Le théorème d'isogénie de Tate

(exposé au groupe de travail de Gaëtan Chenevier)

<u>NB</u> Si ce qui suit semble un roman sans fin, c'est parce que j'ai fait beaucoup (trop) de rappels. Néanmoins, ces histoires de var. ab. sur des corps finis sont toujours plus subtiles que l'on pense et la littérature n'est pas vraiment abondante (pour plein de merveilles sur le sujet, laissez tomber ces notes et allez voir les pages de F. Oort et Ching Li-Chai).

<u>Quelques notations</u> k sera toujours un corps, souvent de caractéristique $p>0$, très souvent fini. G_k sera le groupe de Galois absolu de k, $Gal(\bar{k}/k)$, Sch_S la catégorie des S-schémas, $Schgr_S$ celle des S-schémas en groupes (flèches évidentes à chaque fois), Ab_S = schémas abéliens sur S, $Ab_k := Ab_{\operatorname{spec} k}$

<u>I Rappels sur Ab_k</u> Je ne donne aucune démo, elles sont en général assez difficiles, mais les résultats sont parfaitement classiques. A vos livres préférés! (ie, Mumford)

Une variété abélienne sur k = schéma en groupes sur k, propre, géométriquement intègre. Par homogénéité elle est lisse sur k, par rigidité tout morphisme de schémas respectant les origines est un homomorphisme (ie un morphisme dans Ab_k) et donc la loi de groupe est commutative. Un thm très nontrivial assure que tout élément de Ab_k est k-projectif. On note Ell_k = les courbes elliptiques sur k, ie var. ab de dimension 1 sur k.

Quelques "rappels" sur le schéma de Picard (voir les exposés de Grothendieck dans FGA ou le livre de Mumford pour une autre approche), ou enfin le livre Néron models). On ne prend qu'un cas très particulier, mais fondamental:

Si $X \in Sch_k$ est propre et $X(k) \neq \emptyset$ il existe un k-schéma séparé localement de type fini noté $Pic_{X/k}$ tq

1) $\forall T \in Sch_k$, $0 \to \operatorname{Pic} T \xrightarrow{pr_T^*} \operatorname{Pic} X_T \to Pic_{X/k}(T) \to 0$

2) $T_{Pic_{X/k}, e} \simeq H^1(X, \mathcal{O}_X)$ (e = origine du sch. en gr $Pic_{X/k}$: que c'est un sch en gr est évident sur 1), car cela se lit sur le foncteur des points)

3) Si $X \in Ab_k$, $Pic_{X/k}$ est lisse et $Pic^0_{X/k}$ (composante neutre de $Pic_{X/k}$) est une variété abélienne de même dimension que X. On la note X^t.

On ne dit rien de plus sur ce théorème mis à part le fait qu'il est très profond. $A \mapsto A^t$ est fonctorielle : tout $f : A \to B$ dans Ab_K induit par pullback sur des ($T \in Sch_K$)-points un morphisme $f^t : A^t \to B^t$ qui préserve les origines, qui est donc un morphisme dans Ab_K. Par le (difficile) théorème du carré de Weil on peut montrer que $(f+g)^t = f^t + g^t$. Tout ceci marche sans problème pour Ab_S.

Thm de double dualité (Cartier-Nishi) $A \in Ab_K$ (ou Ab_S), alors $A \simeq A^{tt}$ canoniquement. (voir le livre de F. Oort, Commutative group schemes, III 20 ; voir aussi Mumford).

II Frobeniuseries 1) Frobenius absolu si $S \in Sch_{\mathbb{F}_p}$, on note $F_S : S \to S$ le morphisme qui envoie $x \in S$ sur x et $f \in \mathcal{O}_S(U)$ sur $f^p \in \mathcal{O}_S(U)$. Il est immédiat que c'est fonctoriel (ie

$$\begin{tikzcd} S_1 \arrow[r, "f"] \arrow[d, "F_{S_1}"'] & S_2 \arrow[d, "F_{S_2}"] \\ S_1 \arrow[r, "f"] & S_2 \end{tikzcd}$$

commute), compatible avec le produit ($F_{S_1 \times_{\mathbb{F}_p} S_2} = F_{S_1} \times F_{S_2}$)

2) Frobenius relatif On se donne $S \in Sch_{\mathbb{F}_p}$, $X \in Sch_S$ et on définit

$$\begin{tikzcd} X \arrow[r, dashed, "F_{X/S}"] \arrow[rr, bend left, "F_X"] \arrow[dr, bend right, "\pi"'] & X^{(p/S)} \arrow[r] \arrow[d] & X \arrow[d, "\pi"] \\ & S \arrow[r, "F_S"] & S \end{tikzcd}$$

$X^{(p)} = X^{(p/S)} = X \times_{S, F_S} S$

$F_{X/S}$ comme dans le diagramme

☡ F_X n'est pas (en général) un morphisme dans Sch_S, alors que par construction $F_{X/S}$ l'est. Si X "est donné par des équations", $X^{(p)}$ est donné par les équations obtenues en faisant $a \mapsto a^p$ à chaque coefficient, alors que $F_{X/S}$ s'obtient en faisant $x \mapsto x^p$ à chaque inconnue.

Prop 1) compatibilité par chang. de base : $(X_T)^{(p/T)} \simeq (X^{(p/S)})_T$, $(F_{X/S})_T = F_{X_T/T}$

2) compatibilité avec Fr absolu si $S = \mathrm{Spec}\, \mathbb{F}_p$: $X^{(p/S)} = X$, $F_{X/S} = F_X$

3) fonctorialité en $X \in Sch_S$.

4) compatibilité avec les produits.

Tout ceci est immédiat. Noter qu'en particulier, si $G \in Schgr_S$, alors $G^{(p/S)} \in Schgr_S$ et $F_{G/S}$ est un morphisme dans $Schgr_S$.

3) Frobenius relatif itéré, enfin π_A On fait le même coup.

$$\begin{tikzcd} X \arrow[r, dashed, "F_{X/S,n}"] \arrow[rr, bend left, "F_X^n"] \arrow[dr, bend right] & X^{(p^n/S)} \arrow[r] \arrow[d] & X \arrow[d] \\ & S \arrow[r, "F_S^n"] & S \end{tikzcd}$$

On obtient un S-morphisme $F_{X/S,n} : X \to X^{(p^n/S)}$

et ceci est $\begin{cases} \text{fonctoriel en } X \in Sch_S \\ \text{compatible avec les produits et le chang. base en } S: \left(X^{(p^n/S)}\right)_T \simeq (X_T)^{(p^n/T)} \end{cases}$

On vérifie que $F_{X/S,n} = F_{X^{(p^{n-1}/S)}/S} \circ \dots \circ F_{X/S}$ $\qquad \left(F_{X/S,n}\right)_T = F_{X_T/T,n}$

En particulier, $X^{(p^n/S)} = \left(X^{(p^{n-1}/S)}\right)^{(p/S)}$ et si $A/_{\mathbb{F}_q}$ est une var. ab

avec $q=p^n$, on obtient un morphisme de $Ab_{\mathbb{F}_q}$:

$$\pi_A = \pi_{A,\mathbb{F}_q} : A \xrightarrow{F_{A/S}} A^{(p)} \xrightarrow{F_{A^{(p)}/S}} \dots \longrightarrow A^{(p^n)} = A.$$

($S = \operatorname{Spec} \mathbb{F}_{p^n}$). Donc $\pi_A \in End_K(A)$. Il va jouer un rôle crucial dans la suite.

Rq si on fixe un K fini et $A \in Ab_K$, on écrit $\pi_A = \pi_{A,K}$ défini comme avant

Clairement $\pi_{A \times_K L} = (\pi_A)^{[L:K]}$. π_A c'est aussi F_A^n si $K = \mathbb{F}_{p^n}$.

4) Frobenius, Verschiebung, dualité Dans SGA 3, exp VII A, 4.2-4.3 on construit pour tout $G \in Schgr_S$ commutatif plat un morphisme de groupes fonctoriel $V_G : G^{(p/S)} \longrightarrow G$ tq $\begin{cases} F_{G/S} \circ V_G = p\, id_{G^{(p/S)}} \\ V_G \circ F_{G/S} = p \cdot id_G \end{cases}$ On pose

$$V_{G,n} = G^{(p^n/S)} \xrightarrow{V_{G^{(p^{n-1}/S)}}} G^{(p^{n-1}/S)} \longrightarrow \dots \xrightarrow{V_G} G$$

alors $\begin{cases} V_{G,n} \circ F_{G/S,n} = p^n\, id_G \\ F_{G/S,n} \circ V_{G,n} = p^n\, id_{G^{(p^n)}} \end{cases}$ Ce G est compatible avec produit et chang. base.

Thm de dualité 1) $\begin{matrix} G \\ \downarrow \\ S \end{matrix}$ ($S \in Sch_{\mathbb{F}_p}$ local. noeth) fini plat $\in Schgr_S$, alors

$(F_{G/S})^D = V_{G^D}$ et $(V_G)^D = F_{G^D/S}$ où D est le foncteur dualité de Cartier.

2) $A \in Sch_S$ un schéma abélien $\Rightarrow \begin{cases} (F_{A/S})^t = V_{A^t} \\ (V_A)^t = F_{A^t} \end{cases}$

Voir SGA 3, VII A, 4.3.3.

5) Quelques sorites Si $X \in Sch_S$ est de type fini, alors

a) si $F_{X/S}$ isom. $\Rightarrow X/S$ non ramifié

b) X/S étale $\Rightarrow F_{X/S}$ isom

c) donc, pour X/S plat de type fini, X/S étale ssi $F_{X/S}$ isom.

Pour le a), le point est que $F^*_{X/S}\Omega_{X^{(p)}/S} \longrightarrow \Omega_{X/S}$ est 0 (le faire en passant en affine, facile), il suffit alors d'utiliser une des suites exactes fondamentales.

Le b) est facile: $X^{(p)}/S$ sera aussi étale (chang de base), donc $F_{X/S}$ aussi (car morph entre des sch étales); or il est clairement fini $\Rightarrow$ c'est un isom

4

Voir SGA 5, XIV pour : G/S local de pres finie est étale ssi $F_{G/S}$ est un isom.

Thm car $k = p$, G k-groupe fini connexe, alors $k[\ker(F_{G/k})] \simeq k[x_1 \ldots x_d]/(x_1^p, \ldots, x_d^p)$, $d = \dim_k T_{G,e}$

Voir Fontaine ou Tate (articles sur les groupes p-div).

III Isogénies - épisode 1 1) Rappels sur les quotients Voir SGA 3, exp IVA, thm 3.1, 3.2 pour le théorème profond, mais utile suivant :

Thm $G \in Schgr_k$ de type fini, $H \hookrightarrow G$ sous k-groupe fermé. Alors $\exists !$ k-schéma séparé de type fini G/H et un unique morphisme H-invariant $\pi : G \to G/H$, fp (ie fidèlement plat) tq

1) $G \times H \to G \times_{G/H} G$ est un isom 2) π est universel parmi les mor H-invar $G \to X$, X un schéma.

