Le théorème de Honda

p : nbe premier $\quad q = p^r$ avec $r \geq 1 \quad k = \mathbb{F}_q \subset \overline{k}$

$G = \mathrm{Gal}(\overline{k}/k)$

Rappel de l'épisode précédent

On a (Benjamin) montré le théorème suivant :

Th (Tate) : Soient A, B deux var ab /k alors la flèche

$$\phi_0 : \mathrm{Hom}_k(A,B) \otimes_{\mathbb{Z}} \mathbb{Z}_p \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{Z}_p[G]}(T_p A, T_p B)$$

est un isomorphisme

On en avait déduit l'injectivité de l'application

$$\{\text{var ab simples sur } k\}/\sim \xrightarrow{\Psi} \left\{\begin{array}{l} q\text{-nombres de Weil} \\ \text{à conj- près} \end{array}\right\}$$

$$A \longmapsto \pi_A$$

où $A \sim B$ si A est isogène à B.

On se propose de montrer que cette application est en fait une bijection

Prop : Soit A var ab simple /k $\quad E = \mathrm{End}_k^0(A) = \mathrm{End}_k(A) \otimes \mathbb{Q}$

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

Alors E est une algèbre à division de centre F dont les invariants sont donnés par :

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

I - Variétés abéliennes de type CM

Def (K un corps quelconque) : A une var ab / K, $g = \dim A$, M un cdN
On dit que A est à multiplication complexe par M si l'on s'est donné une flèche $i : \mathcal{O}_M \longrightarrow \mathrm{End}_K(A)$ et que $[M : \mathbb{Q}] = 2g$

Sur $\mathbb{C}$: Une var ab sur $\mathbb{C}$ est une tore complexe $A = \mathbb{C}^g/\Lambda$ polarisable i.e.

$$\left| \begin{array}{l} \exists\, \psi : \Lambda \times \Lambda \longrightarrow \mathbb{Z} \text{ bilinéaire antisymétrique} \\ \text{tq } \psi_{\mathbb{R}}(iu, iv) = \psi_{\mathbb{R}}(u,v) \quad \psi_{\mathbb{R}}(iu, u) > 0 \quad \forall u, v \in \Lambda \otimes \mathbb{R} = \mathbb{C}^g \end{array} \right.$$

Soit $A = \mathbb{C}^g/\Lambda$ une var abélienne complexe. On a deux flèches
$\rho_1 : \mathrm{End}_{\mathbb{C}}(A) \longrightarrow M_g(\mathbb{C})$, $\rho_2 : \mathrm{End}_{\mathbb{C}}(A) \longrightarrow M_{2g}(\mathbb{Z})$
et $\rho_{2,\mathbb{C}} \simeq \rho_1 \oplus \overline{\rho}_1$

Si A est à multiplication complexe par M, $\iota : \mathcal{O}_M \longrightarrow \mathrm{End}_{\mathbb{C}}(A)$
$\Phi_M = \{ \varphi : M \hookrightarrow \mathbb{C} \}$ alors $\rho_{2, \mathbb{C}} \circ \iota \simeq \bigoplus_{\varphi \in \Phi_M} \varphi$
donc $\exists\, \Phi \subset \Phi_M$ tq $\Phi_M = \Phi \sqcup \overline{\Phi}$
$\cdot\ \rho_1 \circ \iota \simeq \bigoplus_{\varphi \in \Phi} \varphi$

Def : On dit alors que A est de type (M, Φ)

Déf : On appelle type CM tout couple (M, Φ) où M est un cdN, Φ un ens de plongements $M \hookrightarrow \mathbb{C}$ tq $\exists$ une var ab $A/\mathbb{C}$ de type (M, Φ)

Prop : Soit M un corps CM et ϕ un ens de plongements $M \hookrightarrow \mathbb{C}$ tq $\Phi_M = \phi \sqcup \overline{\phi}$
alors (M, ϕ) est un type CM

Preuve : Prendre $\Lambda = \{ (\varphi_1 x, \dots, \varphi_g x) \mid x \in \mathcal{O}_M \} \subset \mathbb{C}^g$ $\quad A = \mathbb{C}^g/\Lambda$ (avec $\mathcal{O}_M \hookrightarrow \mathbb{C}^g$)

$\phi = \{\varphi_1, \dots, \varphi_g\}$

Il suffit de vérifier que A est polarisable

M^+ le sous-corps tot-réel maximal de M. $M = M^+[\xi]$ avec ξ^2 tot réel positif.

