Variétés abéliennes CM et la conjecture de Manin-Mumford

Geometrie diophantienne

David Corwin

0 Résumé

Les conjectures de Mordell-Lang et Manin-Mumford disent que si V est une sous-variété d'un groupe algébrique G qui contient "beaucoup" de points de torsions, alors G est un translaté d'un sous-groupe algébrique au cas où G est un tore ou une variété abélienne.

Certaines preuvent s'appuient sur des arguments galoisiens. Essentiellement, on utilise l'action de galois pour montrer que s'il existe certains points de torsions, il en existe plusieurs autres. Pour cela, il faut donc une bonne description de l'action de Galois sur les points de torsion de G. Dans le cadre des tores, c'est facile, car les points de torsions sont tout simplement les racines d'unité. Cependant, dans le cadre des variétés abéliennes, la description n'est pas si facile.

Ici, on decrit certains résultats à propos de l'action de Galois sur les points de torsion des variétés abéliennes et leurs conséquences pour la conjecture de Manin-Mumford.

Ceci a été écrit comme travail pour le cours du Professeur Daniel Bertrand du programme M2 de Jussieu de 2012 sur la "geometrie diophantienne".

1 Notations

Pour un corps de nombres K, soit Σ_K l'ensemble des places finis de K, Σ_K^∞ les places infinis, et $\overline{\Sigma_K}$ toutes les places. Pour chaque place v de K, soit K_v le completé en v, $\mathcal{O}_v$ son anneau d'entiers, et U_v son groupe d'unités. Pour un nombre premier p, U_p dénote donc les unités p-adiques.

Tout corps est de caractère 0, sauf si on dit autrement. Si L/K est une

extension Galoisienne, $G(L/K)$ dénote le groupe de Galois, et G_K dénote le groupe de Galois absolu de K. Si w, v sont des places de L, K respectivement, $D(w/v)$ et $I(w/v)$ sont les groupes de décomposition et d'inertie.

On ecrit V/K pour noter qu'une variété V est définie sur K. Si σ est un automorphisme de $\overline{(K)}$, il envoie V et toute structure associe à V à une telle structure sur $\sigma(V)$. On dénote par $V(K)$ les K-points de V, et si G/K est un groupe algébrique, $G[m]$ dénote le sous-groupe de m-torsion, vu comme groupe algébrique sur K. Si ce n'est pas noté, on utilise $G[m]$ pour indiquer le groupe abstrait $G[m](\overline{K})$.

2 Conjecture de Manin-Mumford et théorie de Galois

Ici, on explique la conjecture de Manin-Mumford, esquissé au-dessus, et on indique comment on peut la resoudre avec des informations sur l'action de Galois sur les points de torsion.

2.1 La Conjecture de Manin-Mumford-Mordell-Lang

Théorème 2.1 (Manin-Mumford-Mordell-Lang)**.** *Soit G/K un groupe algébrique semi-abélien (c'est-à-dire, un groupe algébrique connexe tel que son composant affine est un tore) et W/K une sous-variété de G. Si $W \cap G_{tor}$ est dense dans W, alors W est un translaté par un élément de G_{tor} d'un sous-groupe algébrique.*

(Notez que ceci n'est qu'un cas spécial de la conjecture generale de Lang, où les points de torsion sont remplacés par le groupe de division d'un sous-groupe de G de type fini.)

En particulier, si G est un tore ou une variété abélienne et W contient l'identité, alors W est un sous-tore ou sous-variété abélienne, respectivement.

Une des preuves utilise des arguments Galoisiens de la façon suivante. Comme W est définie sur K, l'action de G_K sur les points de G envoie W sur elle-même. En particulier, cela envoie des points de torsion contenus dans W à des autres points de torsion dans W. En utilisant le groupe de Galois pour montrer que W contient de plus en plus de points de torsion, on recupère des informations de plus en plus fortes sur W. Puis, avec des arguments de la théorie de l'intersection, on peut ainsi conclure.