De plus, on a 3) $\forall K' \supset k$ corps, $G_{K'}/H_{K'} \longrightarrow (G/H)_{K'}$ est un isom

4) si G est k-lisse, G/H aussi et si de plus $H \triangleleft G$, $G/H \in Schgr_k$

Applications $G \xrightarrow{f} H$ mor de k-sch en gr type fini $\Rightarrow$ $G/_{\ker f} \in Schgr_k$ type fini et $G/_{\ker f} \to H$ est une imm fermée (SGA 3, exp VI B cor 1.4.2). Donc si f surjectif et H lisse $\Rightarrow$ $G/_{\ker f} \simeq H$. En particulier, si $G, H \in Ab_k$ $G/\ker f$ est une var ab sur k, que l'on peut voir comme sous-var ab de H. On écrit parfois $f(G)$ pour ceci.

Def et prop $f : A \to B$ morphisme ds Ab_k avec $\dim A = \dim B$. On dit que f est une isogénie si 1) f surjectif $\Leftrightarrow$ 2) $\ker f \in Schgr_k$ est fini 3) f est fini fp fidèlement plat (dernière fois !)

$1 \Rightarrow 2$ $A \xrightarrow{fp} A/\ker f \xrightarrow{\sim} B$ est fp et on applique le thm de dimension. $2 \Rightarrow 3$ Im f est un fermé de B de même dim $\Rightarrow$ f surj. On a vu alors que f est fp. Il reste f fini, or il est propre à fibres finies (les fibres étant des translatés de $\ker f$). $3 \Rightarrow 1$ évident

2) Séparabilité, 2 exemples fondamentaux

Soit f une isogénie $A \to B$, alors f est fini fp $\Rightarrow$ $f_* \mathcal{O}_A$ est localement libre de rg fini sur $\mathcal{O}_B$ et on obtient ainsi

constant par connexité

$$[K(A) : K(B)] = rg_{\mathcal{O}_B}(f_* \mathcal{O}_A) = |\ker f| \overset{def}{=} \deg f.$$

⑤ Z Pour $G \in Schgr_k$ fini on note $|G| = \dim_k H^0(G, \mathcal{O}_G)$. A ne pas confondre avec $|\ker f|$ comme cardinal d'un ensemble! Le "théorème de Lagrange" (qui doit tourner dans sa tombe) assure que $|G| = |H| \cdot |G/H|$ si $H \hookrightarrow G$ sous k-sch en gr de $G \in Schgr_k$ fini commutatif. On en déduit que $g \circ f$ reste une isogénie si f, g le sont et que $\deg(g \circ f) = \deg f \cdot \deg g$.

Prop. On dit que l'isogénie f est <u>séparable</u> si 1) f est étale comme morphisme $\Leftrightarrow$ 2) $\ker f$ est un k-sch. étale $\Leftrightarrow$ 3) $k(A)/f^*k(B)$ est séparable.

On dit que f est <u>purement inséparable</u> si 1) f est radiciel $\Leftrightarrow$ 2) $k(A)/f^*k(B)$ purement inséparable $\Leftrightarrow$ 3) $\ker f$ est connexe.

Les <u>idées</u> Pour séparable $1 \Leftrightarrow 2$ clair ainsi que $1 \Rightarrow 3$. Or si on a 3) f est étale en η_A (point générique), par propreté et irréductibilité c'est vrai sur un ouv dense $\Rightarrow$ partout (homogénéité). Pour inséparable c'est plus difficile $1 \Rightarrow 2$ clair (par def!) $2 \Rightarrow 3$ on écrit $A \longrightarrow \underbrace{A/(\ker f)^0 \longrightarrow B}_{\text{isog de } \ker = (\ker f) \text{ et, donc étale}}$ et on utilise le cas séparable

$3 \Rightarrow 1$ Il suffit $\forall L \supset K$ corps, $A(L) \longrightarrow B(L)$ est injective, or la fibre en un $x \in B(L)$ est $\simeq (\ker f)_L$, qui reste connexe (fait général!) et fini, donc un point. ☒

Application Toute isogénie $f : A \longrightarrow B$ se factorise "uniquement" (en un sens évident) $A \xrightarrow{g} C \xrightarrow{h} B$.
g : pur. insep, h : sep

En effet, la prop + la suite exacte $1 \to G^0 \to G \to G_{et} \to 1$ assurent que le "seul" choix est $A \longrightarrow A/(\ker f)^0 \longrightarrow B$. En fait, si car $k = p$ est <u>parfait</u> $G \longrightarrow G_{et}$ induit un isom $G_{red} \simeq G_{et}$ et la suite splitte canoniquement (SGA 3, exp XVII) Si G commutatif, $G = G^0 \times G_{et}$ canoniq.

<u>Exemples</u> 1) <u>Multiplication par n</u> Il est assez délicat (voire très ...) de montrer que $[n]_A : A \longrightarrow A$ est une isogénie de degré n^{2g}, $g = \dim A$, $\forall A \in Ab_k$. Cela ~~[illegible]~~ utilise le thm du carré de Weil + la théorie des intersections. Voir Mumford. Ce qui est facile et fondamental : si $(n, \mathrm{car}\, k) = 1$, $[n]_A$ est étale, donc $A[n] \overset{def}{:=} \ker [n]_A$ est étale sur k. En effet, $\forall G \in Schgr_k$ de loi m, $dm : T_{G \times G, e \times e} = T_{G,e} \oplus T_{G,e} \longrightarrow T_{G,e}$ est juste $(u, v) \longmapsto u + v$ (trivial), donc (récurrence) $d[n]_A$ est $x \longmapsto nx$ sur Lie A

et c'est un isom. Par le critère jacobien, $[n]_A$ est étale. On en déduit facilement que si k est <u>alg clos</u> (séparablement clos <u>ne suffit pas</u>), $A(k)$ est un groupe (abstrait) divisible, et que si $\mathrm{car}\, k \nmid n$ (k arbitraire), $A[n](k^s) \simeq (\mathbb{Z}/n\mathbb{Z})^{2g}$ (appliquer le résultat d'avant à $d \mid n$, $\forall d$).

2) Soit maintenant $A \in Ab_k$ ($\mathrm{car}\, k = p$) de dimension g. Alors $\ker F_{A/k}$ est un point (comme ensemble!) fermé et en prenant des ouverts affines en A et $A^{(p)}$ autour de ce point et son image, on voit que l'algèbre associée est de la forme $k[x_1 \ldots x_d]/(x_1^p, \ldots, x_d^p, f_1, \ldots, f_n)$, donc Ker est fini fini comme k-schéma. Comme on l'a remarqué avant, si $g = \dim A = \dim T_{A,e}$, l'algèbre assoc doit être de la forme $k[x_1 \ldots x_g]/(x_1^p, \ldots, x_g^p)$, qui a $\dim_k = p^g$ et qui est connexe. Donc : $F_{A/k} : A \longrightarrow A^{(p/k)}$ est une isogénie purement inséparable de degré p^g. On peut alors itérer et déduire que si $A/k = \mathbb{F}_q$ a dimension g, π_A est une isogénie de degré q^g. Whoops, je suis débile, c'est trivial par le dernier thm de III.

3) <u>lemme de factorisation, p-rang</u> Soit $f : A \to B$ une isogénie tq $\ker f$ soit tué par N (ie $\ker f \hookrightarrow A[N]$ comme schémas en groupes). Alors $\ker f \hookrightarrow \ker [N]_A$ et vu que $B \simeq A/\ker f$ et que $A/\ker[N]_A \simeq A$, on a (propr. univ du quotient) une factorisation
$$\begin{tikzcd} A \arrow[r, "f"] \arrow[rr, bend right, "{[N]_A}"'] & B \arrow[r, "g"] & A \end{tikzcd}$$
Comme $g \circ f = [N]_A \Rightarrow (f \circ g) \circ f = f \circ [N]_A = [N]_B \circ f$. Or f est fp $\Rightarrow f \circ g = [N]_B$. En particulier, si $N = \deg f$, un classique thm de Deligne assure que ceci marche et donc on a une telle factorisation. Bien sûr, g reste une isogénie car $[N]$ est surjective. Ceci montre qu'être isogène est une relation d'équivalence (joyeux!). On écrira $A \underset{k}{\sim} B$.

Rq Si $A \xrightarrow{f} B$ est une isogénie on veut relier $|\ker f(\bar{k})|$ et $\deg f$ c'est compatible avec les suites exactes, donc il reste à voir les cas f séparable / pur. insep.
Si f séparable, $\ker f$ est étale donc $|\ker f(\bar{k})| = |\ker f(k^s)| = |\ker f| = \deg f$
Si f purement inséparable, $\ker f$ est k-fini connexe $\Rightarrow |\ker f(\bar{k})| = 1$.

On en déduit que $|\ker f(\bar{k})| = |(\ker f)_{et}| = [K(A) : K(B)]_{sep}$

<u>Retour</u> Avec $f = [p^m]_A : A \longrightarrow A$ factorisé $A \xrightarrow[\text{pur. insep}]{g} B \xrightarrow[\text{sep}]{h} A$, on obtient $|A[p^m](\bar{k})| = |(\ker f)(\bar{k})| = \deg h$. Or vu que $\deg g \cdot \deg h = \deg f = p^{2mg}$ et que $[p^m]_A = V_{A,m} \circ F_{A/k,m}$, $F_{A/k,m}$ pur. insep de deg $mg \Rightarrow \deg h = p^{\tilde{f}}$

avec $0 \leq \tilde{f} \leq mg$. Si on prend $m=1$, $A[p](\bar{K}) \simeq (\mathbb{Z}/p\mathbb{Z})^f$ pour un $0 \leq f \leq g$ (tout élément du gr. ab $A[p](\bar{K})$ est tué par p!) la surjectivité de p^m sur $A(\bar{K})$ (vu avant) montre alors que $A[p^m](\bar{K}) \simeq (\mathbb{Z}/p^m\mathbb{Z})^f$ $\forall m$ (étudier $A[p^m](\bar{K}) \xrightarrow{p^{m-1}} A[p](\bar{K})$). On appelle ce f le p-rang de A.

Prop $f = f(A)$ est un invariant d'isogénie et stable par extension du corps de base. De plus, $f(A \times B) = f(A) + f(B)$.

