ième de l'unité $\underset{K_\zeta}{\underset{\parallel}{\mathbb{Q}[\zeta]}}$ est CM

et f_{K_ζ} est l'ordre de p modulo $\frac{n}{p^{v_p}}$ donc on peut choisir n tq $N | f_{K_\zeta}$

alors la composée de K_q et F est un corps CM ~~K~~ L qui contient F et tq

$$\forall w | p \qquad \frac{w(\pi)}{w(q)} e_K f_K \in \mathbb{Z}$$

il ne reste plus qu'à prendre la clôture normale de L ■

<u>Lemme</u> $\exists \phi \subset \mathrm{Hom}_{\mathbb{Q}}(L, \mathbb{C})$ tq $\forall w | p$

$$\frac{w(\pi)}{w(q)} = \frac{\mathrm{card}\{\varphi \in \phi / \varphi(w) = w_0\}}{e_L f_L}$$

pour un certain $w_0 | p$

<u>Preuve</u> $\forall w | p \qquad n_w = e_L f_L \frac{w(\pi)}{w(q)} \in \mathbb{N}$

notons $\forall w | p \quad H_w = \{\varphi \in \mathrm{Hom}_{\mathbb{Q}}(L, \mathbb{C}) / \varphi(w) = w_0\}$

alors les H_w forment une partition de $\mathrm{Hom}_{\mathbb{Q}}(L, \mathbb{C})$

Soit $w | p$ si $\rho(w) = w$, on choisit

$$\phi_w \subset H_w \text{ tq } \rho(\phi_w) \cup \phi_w = H_w$$
$$\text{et } \rho(\phi_w) \cap \phi_w = \emptyset$$

si $\rho(w) \neq w$ on définit $\phi_{\rho(w)}$ et ϕ_w simultanément par

ϕ_w une partie quelconque de H_w de cardinal n_w

et $\phi_{\rho(w)} = H_{\rho(w)} \setminus \rho(\phi_w)$

Et on pose $\phi = \bigcup_{w | p} \phi_w$

Comme $n_{\rho(w)} + n_w = e_L f_L = \mathrm{card}\, H_w$ et par construction,

<u>ϕ convient</u> ■

D'après la section précédente (L, ϕ) est un type CM

Donc il existe une variété abélienne A définie sur un corps de nombres K de type (L, ϕ), quitte à agrandir K, on peut supposer que A a bonne réduction partout ~~et~~ que $L \subset K$ ~~et~~, que $K/\mathbb{Q}$ est galoisienne et que ~~$f_K \ldots$~~ $v_p(q) | f_K$

Choisissons une place finie $\mathfrak{P}$ de K au dessus de w_0

Notons A_0 la réduction de A modulo $\mathfrak{P}$

k_0 le corps résiduel en $\mathfrak{P}$

$q_0 = |k_0| = p^{f_K}$

On a une flèche

$$\mathcal{O}_L \to \mathrm{End}_K(A) \to \mathrm{End}_{k_0}(A_0)$$, comme A_0 et A ont même dimension, on en déduit l'existence de $\pi_0 \in L$ induisant le Frobenius sur A_0 via le lemme suivant

<u>Lemme</u> Soit A_0 une variété abélienne sur k_0 à multiplication complexe par L, alors L est égal à son commutant dans $\mathrm{End}^0_{k_0}(A_0)$.

<u>Preuve</u> Soit α tq $L = \mathbb{Q}[\alpha]$ alors α est algébrique de degré $2\dim A_0$ ~~donc l'image de α dans $\mathrm{End}^0_{k_0}(A_0)$ est diagonalisable à~~

Il suffit de montrer que le commutant de $L \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}_\ell$ est égal à son commutant dans $\mathrm{End}_{\overline{\mathbb{Q}}_\ell}(V_\ell(A_0) \otimes_{\mathbb{Q}_\ell} \overline{\mathbb{Q}}_\ell)$ puisque

$$\mathrm{End}_{k_0}(A_0) \underset{\mathbb{Z}}{\otimes} \overline{\mathbb{Q}}_\ell \longrightarrow \mathrm{End}_{\overline{\mathbb{Q}}_\ell}(V_\ell(A) \underset{\mathbb{Q}_\ell}{\otimes} \overline{\mathbb{Q}}_\ell)$$ est une

injection. Or l'image de α y est diagonalisable avec $2\dim A_0$ valeurs propres distinctes. Donc le commutant de α = polynôme en α = $L \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}_\ell$ ∎