On traite plutôt le cas des variétés abéliennes (c'est-à-dire, Manin-Mumford), l'autre ayant été traité dans le cours. Cependant, l'hypothèse de la section 2.2 reste importante pour tout G énoncé dans la conjecture.

2.2 L'ingrédient galoisien

Du côté Galoisien, on voudrait donc montrer que les points de torsion de G ont "beaucoup" de conjaugés (sous l'action de Galois). Dans cette sous-section, on va decrire une hypothèse à propos de l'action de Galois sur les points de torsion de G, qui nous permettra de résoudre tout de suite la conjecture au cas où W est de dimension 1. Ensuite, dans les sections qui suivent, on va discuter comment on peut arriver à montrer que cette hypothèse sur l'action de Galois est valable pour plusieurs types de groupes algébriques G.

Soit N un entier. Outre l'action de Galois, les endomorphismes de G agissent sur $G[N]$. On voudrait savoir combien de ces endomorphismes ont la même action qu'un élément du groupe de Galois.

On se limite aux endomorphismes dans $\mathbb{Z}$, surtout car certains G n'ont que ces endomorphismes-là. Cependant, on va voir que cela suffit.

On note que $n \in \mathbb{Z}$ agit comme un automorphisme de $G[N]$ si et seulement si n est premier à N. Comme $G[N]$ est isomorphe à une puissance de $(\mathbb{Z}/N)$, cela induit donc une action de $(\mathbb{Z}/N)^\times$ sur $G[N]$. On note H_N le sous-groupe de $n \in (\mathbb{Z}/N)^\times$ tel qu'il existe $\sigma \in G_K$ tel que $\sigma x = nx \, \forall x \in G[N]$. On suppose l'hypothèse suivante:

Hypothèse 2.2. *Il existe un nombre $c(G/K)$, indépendent de N, tel que $[(\mathbb{Z}/N)^\times : H_N] \leq c$.*

C'est-à-dire, à indice borné près, tous les multiples de x qui engendrent le même sous-groupe sont conjugés à x. Comme on va montrer tout de suite, cela nous permet de résoudre Manin-Mumford.

2.3 Preuve de Manin-Mumford

Dans cette partie, on utilise l'hypothèse au-dessus pour demontrer le lemme suivant, qui nous permettra de résoudre le théorème dans plusieurs cas:

Lemme 2.3. *Avec les notations du théorème 2.1, on suppose que W soit une courbe. Si G satisfait à 2.2, il existe un entier $m > 1$ tel que $W = W^{(m)}$, où $W^{(m)}$ est l'image de W sous l'application $[m] : G \to G$.*

Preuve. Cette démonstration est due à Lang (voir, par exemple, une reproduction dans [2]). Soit $r = c!$, où c est donnée par l'hypothèse.

Suppose qu'il existe $x_n \in W$ d'ordre exact n dans G. Soit d le plus petit entier qui soit premier à n. On sait que $[(\mathbb{Z}/n)^\times : H_n]$ divise r, donc $d^r \in H_n$, c'est-à-dire il existe $\sigma \in G_K$ tel que $\sigma(x_n) = d^r x_n$. Alors,

$$d^r x_n \in X \cap X^{(d^r)}.$$

Puis, pour tout $\sigma \in H_n$, considérons

$$\sigma(d^r x_n) = d^r \sigma(x_n)$$

Car W est défini sur K, tous ces points sont dans $W \cap W^{(d^r)}$. En plus, ils sont tous distincts (pour $\sigma \in H_n$ distincts), alors il en existe $|H_n| \geq \dfrac{\phi(n)}{c}$.

Cependant, si $W \neq W^{(d^r)}$, le théorème de Bezout nous dit qu'il y a au plus $\deg(W)\deg(W^{(d^r)})$ points dans l'intersection.

Pour m entier, la théorie de l'intersection nous dit que le cycle $[m]^*(W)$ est un multiple du cycle $W^{(m)}$. Le premier est de degré $m^{2g}\deg(W)$ car $[m]$ est de degré m^{2g}, donc $\deg(W^{(d^r)}) \leq m^{2g}\deg(W)$.