Pour l'isogénie c'est évident : si $A \xrightarrow{f} B$ isogénie, $0 \to \ker f \to A \to B \to 0$ donne $0 \to (\ker f)[p^m] \to A[p^m] \to B[p^m] \to \dots \Rightarrow |\ker(A[p^m](\bar{K}) \to B[p^m](\bar{K}))| \leq \deg f \Rightarrow f(A) \leq f(B)$. Or $A \underset{K}{\sim} B \Rightarrow B \underset{K}{\sim} A \Rightarrow$ OK. Pour le produit, c'est clair. Pour le rang, c'est plus subtile, mais pas trop : utiliser la suite connexe-étale et les compatibilités de ses termes avec extension à un corps alg clos.

On dit qu'une courbe ell $E/K \supset \mathbb{F}_p$ est supersingulière si son p-rang est 0. Sinon, on dit qu'elle est ordinaire. ⚠ ceci n'est pas la bonne déf en dim plus grande. On y reviendra (I hope so...)

4) Isogénies et changement de base Il est clair que si $A \underset{K}{\sim} B$, alors $A_L \underset{L}{\sim} B_L$ $\forall L \supset K$. Par contre, on n'a pas de descente : comme on le voit sur les courbes elliptiques, il arrive que $E_1 \underset{K}{\not\sim} E_2$ sans qu'on ait $E_1 \underset{\bar{K}}{\sim} E_2$. Pour des questions bien plus subtiles sur le sujet, voir l'article de Brian Conrad : Chow's K/k-image and K/k-trace, and the Lang-Néron theorem.

5) Isogénies et dualité Thm si $f: A \to B$ est une k-isogénie, $f^t: B^t \to A^t$ en est une et on a un isomorphisme canonique

$$\ker(f^t) \underset{k\text{-sch gr}}{\simeq} (\ker f)^D, \quad (\text{où } G^D(T) = \mathrm{Hom}_{T\text{-sch gr}}(G_T, \mathbb{G}_{m,T})$$

est le dual de Cartier.

Pour la (difficile) dem, voir F. Oort, Commutative group schemes ou l'article de Oda ~~sur~~ The first de Rham cohomology of je ne sais plus quoi.

IV Polarisations et accouplements On utilisera ceci comme black box, les démos sont faites ds Mumford (voir aussi Oort ou Oda) et ne sont pas terriblement excitantes. Une splendide référence (comme toujours, d'ailleurs) est l'article de B. Conrad, Polarizations. On ne donne ici que l'essentiel

Si $\mathcal{L}$ est un faisceau inversible sur $A \in Ab_K$, on a un morphisme dans Ab_K $\varphi_{\mathcal{L}} : A \longrightarrow A^t$, $x \longmapsto$ classe de $t_x^* \mathcal{L} \otimes \mathcal{L}^{-1}$ et le point crucial est que si $\mathcal{L}$ est ample, $\varphi_{\mathcal{L}}$ est une isogénie et qu'on a une sorte de réciproque : si $H^0(\mathcal{L}, \mathcal{O}_{\mathcal{L}}) \neq 0$ et si $\operatorname{Ker} \varphi_{\mathcal{L}}$ est fini (ie $\varphi_{\mathcal{L}}$ isogénie), $\mathcal{L}$ est ample (voir Mumford). En fait, ce $\varphi_{\mathcal{L}}$ est une isogénie (si $\mathcal{L}$ ample) symétrique, ie $\varphi_{\mathcal{L}}^{\vee} \circ i_A = \varphi_{\mathcal{L}}$ si $i_A : A \xrightarrow[\text{can}]{\sim} A^{tt}$ (donné par Cartier-Nishi), mais le problème est que $\varphi_{\mathcal{L}}$ ne détermine pas $\mathcal{L}$ à isomorphisme près. Réciproquement, un thm difficile dû à Mumford assure que si <u>K est alg clos</u>, tout morphisme symétrique $\varphi : A \to A^t$ est de la forme $\varphi_{\mathcal{L}}$. En utilisant ceci ~~et~~ le thm de Lang sur $H^1(\bar{K}/K, G) = 1$ on peut montrer que si K est fini, toute isogénie symétrique $\varphi : A \to A^t$ est de la forme $\varphi_{\mathcal{L}}$.

<u>Def</u> une polarisation de A = morphisme symétrique $A \xrightarrow{\varphi} A^t$ (sur K) tq $(1 \times \varphi)^* (\mathcal{P}_A)$ ($\mathcal{P}_A$ fibré de Poincaré) soit ample. C'est alors automatiquement une isogénie.

<u>Thm</u> 1) si $\mathcal{L}$ est ample, $\varphi_{\mathcal{L}}$ est une polarisation. La réciproque est vraie. Donc toute $A \in Ab_K$ ($\forall K$!) a une polarisation.

2) Un morphisme symétrique $\varphi : A \to A^t$ est une polarisation ssi $\exists\, L/K$ extension (et alors c'est vrai $\forall L/K$) alg close et un $\mathcal{L}$ ample sur A_L tq $L \otimes \varphi = \varphi_{\mathcal{L}}$

les polarisations $\longleftrightarrow$ formes quadr. définies positives. Celles principales (ie de deg 1 $\Leftrightarrow$ ce sont des isom $A \to A^t$) $\longleftrightarrow$ formes quadr déf. pos de discr. 1.

3) <u>Accouplement de Weil</u> les théorèmes de dualité assurent qu'on a un accouplement $A[n] \times A^t[n] \xrightarrow{e_n} \mu_{n,K}$. Si $\varphi : A \to A^t$ est une polarisation on en déduit des accouplements

$$e_n^{\varphi} : A[n] \times A[n] \longrightarrow A[n] \times A^t[n] \longrightarrow \mu_n$$
$$(x, y) \longmapsto e_n(x, \varphi(y))$$

<u>Thm de compatibilité</u> e_n^{φ} est un accouplement bilinéaire (ie additif ...) alterné (ie $e_n^{\varphi}(x,x) = 1$ si $x \in A[n](T)$, $T \in Sch_K$), non dégénéré si $(n, \deg \varphi) = 1$.

De plus, $\forall f \in \operatorname{Hom}_K(A, B)$, f^t est la transposé de f sous e_n :

$$e_n(f(x), y) = e_n(x, f^t(y)), \quad (x, y) \in A[n](T) \times B^t[n](T)$$

Enfin, si $(mn, \operatorname{car} K) = 1$, on a $e_n(mx, my) = e_{mn}(x, y)^m$.

On a donc $e_{\ell^n}(x_n,y_n) = e_{\ell^{n+1}}(x_{n+1},y_{n+1})^{\ell}$ si $x \in T_\ell A = \varprojlim A[\ell^n](\bar{K})$
$y \in T_\ell A^t$

ce qui fait que

$$T_\ell A \times T_\ell A^t \xrightarrow{e_\ell} \mathbb{Z}_\ell(1) = \varprojlim \mu_{\ell^n}$$
$$((x_n)_n, (y_n)_n) \longmapsto (e_{\ell^n}(x_n,y_n))$$

est un accouplement parfait si $\ell \neq \mathrm{car}\, K$, $\mathbb{Z}_\ell$-bilinéaire et tq $e_\ell(x, T_\ell(f^t)(y)) = e_\ell(T_\ell(f)(x), y)$, $\forall f \in \mathrm{Hom}_K(A,B)$. Enfin, il est G_K-équivariant.

Donc toute polarisation $\varphi : A \to A^t$ induit un accouplement bilinéaire alterné Galois équivariant $T_\ell A \times T_\ell A \xrightarrow{e_\ell^\varphi} \mathbb{Z}_\ell(1)$.

3) Quelques applications de ce baratin. Une remarque : $A \xrightarrow{f} B$ isogénie, $\varphi : B \to B^t$ polar. $\Rightarrow$ $f^t \circ \varphi \circ f$ polar sur A (clairement, c'est une isog et si $\varphi_L = \varphi_{\mathcal{L}}$, $\mathcal{L}$ ample, $(f^t \circ \varphi \circ f)_L = \varphi_{f_L^* \mathcal{L}}$ (le faire sur les points) et $f_L^* \mathcal{L}$ reste ample car f est fini.

Thm de Poincaré $A \in Ab_K$ avec k parfait, $B \hookrightarrow A$ sous-var ab, alors $\exists$ C sous var ab (tout est sur k) tq
$$B \times C \longrightarrow A$$
$$(b,c) \longmapsto b+c$$
soit une isogénie.

Rq k parfait est inutile, mais la preuve est plus subtile (voir B. Conrad, ?) et on n'en aura pas besoin. Le point crucial dans ce qui suit est que $\forall G \in Schgr_K$ avec k parfait, G_{red} est un sous k-sch en gr fermé (car $G_{red} \times G_{red}$ reste réduit) ce qui est faux en général. Voir SGA 3 exp VIA.B. On utilisera le fait nontrivial suivant (SGA exp 6A, 2.1.1, 2.2, 2.4) : $\forall G \in Schgr_K$ local. type fini, G^0 est un sous-sch en gr fermé et ouvert, géométriquement irréd.

Preuve On prend $\mathcal{L}$ ample sur A, $\varphi_{\mathcal{L}} : A \to A^t$ la polar. assoc, $i : B \hookrightarrow A$ imm fermée $\Rightarrow$ $B \xrightarrow{i} A \xrightarrow{\varphi_{\mathcal{L}}} A^t \xrightarrow{i^t} B^t$. On pose $C = ((\ker i^t \circ \varphi_{\mathcal{L}})^0)_{red}$, qui est irréd par la rq. C'est un k-sch en gr geom intègre (k parfait) et clairement propre sur $\mathrm{Spec}\, k$ $\Rightarrow$ une sous-var ab de A. Si
$$f : B \times C \longrightarrow A$$
$$(b,c) \longmapsto b+c$$
, $\ker f \simeq B \cap C \hookrightarrow B \cap \ker i^t \circ \varphi_{\mathcal{L}} \hookrightarrow \ker(i^t \circ \varphi_{\mathcal{L}} \circ i)$, fini car $i^t \circ \varphi_{\mathcal{L}} \circ i$ isogénie. Maintenant, ~~est donc~~ $\dim C \geq \dim A - \dim B$ et $\dim B \times C = \dim B + \dim C$ (car B, C geom. intègres). Ceci permet de conclure que f est surj $\Rightarrow$ une isogénie. ∎

Une récurrence sur la dimension permet alors de démontrer le très important résultat : $\forall A \in Ab_K$, $\exists\, n_i \geq 1$ et $A_i \in Ab_K$ 2 à 2 non isogènes simples tq $A \underset{K}{\sim} A_1^{n_1} \times \cdots \times A_s^{n_s}$.

Rappel : A est dite simple si elle n'a pas de sous-variété abelienne nontriviale. Clairement $\forall f \in \mathrm{End}_K A \setminus \{0\}$, f est une isogénie (car $A/\ker f \underset{\text{sous-var ab}}{\hookrightarrow} A$, donc ça doit être A et f est surj).