Par le Th d'approximation $\exists\, x \in M^+$ tq $\forall \varphi \in \phi \quad \varphi(x)\, \mathrm{Im}(\varphi(\xi)) > 0$

Quitte à remplacer ξ par $a\xi$, ops que $\mathrm{Im}(\varphi(\xi)) > 0\ \forall \varphi \in \phi$

$$\psi : \mathbb{C}^g \times \mathbb{C}^g \longrightarrow \mathbb{R}, \quad (z, w) \longmapsto \sum_{j=1}^{g} \varphi_j(\xi)(\bar{z}_j w_j - \bar{w}_j z_j)$$

$\psi(iz, iw) = \psi$ $\quad \psi(ig, g) > 0$ et $\psi(x, y) = \mathrm{Tr}_{M/\mathbb{Q}}(\bar{x}\xi y) \in \mathbb{Z}$ pour $x, y \in \mathcal{O}_M$

donc A est polarisable ∎

Cor : H corps CM Φ ens de plongements $H \hookrightarrow \mathbb{C}$ tq $\Phi_H = \Phi \sqcup \overline{\Phi}$
Alors il existe K un cdN et A/K var ab de type CM (H, Φ)

Preuve : On a construit une telle var. ab / $\mathbb{C}$ A
$\exists$ un certain corps $\mathbb{Q}[x_1, \dots, x_d]$ de t.f. sur $\mathbb{Q}$ sur lequel A
et $\iota : \mathcal{O}_H \longrightarrow \mathrm{End}_{\mathbb{C}}(A)$ sont définis
Puis par spécialisations successives on en déduit le résultat ▨

~~II 2 La Formule de Shimura Taniyama~~

II – Réduction des variétés abéliennes

R AVD $K = \mathrm{Frac}(A)$ $k = R/\mathfrak{M}$
$\mathfrak{M}$ = idéal max

Def : A/K var ab a bonne réduction sur R s'il existe un schéma abélien
$\mathcal{A}/R$ = R-schéma propre lisse à fibre connexe
tq la fibre générique soit $\simeq A$.

Th (Neron, Ogg-Shafarevitch, Serre-Tate) : A/K var abélienne KcdN
a bonne réduction en $\mathfrak{P}$ si pour un certain $\ell \neq \mathrm{car}(\mathcal{O}_K/\mathfrak{P})$, le groupe
d'inertie I en $\mathfrak{P}$ agit trivialement sur $T_\ell A$

Cor : Soit A/K une var ab sur KcdN à mult complexe par (H, Φ)
alors après une extension finie, A a bonne réduction en toute place divisant $\mathfrak{P}$

Preuve : On a vu que $H_1(A_{\mathbb{C}}, \mathbb{Q})$ est alors un espace vectoriel de dim 1
sur E. Donc $V_\ell A = H_1(A, \mathbb{Q}) \otimes \mathbb{Q}_\ell$ est un $E \otimes \mathbb{Q}_\ell$-module
libre de rang 1. Par conséquent $E \otimes \mathbb{Q}_\ell$ est son propre stabilisateur
dans $\mathrm{End}_{\mathbb{Q}_\ell}(V_\ell A)$.
L'image de $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ pour l'action sur $V_\ell A$ est donc dans
$(E \otimes \mathbb{Q}_\ell)^\times$. Cette image est même compacte donc admet un
pro-ℓ sous-groupe d'indice fini
I admet un pro-p sous-groupe d'indice fini
L'image de I est donc finie ▨

III - Formule de Shimura-Taniyama

Th : Soit A/K var ab sur K cdN de type CM (M, Φ) qui a bonne réduction en $\mathfrak{P}$. On suppose que H^{gal}_{CK} et on note $\bar{A}$ la réduction de $A \bmod \mathfrak{P}$

