Mordell conjecture

https://phanpu.github.io/

November 2023

Contents

Preface

Theorem 0.0.1. Let K be a number field. Let C/K be a smooth projective curve of genus ≥ 2. Then the set $C(K)$ of K-rational points is finite.

Remark 0.0.2. *Clearly we can omit the words "smooth" and "projective" by taking the normalization and the projective locus.*

Chapter 1

The method from Faltings

1.1 An overview

1.1.1 Tate conjecture for Abelian varieties over finite fields

In 1966, Tate proved the following two results: let k be a finite field, and ℓ a prime number with $\ell \neq \text{char } (k)$, then

- for any two Abelian varieties A, B over k, the natural map

$$\mathbb{Z}_\ell \otimes \text{Hom}(A, B) \to \text{Hom}(T_\ell A, T_\ell B)^{\text{Gal}(k_s/k)}$$

  is an isomorphism. Here the right hand is the group of $\mathbb{Z}_\ell$-linear maps fixed by $\text{Gal}(k_s/k)$.

- for any Abelian variety A over k the representation

$$\rho_\ell : \text{Gal}(k_s/k) \to \text{GL}(V_\ell A)$$

  is semisimple.

Since we hope to obtain a more general result, we temporarily omit the assumption that k is a finite field.

Preliminaries

We first list some properties for Abelian varieties, which can be found in van der Geer's book or Milne's note:

Proposition 1.1.1. Let A and B be Abelian varieties over a field k.

If ℓ is a prime number, $\ell \neq \text{char } (k)$. Then the map

$$\mathbb{Z}_\ell \otimes \text{Hom}(A, B) \to \text{Hom}(T_\ell A, T_\ell B)$$

is injective, and has a torsion-free cokernel.

Proposition 1.1.2. Let A be an Abelian variety over a field k. Also, let ℓ be a prime number with $\ell \neq \mathrm{char}\ (k)$. For any $\mathrm{Gal}(\bar{k}/k)$-stable submodule W of finite index in $T_\ell A$, then there is an Abelian variety B and an isogeny $u : B \to A$ such that W is exactly the image of the induced map

$$T_\ell u : T_\ell B \to T_\ell A$$

Proposition 1.1.3 (Zarhin's trick)**.** Let A be an Abelian variety over a field k. Then $A^4 \times (A^D)^4$ carries a principal polarization.

Proposition 1.1.4. Up to isomorphism, an Abelian varieties has only finitely many direct factors.

The proof

We first do some reductions.

Proposition 1.1.5. The map

$$T_\ell : \mathbb{Z}_\ell \otimes \mathrm{Hom}(A, B) \to \mathrm{Hom}(T_\ell A, T_\ell B)^{\mathrm{Gal}(k_s/k)}$$

is an isomorphism if and only if the map

$$V_\ell : \mathbb{Q}_\ell \otimes \mathrm{Hom}(A, B) \to \mathrm{Hom}(V_\ell A, V_\ell B)^{\mathrm{Gal}(k_s/k)}$$

is an is an isomorphism.

Proof. By 1.1.1 the map T_ℓ is injective and $\mathrm{Coker}(T_\ell)$ is torsion-free (hence free). Then T_ℓ is an isomorphism if and only if $\mathrm{Coker}(T_\ell)$ is free of rank 0, and further equivalently $\mathrm{Coker}(T_\ell) \otimes \mathbb{Q}_\ell$ is a 0th-dimensional vector space. Now the result follows from that $\mathbb{Q}_\ell$ is flat over $\mathbb{Z}_\ell$. ■

Proposition 1.1.6. If C is an Abelian variety over k such that

$$\mathbb{Q}_\ell \otimes \mathrm{End}(C) \to \mathrm{End}(V_\ell C)^{\mathrm{Gal}(k_s/k)}$$

is an isomorphism, then for any Abelian varieties A, B over k, the map

$$\mathbb{Q}_\ell \otimes \mathrm{Hom}(A, B) \to \mathrm{Hom}(V_\ell A, V_\ell B)^{\mathrm{Gal}(k_s/k)}$$

is an is an isomorphism.

Proof. Let $C = A \times B$. Then, there are decompositions

$$\mathbb{Q}_\ell \otimes \mathrm{End}(C) = \mathbb{Q}_\ell \otimes \mathrm{End}(A) \oplus \mathbb{Q}_\ell \otimes \mathrm{Hom}(A, B) \oplus \mathbb{Q}_\ell \otimes \mathrm{Hom}(B, A) \oplus \mathbb{Q}_\ell \otimes \mathrm{End}(B)$$

$$\mathrm{End}(V_\ell C)^G = \mathrm{End}(V_\ell A)^G \oplus \mathrm{Hom}(V_\ell A, V_\ell B)^G \oplus \mathrm{Hom}(V_\ell B, V_\ell A)^G \oplus \mathrm{End}(V_\ell B)^G$$

where $G = \mathrm{Gal}(k_s/k)$. The result then follows immediately. ■

Now we consider a "finiteness condition", which is denoted by $\mathrm{Fin}(A/k)$: up to isomorphism there are finitely may Abelian varieties B over k for which there is an isogeny $A \to B$ of degree a power of ℓ.

Lemma 1.1.7. Under the assumption $\mathrm{Fin}(A/k)$, for every sub-vector space $W \subseteq V_\ell A$ that is stable under $\mathrm{Gal}(k_s/k)$, there exists an element $u \in \mathbb{Q}_\ell \otimes \mathrm{End}(A)$ such that $W = u(V_\ell A)$.

Proof. Let $W_n = W \cap T_\ell A + \ell^n \cdot T_\ell A$. Then $\ell^n \cdot T_\ell A \subseteq W_n \subseteq T_\ell A$. W_n is then of finite index in $T_\ell A$, and by 1.1.2 it is the image of $T_\ell v_n : T_\ell A_n \to T_\ell A$, where $v_n : A_n \to A$ is an isogeny.

By the assumption $\mathrm{Fin}(A/k)$, there is a sub-sequence $\{n_i\}$ such that

$$A_{n_1} \cong A_{n_2} \cong \cdots$$

Fix an $n \in \{n_i\}$, let w_i be the composite

$$w_i : A \xrightarrow{v_n^{-1}} A_n \xrightarrow{\sim} A_{n_i} \xrightarrow{v_{n_i}} A$$

Then w_i is an element in $\mathbb{Q}_\ell \otimes \mathrm{End}(A)$. Choose an element $u \in \mathbb{Q}_\ell \otimes \mathrm{End}(A)$ be the limit of a sub-sequence. Then $u(V_\ell A) = (\lim v_n(V_\ell A_n)) \otimes \mathbb{Q}_\ell = \mathbb{Q}_\ell \otimes \lim W_n = W$. ∎

Now we return to the proof of Tate conjecture, in fact, we will prove a more general version.

Theorem 1.1.8. Let A be an Abelian variety over an arbitrary field k, and let ℓ be a prime number different from char (k). Assume that 1.1.7 is true for A and A^2, then the representation

$$\rho_\ell : \mathrm{Gal}(k_s/k) \to \mathrm{GL}(V_\ell A)$$

is semisimple and the map

$$\mathbb{Q}_\ell \otimes \mathrm{End}(A) \to \mathrm{End}(V_\ell A)^{\mathrm{Gal}(k_s/k)}$$

is an isomorphism.

Proof. Suppose we have a Galois-stable subspace $W \subseteq V_\ell A$. By 1.1.7, there exists an endomorphism $u \in \mathbb{Q}_\ell \otimes \mathrm{End}(A)$, such that W is exactly the image of $u : V_\ell A \to V_\ell A$. We consider the right ideal $u \cdot (\mathbb{Q}_\ell \otimes \mathrm{End}(A))$, since $\mathbb{Q}_\ell \otimes \mathrm{End}(A)$ is a semi-simple algebra, $u \cdot \mathbb{Q}_\ell \otimes \mathrm{End}(A)$ is generated by an idempotent e. In addition, $W = u(V_\ell A) = e(V_\ell A)$ and its complement is $(1-e)(V_\ell A)$. Obviously, $(1-e)(V_\ell A)$ is also Galois-stable, hence ρ_ℓ is semi-stable.

Let C be the centralizer of $\mathrm{End}(A) \otimes \mathbb{Q}_\ell$ in $\mathrm{End}(V_\ell A)$, let B be the centralizer of C. The double centralizer theorem gives that $B = \mathrm{End}(A) \otimes \mathbb{Q}_\ell$. Choose an element $\alpha \in \mathrm{End}(V_\ell A)^{\mathrm{Gal}(k_s/k)}$, it suffices to show that $\alpha \in B$. Consider the graph of α

$$W \triangleq \{(x, ax) | x \in V_\ell A\}$$

this is a Galois-stable subspace of $V_\ell A \times V_\ell A$, and then by 1.1.7 there exists an element $u \in \mathrm{End}(A \times A) \otimes \mathbb{Q}_\ell$ such that $W = u(V_\ell(A \times A))$. For any $c \in C$, the matrix $\begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix} \in \mathrm{End}(V_\ell A \times V_\ell A)$ commutes with $\mathrm{End}(A \times A) \otimes \mathbb{Q}_\ell$, and in particular, with u. Then $\begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix} W \subseteq W$. This says that, for any $x \in V_\ell A$, $(cx, c\alpha x) \in W$. By the definition of the graph, α maps cx to $c\alpha x$, and then α commutes with c. Hence, $\alpha \in B$. ∎

Proposition 1.1.9 (finiteness theorem)**.** Now all we need is that the condition $\mathrm{Fin}(A/k)$ holds when k is a finite field. Indeed, there is a stronger condition: there are only finitely many Abelian varieties of the dimension g (up to isomorphism) over k.