<u>Thm de descente des polarisations</u> Soit $A \xrightarrow{f} B$ une isogénie et $A \xrightarrow{\varphi} A^t$ une ~~polarisation~~ isogénie symm. On peut alors écrire $\varphi = f^t \circ g \circ f$ avec $g : B \longrightarrow B^t$ isogénie symm. ssi $\begin{cases} \ker f \subset \ker \varphi \\ \ker f \text{ est totalement isotrope pour } e_\varphi : \ker\varphi \times \ker\varphi \longrightarrow \mathbb{G}_m \end{cases}$

De plus, g sera une polarisation ssi φ l'est.

Voir le livre de Moonen et Van der Geer pour la preuve. Le thm est très important, car il permet de démontrer les résultats suivants (loc. cit) :

- $A \in \mathrm{Ab}_K$ avec <u>K alg clos</u> $\Rightarrow$ A est isogène à une var ab ayant une polaris. principale.
- astuce de Zarhin. $A \in \mathrm{Ab}_K$ (K <u>quelconque</u>) $\Rightarrow$ $A^4 \times (A^t)^4$ a une polarisation principale. Idée : si φ est une polar sur A, soit $B = A^4$, on a une polar. $\varphi^4 : B \to B^t$. Si $f \in \mathrm{End}_K B$, on montre que la polarisation $\varphi^4 \times \varphi^4 : B \times B \longrightarrow B^t \times B^t$ descend en une polarisation sur $B \times B^t$ via l'isogénie $g : B \times B \longrightarrow B \times B^t$, $(b_1, b_2) \mapsto (b_1 - f(b_2), \varphi^4(b_2))$ (qui vérifie clairement $\deg g = \deg \varphi^4$) ssi $\exists\, h \in \mathrm{End}\, B^t$ tq $h \circ \varphi^4 = \varphi^4 \circ h$ et $1 + h^t f \in \mathrm{End}_K B$ tue $\ker \varphi^4$. On prend alors f l'endomorphisme $(x_1, \dots, x_4)^t \mapsto X \begin{pmatrix} x_1 \\ \vdots \\ x_4 \end{pmatrix}$ pour une matrice quaternion X choisie tq les entrées de $I_4 + {}^t X X$ soient multiples d'un N qui tue $\ker \varphi^4$ (ça existe toujours par le thm des 4 carrés)

4) <u>Théorèmes de finitude</u> Les choses sont loin d'être évidentes, on va se contenter de bien ~~...~~ contempler leur beauté :

<u>Thm</u> : si $g, d \geq 1$ sont donnés, ainsi que K fini, il n'y a qu'un nombre fini de classes d'isom de var ab de dimension g sur K, ayant une K-polaris de degré d.

Le point est que la théorie des intersections (qui reste du chinois pour moi) assure que toute polarisation $\varphi : A \longrightarrow A^t$ de degré d est de la forme $\varphi_{\mathcal{L}}$ pour $\mathcal{L}$ ample (on utilise K fini et l'astuce de Lang), que $\mathcal{L}^3$ est très ample et permet de plonger A comme une sous K var fermée de degré $6^g \cdot d\, g!$ dans $\mathbb{P}_K^{6^g d - 1}$

(11) Une telle variété est dét à isom près par sa forme de Chow => la classe d'isom est déf par un nb fini d'éq à coeff ds K, de deg borné en termes de g, d => clr.
Voir l'article de Milne ds le livre de Silverman pour des détails.

<u>Thm 2 (Zarhin, Lenstra, Oort)</u> $A \in Ab_K$ (K quelconque) =>

$$\{\text{sous } K \text{ var ab de } A\} / \mathrm{Aut}_K(A) \quad \text{est fini.}$$

Voir leur article, Abelian subvarieties, le point est que si $B \hookrightarrow A$ sous K var ab, $I(B) = \{f \in \mathrm{End}_K A \mid f(A) \subset B\}$ est un idéal (à gauche) de $\mathrm{End}_K(A)$ et B est dét à action de $\mathrm{Aut}_K(A)$ près par le sous $\mathrm{End}_K(A) \otimes \mathbb{Q}$ module $I(B) \otimes_{\mathbb{Z}} \mathbb{Q}$.
On conclut par le thm de Borel et Harish-Chandra : A $\mathbb{Q}$-algèbre finie (comme $\mathbb{Q}$-ev) semisimple, M un A-module de type fini qui est un idéal à gauche, L un $\mathbb{Z}$-réseau de M =>

$$\{\text{sous } A \text{ modules de } M\} / \begin{smallmatrix}\text{autom de } A\text{-mod de } M \\ \text{tq } \varphi(L) = L\end{smallmatrix} \quad \text{est fini.}$$

<u>Thm 3 (Zarhin)</u> Si K est fini et $g \geq 1$ est donné,

$$\{A \in Ab_K,\ \dim A = g\} / \text{isom} \quad \text{est fini.}$$

L'astuce est diabolique : A s'identifie à une sous K-var ab de $(A \times A^t)^4$ qui a une polarisation de degré 1. On met ensemble les thm 1 et 2 ! Alléluia !

<u>V Module de Tate, $\mathrm{End}_K(A)$, épisode 1</u> 1) Si $A/_K \in Ab_K$ on note

$$T_\ell A = \varprojlim_n A[\ell^n](\overline{K}),$$ relativement aux flèches $A[\ell^n](\overline{K}) \xrightarrow{\ell} A[\ell^{n-1}](\overline{K})$ (surjectives, comme on l'a vu). Ce n'est pas une bonne notion que si $\ell \neq \mathrm{car}\, K$, ce qu'on supposera toujours. On a vu que $A[\ell^n](\overline{K}) \simeq (\mathbb{Z}/\ell^n\mathbb{Z})^{2g}$, ce qui fait que $T_\ell A$ devient un $\mathbb{Z}_\ell$ module libre de rg $2g$ (l'isomorphisme $T_\ell A \simeq \mathbb{Z}_\ell^{2g}$ n'est <u>pas</u> canonique) la topologie ℓ-adique sur $T_\ell A$ est alors celle de la limite projective avec $A[\ell^n](\overline{K})$ discret. Enfin, G_K agit de façon ~~discrète~~ continue sur $A[\ell^n](\overline{K})$, donc agit continûment sur $T_\ell A$ pour la top ℓ-adique. Connaître $T_\ell A$ + action de G_K, c'est connaître tous les sch en groupes $A[\ell^n]$ (car <=> connaître $T_\ell A / \ell^n T_\ell(A) = A[\ell^n](K^s)$ + actions de G_K et $A[\ell^n]$ est étale sur K). Enfin, la construction est fonctorielle : tout $f \in \mathrm{Hom}_K(A, B)$ induit $T_\ell f : T_\ell A \to T_\ell B$ $(x_n)_n \mapsto (f(x_n))_n$ $\mathbb{Z}_\ell$-linéaire, G_K équiv.

Thm marrant $A \xrightarrow{f} B$ isogénie de degré n dans Ab_K, alors
$0 \to T_\ell A \xrightarrow{T_\ell f} T_\ell B \longrightarrow$ ℓ-Sylow de $(\operatorname{Ker} f)(K^s) \to 0$ est exacte comme

suite de $\mathbb{Z}_\ell[G_K]$ modules.

Idée (pour les détails voir Moonen-Van der Geer) Comme $\mathbb{Z}_\ell[G_K]$ modules on a

$T_\ell A = \operatorname{Hom}(\mathbb{Q}_\ell/\mathbb{Z}_\ell, A(K^s))$ ce qui fait qu'on a

$0 \to \underbrace{\operatorname{Hom}(\mathbb{Q}_\ell/\mathbb{Z}_\ell, (\operatorname{Ker} f)(K^s))}_{0 \text{ car } \operatorname{Ker} f \text{ fini}} \to T_\ell A \xrightarrow{T_\ell f} T_\ell B \to \operatorname{Ext}^1(\mathbb{Q}_\ell/\mathbb{Z}_\ell, (\operatorname{Ker} f)(K^s)) \to \operatorname{Ext}^1(\mathbb{Q}_\ell/\mathbb{Z}_\ell,$
ds la cat de $\mathbb{Z}$-modules

$A(K^s)) \to \dots$ (venue via $0 \to (\operatorname{Ker} f)(K^s) \to A(K^s) \to B(K^s) \to 0$).

Or $\operatorname{Ext}^1(\mathbb{Q}_\ell/\mathbb{Z}_\ell, (\operatorname{Ker} f)(K^s)) \simeq$ ℓ-Sylow de $(\operatorname{Ker} f)(K^s) \simeq \operatorname{Hom}(\mathbb{Z}_\ell$, ce ℓ-Sylow$) \simeq$

ce ℓ-Sylow (K^s) (via $0 \to \mathbb{Z}_\ell \to \mathbb{Q}_\ell \to \mathbb{Q}_\ell/\mathbb{Z}_\ell \to 0$) et si K est parfait (avec un peu

plus de boulot si K n'est pas parfait) $\operatorname{Ext}^1(\mathbb{Q}_\ell/\mathbb{Z}_\ell, A(K^s)) = 0$ car $A(K^s)$ est divisible.

2) Encore des factorisations! Prop 1 1) Si $f \in \operatorname{Hom}_K(A, B)$ et $\ell^n \mid T_\ell f$ dans

$\operatorname{Hom}_{\mathbb{Z}_\ell}(T_\ell A, T_\ell B)$, alors ℓ^n divise f dans $\operatorname{Hom}_K(A, B)$

2) K parfait, φ polar. de A tq l'acc. $e_\varphi : T_\ell A \times T_\ell(A) \to \mathbb{Z}_\ell(1)$ tombe dans

$\ell^n \mathbb{Z}_\ell(1) \Rightarrow \exists\, \tilde{\varphi}$ polar de A tq $\varphi = \ell^n \tilde{\varphi}$.

1) est trivial car la surj. de $\ell : A(K^s) \to A(K^s)$ assure que $\ell^n \mid T_\ell f$ ssi f

est 0 sur $A[\ell^n](K^s) \underset{A[\ell^n] \text{ étale}}{\Longleftrightarrow}$ f est 0 sur $A[\ell^n]$ $\underset{\text{voir la section sur les quotients}}{\Longleftrightarrow}$ $\ell^n \mid f$. Pour 2 voir l'article de Milne (mais on n'en aura pas besoin)

LE thm clé Soit X un sous $\mathbb{Z}_\ell$-module de $T_\ell A$ d'indice ~~...~~ fini, G_K stable.
Il existe alors $B \in Ab_K$ et $f : B \to A$ une K-isogénie ~~de degré~~ tq
$(T_\ell f)(T_\ell B) = X$

c'est la "machine à produire des endom" et une sorte de réciproque du thm marrant.