Soit donc $\pi_0 \in L$ qui induit le Frobenius sur A_0
alors d'après le théorème de décomposition du Frobenius

$$\pi_0 \mathcal{O}_L = \prod_{\varphi \in \Phi} \varphi^{-1}(N_{K/L}\, \mathfrak{P})$$

ce qui est équivalent à :

$$\forall w | p \quad \frac{w(\pi_0)}{w(q_0)} = \frac{\mathrm{card}\{\varphi \in \Phi \,/\, \varphi(w) = w_0\}}{e_L f_L}$$

ainsi $\forall w | p \quad \dfrac{w(\pi_0)}{w(q_0)} = \dfrac{w(\pi)}{w(q)}$

~~Quitte à remplacer (K, p) par (K', p') où~~

~~Puisque $f_K \geq v_p(q)$ on~~

Puisque $v_p(q) \mid f_K$ on a $q_0 = q^N$

d'où $w\left(\frac{\pi_0}{\pi^N}\right) = 0 \ \forall w \mid p$

de même $\forall$ place finie (car si v finie $\nmid p$

$v(\pi_0) = v(\pi^N) = 0$)

En une place archimédienne w, on a :

$$|\pi_0|_w = q_0^{1/2} \text{ et } |\pi|_w = q^{1/2}$$

d'où $\left|\frac{\pi_0}{\pi^N}\right|_w = 1$ donc $\frac{\pi_0}{\pi^N}$ est une racine de l'unité

or si k_1 est une extension finie de k_0 de degré k, le frobenius de $A \times_{k_0} k_1$ sera conjugué à π_0^k

Donc quitte à étendre les scalaires on a prouvé ~~que π_0~~ qu'il existe une variété abélienne A/k_1, k_1 extension finie de k tel que le frobenius de A soit conjugué à une puissance de π.

~~Lemme : Soit $j \in \mathbb{N}^*$ tel que~~

$A = A_1 \times_{k_1} A_2 \times \dots \times_{k_1} A_r$ la décomposition de A en var. ab. simples

alors $f_A = \prod f_{A_i}$ donc ~~la il existe une variété~~ l'un des facteurs A_i a son frobenius conjugué à une puissance de π

restriction des scalaires à la Weil

Soit $S' \to S$ un morphisme de schémas

X' un schéma sur S'

on a un foncteur

$$Sch/S \longrightarrow Ens$$
$$T \longmapsto Hom_{S'}(T \times_S S', X')$$

Si ce foncteur est représentable par un schéma X sur S, X s'appelle la restriction des scalaires à la Weil de X'.

On le notera $Res_{S'/S}(X)$

On se place ici dans le cas $S = Spec\, k$ $S' = Spec\, k'$

où k'/k est une extension finie de corps

si X' est une variété projective sur k' définie par un système d'équations
$$\begin{cases} P_1(x_0, \ldots, x_d) = 0 \\ \vdots \\ P_r(x_0, \ldots, x_d) = 0 \end{cases}$$

alors la restriction des scalaires à la Weil de X' existe.

il suffit d'écrire $X_i = \sum_{j=1}^{k} Y_{i,j}\, s_j$

où $s_1, \ldots, s_k$ est une base de k'/k

alors en décomposant $P_\ell(x_0, \ldots, x_d) = 0$

on obtient k équations $P_{\ell,1}, \ldots, P_{\ell,k}$ sur les $Y_{i,j}$

il suffit de prendre $X = Proj\left(k[Y_{i,j}]/J\right)$

où $J = (P_{\ell,j})$

Le schéma obtenu $Res_{k'/k}(A)$ pour A une variété abélienne sur k'

est encore une variété abélienne sur k

Les morphismes définissant la structure de schéma en groupe s'obtiennent via le lemme de Yoneda ayant par exemple le morphisme de foncteur

$$Hom(\cdot \times_k k', A \times_{k'} A) \xrightarrow{m} Hom(\cdot \times_k k', A)$$

(on a $Res_{k'/k}(A \times_{k'} A) = Res_{k'/k}(A) \times_k Res_{k'/k}(A)$)

~~La suite~~

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

Preuve : Soit A' la variété abélienne sur k obtenue par restriction des scalaires à la Weil de A.

Alors les $\bar{k}$ points de A' $\operatorname{Spec} \bar{k} \to A'$

correspondent bijectivement aux $\bar{k} \otimes k_j$ points de A

$\operatorname{Spec} \bar{k} \otimes_k k_j \to A$

qui eux même ne sont rien d'autre qu'un j-uplet de $\bar{k}$-points de A $\operatorname{Spec} \bar{k} \to A$.

Et par cette bijection les $\bar{k}$ point de A' de ℓ torsion correspondent aux j-uplets de $\bar{k}$ point de A de ℓ torsion.

Par conséquent $V_\ell(A')$ est canoniquement isomorphe à $V_\ell(A)^j$ comme ~~Gal~~ $\mathbb{Q}_\ell[\mathrm{Gal}(\bar{k}/k_j)]$ module.

L'action du Frobenius de A'/k ~~se~~ se traduit par une permutation d'ordre j sur les facteurs de $V_\ell(A)^j$.