Proof. By 1.1.3 and 1.1.4, it suffices to show that there are finitely many principal polarization Abelian varieties over k. Note that they can be treated as the k-points of the stack $\mathcal{A}_{g,d}(k)$, this is a stack of finite type over k, hence the k-points are finite. ■

1.1.2 An overview of the Faltings' proof

Now let K be a number field. First we state the Mordell conjecture.

[Mor]. (The Mordell conjecture). If X is a projective and smooth curve over K of genus $g \geq 2$, then $\#X(K)$ is finite.

In 1968, Parshin proved that the Shafarevich conjecture implies the Mordell conjecture, which we will discuss in the end of this note.

[Sha1]. (The Shafarevich conjecture for curves). There exists only finitely many (smooth, projective) curves (up to isomorphism) defined over K of genus g and with good reduction outside of S, where S is a finite set of places.

[Sha2]. (The Shafarevich conjecture for Abelian varieties). There exists only finitely many Abelian varieties over K (up to isomorphism) of dimension g with good reduction outside S, and with a polarization of degree d.

Remark 1.1.10. *Note that by taking the Jacobians, [Sha2] implies [Sha1].*

Indeed, [Sha2] remains true if we remove the polarized assumption.

Remark 1.1.11. *For the concepts of reduction types, one can see this note.*

Remark 1.1.12. *Prop 4.1 in Conrad's note tells us that to have semistable reduction is transitive under isogeny.*

As we shall discuss later, the Tate conjecture implies [Sha2].

[Ta1]. (Tate conjecture). For any Abelian variety A over K the representation

$$\rho_\ell : G_K \to \mathrm{GL}(V_\ell A)$$

is semisimple, where G_K is the absolute Galois group.

[Ta2]. For any two Abelian varieties A, B over K, the natural map

$$\mathbb{Z}_\ell \otimes \mathrm{Hom}(A, B) \to \mathrm{Hom}(T_\ell A, T_\ell B)^{G_K}$$

is an isomorphism.

To prove this Tate conjecture, we will prove a slightly different finiteness condition.

The method is to construct the "heights" for Abelian varieties. In fact, there exists a moduli space $\mathcal{A}_g$ of Abelian varieties of dimension g with an embedding $\mathcal{A}_g \to \mathbb{P}^N$ by using a power of the

Hodge bundle, and then there exists a "canonical" height inherited from the height of $\mathbb{P}^N$, which is called the moduli-theoretic height

$$H : \mathcal{A}_g(K) \to \mathbb{R}$$

For the height H, we have the following property:

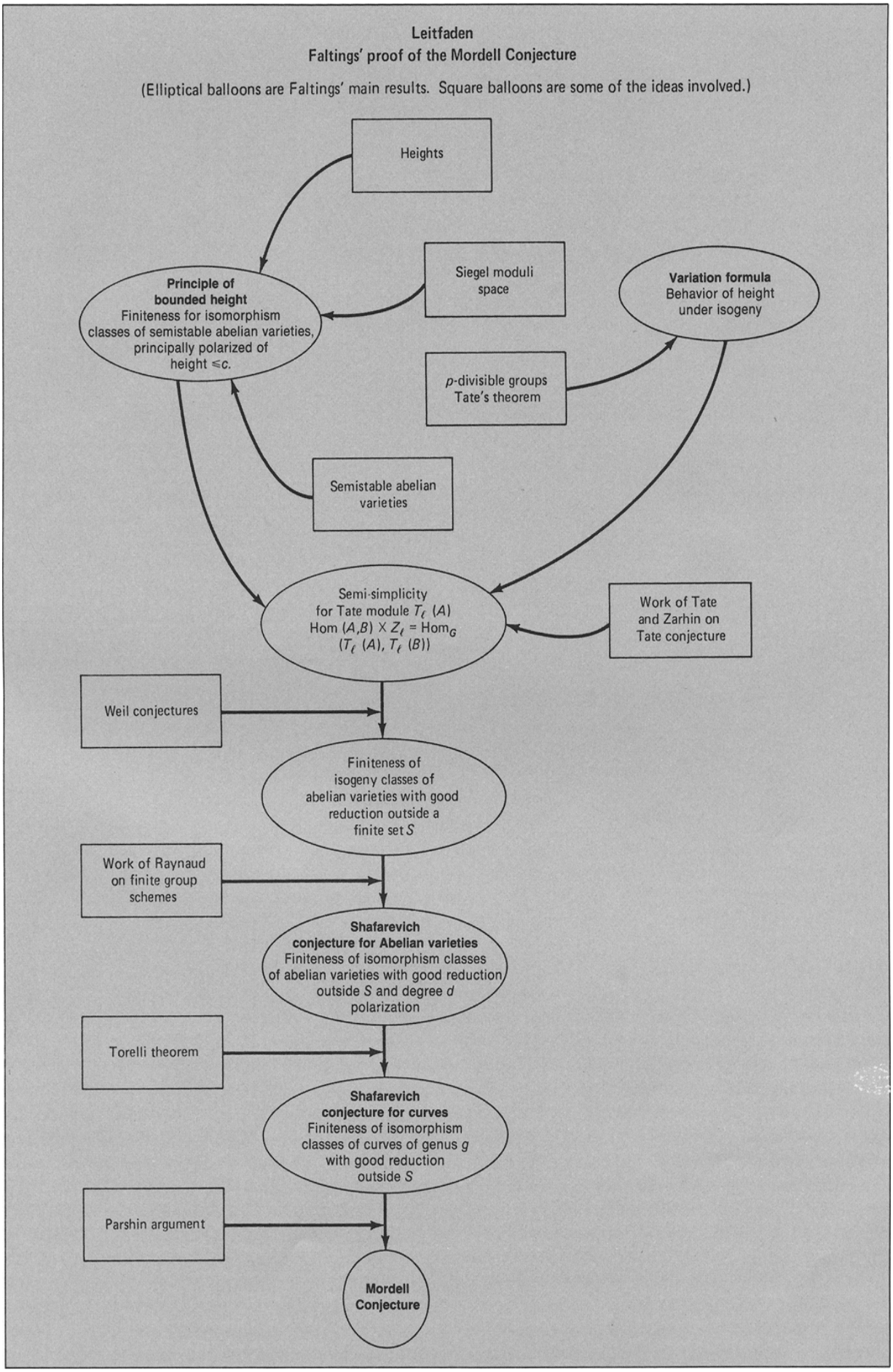
[H1]. Let C be a constant. Then there are only finitely many isomorphism classes of polarized Abelian varieties (A, λ) over K of dimension g, with λ degree d, having semistable reduction everywhere and $H(A, \lambda) \leq C$.

Remark 1.1.13. *Although [H1] states for the Abelian varieties with semistable reduction, for a general Abelian variety A, we can reach this point by a theorem from Grothendieck: A will have semistable reduction after a finite extension $L \supseteq K$, the proof can be found in Conrad's note.*

If [H1] holds true, and if H changes "slightly" under the isogeous class of a fixed Abelian variety A, then we may conclude that $\mathrm{Fin}(A/K)$ holds (here needs some arguments). However, unfortunately, we have not found a way to describe H under an isogeny class. Faltings constructed a new height h which has not much difference with H, but is bounded under isogenous.

[H2]. Let A be an Abelian variety over K having semistable reduction everywhere. Then h is eventually constant in the sequence $\{A_n\}$ (see the proof of 1.1.7).

[H3]. Let C be a constant. Then there are only finitely many isomorphism classes of polarized Abelian varieties (A, λ) over K of dimension g, with λ degree d, having semistable reduction everywhere and $h(A, \lambda) \leq C$.


Leitfaden
Faltings' proof of the Mordell Conjecture
(Elliptical balloons are Faltings' main results. Square balloons are some of the ideas involved.)
Heights
Siegel moduli space
Principle of bounded height
Finiteness for isomorphism classes of semistable abelian varieties, principally polarized of height ≤c.
Variation formula
Behavior of height under isogeny
p-divisible groups
Tate's theorem
Semistable abelian varieties
Semi-simplicity for Tate module T_ℓ (A)
Hom (A,B) × Z_ℓ = Hom_G (T_ℓ (A), T_ℓ (B))
Work of Tate and Zarhin on Tate conjecture
Weil conjectures
Finiteness of isogeny classes of abelian varieties with good reduction outside a finite set S
Work of Raynaud on finite group schemes
Shafarevich conjecture for Abelian varieties
Finiteness of isomorphism classes of abelian varieties with good reduction outside S and degree d polarization
Torelli theorem
Shafarevich conjecture for curves
Finiteness of isomorphism classes of curves of genus g with good reduction outside S
Parshin argument
Mordell Conjecture

1.2 The proof of [H1] and [H3]

1.2.1 The classical theory of heights

We first introduce the theory of height functions, which is a reading note for Silverman's paper.

Absolute values

Remark 1.2.1. *We will use the following notations:*

- $K/\mathbb{Q}$, *a number field.*
- M_K, *the set of absolute values on* K *extending the usual absolute values on* $\mathbb{Q}$.
- $\|\cdot\| = |\cdot|_v^{[K_v:\mathbb{Q}_v]}$.

Height on projective space

Definition 1.2.2. Let $P \in \mathbb{P}^n(K)$. The height of P (relative to K) is defined by the formula

$$H_K(P) = \prod_{v \in M_K} \max\{\|x_0\|_v, \cdots, \|x_n\|_v\}$$

Proposition 1.2.3. For a finite extension L/K, we have the formula

$$H_L(P) = H_K(P)^{[L:K]}$$

Proposition 1.2.4. For all points P, $H_K(P) \geq 1$, as we can choose homogeneous coordinates for P with $x_i = 1$ for some i.