Dem si $pr_n : T_\ell A \to A[\ell^n](K^s)$ est ce que l'on pense, on soit $X_n = pr_n(X)$ (pris tq $X \supset \ell^n T_\ell A$)

$\subset A[\ell^n](K^s)$ comme un sous K-sch en gr de $A[\ell^n]$ le morphisme
G_K stable

quotient $A \xrightarrow{\pi} A/X_n$ est par def une isogénie de Ker $= X_n$. ~~de deg $\pi = |X_n|$~~

Comme $\operatorname{Ker} \pi \subset A[\ell^n] = \operatorname{Ker} \ell^n$, on a une isogénie $f : B = A/X_n \longrightarrow A$

tq $\begin{cases} \pi \circ f = \ell^n \\ f \circ \pi = \ell^n \end{cases}$. C'est un jeu d'écriture en utilisant ces relations et

$0 \to X_n \to A(\bar{K}) \xrightarrow{\pi} B(\bar{K}) \to 0$ de déduire que

ce f et $B = A/X_n$ marchent.

(13) 3) Injectivité de la flèche de Tate. Si $f \in \mathrm{End}_K(A)$ on pose $\deg f = 0$ si f n'est pas une isogénie. La théorie de l'intersection (voir Mumford) assure que $\forall f_i \in \mathrm{End}_K A$ $\exists$ $P \in \mathbb{Q}[x_1 \ldots x_s]$ homogène de degré $2g$ tq $\deg(\alpha_1 f_1 + \cdots + \alpha_s f_s) = P(\alpha_1, \ldots, \alpha_s)$ $\forall$ $\alpha_i \in \mathbb{Z}$. On note $P_f \in \mathbb{Q}[x]$ le pol. unitaire tq $P_f(n) = \deg([n]_A - f)$ $\forall$ $n \in \mathbb{Z}$. Tout ce baratin s'étend à $\mathrm{End}^\circ_K(A) = \mathrm{End}_K(A) \underset{\mathbb{Z}}{\otimes} \mathbb{Q}$.

Thm important La flèche $\mathrm{Hom}_K(A,B) \underset{\mathbb{Z}}{\otimes} \mathbb{Z}_\ell \longrightarrow \mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell A, T_\ell B)$ venue via $f \otimes \lambda \longmapsto \lambda T_\ell f$ est injective et $\mathrm{Hom}_K(A,B)$ est $\mathbb{Z}$-libre de rg $\leq 4 g_A g_B$.

$\angle$ contrairement à ce qu'on peut entendre souvent, la $2^{ième}$ assertion n'est pas une conséquence formelle de la $1^{ère}$. Il faut montrer que Hom est de type fini (clairement il est sans torsion).

Dem le point clé est : $M \subset \mathrm{Hom}_K(A,B)$ de type fini $\Rightarrow$ $M' = \{f \in \mathrm{Hom}_K(A,B) \mid \exists\, n \in \mathbb{Z}^*, nf \in M\}$ l'est aussi. Par Poincaré on peut supposer A, B simples, isogènes (sinon c'est clair) et même $A = B$ (justifications évidentes). Or alors M' est un sous-gr discret du $\mathbb{Q}$ ev $M \underset{\mathbb{Z}}{\otimes} \mathbb{Q}$ de dim finie (car $\forall$ $f \in \mathrm{End}_K A \setminus \{0\}$ f est une isogénie et $\{u \in M \underset{\mathbb{Z}}{\otimes} \mathbb{Q} \mid |\deg u| < 1\}$ est un vois de 0 car deg est un pol homogène).

L'injectivité est alors facile : si $f_i \in \mathrm{Hom}_K(A,B)$ sont $\mathbb{Z}$-libres et $\sum a_i T_\ell(f_i) = 0$, prendre $M = \sum \mathbb{Z} f_i$, alors $(M')' = M'$ et $M' \otimes \mathbb{Z}_\ell \to \mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell A, T_\ell B)$ n'est pas injective. Donc, si $g_1, \ldots, g_s$ $\mathbb{Z}$-base de M', $\sum b_i T_\ell(g_i) = 0$ avec $g_i \in \mathbb{Z}_\ell$ pas tous dans $\ell \mathbb{Z}_\ell$.
On écrit $b_i = \underset{\in \mathbb{Z}}{\underbrace{(b_i)_0}} + \ell c_i$ $\underset{\text{lemmes de factorisation}}{\Rightarrow}$ $\sum (b_i)_0\, g_i = \ell h$, $h \in \mathrm{Hom}_K(A,B)$. Or $h \in (M')' = M'$ $\Rightarrow$ $\ell \mid (b_i)_0$ $\Rightarrow$ $\ell \mid b_i$, faux.

Conclusion : la flèche est inj et $\mathrm{rang}_{\mathbb{Z}} \mathrm{Hom}_K(A,B) \leq 4 g_A g_B$. Par le point clé si $g_1, \ldots, g_s \in \mathrm{Hom}_K(A,B)$ est une $\mathbb{Q}$-base de $\mathrm{Hom} \otimes \mathbb{Q}$, et si $M = \sum \mathbb{Z} g_i$, on a $\mathrm{Hom}_K(A,B) \subset M'$, de type fini.

Cor $A \in \mathrm{Ab}_K \Rightarrow \mathrm{End}^\circ_K(A) = \mathrm{End}_K(A) \underset{\mathbb{Z}}{\otimes} \mathbb{Q}$ est une $\mathbb{Q}$-alg semisimple de dim finie sur $\mathbb{Q}$.

Via Poincaré et ce thm, le seul point à voir est que $A \underset{K}{\sim} B \Rightarrow \mathrm{End}^\circ_K(A) \underset{\mathbb{Q}}{\simeq} \mathrm{End}^\circ_K(B)$, or ceci est clair : prendre $f : A \to B$ de degré n, $g : B \to A$ tq $g \circ f = n$, $f \circ g = n$, alors $\mathrm{End}^\circ_K(A) \longrightarrow \mathrm{End}^\circ_K(B)$ $x \longmapsto \frac{1}{n} f \circ x \circ g$ est un isom de $\mathbb{Q}$-alg (trivial). L'inverse est $y \longmapsto \frac{1}{n} g\circ y \circ f$). On vérifie que cet isom est vraiment canonique, au sens où il ne dépend pas de n et g. Si k est fini, la fonctorialité du Frobenius assure qu'il envoie π_A sur π_B. Donc 2 k-var ab isogènes A, B ont la propr que $\mathbb{Q}(\pi_A) \simeq \mathbb{Q}(\pi_B)$ ~~il suffit à voir que~~

$\pi_A \longmapsto \pi_B$

4) Un théorème horriblement important

le machin défini avant, $P_f(n) = \deg([n]-f)$

Superthm Si $l \neq \operatorname{car} k$ (as usual!) et $f \in \operatorname{End}_k(A)$, P_f = le polynôme caractéristique de $V_l f \in \operatorname{End}_{\mathbb{Q}_l}(V_l A)$, où $V_l A = T_l A \underset{\mathbb{Z}_l}{\otimes} \mathbb{Q}_l$.

Idée le point crucial est le thm marrant, qui assure (via un petit argument avec la base adaptée) que $v_l(\deg f) = v_l(\det T_l f)$ (si f n'est pas une isogénie, ceci est clair car $T_l \operatorname{Ker} f \subset \operatorname{Ker} T_l f$) On remplace f par ~~$F(f) \in \mathbb{Z}[x]$~~ $F(f)$ avec $F \in \mathbb{Z}[x]$ pour déduire que $v_l\left(\prod_{\substack{P_f(z)=0 \\ z\in\overline{\mathbb{Q}}_l}} F(z)\right) = v_l\left(\prod_{\chi_{T_l f}(z)=0} F(z)\right)$, d'où

$v_l\left(\prod_{P_f(z)=0} (x-z)\right) = v_l\left(\prod_{\chi_{T_l f}(z)=0} (x-z)\right) \; \forall x \in \overline{\mathbb{Q}}_l$ (prendre F = pol min de x)

Après c'est un jeu d'analyse p-adique. Voir Mumford pour une autre approche.

Cor $P_f \in \mathbb{Z}[x]$ et $P_f(f) = 0$ dans $\operatorname{End}_k(A)$

C'est clair, car les valeurs propres de $V_l f$ sont des entiers algébriques ($\operatorname{End}_k(A)$ est entier sur $\mathbb{Z}$, donc $T_l f$ vérif éq à coeff $\in \mathbb{Z}$ unitaire ; sinon parce que $V_l f$ stabilise le réseau $T_l A$), donc les coeff de P_f sont entiers alg dans $\mathbb{Q} \Rightarrow$ dans $\mathbb{Z}$. Enfin, $T_l(P_f(f)) = P_f(T_l f) = \chi_{T_l f}(T_l f) = 0 \Rightarrow P_f(f) = 0$

On notera $f_A = P_{\pi_A}$ si $A \in \mathrm{Ab}_k$, k fini. Bien sûr, la multiplicativité du degré assure que $f_{A^n} = f_A^n$. Par ce qu'on a vu jusqu'à présent, $f_A \in \mathbb{Z}[x]$ est unitaire de deg $2g$, de terme constant q^g ($k = \mathbb{F}_q$) et $f_A(\pi_A) = 0$ dans $\operatorname{End}_k(A)$.

VI L'algèbre $\mathbb{Q}(\pi_A)$, les conjectures de Weil

1) Commençons avec $g=1$, ie A courbe elliptique. Tout a été fait avant :

(15) $T_\ell \pi_A$ agit sur $V_\ell A$ de dim 2 sur $\mathbb{Q}_\ell$, son det est $\deg \pi_A = q$ (si $k = \mathbb{F}_q$) et comme $\deg(m+n\pi_A) \geq 0$ $\forall m,n \in \mathbb{Z}$ => le polynôme caract de π_A est $X^2 - a_q X + q$ avec $a_q^2 \leq 4q$. Par ce qu'on a vu, $\pi_A - id$ est séparable (une isogénie car 1 n'est pas racine de P_{π_A}) et

$$|A(k)| = |\mathrm{Ker}(\pi_A - id)| = |\deg(\pi_A - id)| = P_{\pi_A}(1) = 1+q-a_q$$

Si on écrit $P_{\pi_A} = (X-\alpha_1)(X-\alpha_2)$, on a $|\alpha_1| = |\alpha_2| = \sqrt{q}$ et par chang. base $A \longmapsto A_{\mathbb{F}_{q^n}}$ et fonctorialité du Frobenius ($\pi_{A_{\mathbb{F}_q^n}} = \pi_A^n$) on a

$$|A(\mathbb{F}_{q^n})| = |\mathrm{Ker}(\pi_A^n - 1)| = |\deg(\pi_A^n - 1)| = (\alpha_1^n - 1)(\alpha_2^n - 1) = q^n - (\alpha_1^n + \alpha_2^n) + 1.$$

Alors $\log Z(A/k, T) = \sum_{n\geq 1} |A(\mathbb{F}_{q^n})| \frac{T^n}{n} = \log \frac{(1-\alpha_1 T)(1-\alpha_2 T)}{(1-T)(1-qT)}$ => les conj de Weil.