Dans une base adaptée à la décomposition de $V_\ell(A)^j = V_\ell(A')$ la matrice M' de $\pi_{A'}$ s'écrit alors

$$M' = \begin{pmatrix} 0 & & M \\ M & \ddots & \\ & \ddots & 0 \\ 0 & & M \end{pmatrix}$$ ~~où M est la matrice de π_A agissant sur $V_\ell(A)$~~

d'où $$M'^j = \begin{pmatrix} M^j & & 0 \\ & \ddots & \\ 0 & & M^j \end{pmatrix}$$

~~donc $(X_{M'^j}) = (X_{M^j})^j$ π^j est une valeur propre~~

Soit λ tq λ^j soit valeur propre de M^j

$$M^j X = \lambda^j X \quad X \neq 0$$

donc $\begin{pmatrix} X \\ MX \\ \vdots \\ M^{j-1}X \end{pmatrix}$ est vecteur propre de M' pour la valeur propre λ

Or M^j doit être la matrice de π_A (agissant sur $V_p(A)$)

donc π^j est ~~racine~~ valeur propre de M^j

Par conséquent π est racine de $\chi_{M'}$

et donc π est racine d'un des polynôme caractéristique d'un facteur simple de A'

donc π est conjugué au Frobenius d'un facteur simple de A

II - Invariants aux places $\not{p}$ et courbes elliptiques

A) Invariants

On montre comment obtenir (1) aux places ne divisant pas p.

→ si $v \nmid p$ est une place finie

alors $v | \ell$ $\ell \neq p$

Par le théorème de Tate

($F_\ell = F \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$) $F_\ell \otimes_F E = \mathbb{Q}_\ell \otimes_{\mathbb{Q}} E$ s'identifie

à $\mathrm{End}_{F_\ell} V_\ell(A) = M_e(F_\ell)$

en tant que F_ℓ-algèbre. Or, $F_\ell \simeq \prod_{v|\ell} F_v$

~~$F_\ell \otimes_F E \simeq \prod_{v|}$~~ d'où $F_v \otimes_F E$ s'identifie à $M_e(F_v)$

i.e. E split au dessus de v.

→ si $v | \infty$ alors si v est complexe, le résultat est évident

si $F = \mathbb{Q}[\pi]$ a des places réelles alors $\pi^2 = q$

on a deux cas :

1) si $\pi \in \mathbb{Q}$ alors $F = \mathbb{Q}$ et comme

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

on a $E \neq F$

donc les invariants de E ne sont pas tous nuls et ont pour somme 0.

Or, seul la place à l'∞ et p ont potentiellement des invariants non nuls donc $\mathrm{inv}_\infty(E) = \frac{1}{2}$

et par conséquent $\mathrm{inv}_p(E) = \frac{1}{2}$.

2) si $\pi \notin \mathbb{Q}$ $F/\mathbb{Q}$ est une extension ~~xxx~~ quadratique

$\pi = \sqrt{q}$

$F = \mathbb{Q}[\sqrt{p}]$

alors $f_A = (T^2 - q)^e$ pour un certain $e \geq 1$

Soit $A' = A \times_k k'$ où k' est l'unique extension quadratique de k

alors $f_{A'} = (T - q)^{2e}$ la décomposition de A' en var. ab. simples

Soit $A' = A_1 \times_k \cdots \times_k A_r$

~~alors $\mathrm{End}^0_{k'}(A') = \prod_{i,j} \mathrm{End}(A_i) \; \mathrm{Hom}^0_k(A_i, A_j)$~~

alors ~~et~~ $f_{A'} = \prod f_{A_i}$ donc les A_i sont du type précédent et par conséquent ayant même classe de conjugaison pour leur frobenius, on a A_i isogène à A_j $\forall i,j$

donc $\mathrm{Hom}^0_{k'}(A_i,A_j) \simeq \mathrm{End}^0_{k'}(A_j) \simeq D_p$ → unique algèbre de quaternions sur $\mathbb{Q}$ ramifiée en p et l'∞ exactement

~~et~~

~~Donc $\mathrm{End}^0_{k'}(A') \simeq M_r(D_p)$~~

~~$\mathrm{End}^0_k(A) = E$~~

~~or $F = \mathbb{Q}[\pi_A]$ par le théorème du bicommutant, comme~~
~~$F = \mathrm{Comm}(E)$, on a $E = \mathrm{Comm}(F)$ dans $M_r(D_p)$~~
~~donc E contient l'injection diagonale de D_p dans $M_r(D_p)$.~~
~~Par conséquent, comme D_p est ramifiée en l'∞ E est ramifié en les~~
~~deux places à l'∞ de F~~ —

B) Courbes elliptiques

Quand un q-nombre de Weil est-il associé à une courbe elliptique ?