Definition 1.2.5. Let $P \in \mathbb{P}^n(\bar{\mathbb{Q}})$. The absolute height of P is defined by

$$H(P) = H_K(P)^{1/[K:\mathbb{Q}]}$$

where K is any number field with $P \in \mathbb{P}^n(K)$. Let $h(P) = \log H(K)$.

Example 1. If $P \in \mathbb{P}^n(\mathbb{Q})$. Let $[x_0, \cdots, x_n]$ be a homogeneous coordinate such that $x_i \in \mathbb{Z}$ for all i and $\gcd(x_0, \cdots, x_n) = 1$. Then for finite prime p, $\max\{\|x_0\|_p, \cdots, \|x_n\|_p\} = 1$, hence

$$H(P) = \max\{|x_0|, \cdots, |x_n|\}$$

Theorem 1.2.6 (Finiteness theorem)**.** Let C and d be constant. Then

$$\{P \in \mathbb{P}^n(\bar{\mathbb{Q}}) : H(P) \leq C,\ [\mathbb{Q}(P) : \mathbb{Q}] \leq d\}$$

is a finite set.

Proof. From the above example, the theorem is clear for $P \in \mathbb{P}^n(\mathbb{Q})$.

In general, choose homogeneous coordinates $P = [x_0, \cdots, x_n]$ with some $x_i = 1$. Then

$$H([x_0, \cdots, x_n]) \geq H([1, x_i])$$

so we reduce to the case $P = [1, x]$ and $[\mathbb{Q}(x) : \mathbb{Q}] = d$.

Let $x^{(1)}, \cdots, x^{(d)}$ be the conjugates of x over $\mathbb{Q}$, and $1 = s_0, \cdots, s_d$ be the elementary symmetric polynomials. Then x is a root of the polynomial

$$F(T) = \prod (T - x^{(i)}) = \sum_{j=0}^{d} (-1)^j s_i T^{d-j}$$

Note that $|s_j|_v \leq C_d^j |x|_v < d!|x|_v$, we have

$$\begin{aligned}
H([s_0, \cdots, s_d]) &= \prod_{v \in M_{k(x)}} \max_i \{\|s_i\|_v^{\frac{1}{[\mathbb{Q}(x):\mathbb{Q}]}}\} \\
&= \prod_{v \in M_{k(x)}} \max_i \{|s_i|_v^{\frac{[\mathbb{Q}(x)_v:\mathbb{Q}_v]}{[\mathbb{Q}(x):\mathbb{Q}]}}\} \\
&= \prod_{|x|_v \leq 1} \max_i \{|s_i|_v^{\frac{[\mathbb{Q}(x)_v:\mathbb{Q}_v]}{[\mathbb{Q}(x):\mathbb{Q}]}}\} \cdot \prod_{|x|_v > 1} \max_i \{|s_i|_v^{\frac{[\mathbb{Q}(x)_v:\mathbb{Q}_v]}{[\mathbb{Q}(x):\mathbb{Q}]}}\} \\
&< \prod_{|x|_v \leq 1} (d!)^{\frac{[\mathbb{Q}(x)_v:\mathbb{Q}_v]}{[\mathbb{Q}(x):\mathbb{Q}]}} \cdot \prod_{|x|_v > 1} \left((d!)^{\frac{[\mathbb{Q}(x)_v:\mathbb{Q}_v]}{[\mathbb{Q}(x):\mathbb{Q}]}} \cdot |x|_v^{\frac{[\mathbb{Q}(x)_v:\mathbb{Q}_v]}{[\mathbb{Q}(x):\mathbb{Q}]}} \right) \\
\left(\sum [\mathbb{Q}(x)_v : \mathbb{Q}_v] = [K(x) : \mathbb{Q}]\right) &= d! \cdot \prod_{|x|>1} |x|_v^{\frac{[\mathbb{Q}(x)_v:\mathbb{Q}_v]}{[\mathbb{Q}(x):\mathbb{Q}]}} \\
&\leq d! \cdot C
\end{aligned}$$

Then the choices of $[s_0, \cdots, s_d]$ is finite. Hence the choices of x is finite. ■

Heights on projective varieties

Definition 1.2.7. Let V be a smooth projective variety over $\bar{\mathbb{Q}}$. Let $F : V \to \mathbb{P}^n$ be a morphism. The (logarithmic) height on V relative to F is defined by

$$h_F : V \to \mathbb{R}, \quad h_F(P) = h(F(P)) = \log H(F(P))$$

Theorem 1.2.8. Let $\mathcal{L}$ be a sheaf without base-points on V, that is, $\mathcal{L}$ is generated by global section. Let $F : V \to \mathbb{P}^n$ and $G : V \to \mathbb{P}^n$ be two morphisms of V which are associated to $\mathcal{L}$ (depending on the generators). Then

$$h_F = h_G + O(1)$$

that is, $|h_F(P) - h_G(P)|$ is bounded as P ranges over V.

Proof. ■

Definition 1.2.9. The group of functions mod $O(1)$ on V, denoted by $\mathcal{H}(V)$, is defined by

$$\mathcal{H}(V) = \{\text{functions } h : V \to \mathbb{R}\}/\{\text{bounded functions}\}$$

Definition 1.2.10. Let $\mathcal{L}$ be a sheaf generated by global sections. The height function associated to $\mathcal{L}$ is the class function $h_{\mathcal{L}} \in \mathcal{H}(V)$ obtained by taking the height function h_F for any morphism F associated to $\mathcal{L}$.

Proposition 1.2.11. Let $\mathcal{L}$ and $\mathcal{M}$ be sheaves generated by global section. Then

$$h_{\mathcal{L}\otimes\mathcal{M}} = h_{\mathcal{L}} + h_{\mathcal{M}} + O(1)$$

Proof. Let $F = [f_0, \cdots, f_n]$ and $G = [g_0, \cdots, g_m]$ be morphisms associated to $\mathcal{L}$ and $\mathcal{M}$ respectively. Then

$$[\cdots, f_i g_j, \cdots] : V \to \mathbb{P}^{nm+n+m}$$

is associated with $\mathcal{L} \otimes \mathcal{M}$. Now the result follows from that

$$\max\{\cdots, \|f_i g_j\|_v, \cdots\} = \max\{\cdots, \|f_i\|_i, \cdots\} \cdot \max\{\cdots, \|g_j\|_v, \cdots\}$$

■

Now we generalize the definition of heights to all invertible sheaves.

Definition 1.2.12. Let $\mathcal{L} \in \mathrm{Pic}(V)$ be any invertible sheaf. Choose sheaves $\mathcal{L}_1$ and L_2 which are generated by global section such that $\mathcal{L} = \mathcal{L}_1 \otimes \mathcal{L}_2^{-1}$. Then the height function on V associated to $\mathcal{L}$ is the function defined by

$$h_{\mathcal{L}} = h_{\mathcal{L}_1} - h_{\mathcal{L}_2} \in \mathcal{H}(V)$$

Theorem 1.2.13 (Height machine)**.** (a) There exists a unique homomorphism

$$\mathrm{Pic}(V) \to \mathcal{H}(V), \quad \mathcal{L} \mapsto h_{\mathcal{L}}$$

(b) If $f : V \to W$ is a morphism of smooth varieties, and $\mathcal{L}$ is an invertible sheaf on W, then

$$h_{f^*\mathcal{L}} = h_{\mathcal{L}} \circ f + O(1)$$

Corollary 1.2.14 (Finiteness)**.** If $\mathcal{L}$ is an ample sheaf on V, then for all constants C and d, the set

$$\{P \in V(\bar{\mathbb{Q}}) : h_{\mathcal{L}} \le C,\ [\mathbb{Q}(P) : \mathbb{Q}] \le d\}$$

is finite.

Note that for invertible sheaves $\mathcal{L}$ generated by global sections we already have $h_{\mathcal{L}}(P) + O(1) = \log H(F_{\mathcal{L}}(P)) \ge 1$.

Proposition 1.2.15 (Positivity)**.** For any invertible sheaf $\mathcal{L}$ on V with base locus B is not all of V, then there is a rational map $F : V \to \mathbb{P}^n$ associated to $\mathcal{L}$ which is a morphism on the complement of B. Then

$$h_{\mathcal{L}}(P) \ge O(1)\ \forall P \notin B$$

Proof. Let Z be the corresponding divisor with B, then Z is a positive divisor contained in C, where C is the corresponding divisor of $\mathcal{L}$.

Let X and Y be very ample positive divisors such that $Z \sim Y - X$. Let $\{f_0, \cdots, f_n\}$ be a basis for $\mathcal{L}(X)$. Since Z is positive, we can extend this basis to a basis

$$\{f_0, \cdots, f_n, g_1, \cdots, g_m\}$$

of $\mathcal{L}(Y)$. Let f and g be the corresponding associated with X and Y, as well as the base above, then

$$h_g(P) \geq h_f(P)$$

this proves the proposition. ■

Proposition 1.2.16 (quasi-equivalence)**.** Let $\mathcal{L}$ and $\mathcal{M}$ be algebraically equivalent sheaves on V, and assume that $\mathcal{L}$ is ample. Then for all $\epsilon > 0$,

$$(1-\epsilon)h_{\mathcal{L}} - O(1) \leq h_{\mathcal{M}} \leq (1+\epsilon)h_{\mathcal{L}} + O(1)$$

Heights on Abelian varieties

Theorem 1.2.17. By the cube theorem, let $A/\bar{\mathbb{Q}}$ be an Abelian variety, and let $\mathcal{L}$ be an invertible sheaf on A. Then for all $P, Q, R \in A$,

$$h_{\mathcal{L}}(P+Q+R) - h_{\mathcal{L}}(P+Q) - h_{\mathcal{L}}(P+R) - h_{\mathcal{L}}(Q+R) + h_{\mathcal{L}}(P) + h_{\mathcal{L}}(Q) + h_{\mathcal{L}}(R) = O(1)$$

The constant $O(1)$ only depends on A and $\mathcal{L}$.