Alors i) $\bar{A}$ est de type CM (M, Φ)

ii) $\pi_{\bar{A}} \in \mathcal{O}_M$

iii) $(\pi_{\bar{A}}) = \prod_{\varphi \in \Phi} \varphi^{-1}\left(N_{K/\varphi(M)} \mathfrak{P}\right)$

Preuve : i) Vient de l'existence de modèles de Néron

ii) Puisque la flèche $\mathrm{End}^{\circ}_{k} \bar{A} \longrightarrow \mathrm{End}_{\mathbb{Q}_\ell[\pi_{\bar{A}}]} (V_\ell \bar{A})$ $k = \mathcal{O}_K/\mathfrak{P}$

est injective, $V_\ell \bar{A}$ est un $M \otimes \mathbb{Q}_\ell$-module libre de rang 1 donc le centralisateur de $M \otimes \mathbb{Q}_\ell$ dans $\mathrm{End}_{\mathbb{Q}_\ell}(V_\ell \bar{A})$ est lui-même d'où $\pi_{\bar{A}} \in M$ puis $\pi_{\bar{A}} \in \mathcal{O}_M$ ($\pi_{\bar{A}}$ est un entier alg)

Pour la preuve de iii), on aura besoin du résultat suivant de Giraud

Prop (Giraud) : Soit A/k var ab de type CM (M, Φ) alors si

$$\mathrm{Lie}(A) \underset{\mathcal{O}_M\text{-mod}}{\simeq} \bigoplus \mathcal{O}_M/Q_i$$

on a $\prod Q_i = (\pi_A)$

Preuve de prop $\Rightarrow$ iii) : Soit $\mathcal{A}/\mathcal{O}_{K,\mathfrak{P}}$ le modèle de Néron de A

$L = \mathrm{Lie}(\mathcal{A})$ est un $\mathcal{O}_{K,\mathfrak{P}}$-module libre de rang $g = \dim_K(A)$ muni d'une action de $\mathcal{O}_E \subset M$

$\det_L : \mathcal{O}_E \longrightarrow \mathcal{O}_{K,\mathfrak{P}}$ associé est donné par $\det_L(x) = \prod_{\varphi \in \Phi} \varphi(x)$

$\bar{L} = \mathrm{Lie}(\bar{A}) = L \otimes_{\mathcal{O}_{K,\mathfrak{P}}} k$ est un $\mathcal{O}_E \otimes_{\mathbb{Z}} k$-module de longueur finie

Les $\mathcal{O}_E/\mathfrak{p} \otimes k$-modules simples sont de la forme $\mathcal{O}_E/\varphi^{-1}(\mathfrak{P}) \otimes_{\varphi} k$ $\varphi : E \hookrightarrow K$

et le déterminant associé est $\mathcal{O}_E \longrightarrow k$, $x \longmapsto \varphi(x) \bmod \mathfrak{P}$

Par conséquent $\bar{L}$ admet une suite de Jordan-Hölder dont les quotients successifs sont les $\mathcal{O}_E/\varphi^{-1}(\mathfrak{P}) \otimes_{\varphi} k$ pour $\varphi \in \Phi$ avec multiplicité 1

$\left[\ell = \text{comme } \mathcal{O}_E\text{-module } \left(\mathcal{O}_E/\varphi^{-1}(\mathfrak{P})\right)^{[k : \mathcal{O}_E/\varphi^{-1}(\mathfrak{P})]}\right.$

donc $(\pi_{\bar{A}}) = \prod_{\varphi \in \Phi} \varphi^{-1}(\mathfrak{P})^{f(\mathfrak{P}/p, \varphi(E))}$

Preuve de la prop de Giraud :

Pour M un $\mathcal{O}_E$-module de t. f. on note

$$A^M : \mathrm{Sch}/_k \longrightarrow \mathrm{Ab}$$
$$S \longmapsto \mathrm{Hom}_{\mathcal{O}_E}(M, A(S))$$