On a alors

$$\frac{\phi(n)}{c} \leq d^{2gr}\deg(W)^2.$$

Une estimation nous dit que pour tout n, $\phi(n) \geq \dfrac{\sqrt{2}}{2}$. On a donc

$$C\sqrt[4gr]{n} \leq d,$$

où C est un constant. Comme on a choisi d le plus petit, ceci veut dire que tous les nombres premiers moins que $C\sqrt[4gr]{n}$ divisent n. Mais pour un n assez grand, ce produit est plus grand que n (par une estimation simple sur la densité des nombres premiers). Cela nous donne une contradiction, et le lemme est vrai pour $m = d^r$. □

Finalement, on peut finir la démonstration de Manin-Mumford au cas où W est une courbe:

Preuve. Si W est une courbe, ceci veut dire que W est un recouvrement non-trivial d'elle-même. Pour un recouvrement $\phi : C_1 \to C_2$ non-ramifié de courbes, la formule de Hurwitz nous dit

$$2g_1 - 2 = (\deg(\phi))(2g_2 - 2),$$

où g_1, g_2 dénotent les genres, respectivement. Le lemme nous dit alors que le genre de W est 1.

Un translaté de W par un point de torsion contient l'identité de G. D'après un théorème de la géométrie algébrique, un morphisme d'une variété abélienne dans un groupe alebrique qui envoie l'identité sur l'identité est un homomorphisme. Alors, si on munit W d'une structure de courbe elliptique avec l'identité de G comme identité, W est donc une sous-variété abélienne de G. □

3 Variétés abéliennes CM

Ici, on explique comment montrer l'hypothèse 2.2 au cas où G est une variété abélienne de type CM. Dans ce cas, on peut décrire l'action de Galois de façon tres explicite.

3.1 Le grand théorème de la multiplication complexe

Définition 3.1. Une variété abélienne A/K de dimension g est dit de *type CM* si son anneau d'endomorphismes contient un ordre dans un algèbre étale sur $\mathbb{Q}$ de degré $2g$.

On peut en déduire que cette algèbre doit être une extension totalement imaginaire quadratique d'une algèbre totalement réel, ou qu'il existe une unique conjugaison complexe sur E, ce qui revient au même. On dénote par E l'algèbre et par E l'ordre. On se limite au cas où $R = \mathcal{O}_E$.

On suppose que K contienne tout homomorphisme de E dans $\overline{E}$. L'espace tangent de A en 0 est un K-espace vectoriel de dimension g. Si on étend à un corps K qui deploie E, l'espace tangent est un module où E agit par la moitié de ses plongements dans K, ce qu'on appelle un *type CM*; les autres sont donnés par conjugaison complexe. Cela nous donne une norme $N_\Phi : K^\times \to E^\times$ qui envoient un élément de K au produit de ses normes sous tous les plongements de E dans K. Si on multiplie la norme d'un élément avec sa conjugaison complexe, on recupère sa norme habituelle dans $\mathbb{Q}$.

On peut maintenant constater cette version assez faible du grand théorème de la multiplication complexe, qui nous donne précisément l'action sur les points de torsion de A:

Théorème 3.2. *Soit N un entier et $\sigma \in G_K$ tel que σ est $(\mathfrak{a}, K^{ab}/K)$ pour un ideal $\mathfrak{a}$ de K. Alors, il existe $\alpha \in E$ tel que l'action de α sur $E[N]$ et*

$$(\alpha) = N_\Phi(\mathfrak{a})$$

Pour la démonstration, voir, par exemple, [3] ou [4].

3.2 L'hypothèse sur l'action de Galois

Cette description concrète de l'action de G_K sur les points de torsion nous permet de montrer l'hypothèse pour une variété abélienne A/K de type CM. On esquisse l'idée.