Corollary 1.2.18. (a) Let n be an integer, and let $[n] : A \to A$ be the multiplication-by-n map. Then

$$h_{\mathcal{L}} \circ [n] = \frac{n^2+n}{2} h_{\mathcal{L}} + \frac{n^2-n}{2} h_{\mathcal{L}} \circ [-1] + O(1)$$

(b) Taking $R = -Q$, we have

$$h_{\mathcal{L}}(P+Q) + h_{\mathcal{L}}(P-Q) = 2h_{\mathcal{L}}(P) + h_{\mathcal{L}}(Q) + h_{\mathcal{L}}(-Q) + O(1)$$

by (a), if $h_{\mathcal{L}}$ is even, then

$$h_{\mathcal{L}}(P+Q) + h_{\mathcal{L}}(P-Q) = 2h_{\mathcal{L}}(P) + 2h_{\mathcal{L}}(Q) + O(1)$$

if $h_{\mathcal{L}}$ is odd, then h is linear (modulo $O(1)$)

$$h_{\mathcal{L}}(P+Q) = h_{\mathcal{L}}(P) + h_{\mathcal{L}}(Q) + O(1)$$

Theorem 1.2.19. Let $A/\bar{\mathbb{Q}}$ be an Abelian variety, and let $\mathcal{L}$ be an invertible sheaf on A.

(a) There is a unique function

$$\hat{h}_{\mathcal{L}} : A \to \mathbb{R}$$

with the following

(i) $\hat{h}_{\mathcal{L}}$ is a quadratic function (i.e. the map

$$\langle \cdot, \cdot \rangle : A \times A \to \mathbb{R}$$
$$\langle P, Q \rangle = \hat{h}_{\mathcal{L}}(P+Q) - \hat{h}_{\mathcal{L}}(P) - \hat{h}_{\mathcal{L}}(Q)$$

is bilinear).

(ii) $\hat{h}_{\mathcal{L}} = h_{\mathcal{L}} + O(1)$ on A.

(b) Assume that $\mathcal{L}$ is ample and symmetric. Then

(i) $\hat{h}_{\mathcal{L}}(P) \geq 0$.

(ii) $\hat{h}_{\mathcal{L}}(P) = 0$ if and only if P is a point of finite order.

(iii) More generally, $\hat{h}_{\mathcal{L}}$ is a positive definite quadratic form on $A(\bar{\mathbb{Q}}) \otimes \mathbb{R}$.

The proof of [H1]

We will use the Siegel modular variety $\mathcal{A}_{g,d}$, and the fact that it has a canonical morphism $\mathcal{A}_{g,d} \to \mathbb{P}^N$. In Milne's note, $\mathcal{A}_{g,d}(K)$ maps to an algebraic variety bijectively when K is algebraically closed.

From 1.2.6, we know that there are finitely many (A, λ) such that $H(A, \lambda) \leq C$. However, job's not finished. Two pairs (A, λ) and (B, λ') send to the same point if and only if they are $\bar{\mathbb{Q}}$-isomorphic, but this does not mean that they are K-isomorphic. Hence, all we need is the following lemma:

Lemma 1.2.20. Let (A_0, λ_0) be a fixed polarized Abelian variety over K with semistable reduction everywhere, then, up to K-isomorphism, there are finitely many Abelian varieties (A, λ) with semistable reduction everywhere such that $(A, \lambda) \cong (A_0, \lambda_0)$ after base change to $\bar{\mathbb{Q}}$.

Proof. Let Σ be the set of pairs (A, λ) satisfying $(A, \lambda) \cong (A_0, \lambda_0)$ over $\bar{\mathbb{Q}}$.

Let S be the set of primes of K at which A_0 has bad reduction. Then S is also the set at which A has bad reduction for all $A \in \Sigma$.

Fix a number $\ell \geq 3$ which is a power of a prime number. Let $L = K(A[\ell])$, this is a finite extension of K with degree $\leq \#(\mathrm{GL}_{2g}(\mathbb{Z}/\ell\mathbb{Z}))$, and is unramified outside S and $\{v : v|\ell\}$. Then the discriminant $D(L/K) = \prod(L_w/K_v)$ is bounded. By Hermite theorem there are finitely many extensions L/K. Hence, there exists a finite field extension L/K such that L contains all ℓ-torsion points in A for all $A \in \Sigma$.

We claim (A, λ) must be isomorphic to (A_0, λ_0) over L. Let $\alpha : (A, \lambda) \to (A_0, \lambda_0)$ be an isomorphism over $\bar{\mathbb{Q}}$. Then for any $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/L)$, $\sigma \circ \alpha \circ \sigma^{-1} \circ \alpha^{-1}$ is an automorphism of (A_0, λ_0) fixed ℓ-torsion points. Then by 1.1.1 it must be identity on A_0. Hence we reduce the field $\bar{\mathbb{Q}}$ to L.

Now given an isomorphism $\alpha : (A, \lambda) \to (A_0, \lambda_0)$ over L, we know that $\alpha_\sigma = \sigma \circ \alpha \circ \sigma^{-1} \circ \alpha^{-1} = (\sigma\alpha) \circ \alpha^{-1}$ is an automorphism of $((A_0)_L, (\lambda_0)_L)$. Hence we obtain a crossed homomorphism $\mathrm{Gal}(L/K) \to \mathrm{Aut}((A_0)_L, (\lambda_0)_L)$. Then there is a map sending $\alpha : A_L \to (A_0)_L$ to an element in

$$H^1(\mathrm{Gal}(L/K), \mathrm{Aut}(A_L, \lambda_L))$$

If α_1 and α_2 map to the same element, that is, there exists $\beta \in \mathrm{Aut}(A_L, \lambda_L)$ such that

$$(\alpha_1)_\sigma = (\sigma\beta) \circ (\alpha_2)_\sigma \circ (\sigma\beta)$$

(Note that this is non-Abelian group cohomology and the multiplication for $\mathrm{Aut}(A_L, \lambda_L)$ here can be treated as $f \cdot g = g \circ f$) and then we obtain an isomorphism $(A_1)_L \to (A_2)_L$ which is invariant under the composite with $\sigma \in \mathrm{Gal}(L/K)$, hence is an K-isomorphism. Therefore, we obtain an injective map (in fact it is bijective)

$$\{(A, \lambda) : (A, \lambda) \text{ is isomorphic to } (A_0, \lambda_0) \text{ over } L\}/K\text{-isomorphism} \to H^1(\mathrm{Gal}(L/K), \mathrm{Aut}(A_L, \lambda_L))$$

Then Σ is finite. ■

Remark 1.2.21. *The reduction to a finite extension L can be generalized, see van der Geer's book (12.13).*

The last part is an example of Galois descent, see Poonen's book section 4.5.

1.2.2 Heights and metrized line bundles

Metrized line bundles on $\mathrm{Spec}(R)$

Remark 1.2.22. *Let R be the ring of integers of K. Then a line bundle $\mathcal{L}$ on $\mathrm{Spec}R$ corresponds to a projective R-module of rank 1. (If further R is a PID, then $\mathcal{L}$ is a free module).*

Definition 1.2.23. A metrized line bundle on $\mathrm{Spec}(R)$ is a pair $(\mathcal{L}, |\cdot|)$, where $\mathcal{L}$ is a line bundle on $\mathrm{Spec}R$, and for each archimedean absolute value $v \in M_K^\infty$, $|\cdot|_v$ is a v-adic norm (metric) on the one-dimensional K_v vector space $\mathcal{L} \otimes_R K_v$.

The degree of a metrized line bundle $(\mathcal{L}, |\cdot|)$ is defined as

$$\deg(\mathcal{L}, |\cdot|) = \log \#(\mathcal{L}/Rt) - \sum_{v \in M_K^\infty} \log \|t\|_v$$

where we choose $t \in \mathcal{L}$ with $t \neq 0$.

Example 2. If R is a PID, then we can choose t such that $\mathcal{L} = Rt$. Then $\deg(\mathcal{L}, |\cdot|) = -\sum_{v \in M_K^\infty} \log \|t\|_v$.

Remark 1.2.24. *For v a finite place, $\mathcal{L} \otimes \mathcal{O}_{K_v}$ is free from this useful result, if we choose a generator l_v, then we may define $\|a \cdot l_v\|_v = \|a\|_v$ for $a \cdot l_v \in \mathcal{L} \otimes K_v$. By Chinese remainder theorem*

$$\#(\mathcal{L}/Rt) = \#\left(\prod_{v \text{ finite}} \mathcal{L} \otimes R_v/R_v t\right) = \prod_{v \text{ finite}} \#(\mathcal{L} \otimes R_v/R_v t)$$

Suppose $t = a \cdot l_v$ for $a \in K_v$, then

$$\#(\mathcal{L} \otimes R_v/R_v t) = \#(\mathcal{O}_{K_v}/(a)) = \|a\|_v^{-1} = \|t\|_v^{-1}$$

Then

$$\deg(\mathcal{L}, |\cdot|) = -\sum_{v \in M_K} \log \|t\|_v$$

Example 3. Let A/K be an Abelian variety, and $N(A)/\mathcal{O}_K$ be the Neron model. Then we get the Hodge bundle $\omega_A = e^*(\Omega^g_{N(A)/\mathcal{O}_K})$ over $\mathrm{Spec}(\mathcal{O}_K)$. For any infinite place $K \hookrightarrow \mathbb{C}$, consider the hermitian metric on $\omega_A \otimes_K \mathbb{C}$ defined by

$$|\alpha|^2 = \frac{1}{2^g}\int_{A(\mathbb{C})} |\alpha \wedge \bar{\alpha}|$$

If $N(A)$ is semi-Abelian, we set the Faltings height h to be $h(A) = \dfrac{1}{[K:\mathbb{Q}]}\deg(\omega_A)$.