- Alors $A^{\mathcal{O}_E^n} \simeq A^n$ et si $M_1 \to M_2 \to M_3 \to 1$ est exacte

$$1 \to A^{M_3} \to A^{M_2} \to A^{M_1} \text{ aussi}$$

donc les A^M sont représentables

- Si M est projectif, $\exists M'$ tq $M \oplus M' \simeq \mathcal{O}_E^n$

et alors $A^M \times A^{M'} \simeq A^n \Rightarrow A^M$ est une var ab

- Si $I \subset \mathcal{O}_E$ idéal, on note $A[I] = A^{\mathcal{O}_E/I}$

alors $\mathrm{Lie}(A[I]) = (\mathrm{Lie}\, A)[I]$

Lemme : $\alpha^I : A \to A^I$ est une isogénie de degré $|\mathcal{O}_E/I|$

Preuve : $T_\ell(A^I) = \mathrm{Hom}_{\mathcal{O}_E}(I, T_\ell(A)) = \mathrm{Hom}_{\mathcal{O}_E \otimes \mathbb{Z}_\ell}(I \otimes \mathbb{Z}_\ell, T_\ell(A))$

pour $\ell \nmid |\mathcal{O}_E/I|$ $\qquad = T_\ell(A)$

donc $\dim(A^I) = \dim(A)$

Comme $\ker(\alpha^I) = A[I]$ est fini, α^I est bien une isogénie

Si $I = (\lambda)$ alors $A^I \simeq A$ et α^I s'identifie à $\lambda \in \mathrm{End}_k(A)$

On a alors $\deg \alpha^I = \deg \lambda = N(\lambda) = [\mathcal{O}_H : I]$

(↑ fonction polynômiale qui coïncident pour $n \in \mathbb{N}$)

Si $I = I_1 I_2$

$$\alpha^I_I : A \xrightarrow{\alpha^{I_1}} A^{I_1} \xrightarrow{\alpha^{I_2}_{A^{I_1}}} A^{I_1 I_2} = (A^{I_1})^{I_2}$$

Or $A^{I_1}[I_2] = A[I_2]$ donc $\deg(\alpha^I) = \deg(\alpha^{I_1}) \deg(\alpha^{I_2})$

Il ne reste plus à utiliser le fait que $\mathrm{RC}(\mathcal{O}_E)$ est fini ∎

Puisque $\pi_A = 0$ sur $L = \mathrm{Lie}(A)$, on a

$$L = L[P_1^{n_1}] \oplus \cdots \oplus L[P_s^{n_s}] \text{ où } (\pi_A) = P_1^{n_1} \cdots P_s^{n_s}$$

Un résultat matriciel que $|L[P_i^{n_i}]| = \left|\mathcal{O}_{\mathfrak{k}} / \mathfrak{p}_i^{n_i}\right| = \deg A[P_i^{n_i}]$

Ou encore, seulement que $|L[P_i^{n_i}]| \geq \deg A[P_i^{n_i}]$ car

$$q^g = |L| = \prod |L[P_i^{n_i}]|$$

et
$$q^g = \deg(\pi_A) = \prod \deg A[P_i^{n_i}]$$

On a $\mathcal{O}_{\ker(\pi_A),0} = \mathcal{O}_{A,0} / \pi_A^{\#}(\mathfrak{I}_{A,0})\mathcal{O}_{A,0} \simeq \widehat{\mathcal{O}}_{A,0} / \pi_A^{\#}(\widehat{\mathfrak{I}}_{A,0})\widehat{\mathcal{O}}_{A,0}$

$$\simeq k[x_1, \ldots, x_g] / (x_1^q, \ldots, x_g^q) \quad q = |k|$$

$\left(\widehat{\mathcal{O}}_{A,0} \simeq k[[x_1, \ldots, x_g]] \text{ et } \pi_A^{\#}(x_i) = x_i^q\right)$