On doit avoir $2 = 2\dim A = [E:F]^{\frac{1}{2}}\,[F:\mathbb{Q}]$

1er cas / $F = \mathbb{Q}$ ~~on a alors~~ ~~Et~~
alors $E \simeq D_p$ et A est une courbe supersingulière
~~Car sinon on a une flèche injective~~
~~$\mathrm{End}^0(E) \otimes_{\mathbb{Q}} \mathbb{Q}_p \hookrightarrow \mathrm{End}(T_p$~~

Car ~~alors~~ $f_A = (T - q^{\frac{1}{2}})^2$ et $\mathrm{tr}(\pi_A) \in p\mathbb{Z}$

2e cas / $F/\mathbb{Q}$ est quadratique et on doit avoir $E = F$
i.e. les invariants de E sont triviaux
soit $X^2 + aX + q$ le polynôme minimal de π
on doit avoir $\Delta = a^2 - 4q < 0$ (sinon $E \neq F$)
(F n'a pas de place réelles

9

→ s'il n'y a ~~qu'une~~ qu'une place v au dessus de p

alors $v(\pi) = v(\bar{\pi}) = \frac{v(q)}{2}$

et $[F_v : \mathbb{Q}_p] = 2$ donc $\mathrm{inv}_v(E) = 0$ et $F = E$

A est bien alors une courbe elliptique et alors comme

$v(a) = v(\pi + \bar{\pi}) \geq \frac{v(a)}{2}$ $\quad q \mid a^2$ et $\mathrm{tr}(\pi_A) = -a \in p\mathbb{Z}$

A est supersingulière.

→ s'il y a deux places v et v' au dessus de p

alors $[F_v : \mathbb{Q}_p] = [F_{v'} : \mathbb{Q}_p] = 1$

~~or~~ inv_v

or, $\frac{v(\pi)}{v(q)} + \frac{v'(\pi)}{v(q)} = 1$ donc on doit avoir

$v(\pi) = 0$ et $v'(\pi) = v(q)$ ou l'inverse

ceci arrive si et seulement si $(a, p) = 1$

et alors A n'est pas supersingulière.

$\mathrm{Res}_{k'/k}(A')$ est une variété abélienne sur k de polynôme caractéristique $(T^2-q)^{2e}$ donc $\mathrm{Res}_{k'/k}(A') \simeq_k A \times_k A$

on a un morphisme $\mathrm{End}^0_{k'}(A') \to \mathrm{End}^0_k(\mathrm{Res}_{k'/k}(A')) \simeq M_2(E)$

de $\mathbb{Q}$-algèbres

injectif

D'où un morphisme $F \otimes_{\mathbb{Q}} \mathrm{End}^0_{k'}(A') \xrightarrow{\varphi} \mathrm{End}^0_k(\mathrm{Res}_{k'/k}(A'))$

qui envoit $\pi \in F$ sur le frobenius de $\mathrm{Res}_{k'/k}(A')$

(F s'identifie au centre de $\mathrm{End}^0_k(\mathrm{Res}_{k'/k}(A'))$)

Comme le Frobenius ~~n'est pas~~ de $\mathrm{Res}_{k'/k}(A')$ n'est pas dans l'image de $\mathrm{End}^0_{k'}(A')$

l'image de $F \otimes_{\mathbb{Q}} \mathrm{End}^0_{k'}(A')$ contient strictement l'image de $\mathrm{End}^0_{k'}(A')$

dans $\mathrm{End}^0_k(\mathrm{Res}_{k'/k}(A'))$ qui est d'indice 2

(car $\dim \mathrm{End}^0_{k'}(A') = (2\dim A)^2$

et $\dim \mathrm{End}^0_k(\mathrm{Res}_{k'/k}(A'))$
$= \dim \mathrm{End}^0_k(A \times A)$
$= 4 \cdot \dim(\mathrm{End}_k(A))$
$= 4 \cdot 2 \cdot (\dim A)^2$)

Donc $\mathrm{Im}\,\varphi = \mathrm{End}^0_k(\mathrm{Res}_{k'/k}(A'))$ en raison des dimension,

φ est un isomorphisme.

Par conséquent

$F \otimes_{\mathbb{Q}} M_2(D_p) \simeq M_2(E)$

Donc $E \sim F \otimes_{\mathbb{Q}} D_p$ et comme D_p est non ramifié à la place à l'∞ et F aussi

on a que E est ramifié aux deux places à l'∞

c'est pas en la place $v(p)$.

?≡÷?≡? └3n └■n≡n?² └ n■n.?n nn?nnnµ? ≡° ≡≡ ≡? n.?² └ n√ n∈ ├└≡≡nn■≡ ² ╓≡└.÷<└
<≥?nn ≈0└° └n√ └ü╨0■² └≥└ ² nnnn⌡└■<.≡n?└ └nn°