Rq précisons un peu : si $f : A \to B$ est une isogénie séparable, $\mathrm{Ker} f$ est étale donc $|\mathrm{Ker} f| = |(\mathrm{Ker} f)(k^s)| = \deg f$. Par fonctorialité,

$$A(\mathbb{F}_{q^n}) = \ker(F_{A/k,n} - 1)(k^s), \text{ d'où la conclusion car } F_{A/k,n} = \pi_A^n.$$

En général, cet argument montre que si on factorise $P_{\pi_A} = \prod_{i=1}^{2g}(X - a_i)$ ($a_i \in \overline{\mathbb{Z}}$), alors $|A(\mathbb{F}_{q^n})| = \prod_{i=1}^{2g}(a_i^n - 1)$. Mais c'est 1000 fois plus profond de montrer que $|a_i| = \sqrt{q}$. Le point est de remplacer la propriété de positivité de deg par l'involution de Rosati : on fixe $\mathcal{L}$ ample sur A, $\varphi_\mathcal{L} : A \to A^t$ le truc induit. Comme on a vu 10 fois (lemme de factorisation) la flèche

$$\mathrm{End}^\circ_k(A) \longrightarrow \mathrm{End}^\circ_k(A)$$
$$f \longmapsto \varphi_\mathcal{L}^{-1} \circ f^t \circ \varphi_\mathcal{L} = f^\dagger$$

a un sens (ie $\varphi_\mathcal{L}^{-1}$ existe dans $\mathrm{End}^\circ_k(A)$ – PAS ds $\mathrm{End}_k(A)$)

On peut montrer que $(fg)^\dagger = g^\dagger f^\dagger$, $(f^\dagger)^\dagger = f$, $(af)^\dagger = a f^\dagger$ si $a \in \mathbb{Q}$, $(f+g)^\dagger = f^\dagger + g^\dagger$, que $e_\ell(f(x), T_\ell(\varphi_\mathcal{L})(y)) = e_\ell(x, T_\ell(\varphi_\mathcal{L}) f^\dagger(y))$ et, le plus important (et difficile), que $f \mapsto \mathrm{Tr}(f f^\dagger)$ est une forme quadr définie positive sur $\mathrm{End}^\circ_k(A)$, à val ds $\mathbb{Q}$. Ici

$$\mathrm{Tr} : \mathrm{End}^\circ_k(A) \longrightarrow \mathbb{Q}$$
$$f \longmapsto \text{trace de } V_\ell f \in \mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(A)).$$

<u>Point clé</u> : $\pi_A^\dagger \pi_A = q$. Par fonctorialité de π_A, cela revient à dire que $\pi_{A^t} \circ (\pi_A)^t = q$. Or LHS $= F^n_{A/k} \cdot V^n_A = p^n = q$ par ce qu'on a vu (pour

une autre preuve avec des faisceaux voir Mumford).

C'est ce petit machin qui nous donnera tout :

Claim $\mathbb{Q}[\pi_A] \subset \mathrm{End}_k^0(A)$ est une algèbre séparable, stable par Rosati

C'est clair qu'elle est stable et de $\dim_{\mathbb{Q}} < \infty$, il reste à voir qu'elle est réduite. Or si $f \in \mathbb{Q}[\pi_A] \setminus \{0\}$ on a $f^\dagger f = g \neq 0$ (car Rosati def positive) et $g = g^\dagger \Rightarrow g^2 \neq 0$, on itère $\Rightarrow g^{2^n} \neq 0 \ \forall n \Rightarrow$ clr.

$\rightarrow$ (zut, c'est pas vraiment clair : π_A isogénie $\Rightarrow$ $\mathbb{Q}[\pi_A] \to \mathbb{Q}[\pi_A]$, $u \mapsto \pi_A u$ injective $\Rightarrow \pi_A^{-1} \in \mathbb{Q}[\pi_A] \Rightarrow \pi_A^\dagger = q\pi_A^{-1} \in \mathbb{Q}[\pi_A]$, ok)

Si on pose $\mathbb{Q}[\pi_A] = \prod_1^t K_i$, K_i corps de nb, Rosati preserve chaque facteur K_i car elle est définie positive sur $\mathbb{Q}[\pi_A]$. On en déduit facilement (ou pas) que les K_i sont totalement réels ou des corps CM où Rosati agit comme conjugaison complexe, donc $\forall\ \varphi : \mathbb{Q}[\pi_A] \to \mathbb{C}$ un plongement, $\underbrace{\varphi(\pi_A^\dagger) = \overline{\varphi(\pi_A)}}_{\text{un peu abusé...}} \Rightarrow |\varphi(\pi_A)| = \sqrt{q}$. On vient donc de dem les

Conjectures de Weil les racines du pol caract du π_A ont module $\sqrt{q}$ et sont des q-nb de Weil si A est simple, ie des entiers algébriques dont les conjugués ont module $\sqrt{q}$.

2) Autre point clé pour le thm de Tate

Thm clé Soit F_ℓ la sous-algèbre de $\mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(A))$ ($A \in \mathrm{Ab}_k$, $k = \mathbb{F}_q$ fini) engendrée par les automorphismes induits par G_k. Alors

$$F_\ell \simeq \mathbb{Q}_\ell \otimes_{\mathbb{Q}} \mathbb{Q}[\pi_A]$$

et il existe ℓ tq $F_\ell \simeq \mathbb{Q}_\ell^n$ pour un certain n.

Le 1er point est clair, car $\langle \mathrm{Fr}_k \in G_k \rangle$ est dense ds G_k et que π_A agit sur $A(\bar{k})$ comme Fr_k, donc pareil sur $V_\ell(A)$. Pour l'autre point on a vu que $\mathbb{Q}[\pi_A] \simeq \prod_1^t K_i$ avec K_i corps de nombres $\Rightarrow F_\ell \simeq \prod_{i=1}^t \mathbb{Q}_\ell \otimes_{\mathbb{Q}} K_i \simeq \prod_{i=1}^t \prod_{v \text{ place de } K_i \mid \ell} K_v$, donc il reste à voir que si K_i sont des corps de nombres $\exists\ \ell$ tq $\mathbb{Q}_\ell \otimes_{\mathbb{Q}} K_i \simeq \mathbb{Q}_\ell^{n_i}$, $\forall i \Leftrightarrow \forall f \in \mathbb{Z}[X]$ (prendre f = produit des polyn minimaux d'un el primitif de $K_i/\mathbb{Q}$) $\exists$ une ∞ de ℓ tq f se décompose ds $\mathbb{Q}_\ell[X]$

(17) Or ceci vient de Chebotarev + Hensel ($\exists \infty$ de l tq f se décompose mod l).

3) Frobenius et Independence Day. On a vu que $\mathbb{Q}[\pi_A] \subset \mathrm{End}^0_k(A)$ est séparable et que la flèche de Tate est injective $\Rightarrow V_\ell \pi_A \in \mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(A))$ est semisimple. De plus, P_{π_A} = pol car de $V_\ell \pi_A$ ne dépend pas de $\ell \neq \mathrm{car}\, k$ par le super thm. Si on écrit $P_{\pi_A} = \prod_{\substack{Q \in \mathbb{Q}_\ell[X] \text{ unitaire} \\ \text{irred}}} Q^{n_Q}$, il est élémentaire que

$\dim_{\mathbb{Q}_\ell} \{X \in M_{2g}(\mathbb{Q}_\ell) \mid X V_\ell \pi_A = V_\ell \pi_A X\} = \sum_Q n_Q^2 \deg Q$. Mais $P_{\pi_A} \in \mathbb{Z}[X]$ (vu!) et on peut faire la même manip sur $\mathbb{Q}[X]$. Naturellement, on tombe sur la même chose. Donc $\dim_{\mathbb{Q}_\ell} \{X \in M_{2g}(\mathbb{Q}_\ell) \mid X V_\ell \pi_A = V_\ell \pi_A X\}$
$= \sum_{\substack{R \in \mathbb{Q}[X] \text{ unitaire} \\ \text{irred}}} n_R^2 \deg R$ (si $P_{\pi_A} = \prod R^{n_R}$). Comme on a vu, $V_\ell \pi_A$
= end. induit par $\mathrm{Fr}_k \in G_k \Rightarrow$

Thm d'indépendance: $\dim_{\mathbb{Q}_\ell}$ $\mathrm{End}_{\mathbb{Q}_\ell[G_k]}(V_\ell A)$ ne dépend pas de $\ell \neq \mathrm{car}\, k$.

VII Finally, enfin et in the end: le thm de Tate

Thm "ultime" (Tate). Si k est fini, $\ell \neq \mathrm{car}\, k$ et $A, B \in \mathrm{Ab}_k$,

$$\mathbb{Z}_\ell \otimes_{\mathbb{Z}} \mathrm{Hom}_k(A,B) \xrightarrow{\Phi} \mathrm{Hom}_{G_k}(T_\ell(A), T_\ell(B)) \text{ est bijective.}$$

1) Réductions. 1) Il suffit de mq $\mathrm{id} \otimes \Phi \otimes$ $\mathbb{Q}_\ell \otimes_{\mathbb{Z}} \mathrm{Hom}_k(A,B) \longrightarrow \mathrm{Hom}_{\mathbb{Q}_\ell(G_k)}(V_\ell(A), V_\ell B)$ ~~est~~ surjective: le point est que $\mathrm{coker}\, \Phi$ n'a pas de torsion (tout ce qu'on veut est Φ surjective, on a vu qu'elle était injective long time ago!): il suffit en effet de voir que si $\ell g \in \mathrm{Im}\, \Phi$, alors $g \in \mathrm{Im}\, \Phi$. Or $\exists\, u_n \in \mathrm{Hom}_k(A,B)$ et $x_n \in \mathrm{Hom}_{G_k}(T_\ell A, T_\ell B)$ tq $T_\ell(u_n) + \ell^n x_n = \ell g$ (tronquer les p-adiques!) donc $\ell \mid T_\ell(u_n)$ et par le lemme de factorisation (always Coca-Cola!) $\exists\, v_n \in \mathrm{Hom}_k(A,B)$ tq $u_n = \ell v_n \Rightarrow g = \underbrace{T_\ell(v_n)}_{\in \mathrm{Im}\,\Phi_0} + \ell^{n-1} x_n \overset{n \to \infty}{\Rightarrow} g \in \mathrm{Im}\, \Phi_0$, fermé (car Hom_k libre)

2) Il suffit de le faire (le 1!) pour $A = B$. C'est du abstract nonsense évident: si on arrive à faire 1 avec $A = B$, on sait le faire avec $C = A \times B$ $\Rightarrow$ on sait le faire avec A, B. (bla...) $C = A \times B$

3) Il suffit de faire 2 pour un seul $\ell \neq p$. C'est clair, car $\mathbb{Q}_\ell \otimes_{\mathbb{Z}} \mathrm{End}_k(A) \hookrightarrow$

$\mathrm{End}_{\mathbb{Q}_\ell[G_k]}(V_\ell A)$ et on a vu que $\dim_{\mathbb{Q}_\ell}$ RHS ne dépend pas de $\ell \neq$ car k

Prenons ds la suite un $\ell \neq$ car k comme ds le thm clé : F_ℓ = sous-alg de $\mathrm{End}_{\mathbb{Q}_\ell[G_k]}$ (bla) eng par $G_k \simeq \mathbb{Q}_\ell^n$ pour un n.