Metrized line bundles on varieties

Remark 1.2.25. *Let V/K be a projective variety. For any line bundle $\mathcal{L}$, the stalk $\mathcal{L}_P$ is an one-dimensional $k(P)$ vector space.*

Definition 1.2.26. Let $v \in M_K$. A v-adic metric on $\mathcal{L}$ consisting of a (non-trivial) v-adic norm $|\cdot|_v$ on each fiber $\mathcal{L}_P \otimes K_v$ such that the norms "vary continuously with $P \in V(K_v)$". (That is, if $f \in H^0(U, \mathcal{L})$ is a section on some open set U, and if $U(K_v)$ is given the v-adic topology, then the map

$$U(K_v) \to [0, \infty), \quad P \mapsto |f_P|_v$$

is continuous.)

Lemma 1.2.27. Let $v \in M_K^\infty$, and suppose that $|\cdot|_v$ and $|\cdot|'_v$ are two v-adic metrics on $\mathcal{L}$. Then there exist constants $c_1, c_2 > 0$ such that

$$c_1|\cdot|_v \le |\cdot|'_v \le c_2|\cdot|_v$$

Proof. For each $P \in V(K_v)$, choose some $f_P \in \mathcal{L}_P$ with $f_P \neq 0$. Then $|f_P|_v/|f_P|'_v$ is independent the choice of f_P, since $\mathcal{L}_P$ is 1-dimensional over $k(P)$. Hence we obtain a well-defined map

$$F : V(K_v) \to (0, \infty), \quad P \mapsto |f_P|_v/|f_P|'_v$$

But F is continuous, and since V is projective, $V(K_v)$ is compact. Therefore, there exist constants c_1, c_2 such that $c_1 \le F(P) \le c_2$ for all $P \in V(K_v)$. ∎

Proposition 1.2.28. Assume that $\mathcal{L}$ is very ample, and fix an embedding $V \subseteq \mathbb{P}^n_K$ corresponding to $\mathcal{L}$. Any point $P \in V(K)$ extends to a point $P : \mathrm{Spec}(R) \to \mathbb{P}^n_{\mathbb{Z}}$. Hence if we are given v-adic metrics on $\mathcal{O}(1)$ for each $v \in M_K^\infty$, then by pull-back $P^*\mathcal{O}(1)$ becomes a metrized line bundle on $\mathrm{Spec}(R)$. Also,

$$\deg P^*\mathcal{O}(1) = [K:\mathbb{Q}]h_\ell(P) + O(1)$$

Distance functions and logarithmic singularities

Definition 1.2.29. Let X be a closed subset of V and U its complement. Let $v \in M_K^\infty$. A logarithmic distance function for X is a map:

$$d_X : U(\bar{K}_v) \to [0, \infty)$$

with the property that if $f_1 = \cdots = f_r = 0$ are local equations for X, that is, X is defined by these equations, then

$$|d_X(P) - \log^+ \min_{1\le j\le r}\{|f_j(P)|_v^{-1}\}|$$

extends to a bounded function on any open subset of $V(\bar{K}_v)$ on which the f_j are regular.

Proposition 1.2.30. Let $\mathcal{L}$ be an ample line bundle on V/K. Then there exists a constant $c > 0$ such that

$$h_{\mathcal{L}}(P) > cd_X(P) + O(1),\ P \in U(K)$$

Definition 1.2.31. Let V, X, U be as above, let $\mathcal{L}$ be a line bundle on V, and let $|\cdot|'_v$ be a v-adic metric on the restriction $\mathcal{L}|_U$. We say that $|\cdot|'_v$ has logarithmic singularities along X if for any v-adic metric $|\cdot|_v$ defined on all of $\mathcal{L}$, there are constants $c_1, c_2 > 0$ such that

$$\max\{|\cdot|_v/|\cdot|'_v, |\cdot|'_v/|\cdot|_v\} \le c_1(d_X + 1)^{c_2} \quad \text{on } U(\bar{K}_v)$$

If $(\mathcal{L}|_U, |\cdot|')$ is a metrized line bundle, then we say that it has logarithmic singularities along X if $|\cdot|'_v$ has logarithmic singularities along X for each $v \in M_K^\infty$.

Theorem 1.2.32 (Faltings)**.** With the same hypothesis, assume that $\mathcal{L}$ is very ample. Then

$$\{x \in U(K) | h_{\mathcal{L},|\cdot|'_v} < C\}$$

is finite.

Proof. ■

Now we can prove [H3].

By Gabber's lemma, there is a diagram

$$\begin{array}{ccc} A^u & \longrightarrow & \overline{A^u} \\ \downarrow\uparrow e & & \downarrow\uparrow e \\ \mathcal{A}_g & \hookrightarrow & \overline{\mathcal{A}_g} \\ \| & & \pi\downarrow \\ \mathcal{A}_g & \hookrightarrow & \mathcal{A}_g^* \end{array}$$

where A^u is the universal Abelian variety (see this note), $\mathcal{A}_g^*$ is the minimal compactification, $\overline{\mathcal{A}_g}$ is the toroidal compactification. The Hodge bundle $\omega_{\mathcal{A}_g}$ and $\omega_{\overline{\mathcal{A}_g}}$ are defined by $e^*(\Omega^g_{A^u/\mathcal{A}_g})$ and $e^*(\Omega^g_{\overline{A^u}/\overline{\mathcal{A}_g}})$. The two compactifications are compatible:

$$\pi^*\mathcal{O}(1) \cong \omega_{\overline{\mathcal{A}_g}}$$

We use the following fact, $(\mathcal{O}(1)|_{\mathcal{A}_g}, |\cdot|^{\mathrm{can}}_{\mathcal{A}_g})$ has log singularities along $\mathcal{A}_g^*\backslash\mathcal{A}_g$. Then

$$\{x \in \mathcal{A}_g(K) | h_{\omega_{\mathcal{A}_g},|\cdot|'_v} < C\}$$

is finite.

1.3 The proof for Tate conjecture over number fields

1.3.1 An overview

We shall prove the following theorem, which is a restatement of [H2], in the following section.

Theorem 1.3.1. Let $B \subseteq A[\ell^\infty]$ be an ℓ-adic group, and denote $B_n = B[\ell^n]$ and $A_n = A/B_n$. If A is semistable everywhere, then $h(A_n)$ is eventually constant as a function of n.

Like section 1.1, the following result will be important, which we will discuss in the last section:

Proposition 1.3.2. If A is an Abelian variety over a number field K, and $W \subseteq V_\ell(A)$ is a sub-representation, then there exists $u \in \mathrm{End}(A) \otimes \mathbb{Q}_\ell$ such that $u(V_\ell A) = W$.

1.1.8 actually gives us how to prove Tate conjecture from 1.3.2.

1.3.2 Under isogeny

Proposition 1.3.3. Let $\phi : A \to B$ be an isogeny of varieties over $\mathrm{Spec}(K)$ which are semistable everywhere. Then there exists a homomorphism of their Neron models $\varphi : N(A) \to N(B)$ over $\mathrm{Spec}(\mathcal{O}_K)$. Let $G = \mathrm{Ker}(\varphi)$, and assume that $s : \mathrm{Spec}(\mathcal{O}_K) \to G$ is the identity section of G. Then

$$h(A) - h(B) = \frac{1}{[K:\mathbb{Q}]} \log(|s^*\Omega^1_{G/\mathcal{O}_K}|) - \frac{1}{2}\log(\deg(\phi))$$

Proof. Recall the definition of faltings' height h: choose $\omega \in \Gamma(A, \Omega^g_{A/K})$. Let $M = \Gamma(N(A), \Omega_{N(A)/\mathcal{O}_K})$, then

$$h(A) = \frac{1}{[K:\mathbb{Q}]}\left(\log|M/\mathcal{O}_K \cdot \omega| - \sum_{i:K\hookrightarrow\mathbb{C}} \frac{1}{2}\log\int_{A(\mathbb{C})} \omega \wedge \bar{\omega}\right)$$

See this site, and by the structure theorem for the finitely generated modules, we may assume that $M = \Gamma(N(A), \Omega^g_{N(A)/\mathcal{O}_K})$ and $N = \Gamma(N(B), \Omega^g_{N(B)/\mathcal{O}_K})$ are free, since otherwise we may take an extension of K.

Now let w and w' be generators of M and N respectively. Also, we assume that $\phi^* w' = aw$, where $a \in \mathcal{O}_K$. Consider $A(\mathbb{C}) = \mathbb{C}^g/\Lambda_1$ and $B(\mathbb{C}) = \mathbb{C}^g/\Lambda_2$, ϕ induces $\Lambda_1 \subseteq \Lambda_2$ with index $\deg(\phi)$. Then

$$\int_{B(\mathbb{C})} \omega' \wedge \bar{\omega'} = \deg(\phi)^{-1}\int_{A(\mathbb{C})} \omega' \wedge \bar{\omega'_B} = \deg(\phi)^{-1}\int_{A(\mathbb{C})} \|a\|_i \omega \wedge \bar{\omega} = \frac{i(a)\overline{i(a)}}{\deg(\phi)}\int_{A(\mathbb{C})} \omega \wedge \bar{\omega}$$

Therefore,

$$h(A)-h(B) = \frac{1}{2[K:\mathbb{Q}]}\sum_{i:K\hookrightarrow\mathbb{C}}\big(\log(|i(a)|^2) - \log(\deg(\phi))\big) = -\frac{1}{2}\log(\deg(\phi)) + \frac{1}{[K:\mathbb{Q}]}\log|N_{K/\mathbb{Q}}(a)|$$

It remains to show that

$$|s^*\Omega^1_{G/\mathcal{O}_K}| = |N_{K/\mathbb{Q}}(a)|$$

First, there is a fiber square

$$\begin{array}{ccc} G & \longrightarrow & N(A) \\ \downarrow & & \downarrow{\scriptstyle \varphi} \\ \mathrm{Spec}(\mathcal{O}_K) & \longrightarrow & N(B) \end{array}$$

Then $|s^*\Omega^1_{N(A)/N(B)}| = |s^*\Omega^1_{G/\mathcal{O}_K}|$.