Avec les notations du théorème, soit $\mathfrak{b} = \mathfrak{a}\overline{\mathfrak{a}}$ (conjugaison complexe). On sait alors que $N_\Phi(\mathfrak{b}) = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a})$. On peut montrer par un argument qui prend

compte de la polarisation que l'α correspondent est en fait dans $\mathbb{Q}$. Alors, modulo -1, chaque membre de $\mathbb{Z}$ qui est la norme numérique d'un idéal de K est égal à un élément de G_K sur $A[N]$.

D'après la théorie des corps de classe, le noyau de l'application d'Artin pour la plus grande extension abélienne de $\mathbb{Q}$ contenue dans K est donné par les normes des ideaux de K dans $\mathbb{Q}$. Comme K est fini sur $\mathbb{Q}$, ce noyau est d'indice fini. Finalement, comme le groupe d'unités de $\mathbb{Z}$ n'est que $\{\pm 1\}$, l'image des α dans $(\mathbb{Z}/N)^\times$ est d'indice borné, et ainsi les H_N sont d'indice borné, d'où l'hypothèse.

4 Variétés abéliennes et théorème de l'image ouverte

Ici, nous expliquons quoi faire dans le cas où la variété n'est pas de type CM.

4.1 Notations

Soit A/K une variété abélienne de dimension g, et soit $n = 2g$. On note $T_\ell(A)$ le module de Tate et $V_\ell(A)$ son tensorisation avec $\mathbb{Q}_\ell$. Pour m entier, on note $\rho_{A,m}$ la representation de G_K sur $A[m]$, i.e. dans $\mathrm{GL}_n(\mathbb{Z}/(m))$. On note ρ_{A,ℓ^∞} la représentation dans $\mathrm{GL}_n(\mathbb{Z}_\ell) = \mathrm{GL}(T_\ell(A))$ et ρ_A la représentation dans $\mathrm{GL}_n(\hat{\mathbb{Z}}) = \prod_\ell \mathrm{GL}_n(\mathbb{Z}_\ell)$. On note G_m, G_{ℓ^∞} les images correspondentes de G_K. On suppose toujours K un corps de nombres. Par "prèsque tout ℓ", on entend "pour tout ℓ sauf un ensemble fini".

4.2 Théorème de l'image ouverte

Quand G n'est pas de type CM, on n'a pas une description concrète de l'action de Galois sur les points de torsion. Cependant, Serre montre que l'image du groupe de Galois dans les automorphismes des points de torsions est "très grand".

Théorème 4.1 (Théorème de l'image ouverte)**.** *Si A/K est une variété abélienne tel que* $\mathrm{End}(A) = \mathbb{Z}$ *et la dimension g de A est impaire ou égal à* 2 *ou* 6*, alors l'image de*

$$\rho_A : G_K \to \mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$$

est ouverte.

En particulier, on a:

Corollaire 4.2. *L'image de G_K est ouverte, donc d'indice fini. Donc, son intersection avec*

$$\hat{\mathbb{Z}}^\times \subseteq \mathrm{GSp}_{2g}(\hat{\mathbb{Z}})$$

et d'indice fini, et alors, l'indice de l'image de G_K dans $\mathbb{Z}/N$ pour tout N entier est borné par cet indice.

Alors, Manin-Mumford est vrai pour les variétés abéliennes qui satisfont aux conditions du théorème.

Maintenant, on va esquisser la preuve du théorème de l'image ouverte. Dans le cas $g = 1$, le théorème n'est pas pertinent à la conjecture de Manin-Mumford car une courbe contenue dans une courbe elliptique est automatiquement toute la courbe. Cependant, c'est toujours intéressant, et les méthodes restent utiles pour les variétés abéliennes de dimension supérieure.

4.3 Coubes elliptiques

Dans [7], Serre a démontrer que l'image ℓ-adique est ouverte pour toute courbe elliptique non-CM, et que l'image adélique est ouverte pour les courbes elliptiques à j non-entier. Dans [5], il etendu la preuve à toute courbe elliptique non-CM. Dans cette section, on va expliquer la preuve pour les courbes elliptiques à j non-entier.