Soit alors $\left\{ \begin{array}{l} \mathrm{End}_k(A) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell \xrightarrow{\varphi} \mathrm{End}_{\mathbb{Q}_\ell[G_k]}(V_\ell(A)) \\ E_\ell = \mathrm{Im}\,\varphi \end{array} \right.$, on veut

E_ℓ = commutant de F_ℓ ds $\mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(A))$ $\underset{\substack{\text{thm bicommutant} \\ E_\ell \text{ semisimple}}}{\Longleftrightarrow}$ F_ℓ = commutant de E_ℓ

Soit $\mathrm{Com}(E_\ell)$ = commutant de F_ℓ ds $\mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(A))$. Clairement $F_\ell \subset \mathrm{Com}(E_\ell)$. Pour l'autre inclusion, vu que $F_\ell \simeq \mathbb{Q}_\ell^n$, il suffit de démontrer

<u>Thm</u> Tout sous-espace isotrope (pour un e_φ venu via une polarisation φ) $W \subset V_\ell(A)$ G_k-stable est $\mathrm{Com}(E_\ell)$ stable. <u>NB</u> si on regarde un peu plus la preuve, on voit que 1) je suis con de faire le cas II 2) c'est vrai sans hyp d'isotropie

<u>Dem</u> Récurrence descendante sur $\dim W$

<u>Cas I (le plus profond)</u> W est maximal isotrope $\Rightarrow \dim_{\mathbb{Q}_\ell} W = g$, donc

$W_n = T_\ell(A) \cap W + \ell^n T_\ell(A)$ est un sous $\mathbb{Z}_\ell$ module de $T_\ell(A)$ G_k-stable, d'indice ℓ^{ng} (thm de la base adaptée. Par un thm clé (voir III 2.) on a des isogénies $f_n : B_n \longrightarrow A$ pour des var. ab B_n, avec $\mathrm{Im}(T_\ell(f_n)) = W_n$. Par le thm de finitude de Zarhin (le truc de Tate marcherait aussi, mais il faudrait produire des polaris, etc, voir l'article de Tate) $\exists\ n_0 < n_1 < \dots$ tq $B_{n_0} \xrightarrow[u_i]{\sim} B_{n_i}$ soient isom sur k.

Si on pose $v_i = f_{n_i} \circ u_i \circ f_{n_0}^{-1} \in \mathrm{End}_k^0(A) \subset E_\ell = \mathrm{Im}\,\varphi$, un jeu d'écriture mq $\underline{v_i(W_n) = W_{n_i}}$ $\Rightarrow v_i$ stabilise W_n. Or $\mathrm{End}_{\mathbb{Z}_\ell}(W_n)$ est compact $\Rightarrow$ WLOG $v_i \xrightarrow{i \to \infty} v \in$ ~~End~~ $\mathrm{Im}\,\varphi$ (comme on l'a vu, ceci est fermé)

si on a ça on a clairement fini !

Claim. $v(W_{n_0}) = T_\ell(A) \cap W$. Or $v(W_{n_0}) \subset \bigcap_i W_{n_i}$ par ce qui précède et vu que tout $x \in \bigcap_i W_{n_i} = T_\ell(A) \cap W$ est dans le compact W_{n_0}, il s'écrit $x = v_i(x_i)$ avec $x_i \in W_{n_0}$, $x_i \longrightarrow x'$ $\Rightarrow x \in v(W_{n_0}) \Rightarrow$ clr.

OUF

<u>Cas II</u> L'argument est standard. si $\dim W < g$, $W^\perp$ est stable par G_k

et par semisimplicité de $F_\ell \simeq \mathbb{Q}_\ell^n$, on a $W^\perp = W \oplus \bigoplus_{i=1}^m L_i$ avec L_i des F_ℓ modules simples, qui sont donc $\simeq \mathbb{Q}_\ell$. Comme l'acc. de Weil est alterné et $\dim_{\mathbb{Q}_\ell} L_i = 1 \Rightarrow W \oplus L_i$ est total isotrope et G_K stable, donc Com (E_ℓ) stable. Or $m \geq 2$ ($\dim W < g$ et accouplement parfait) $\Rightarrow W = (W \oplus L_1) \cap (W \oplus L_2)$ est Com (E_ℓ) stable Double ouf ! Rq cette preuve est débilement compliquée car Zarhin permet de le dem toute de suite

Et là, même si ça paraît incroyable, on a fini la démo ! pour tout sev G_K stable too late pour le changer

VIII Applications

1) Remarquer que si $A, B \in Ab_K$, A est isogène à une sous-var ab de B ssi $\exists\ \varphi \in \mathrm{Hom}_K(A,B)$ de ker fini (car $A/\ker\varphi$ est une sous-var ab de B et est K-isogène à A ssi $\ker\varphi$ fini). De plus, on a déjà vu que pour $\varphi \in \mathrm{Hom}_K(A,B)$, on a $\ker\varphi$ fini $\Leftrightarrow V_\ell(\varphi) : V_\ell(A) \longrightarrow V_\ell(B)$ injectif. (*) (et bien sûr G_K-équivariant). Le thm principal assure la densité de $\mathbb{Q} \otimes \mathrm{Hom}_K(A,B)$ dans $\mathrm{Hom}(V_\ell(A), V_\ell(B)) \Rightarrow$ (via semi-simplicité de $V_\ell \pi_A$)

Thm 1 $A, B \in Ab_K$, K fini, $f_A = P_{\pi_A}$, alors A est K-isogène à une sous-var de B ssi $f_A \mid f_B$ ssi $V_\ell(A) \underset{G_K\text{-rep}}{\simeq}$ sous rep de $V_\ell(B)$ pour un $\ell \neq \mathrm{car}\, K$

Cor Avec le même setup on a

1) $A \underset{K}{\sim} B$ (ie K-isogènes) $\Leftrightarrow$
2) $f_A = f_B$ $\Leftrightarrow$
3) $Z(A/K) = Z(B/K)$ (fct zeta)
4) $|A(L)| = |B(L)|$ $\forall\ L \supset K$ finie

$1 \Leftrightarrow 2$ clair par thm 1 + être isogène est symmétrique $3 \Leftrightarrow 4$ évident et $2 \Leftrightarrow 4$ est facile : on a vu que si $A \in Ab_K$, $|A(K_n)| = \prod_{i=1}^{2g}(1-\alpha_i^n)$ où $f_A = \prod_{i=1}^{2g}(x-\alpha_i)$. Il reste à voir que : (K_n ext de deg n de K)

$$\prod_{i=1}^{2g}(1-\alpha_i^n) = \prod_{i=1}^{2g}(1-\beta_i^n)\ \forall n \Rightarrow \prod(x-\alpha_i) = \prod(x-\beta_i)$$

Il suffit de calculer la fct zeta de 2 termes !

Donc la classe d'isogénie de A est connue une fois connu f_A. Si A est simple, ~~connaître~~ $\mathrm{End}_K^\circ(A)$ est une algèbre à division (lemme de factorisation) donc $\mathbb{Q}(\pi_A)$ est un corps de nombres

Cor 1 $F = \mathbb{Q}[\pi_A]$ est le centre de $\mathrm{End}_K^\circ(A)$, $\forall\ A \in Ab_K$ (K fini)

C'est clair, car on a vu dans la preuve du thm que $F \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ était le centre de $\mathrm{End}^\circ_k(A)\otimes \mathbb{Q}_\ell$

Thm 2 A est isotypique (ie $A \underset{k}{\sim} B^u$ avec B k-simple) ssi f_A est une puissance d'un pol irred ds $\mathbb{Q}[X]$. Alors $\mathrm{End}^\circ_k(A)$ est une $F=\mathbb{Q}[\pi_A]$ algebre simple centrale qui splitte en les places finies v de F tq $v\nmid p$. Elle ne splitte en aucune place réelle.

Dem Par Poincaré $A \underset{k}{\sim} \prod_{i=1}^{s} A_i^{n_i}$, A_i simples 2 à 2 non isogènes et alors clairement $\mathrm{End}^\circ_k(A) \simeq \prod_{i=1}^{s} M_{n_i}(\mathrm{End}^\circ_k(A_i)) \Rightarrow F=\prod_{i=1}^{s} F_i$ avec $F_i=$ centre $(M_{n_i}(\mathrm{End}^\circ_k(A_i)))$. Mais si $f_A=\prod f_i^{m_i}$, $f_i\in\mathbb{Q}[X]$ irred $\neq$
$\Rightarrow F=\prod \mathbb{Q}[X]/f_i(X)$ donc $s=$ nb de facteurs irred de f_A, ce qui rend claire une partie. Pour l'autre, soit $f_A=h^a$, $h\in\mathbb{Q}[X]$ irred $\Rightarrow$
$V_\ell A$ est un $F\otimes\mathbb{Q}_\ell$ module semisimple, libre de rg a sur $F\otimes\mathbb{Q}_\ell=\prod_{v|\ell}F_v$
Par le thm de Tate, $(F\otimes\mathbb{Q}_\ell)\otimes_F \mathrm{End}^\circ_k(A)\simeq \mathbb{Q}_\ell\otimes_{\mathbb{Q}}\mathrm{End}^\circ_k(A)\simeq \mathrm{End}_{\mathbb{Q}_\ell[G_k]}(V_\ell(A))\simeq M_a(F\otimes\mathbb{Q}_\ell) \Rightarrow$ ça splitte en tout $v|\ell$ et cela $\forall \ell\neq \mathrm{car}\,k$.

Voir l'exposé de Raphael pour le reste.