Consider the exact sequence

$$\varphi^*(\Omega^1_{N(B)/\mathcal{O}_K}) \to \Omega^1_{N(A)/\mathcal{O}_K} \to \Omega^1_{N(A)/N(B)} \to 0$$

of sheaves on $N(A)$. Pulling back via s, we have a short exact sequence

$$s^*(\Omega^1_{N(B)/\mathcal{O}_K}) \xrightarrow{\varphi^*} s^*\Omega^1_{N(A)/\mathcal{O}_K} \to s^*\Omega^1_{N(A)/N(B)} \to 0$$

Note that $\det(\varphi^*) = a$ by taking wedge product. Then

$$|\mathrm{Coker}(\varphi^*)| = |\mathrm{Coker}(\det(\varphi^*))| = |\mathcal{O}_K/a\mathcal{O}_K| = |N_{K/\mathbb{Q}}(a)|$$

■

Our next goal is to study $|s^*\Omega^1_{G/\mathcal{O}_K}|$.

Note that G is a quasi-finite separated flat group scheme.

We first prove a lemma for finite group schemes:

Lemma 1.3.4. A finite group scheme G over a field k is etale if and only if its order is invertible in k. In particular if char $(k) = 0$, any finite group scheme is etale over k.

Proof. Note that G is a spectrum of Artin ring over k.

If k has characteristic 0, by the general version for Cartier's theorem, G is reduced, in particular, $G \times_k k^{\mathrm{al}}$. Then every Artin local component is exactly Speck^{al}. Hence, G is etale.

For other cases, suppose G is connected, then G is a spectrum of a local Artin ring A and there is an isomorphism

$$A \otimes_k k^{\mathrm{al}} \cong k^{\mathrm{al}}[x_1, \cdots, x_n]/(x_1^{p^{e_1}}, \cdots, x_n^{p^{e_n}})$$

for $e_i \geq 1$ with the maximal ideal $(x_1^p, \cdots, x_n^p)$. The order of G is then defined by the rank of k-space A, also by the k^{al}-rank of $A \otimes_k k^{\mathrm{al}}$, which is $\max\{p^{e_i-1}\}$. Then for general G with order prime to p, $G^0 \otimes_k k^{\mathrm{al}}$ is trivial, then G is etale. ■

Corollary 1.3.5. If G is a quasi-finite separated flat group scheme over a base S. Assume the fibers of G have orders which are divisible on the base S. Then G is etale over S.

Corollary 1.3.6. Let G be a quasi-finite separated group scheme killed by a power of ℓ over Spec$\mathcal{O}_K$. For each place v above ℓ, let $\mathcal{O}_v$ be the completion at v and let $G_v = G \otimes_{\mathcal{O}_K} \mathcal{O}_v$. Then,

$$|s^*(\Omega^1_{G/\mathcal{O}_K})| = \prod_v |s^*(\Omega^1_{G_v/\mathcal{O}_v})|$$

Proof. Let $M = s^*(\Omega^1_{G/\mathcal{O}_K})$, it is a finite $\mathcal{O}_K$-module. By 1.3.5, $M_v \neq 0$ holds only for $v|\ell$. Then $|M| = \prod_{v|\ell} |M_v|$. ■

Now we discuss $s^*\Omega^1_{G_v/\mathcal{O}_v}$. We will use the structure theorem for quasi-finite morphism (which is a corollary of Zariski's main theorem, one can see lemma 8.1 in this note).

Proposition 1.3.7. Let G be a quasi-finite separated flat group scheme killed by a power of ℓ over a complete discrete valuation ring R with finite residue field. Then G has a canonical subgroup scheme G^0_f which is finite flat and connected over R such that

$$|s^*(\Omega^1_{G/R})| = |R/\mathrm{disc}(G^0)|^{\frac{1}{\#G^0_f}}$$

Proof. By the structure theorem for quasi-finite morphism, $G = G_f \coprod G_\eta$, and G_η has no special fiber. Since $\mathrm{Spec}(R)$ is connected, and $\mathrm{Spec}(R) \xrightarrow{s} G \to \mathrm{Spec}(R)$ is identity, s factors through G_f. Hence

$$s^*(\Omega^1_{G/R}) \cong s^*(\Omega^1_{G_f/R})$$

Let G^0_f be the connected component, then similarly

$$s^*(\Omega^1_{G_f/R}) \cong s^*(\Omega^1_{G^0_f/R})$$

Let $H = G^0_f$. Write $H = \mathrm{Spec}A$, then A is a local ring free of rank $\#H$ over R. Let $I = \mathrm{Ker}(A \to R)$. Note that $I/I^2 = s^*(\Omega^1_{H/R})$ (the second exact sequence for the differential sheaf). In van der Geer's book Prop 3.15, the pull back of $s^*\Omega^1_{G/R}$ under the structure morphism $G \to R$ is isomorphic to $\Omega^1_{G/R}$. In other words, $I/I^2 \otimes_R A \cong \Omega^1_{A/R}$. Thus

$$|\Omega^1_{A/R}| = |s^*(\Omega^1_{H/R})|^{\#H}$$

The ring extension $R \to A$ is monogenic, that is, A is generated by an element α with a minimal polynomial f. Hence, $\Omega^1_{A/R}$ is an A-module generated by $d\alpha$, this is annihilated by $f'(\alpha)$ since $d(f(\alpha)) = 0$. Note that the different ideal $\delta_{A/R}$ is generated by $f'(\alpha)$, then $\Omega^1_{A/R}$ is free of rank 1 over $A/\delta_{A/R}$. Suppose $\delta_{A/R} = \mathfrak{P}^n$, $\mathfrak{P} \cap R = \mathfrak{p}$. Let e, f be the ramification and inertial degrees. Then $\mathrm{disc}_{A/R} = \mathfrak{p}^{fn}$. In addition,

$$|R/\mathrm{disc}| = |R/\mathfrak{p}|^{fn} = |A/\mathfrak{P}|^n = |A/\delta_{A/R}|$$

We complete the proof. ■

With the same hypothesis in 1.3.1, let G_n be the kernel of $N(A) \to N(A_n)$. Following the argument above, it suffices to consider $(G_n \otimes_{\mathcal{O}_K} \mathcal{O}_v)_f$, which will be denoted by $G^f_{n,v}$. Obviously, there are inclusions $i_{n,v} : G_{n,v} \to G_{n+1,v}$. We want to use the result from Tate. But, it is not true that $G_{n,v}$ forms an ℓ-adic group over R. Fortunately, we have the following lemme which says that it will eventually be an ℓ-divisible group.

Lemma 1.3.8. For a large N, the systems

$$H_{n,v} = G^f_{N+n,v}/G^f_{N,v}$$

form an ℓ-divisible groups over $\mathcal{O}_v$ for all places $v|\ell$.

Proof. We drop the index v.

Note that there are natural morphisms

$$\ell : A/B_{n+1} \to A/B_n$$

which induce

$$\ell : H_{n+1} \to H_n$$

The system $\{H_n, i_n\}$ is an ℓ-divisible group if it has the right order in the definition and the induced maps

$$\ell : H_{n+1}/H_n \to H_n/H_{n-1}$$

is an isomorphism.

The order can be checked on the generic fiber. Since $G_n^f = G \cap N(A)[\ell^n]_f$, the generic fiber of $\{G_n^f\}$ is just $B \cap A[\ell^\infty]_f$, which is obviously an ℓ-divisible. Hence the order is suitable.

The natural maps $\ell : H_{n+1}/H_n \to H_n/H_{n-1}$ are surjective, and hence will be eventually isomorphism by considering the order. ■

Tate's result says that $\mathrm{disc}(G_{n,v}^0) = \ell^{d_v n \ell^{h_v n}} = \ell^{d_v n |G_{n,v}^0|}$, where $d_v = \dim \lim_{\to} \{G_{n,v}^0\}$.

Thus by computing we find that $h(A) = h(A_n)$ holds if and only if

$$\frac{1}{2} h[K : \mathbb{Q}] = \sum_{v|\ell} [K_v : \mathbb{Q}_\ell] d_v$$

where h is the height of B/K.

We consider the absolute Galois group $G_\mathbb{Q}$ and the $G_\mathbb{Q}$-modules $W = V_\ell(B) \subseteq V_\ell(A)$. Define $V = \mathrm{Ind}_{G_K}^{G_\mathbb{Q}}(W)$. This is an $h[K : \mathbb{Q}]$-dimensional representation of $G_\mathbb{Q}$.

$$G_{K_v} \to G_K \circlearrowright V_\ell(G) = W$$

$$G_{\mathbb{Q}_\ell} \to G_\mathbb{Q} \circlearrowright \mathrm{Ind}_{G_K}^{G_\mathbb{Q}}(W) = V$$

Note that V is of dimension $[K : \mathbb{Q}]h$.

Lemma 1.3.9. $\mathrm{Res}_{G_{\mathbb{Q}_\ell}} V = \bigoplus_{v|\ell} \mathrm{Ind}_{G_{K_v}}^{G_{\mathbb{Q}_\ell}} \left(\mathrm{Res}_{G_{K_v}} W\right)$.