$\forall i$, $A[P_i^{n_i}] \hookrightarrow \ker(\pi_A)$ et on a $\mathcal{O}_{A[P_i^{n_i}],0} \simeq k[x_1, \ldots, x_g] / I$

$$(x_1^q, \ldots, x_g^q) \subseteq I \subseteq (x_1, \ldots, x_g)$$

Alors $|L[P_i^{n_i}]| = \left|I / (x_1^q, \ldots, x_g^q)\right| \left|\mathfrak{M} / \mathfrak{M}^2 + I\right|$

$$\deg A[P_i^{n_i}] = q^g - \dim_k \left(I / (x_1^q, \ldots, x_g^q)\right)$$

Si $h = \dim_k I \mathfrak{a} / I \cap \mathfrak{M}^2$ alors $|L[P_i^{n_i}]| = q^{g-h}$

et $\dim_k \left(I / (x_1^q, \ldots, x_g^q)\right) \geq q^g - q^{g-h}$

qui revient à faire au cube de base, on a $I \supseteq (x_1, \ldots, x_h)$

d'où l'inégalité ☒

III - La preuve du Th de Honda

Prop : Soient E, E' deux corps CM alors :

i) leur composé est CM

ii) E^{gal} est CM

Preuve : Evident par la caractérisation E est CM $\Leftrightarrow$ la conj-complexe induit un auto non trivial de E qui commute à tous les plongements $E \hookrightarrow \mathbb{C}$ ▨

~~$\forall$ ext gal $K/\mathbb{Q}$~~, on note e_K et f_K ~~les degrés de ramification hors et d'inertie de Ker p~~ l'indice de ramification et le degré résiduel de Ker p

Lemme 1 Soit π un q nbe de Weil. $\exists$ une $L/\mathbb{Q}[\pi]$ galoisienne sur $\mathbb{Q}$ t.q. $\forall v|p$

- $\frac{v(\pi)}{v(q)} e_L f_L \in \mathbb{Z}$
- L est CM

Preuve : $\forall$ plongement $\mathbb{Q}[\pi] \hookrightarrow \mathbb{C}$ $\overline{\pi} = \frac{q}{\pi}$ donc $\mathbb{Q}[\pi]$ est CM ou tot. réel

Dans les deux cas, $\mathbb{Q}[\pi]$ est contenu dans un corps CM

$\frac{v(\pi)}{v(q)}$ v place fini d'une ext finie $L/\mathbb{Q}[\pi]$ ne dépend que de la place de $\mathbb{Q}[\pi]$ en dessous de v

Il suffit donc de m.q $\exists \forall N \in \mathbb{N}^*, \exists E/\mathbb{Q}$ corps CM t.q. $N | e_E f_E$

$E = \mathbb{Q}[\zeta_m]$ f_E = ordre de p modulo $\frac{n}{p^{val_p(n)}}$ ▨

Lemme 2 : π et L comme dans le lemme 2. $\exists \Phi \subseteq Hom_{\mathbb{Q}}(L, \mathbb{C})$ t.q. $\forall v|p$ de L

$$\frac{v(\pi)}{v(q)} = \frac{\#\{\varphi \in \Phi \mid \varphi(v) = v_0\}}{e_L f_L} \text{ et } \Phi_L = \Phi \sqcup \overline{\Phi}$$

pour un certain $v_0|p$ de $\underbrace{\varphi(L)}_{\text{toujours le même car } L/\mathbb{Q} \text{ galoisienne}} \subseteq \mathbb{C}$

Preuve : $\forall v|p$, on pose $n_v = e_L f_L \frac{v(\pi)}{v(q)}$

et $H_v = \{\varphi \in Hom_{\mathbb{Q}}(L, \mathbb{C}) \mid \varphi(v) = v_0\}$

c la conjugaison complexe sur L

Soit $v|p$: • si $c(v) = v$ $H_v \to H_v$, $\varphi \mapsto \overline{\varphi}$ est une involution sans point fixe

Soit $\Phi_v \subseteq H_v$ t.q. $H_v = \Phi_v \sqcup \overline{\Phi_v}$

- Si $\rho(v) \neq v$, on choisit $\Phi_v \subseteq H_v$ et $\Phi_{\rho(v)} \subseteq H_{\rho(v)}$ simultanément