On suppose E/K une courbe elliptique qui n'est pas de type CM. Notez que dans le théorème, pour $g = 1$, on a $\mathrm{GSp}_2 = \mathrm{GL}_2$.

Par l'accouplement de Weil, on sait que le déterminant de la représentation adélique, qui envoit G_K à $\hat{\mathbb{Z}}^\times$, a une image ouverte. En particulier, l'image du déterminant de ρ_{ℓ^∞} est ouverte dans $\mathbb{Z}_\ell^\times$ pour tout ℓ et est égal à $\mathbb{Z}_\ell^\times$ pour presque tout ℓ.

Puis, il faut montrer que les images ℓ-adiques sont ouvertes. Nous ne faisons qu'indiquer la preuve (mais voir un papier que j'ai déjà ecrit, dont le sujet était une preuve complète de ce résultat). D'abord, on admet un lemme de Serre:

Lemme 4.3. *Si E n'est pas de type CM, la représentation de G_K sur $V_\ell(E)$ est irreductible pour tout ℓ, et la représentation sur $E[\ell]$ est irreductible pour presque tout ℓ.*

Preuve. Le lemme se déduit d'un théorème de Shafarevich sur la finitude des classes d'isomorphisme de courbes elliptiques dans une classe d'isogénie et le fait que E est non-CM (en fait, c'est le seul ingrédient qui utilise le fait que E est non-CM). □

Théorème 4.4. *Pour tout ℓ, la représentation $\rho_{E,\ell^\infty} : G_K \to \mathrm{GL}_2(\mathbb{Z}_\ell)$ a une image ouverte.*

Preuve. D'abord, car G_K est compacte, son image est fermé, donc est un sous-groupe de Lie ℓ-adique par le théorème de Cartan. L'image a donc une algèbre de Lie qu'on note $\mathfrak{g}_\ell$, et si cette algèbre est $\mathfrak{gl}_2$, l'image est ouverte.

Comme V_ℓ est irréductible comme représentation de G_K (donc de $\mathfrak{g}_\ell$), le lemme de Schur montre que le commutant de $\mathfrak{g}_\ell$ dans $\mathrm{End}(V_\ell(E))$ est un corps, donc $\mathbb{Q}_\ell$ où une extension quadratique. Si c'est $\mathbb{Q}_\ell$, $\mathfrak{g}_\ell$ est égal à $\mathfrak{sl}_2$ où $\mathfrak{gl}_2$. Par l'accouplement de Weil, le déterminant de G_K est ouvert dans $\mathbb{Z}_\ell^\times$, donc ce n'est pas le premier.

Si le commutant est une extension de $\mathbb{Q}_\ell$, l'algèbre $\mathfrak{g}_\ell$ est contenu dans cette extension, donc est commutative. Alors, après passage à un K plus grand, l'image de G_K est commutative. Puis, on appliquer des arguments de la théorie des corps de classes pour montrer que ce n'est pas possible, et on peut finalement conclure. □

Malheureusement, ceci ne nous permet pas de conclure que l'image de la représentation adélique a une image ouverte. Il est possible, par exemple, que ce ne soit pas surjectif pour une infinitude de ℓ.

4.3.1 Surjectivité pour presque tout ℓ

Heureusement, on peut le résoudre par les deux lemmes suivants:

Lemme 4.5. *Un sous-groupe fermé de* $\mathrm{SL}_2(\mathbb{Z}_\ell)$ *qui s'envoit surjectivement sur* $\mathrm{SL}_2(\mathbb{F}_\ell)$ *est* $\mathrm{SL}_2(\mathbb{Z}_\ell)$.

Lemme 4.6. *Pour presque tout ℓ, l'image $\rho_\ell(G_K)$ contient* $\mathrm{SL}_2(\mathbb{F}_\ell)$.

Du premier lemme, le second lemme nous dit que $\rho_{\ell^\infty}(G_K)$ contient $\mathrm{SL}_2(\mathbb{Z}_\ell)$. Car le déterminant est surjectif pour presque tout ℓ, on peut conclure que $\rho_{\ell^\infty}(G_K)$ est égal à $\mathrm{GL}_2(\mathbb{Z}_\ell)$ pour presque tout ℓ.