Proof. This is a result in the general representation theory.

Consider the coset S

$$G_{\mathbb{Q}_\ell} \backslash G_\mathbb{Q} / G_K$$

The right part $G_\mathbb{Q}/G_K$ can be identified as the inclusions $K \hookrightarrow \bar{\mathbb{Q}}$. Fix a $j : \bar{\mathbb{Q}} \to \overline{\mathbb{Q}_\ell}$. Then it can be identified as $K \hookrightarrow \overline{\mathbb{Q}_\ell}$. Through the embeddings $K \hookrightarrow K_v$, it is divided to parts $K_v \hookrightarrow \overline{\mathbb{Q}_\ell}$ for any $v|\ell$. Then S can be identified as the set of v such that $v|\ell$.

By the Res-Ind formular

$$\mathrm{Res}_{G_{\mathbb{Q}_\ell}}(V) \cong \bigoplus_{s \in S} \mathrm{Ind}_{sG_K s^{-1} \cap G_{\mathbb{Q}_\ell}}^{G_{\mathbb{Q}_\ell}} (W_s) \cong \bigoplus_{v|\ell} \mathrm{Ind}_{G_{K_v}}^{G_{\mathbb{Q}_\ell}} (\mathrm{Res}_{G_{K_v}} W)$$

■

Then we have

$$\mathrm{Res}_{G_{\mathbb{Q}_\ell}} \det(V) = \bigotimes_{v|\ell} \det(\mathrm{Ind}_{GK_v}^{G_{\mathbb{Q}_\ell}} \mathrm{Res}_{G_{K_v}}(W))$$

Theorem 1.3.10. The representation $\det\left(\mathrm{Res}_{G_{K_v}}(W)\right)$ for any $v|\ell$ is Hodge-Tate of weight d_v.

Proof. Basic property in p-adic Hodge theory. ■

Recall the Hodge-Tate decomposition of p-divisible groups.

Theorem 1.3.11. Let G be an ℓ-divisible group over $\mathcal{O}_{K_v}$. Then $T_\ell(G)$ has Hodge-Tate weights 0 and 1 with the multiplicities given by

$$h_0 = d,\ h_1 = d'$$

where $d = \dim(G)$ and $d' = \dim(G^D)$.

Let $t(V) = \sum ih_i$ for Hodge-Tate representation V with weight h_i. Then

$$\begin{aligned} t(\mathrm{Res}_{G_{\mathbb{Q}_\ell}} \det(V)) &= \sum_{v|\ell} t\left(\det(\mathrm{Ind}_{GK_v}^{G_{\mathbb{Q}_\ell}} \mathrm{Res}_{G_{K_v}}(W))\right) \\ &= \sum_{v|\ell} [K_v : \mathbb{Q}_\ell] t(\mathrm{Res}_{G_{K_v}}(W)) \\ &= \sum_{v|\ell} [K_v : \mathbb{Q}_\ell] d_v \end{aligned}$$

Proposition 1.3.12. Let $V' = \mathrm{Res}_{G_{\mathbb{Q}_\ell}} \det(V)$. The unique weight of V' is equal to $\frac{1}{2}hm$.

Proof. By 1.3.10, V' has weight $d = \dim B$.

By this note Prop 1.1.1 and Ex 2.2.10, every character over $G_{\mathbb{Q}_\ell}$ can be written as $\mu_\lambda \cdot \mu^a w^b$, and if it is Hodge-Tate, then a is the weight. Let Frob_p be an Frobenius element for an unramified place p. Then Frob_p is sent to $\lambda \cdot p^a \cdot w^b$. Since $w^{p-1} = 1$, it is a root of unity. The Weil conjecture for Abelian varieties implies that the eigenvalues of Frob_p has absolute value $p^{1/2}$, hence, by taking the det, Frob_p is sent to a number with absolute value $p^{h[K:\mathbb{Q}]/2}$. Then

$$\frac{h[K:\mathbb{Q}]}{2} = a = d$$

■

1.3.3 Proof for 1.3.2

I. If A has a polarization with semistable reduction everywhere.

The proof is same with 1.1.7.

Let $U = W \cap T_\ell A$. Then $\{U/\ell^n U\}$ forms an ℓ-divisible subgroup $G \subseteq A[\ell^\infty]$. Let $A_n = A/G[\ell^n]$. Then we have natural isogeny $\pi_n : A \to A_n$. Also, like the proof in 1.1.7, there are morphisms $f_n : A_n \to A$ sending $T_\ell A_n$ to $W_n = U + \ell^n T_\ell A$. The relation for π_n and f_n is given by $\pi_n \circ f_n = [\ell^n]$.

In order to use [H3] and 1.3.1 to conclude that there is an isomorphic sequence

$$A_{n_1} \xrightarrow{\sim} A_{n_i}$$

for $n_1 < n_2 < \cdots$, we must equipped A_n with a polarization of degree d^2. To do this, we may first assume that W is a maximal isotropic subspace for β_θ, which is the Weil pairing corresponding to the polarization $\theta : A \to A^D$. Consider the pullback $f_n^*\theta$, this is a polarization, but with an unexpected degree. We now use the isotropicity of W. Consider

$$\beta_{f_n^*\theta} : T_\ell(A_n) \times T_\ell(A_n) \to \mathbb{Z}_\ell(1) = \varprojlim \mu_{\ell^m}$$

This is defined by

$$\beta_{f_n^*\theta}(x, y) = \beta_\theta(f_n x, f_n y)$$

Hence, the image of $\beta_{f_n^*\theta}$ is a subset of $\beta_\theta(W_n, W_n)$, which is equal to $\beta_\theta(\ell^n T_\ell A, W_n)+\beta_\theta(W, \ell^n T_\ell W_n)$ by the bilinearity. Thus, $\mathrm{Im}(\beta_{f^*\theta}) \subseteq \ell^n \mathbb{Z}_\ell(1)$. Then

$$e^n_{f_n^*\theta} : A_n[\ell^n] \times A_n[\ell^n] \to \mu_{\ell^n}$$

is trivial. Since the corresponding pairing

$$e : A_n[\ell^n] \times A_n^D[\ell^n] \to \mu_{\ell^n}$$

is non-degenerate, for any $y \in A_n[\ell^n]$, $f_n^*\theta$ maps y to $0 \in A_n^D$. Hence, $f_n^*\theta$ factors as $g \circ [n]_X$, where g is a polarization with degree d^2. Thus we equip A_n with a polarization with degree d^2.

Define $u_i : A \to A_{n_1} \xrightarrow{\sim} A_{n_i} \to A$, and let u be the limit, we obtain what we want.

For general $W \subseteq V_\ell X$, let $\alpha \in \mathbb{Q}_\ell$ be the square root of -1. Consider

$$W' = \{(x, \alpha x) | x \in W\} + \{(y, -\alpha y) | y \in W^D\} \subseteq V_\ell(A^2)$$

This is a $2g$-dimensional isotropic subspace of $\theta \times \theta$ obviously. Let $u \in \mathbb{Q}_\ell \otimes \mathrm{End}(A^2)$ be the endomorphism such that $u(V_\ell A^2) = W'$. Then the image of

$$(p_1 - \alpha p_2) \circ u : V_\ell(A^2) \to V_\ell(A^2) \to V_\ell A$$

is $2W = W$, where p_i is the projection. By composing the natural maps

$$i_1, i_2 : V_\ell A \to V_\ell(A) \oplus V_\ell(A) = V_\ell(A^2)$$

we obtain two elements $u_1, u_2 \in \mathbb{Q}_\ell \otimes \mathrm{End}(A)$ such that $(u_1 + u_2)(V_\ell A) = W$. The set of elements u such that $uV_\ell A \subseteq W$ forms a right ideal of $\mathbb{Q}_\ell \otimes \mathrm{End}(A)$. This ideal is principal generated by an idempotent element u'. This is what we want.

II. If A does not have semistable reduction.

We will show that if 1.3.2 holds for $A \times_K L$, then it holds for A, where L is a finite extension of K. Then we can use 1.1.13.

Since $W \subseteq V_\ell A$ is G_K-invariant, then there exists $u \in \mathrm{End}_L(A_L) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell$ such that $u(V_\ell(A)) = W$. Let

$$u' = \frac{1}{[L : K]} \sum_{\sigma \in G_K/G_L} \sigma(u) \in \mathrm{End}(A) \otimes \mathbb{Q}_\ell$$

Then $u'(V_\ell A) = W$.

III. If A does not have polarizations.

One method is to prove that [H3] holds without assuming the polarized conditions.

We can obtain this result by showing $h(A) = h(A^D)$ for A with semistable reduction everywhere. After this, $h((A \times A^D)^4) = 8h(A)$, and then [H3] holds for general A.

Another method is that we can just prove 1.3.2 for polarized Abelian varieties. By Zarhin's trick $C = A^4 \times (A^D)^4$ is polarized, and then C and C^2 both satisfy 1.3.2. Then for C we can show the result 1.1.8.

For general Abelian variety A, the semi-simplicity follows immediately from $V_\ell(A)$ is a sub-representation of $V_\ell(C)$. Also note that 1.1.6 shows a bi-product that if

$$\mathbb{Q}_\ell \otimes \mathrm{End}(C) \to \mathrm{End}(V_\ell C)^{\mathrm{Gal}(k_s/k)}$$

holds for $C = A^4 \times (A^D)^4$, then it holds for A by taking $B = A^3 \times (A^D)^4$. We complete the proof.