$H_v \longrightarrow H_{\rho(v)}$ est bijective

$\varphi \longmapsto \overline{\varphi}$

$|H_v| = |H_{\rho(v)}| = e_L f_L$

et $n_v + n_{\rho(v)} = e_L f_L \dfrac{v(\pi) + v(\rho_\pi)}{v(q)}$

$= e_L f_L \dfrac{v(\pi) + v(\frac{q}{\pi})}{v(q)} = e_L f_L$

On choisit $\Phi_v \subset H_v$ quelconque ~~choisir~~ de cardinal n_v

et on pose $\Phi_{\rho(v)} = H_{\rho(v)} - \overline{\Phi_v}$

Alors $\Phi = \coprod_{v|p} \Phi_v$ convient ☒

(L, Φ) est un CM type, et on peut donc trouver une var ab A/K de type CM (L, Φ)

Quitte à étendre les scalaires, on peut supposer que :

- $v_p(q) \mid f_K$
- A a bonne réduction en toute place $|p$
- $\varphi(L) \subseteq K \quad \forall \varphi \in \Phi_L$

Soit A_0 la réduction de A en une place $w_0 | p$ de K ($\mathcal{P}_0 \subseteq \mathcal{O}_K$ idéal premier non nul au dessus de la place v_0 de $\varphi(L)$)

Alors $\pi_0 \in \mathcal{O}_L$ et d'après la formule de Shimura-Taniyama

$(\pi_0) = \prod_{\varphi \in \Phi} \varphi^{-1}(N_{K/\varphi(L)} \mathcal{P}_0)$

Alors $\forall v | p$ place $v(\pi_0) = \#\{\varphi \in \Phi \mid \varphi(v) = v_0\} f(w_0 : v_0)$

Soit q_0 le cardinal de $k_0 = \mathcal{O}_K / \mathcal{P}_0$ $\quad v(q_0) = v(\mathcal{P}^{f_K}) = f_K e_L$

D'où $\dfrac{v(\pi_0)}{v(q_0)} = \dfrac{\#\{\varphi \in \Phi \mid \varphi(v) = v_0\}}{e_L f_L} = \dfrac{v(\pi)}{v(q)}$ (↑ Lemme 2)

$q_0 = q^N$ car $v_p(q) \mid f_K$

On a alors $\dfrac{v(\pi_0)}{v(\pi^N)} = 1 \quad \forall v | p$

$v(\pi_0) = v(\pi^N) = 1 \quad \forall v \nmid p$ fini

$|\pi_0|_v = |\pi^N|_v = q_0^{\frac{1}{2}} \quad \forall v | \infty$

Donc $\left\{\frac{\pi_0}{\pi^N}\right\}$ est une racine de l'unité

Si k_1/k_0 est une extension finie de degré r, le Frobenius de $A \times_{k_0} k_1$ sera π_0^r

Donc quitte à étendre les scalaires, on a prouvé qu'il existe une variété abélienne A_0 sur une ext finie k_0/k (deg) telle que π_{A_0} soit conjugué à une puissance de π_k.

Soit $A = R_{k_0/k}(A_0)$ $\quad V_\ell(A) \simeq V_\ell(A_0)^{\mathrm{Gal}(k_0/k)}$

comme $\mathrm{Gal}(\bar{k}/k)$-mod

On en déduit que $\mathbb{Q}[\pi_A] = \mathbb{Q}[\pi_{A_0}]/(X^n - \pi_{A_0})$

Or si $A \sim A_1^{n_1} \times \cdots \times A_s^{n_s}$ $\quad A_i$ var ab simples /k

$A_i \not\simeq A_j$

$$\mathbb{Q}[\pi_A] \simeq \mathbb{Q}[\pi_{A_1}] \times \cdots \times \mathbb{Q}[\pi_{A_s}]$$

$$\pi_A \longmapsto (\pi_{A_1}, \ldots, \pi_{A_s})$$

Comme il existe une surjection $\mathbb{Q}[\pi_A] \twoheadrightarrow \mathbb{Q}[\pi]$, $\exists i$ tq $\mathbb{Q}[\pi_{A_i}] \simeq \mathbb{Q}[\pi]$

$\pi_A \longmapsto \pi$ $\qquad$ $\pi_{A_i} \longmapsto \pi$