La preuve du premier lemme n'est qu'un exercice de la théorie des groupes et des relevements ℓ-adiques, similaire à la preuve du lemme de Hensel.

Dans la preuve du deuxième lemme, on va voir entrer l'hypothèse que $j(E)$ soit non-intégral. Supposons que $v(j(E)) < 0$. On suppose aussi que $v \nmid \ell$, que $\ell \nmid v(j(E))$, et que la représentation de G_K sur $E[\ell]$ est irréductible. D'après le lemme 4.3, tout ceci est vrai pour presque tout ℓ.

Tate avait remarqué que tous les développements Fourier des fonctions elliptiques et modulaires convergent même dans le cas non-archimedien, au cas où $|q|_v < 1$. Ceci veut dire que $|j(q)|_v > 1$, d'où la condition sur $j(E)$. En plus, il a montré que, après passage à une extension finie de K, E est isomorphe sur K_v à une courbe E_q paramétrée par des fonctions elliptiques v-adique. Par cette paramétrisation, on a

$$E_q(\overline{K_v}) \cong \overline{K_v}^\times/(q^\mathbb{Z})$$

non seulement comme groupes abstraits mais comme G_{K_v}-modules, car l'action de G_{K_v} est continue et donc commute avec les développements.

Dans ce modèle, on peut regarder les points $E[\ell]$ comme les ℓ-ième racines d'unité μ_ℓ et les ℓ-ième racines de q. Comme

$$\ell \nmid v(j(E)) = -v(j(E)),$$

l'extension de Kummer

$$K_v(\sqrt[\ell]{q}, \mu_\ell)/K_v(\mu_\ell)$$

est de degré ℓ. Si on choisit un $\sqrt[\ell]{q}$ et $\zeta_\ell \in \mu_\ell$, il existe un élément

$$\sigma \in G(K_v(\sqrt[\ell]{q}, \mu_\ell)/K_v(\mu_\ell)$$

(ou bien dans $G_{K_v(\mu_\ell)} \subseteq G_K$) tel que

$$\sigma(\sqrt[\ell]{q}) = \sqrt[\ell]{q}\zeta_\ell.$$

On peut prendre $\sqrt[\ell]{q}$ et ζ_ℓ comme base de $E_q[\ell] = E[\ell]$. Dans cette base, σ prend la forme

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(F_\ell)$$

Soit $W \subseteq E[\ell] \cong_{\mathbb{F}_\ell} \mathbb{F}_\ell^2$ le sous-espace de $E[\ell]$ fixé par σ. Comme $E[\ell]$ est irréductible, il existe un $\tau \in G_K$ qui envoit W à un autre sous-espace W'. Alors, $\tau\sigma\tau^{-1}$ fixe cet autre sous-espace. Si on prend une base de $E[\ell]$ qui respecte la décomposition $E[\ell] = W \oplus W'$, les matrices de σ et $\tau\sigma\tau^{-1}$ prennent les formes

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

C'est un fait élémentaire que ces matrices engendrent $\mathrm{SL}_2(\mathbb{F}_\ell)$, et on peut ainsi conclure.

4.3.2 Surjectivité adélique

Il nous reste à voir que la surjectivité pour presque tout ℓ nous dit que la représentation adélique est surjective.

Comme on dit, on a résolu la question "verticale", et il ne reste qu'une question "horizontale". En effet, après ce qu'on a déjà remarqué sur les représentations ℓ-adiques et le déterminant, on n'a que de la théorie des groupes à faire. On esquisse l'idée de la preuve.

Soit $H \subseteq G_1 \times G_2$ un sous-groupe fermé de deux groupes profinis G_1, G_2. Soit $N_i = H \cap G_i$ et H_i la projection de H sur G_i. Alors, $H_i = H/(N_{1-i})$, donc

$$H_i/N_i = H/N_1N_2$$

pour chaque i. En effet, il existe un sous-quotient en commun entre G_1, G_2. Autrement dit, pour que N_i puisse être plus petit que H_i, il faut que les groupes G_i se mélangent d'une façon.