2) Bornes pour $\dim_{\mathbb{Q}}\mathrm{End}^\circ_k(A)$ Si on factorise $f_A(T)=\prod_{i=1}^{s}(T-\alpha_i)^{m_i}$ ds $\overline{\mathbb{Q}}[T]$, on a vu 1000 fois (semi-simplicité de $V_\ell\pi_A$) que le commutant de $V_\ell\pi_A$ a dimension $\sum_i^s m_i^2$. Par Tate, $\dim_{\mathbb{Q}}\mathrm{End}^\circ_k(A)=\sum_{i=1}^{s} m_i^2$.
Mais $\sum_{i=1}^{s} m_i=\deg f_A=2g \Rightarrow 2g\leq \dim_{\mathbb{Q}}\mathrm{End}^\circ_k(A)\leq (2g)^2$

Cas d'égalité 1 On a $[\mathrm{End}^\circ_k(A):\mathbb{Q}]=2g \Leftrightarrow m_i=1\ \forall i$, ie f_A est séparable $\Leftrightarrow [\mathrm{End}^\circ_k(A):\mathbb{Q}]=s$. Vu que $[F=\mathbb{Q}[\pi_A]:\mathbb{Q}]=s$ (semisimpl de $V_\ell\pi_A$), on en déduit le

Critère 1 $\mathrm{End}^\circ_k(A)$ est commutative $\Leftrightarrow$ elle a $\dim_{\mathbb{Q}}=2g \Leftrightarrow f_A$ séparable

Cas d'égalité 2 On a $[\mathrm{End}^\circ_k(A):\mathbb{Q}]=(2g)^2 \Leftrightarrow s=1 \Leftrightarrow \mathbb{Q}[\pi_A]=\mathbb{Q}$
Soit $D=\mathrm{End}^\circ_k(A)$, c'est une alg simple centrale si $F=\mathbb{Q}$ et $\mathrm{inv}_\ell D=0$ $\forall \ell\neq p$. Par corps de classe on obtient $D\simeq M_{2g}(\mathbb{Q})$ ou $D\simeq M_g(\mathbb{Q}_{p,\infty})$ ($\mathbb{Q}_{p,\infty}=$ alg de Deuring : l'alg de quaternions ram seulement en p,∞)
Il reste $D\simeq M_g(\mathbb{Q}_{p,\infty})$. On vérifie facilement la réciproque.

Avec des boulot et en utilisant les modules de Dieudonné, on arrive à calculer $\mathrm{inv}_v(D/L)$ aux places $v\,|\,p$. Le théorème final est :

<u>Thm (Tate)</u> Soit $A \in \mathrm{Ab}_K$ une var. ab simple sur $K = \mathbb{F}_q$. Alors

1) le centre de $D = \mathrm{End}^0_K(A)$ est $F = \mathbb{Q}(\pi_A)$ et si on pose $\begin{array}{c} D \\ | \\ F \\ | \\ \mathbb{Q} \end{array}$ $\begin{array}{l} \big) d^2 \\ \\ \big) e \end{array}$

on a $de = 2g$ et $f_A = (\text{pol min de } \pi_A)^d$

2) D splitte aux places finies $\nmid p$, ne splitte en aucune place réelle et si $v\,|\,p$ on a $\mathrm{inv}_v(D/L) = \dfrac{v(\pi_A)}{v(q)}[L_v : \mathbb{Q}_p] \bmod \mathbb{Z}$

On a aussi $\mathrm{inv}_v(D/L) + \mathrm{inv}_{\bar v}(D/L) = 0 \bmod \mathbb{Z}$.
conj complexe

En particulier si on connaît π_A, on connaît D ! On en déduit que

$\underset{K \subset L \text{ finie}}{\mathrm{End}^0_K(A) = \mathrm{End}^0_L(A)} \iff \mathbb{Q}(\pi_A) = \mathbb{Q}(\pi_A^{[L:K]})$ (fonctorialité du Frob)

Ceci entraîne sans mal ($[n]_A$ est une isogénie) que

$$\mathrm{End}_K(A) \neq \mathrm{End}_L(A) \iff \mathbb{Q}(\pi_A) \neq \mathbb{Q}(\pi_A^{[L:K]})$$

<u>Rq sur ce truc</u> Voir l'article de Conrad sur Chow's K/k trace etc pour une preuve moderne du thm de Chow : $A, B \in \mathrm{Ab}_K$, L/K ext tq K est séparablement clos ds L. Alors $\mathrm{Hom}_K(A,B) = \mathrm{Hom}_L(A_L, B_L)$.

<u>Appendice</u> Rappelons que si K est un corps local, CFT nous donne un hom canonique $\mathrm{inv}_K : \mathrm{Br}(K) \longrightarrow \mathbb{Q}/\mathbb{Z}$

$\swarrow$

$\{\text{alg simples centrales sur } K\}/\sim$ où $A \sim B$ si $\exists\, m, n \geq 0$ tq $A \otimes_K M_n(K) \simeq B \otimes_K M_m(K)$

De plus, si $K = \mathbb{R}$ on a $\mathrm{Br} K \simeq \frac{1}{2}\mathbb{Z}/\mathbb{Z}$

$K = \mathbb{C}$, $\mathrm{Br} K = 0$

K corps global $\Rightarrow$ $0 \to \mathrm{Br} K \to \bigoplus_v \mathrm{Br} L_v \xrightarrow{\Sigma} \mathbb{Q}/\mathbb{Z} \to 0$

Se donner une alg simple centrale $\iff$ se donner une famille $\mathrm{inv}_v(D) \in \mathbb{Q}/\mathbb{Z}$ de somme 0, presque tous 0.

En part $\exists$ alg de quater. $\mathcal{Q}_{p,\infty}$ avec $\mathrm{inv} = 0$ en toute place sauf p et ∞ et $\mathrm{inv} = \frac{1}{2}$ en ces 2 places.

- le thm up & down :
$$\begin{array}{ccc} A & \xrightarrow{f} & B \text{ isog} \\ ?\downarrow & & \downarrow \varphi \text{ polar} \\ A^t & \xleftarrow{f^t} & B^t \end{array}$$
? est une polar (car $\varphi = \varphi_{\mathcal{L}} \Rightarrow ? = \varphi_{f^*\mathcal{L}}$ et f fini)

- applic au thm Poincaré :
$$\begin{array}{ccc} B & \overset{i}{\hookrightarrow} & A \\ \downarrow & & \downarrow \varphi \text{ polar choisie} \\ B^t & \xleftarrow{i^t} & A^t \end{array}$$
$C = \left((\ker i^t \circ \varphi)^\circ\right)_{red}$

en déd semi-simplicité de End°_k, définir les var simples.

Z à insister sur les hyp k parfait

$\dim C \geq \dim A - \dim B^t$ (thm fibres) ($\dim B^t = \dim B$)

- accoupl Weil φ polar induit

$e_n^\varphi : A[n] \times A[n] \longrightarrow A[n] \times A^t[n] \longrightarrow \mu_n$ bilin alterné

$(x,y) \longmapsto e_n(x, \varphi(y))$ non deg si $(n, \deg\varphi) = 1$.

tq $e_n(f(x), y) = e_n(x, f^t(y))$

$(mn, car k) = 1 \Rightarrow e_n(mx, my) = e_{mn}(x,y)^m \Rightarrow$ acc$^{2\ell}$ bilin parfait alterné

G_K équivar $T_\ell A \times T_\ell A \xrightarrow{e_\ell^\varphi} \mathbb{Z}_\ell(1)$.

5) Thm de finitude - astuce de Zarhin - énoncé

- finitude du nb classes d'isom var ab dim g sur k avec une k-polar deg d.

- Lenstra, Oort, Zarhin : $A \in Ab_k$

{sous k-var ab}/$Aut_k(A)$ fini.

- Zarhin : {A dim g}/isom fini

6) Module de Tate - le définir, libre rg 2g sur $\mathbb{Z}_\ell$, pas canon, topol

$\varprojlim$ = celle ℓ-adique, action c° de G_K, fonctorialité

- le voir comme $Hom(\mathbb{Q}_\ell/\mathbb{Z}_\ell, A(k^s))$, applic à

la motiver !

$0 \to T_\ell A \xrightarrow{T_\ell f} T_\ell B \longrightarrow \ell\text{-Syl de}(\ker f)(k^s) \to 0$

Ceci part toute isog induit isom G_K-équivar $V_\ell(A) \simeq V_\ell(B)$)

$0 \to Hom(\mathbb{Q}_\ell/\mathbb{Z}_\ell, \ker f(k^s)) \to T_\ell A \xrightarrow{T_\ell f} T_\ell B \longrightarrow Ext^1(\mathbb{Q}_\ell/\mathbb{Z}_\ell, \ker f)(k^s)) \to Ext^1(\mathbb{Q}_\ell/\mathbb{Z}_\ell, A(k^s))$

$= 0$; $\simeq$ sylow $\ker f(k^s)$; $= 0$

$\ell^n | T_\ell f \Leftrightarrow \ell^n | f$

machine des endom : $X \subset T_\ell A$ sous $\mathbb{Z}_\ell$ module d'indice ℓ^{ng}, G_K stable

$\Rightarrow \exists\ f : B \to A$ k-isog deg ℓ^{ng} tq $X = \mathrm{Im}\, T_\ell B$.

une sorte de rec car on a vu que $\mathrm{Im}\, T_\ell B$ sous $\mathbb{Z}_\ell$ mod indice fini G_K stable si $B \to A$ isog le bouclation final

<u>Théo</u> $W \subset V_\ell A$ ~~dim~~ sev G_K stable $\Rightarrow \exists\, u \in \mathrm{Im}\,\Phi$ tq
$$u(V_\ell A) = W.$$

Dém $W_n = T_\ell A \cap W + \ell^n T_\ell A$ $\quad \exists\ B_n \xrightarrow{f_n} A$ isog tq ~~f~~ ~~Im~~ $V_\ell f_n(V_\ell B_n) = W_n$

$\exists\ n_0 < n_1 < \dots$ et ~~u~~

$$\begin{tikzcd} B_{n_0} \arrow[r, "u_i"] \arrow[d, "f_{n_0}"'] & B_{n_i} \arrow[d, "f_{n_i}"] \\ A \arrow[u, dotted, bend right] \arrow[r, dashed] & A \end{tikzcd}$$

isom.

$v_i \in \mathrm{End}^\circ_K(A) \subset \mathrm{Im}\,\Phi$

$$V_\ell v_i(W_{n_0}) = W_{n_i} \subset W_{n_0}$$

WLOG $v_i \longrightarrow v \in \mathrm{End}\,W_{n_0} \cap \mathrm{Im}\,\Phi$

$\downarrow$ fermé !

$v(x) = \lim v_i(x) \in \bigcap W_{n_i} = T_\ell \cap W$

$\in W_{n_0}$

Réc. si $x \in T_\ell \cap W = \bigcap W_{n_i}$ $\Rightarrow x = v_i(\alpha_i)$

$\qquad\qquad\qquad\qquad\qquad\quad \| \qquad\qquad\qquad\quad \alpha_i \in W_{n_0}$

$\qquad\qquad\qquad\qquad\quad v_i(W_{n_0})$

WLOG α_i cv vers α

$\Rightarrow v(W_{n_0}) = T_\ell \cap W \Rightarrow$ clr. $\qquad x = v(\alpha)$.