On peut appliquer un principe similaire à un produit de plusieurs groupes. Plus specifiquement, on note que pour $\ell \geq 5$, le groupe $\mathrm{SL}_2(\mathbb{Z}_\ell)$ a le groupe simple non-abélien $\mathrm{PSL}_2(\mathbb{F}_\ell)$ comme quotient. Tous ces groupes sont non-isomorphes pour ℓ différents. Alors, l'image de G_K dans

$$\prod_{\ell \neq \ell_0} \mathrm{GL}_2(\mathbb{Z}_\ell)$$

ne peut pas avoir $\mathrm{PSL}_2(\mathbb{F}_{\ell_0})$ comme sous-quotient. Comme l'image ℓ_0-adique de Galois est surjective (pour presque tout ℓ_0), elle a $\mathrm{PSL}_2(\mathbb{F}_{\ell_0})$ comme sous-quotient. Donc, l'intersection de $\rho_E(G_K)$ avec

$$\mathrm{SL}_2(\mathbb{Z}_{\ell_0}) \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$$

devrait avoir ce groupe simple non-abélien comme sous-quotient. Un petit lemme nous dit que cela veut dire que cette intersection est égal à $\mathrm{SL}_2(\mathbb{Z}_{\ell_0})$, et après quelques détails téchniques, on peut conclure.

4.4 Variétés abéliennes

Plus tard, dans [6], Serre a démontré le résultat pour les variété abélienne avec anneau d'endomorphisme égal à $\mathbb{Z}$ et dimension impaire, 2, ou 6. Ici, on explique très brièvement cette preuve.

En 1983, Faltings a résolu plusieurs conjectures sur les variétés abéliennes. En particulier, il a montré que l'application

$$\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \to \mathrm{End}(T_\ell(A))^{G_K}$$

est surjective, où A et tous ses endomorphismes sont définis sur K. Si $\mathrm{End}(A) = \mathbb{Z}$, on sait donc que l'image de G_K doit être assez grand.

Peu après, Serre a finalement démontré le théorème au cas où A est une variété abélienne de dimension impaire où $2, 6$. Notons que le fait que l'action est contenu dans le groupe symplectique provient du fait que la polarisation a une description algébrique, donc est défini sur un corps de nombres K et est fixée par G_K. La polarisation nous donne l'accouplement anti-symétrique de Weil sur $T_\ell(A)$.

Avec des arguments très précis de la théorie des groupes $\mathrm{GL}_n(\mathbb{F}_\ell)$, il montre que l'image adélique de Galois a une intersection ouverte avec un tore défini sur $\mathbb{Q}$ et qui contient $\mathbb{G}_m$, ce qui démontre notre résultat désiré.

References

[1] Hindry, Marc. *Autour d'une conjecture de Serge Lang.* Inventiones mathematicae, Vol. 94, 1988, p.575-604.

[2] Lang, Serre. *Complex Multiplication.* New York: Springer-Verlag, 1983.

[3] Milne, James. Complex Multiplication. http://www.jmilne.org/math/CourseNotes/cm.html.

[4] Milne, James. The Fundamental Theorem of Complex Multiplication. http://www.jmilne.org/math/articles/2007c.pdf.

[5] Serre, Jean-Pierre. Proprietes galoisiennes des points d'ordre fini des courbes elliptiques, Invent. Math. Vol. 15, No. 4 (1972), p.259-331.

[6] Serre, Jean-Pierre. *Résumé des cours de 1985-1986* dans *Oeuvres - Collected Papers: Volume IV*. Berlin: Springer, 2003.

[7] Serre, Jean-Pierre. *Abelian l-Adic Representations and Elliptic Curves.* Redwood City, CA: Addison-Wesley, Advanced Book Program, 1989.