Corollary 1.3.13. For any Abelian varieties A_1, A_2 over K, $A_1 \sim_K A_2$ if and only if

$$T_\ell(A_1) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \cong T_\ell(A_2) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$$

as G_K-modules for some ℓ, or equivalently, for any $g \in G$, the traces are same

$$\mathrm{tr}(g \circlearrowright V_\ell(A_1)) = \mathrm{tr}(g \circlearrowright V_\ell(A_2))$$

Proof. If A_1, A_2 are isogeny the result is obvious.

Conversely, suppose this Galois-equivalent isomorphism is given by

$$h : V_\ell A_1 \xrightarrow{\sim} V_\ell A_2$$

First, this isomorphism gives that $\dim(A_1) = \dim(A_2)$. Since they are finitely dimensional $\mathbb{Q}_\ell$-vector spaces, we may find an integer n such that $\ell^n h$ maps the $\mathbb{Z}_\ell$-lattice $T_\ell A_1$ into $T_\ell A_2$. We may assume that $n = 0$. Consider the set

$$U = \{h \in \mathrm{Hom}(T_\ell A_1, T_\ell A_2)^{G_K} | h \text{ is injective}\}$$

It is nonempty and open in $\mathrm{Hom}(T_\ell A_1, T_\ell A_2)^{G_K}$ since it is given by $\det(h) \neq 0$. Note that

$$\mathrm{Hom}(A_1, A_2) \subseteq \mathbb{Z}_\ell \otimes \mathrm{Hom}(A_1, A_2) \cong \mathrm{Hom}(T_\ell A_1, T_\ell A_2)^{G_K}$$

is dense, it intersects with U, and then there exists $f \in \mathrm{Hom}(A_1, A_2)$ such that $T_\ell f$ is in U, i.e., is injective. Note that f is of finite type. Consider the kernel $B = \mathrm{Ker}(f)$, it is a closed subgroup scheme of A_1, the reduced closed subscheme B^0_{red} is a sub-Abelian variety of A_1. This Abelian variety is 0 since its Tate module is 0. This means $\mathrm{Ker}(f)$ is finite. Then f is an isogeny. ■

1.4 Shafarevich conjecture

In this section we prove [Sha2].

We first prove an "isogenous version" without the "polarized condition".

Theorem 1.4.1. There are only finitely many isogenous classes of Abelian varieties over K of dimension g with good reduction outside S.

To prove this, by 1.3.13 and [Ta1], it suffices to prove the following finiteness theorem for semi-simple representations.

Theorem 1.4.2 (Finiteness for semi-simple representations)**.** Let $d = 2g$ be a positive integer. For any $v \notin S$, let $Z_v \subseteq \mathbb{Q}_\ell$ be a finite set. Then up to isomorphism, there exists only finite d-dimensional semi-simple representations of G_K over $\mathbb{Q}_\ell$, unramified outside S, and such that for $v \notin S$ the trace of Frob_v lies in Z_v.

Note that if A has good reduciton at v, let $\mathcal{A}_v$ be the model over $\mathcal{O}_{K,v}$, then Neron-Ogg-Shafarevich criterion implies that $T_\ell(A)$ is isomorphic to $T_\ell(\mathcal{A}_v \times_{\mathcal{O}_{K,v}} \mathbb{F}_v)$ as G_K-representations, which can be found in this paper about the criterion. If this theorem holds true, since the Weil conjecture holds true for Abelian varieties (see van der Geer's book), the characteristic polynomial of Frob_v on $T_\ell(\mathcal{A}_v \times_{\mathcal{O}_{K,v}} \mathbb{F}_v)$ has coefficients in $\mathbb{Z}$ and its roots are all Weil-numbers. Thus the trace of Frob_v, which is the coefficient of t^1, is bounded. Hence Z_v can be chosen.

Now we prove the finiteness theorem for the semi-simple representations.

Proof. The main idea is to construct a finite set of places S', such that if $\mathrm{tr}\rho(\mathrm{Frob}_v) = \mathrm{tr}\rho'(\mathrm{Frob}_v)$ for all $v \in S'$, then ρ and ρ' are isomorphic as G_K-representations.

For a representation $\rho : G_K \to \mathrm{Aut}(V)$, where V is a $\mathbb{Q}_\ell$-vector space with dimension d, choose a G_K-stable $\mathbb{Z}_\ell$-lattice T.

Let M be the sub-$\mathbb{Z}_\ell$-algebra of $\mathrm{End}_{\mathbb{Z}_\ell}(T) \times \mathrm{End}_{\mathbb{Z}_\ell}(T')$ spanned by the image of G_K. M is of rank $\leq 2d^2$.

We then have a natural homomorphism

$$G_K \to M^* \to (M/\ell M)^*$$

By Nakayama's lemma, any set of generators of $M/\ell M$ generates M over $\mathbb{Z}_\ell$.

As a $\mathbb{F}_\ell$-algebra, we have $|(M/\ell M)| \leq \ell^{\dim R}$. The representation $G_K \to (M/\ell M)^*$ must factor through $G_K/H \hookrightarrow (M/\ell M)^\times$ where H is a closed subgroup, and then $G_K/H = \mathrm{Gal}(K'/K)$ for some extension K' with degree $\leq \ell^{2d^2}$ and is unramified outside S and ℓ.

Now we construct S'. Let K_1 be the composite of all field extensions K'/K which satisfy $[K' : K] \leq \ell^{2d^2}$ and is unramified outside $S \cup \{\ell\}$. A consequence of Minkowski's theorem says K_1/K is finite. By Chebotarev's result, we can choose finitely many Frobenius elements $\mathrm{Frob}_{v_1}, \cdots, \mathrm{Frob}_{v_r}$ for $v_1, \cdots, v_r \notin S \cup \{\ell\}$, such that they represent all the conjugacy classes in $\mathrm{Gal}(K_1/K)$. Let S' be the set $\{v_1, \cdots, v_r\}$. This set does not depend on ρ and ρ'.

Note that by the construction, $G_K \to (M/\ell M)^\times$ factors through $\mathrm{Gal}(K_1/K)$, and the set $\{\rho(\mathrm{Frob}_v) | v \in S'\}$ covers the image of G_K in $(M/\ell M)^*$.

If $\mathrm{tr}(\rho(\mathrm{Frob}_v)) = \mathrm{tr}(\rho'(\mathrm{Frob}_v))$ for all $v \in S'$, then for all g,

$$\mathrm{tr}(\rho(g)) \equiv \mathrm{tr}(\rho'(g)) \bmod \ell$$

Thus, let $p_1 : M \to \mathrm{End}_{\mathbb{Z}_\ell}(T)$ be the projection, and define p_2 similarly, then $\mathrm{tr}(p_1(m)) = \mathrm{tr}(p_2(m))$ for all $m \in M$. Choose a set of generators of $M/\ell M$ over $\mathbb{F}_\ell$, and choose a lift in M, Nakayama's lemma tells me they generates M as $\mathbb{Z}_\ell$-module. Hence for any $m \in M$,

$$\mathrm{tr}(p_1(m)) = \mathrm{tr}(p_2(m))$$

Then for any $g \in G_K$,

$$\mathrm{tr}(\rho(g)) = \mathrm{tr}(\rho'(g))$$

This means ρ is isomorphic to ρ'.

Thus, the number of semi-simple representations of G_K satisfying the theorem statements is not more than $\prod_{v \in S'} |Z_v|$. ■

Back to the proof of [Sha2].

We first do a reduction: by 1.1.3 and 1.1.4, it suffices to prove for the case $d = 1$, i.e., for principally polarized Abelian varieties. From this, we need not assume any polarized condition in the original statement.

By 1.4.1, it suffices to show that every isogeny class has finitely many Abelian varieties up to isomorphism.

By the last part of 1.2.20 (or see Poonen's book section 4.5), we know that for an Abelian variety X over a field K with a finite Galois extension L/K, there are finite Abelian varieties B over K up to isomorphism such that $B \times_K L \cong A \times_K L$. Hence, it is convenient that we change the base field K to a bigger one such that A has semistable reduction.

In a word, it remains to show the following theorem.

Theorem 1.4.3. Fix an g-dimensional Abelian variety A over K with a principal polarization λ. Assume that A has good reduction outside S and has semistable reduction everywhere. Then there are finitely many principally polarized Abelian varieties (B, λ') over K such that there exists an isogeny $\phi : (B, \lambda') \to (A, \lambda)$.

Now we prove this theorem.

We can view ϕ as an isogeny $\phi : N(B)^0 \to N(A)^0$ between the connected components of their Neron models. Let G be its kernel. We will reuse the height formula 1.3.3.

First we can control the degree of ϕ.

Lemma 1.4.4. Suppose B is isogenous to A. Further assume that there are isomorphisms

$$\phi_\ell : T_\ell B \cong T_\ell A$$

for all $\ell \in N$ as $\mathbb{Z}_\ell[G_K]$-modules. Let N be a finite set of prime numbers. Then there exists an isogeny

$$\phi : B \to A$$

of degree prime to all elements in N. If ϕ satisfies this property, we shall denote this by $(\deg(\phi), N) = 1$.

Proof. Note that

$$\mathrm{Hom}(B,A)\otimes\left(\bigoplus_{\ell\in N}\mathbb{Z}_\ell\right)\cong\bigoplus_{\ell\in N}\mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell B,T_\ell A)^{G_K}$$

Let $\psi=(\psi_\ell)_{\ell\in N}=\sum f_i\otimes(a_{\ell,i})_{\ell\in N}$ be the element in the left hand corresponding to $(\phi_\ell)_{\ell\in N}$ in the right hand.

Choose $b_i\in\mathbb{Z}$ such that $b_i\equiv a_\ell(\mathrm{mod}\ b)$, and let $\varphi=\sum f_ib_i$. Then the ℓ-coordinate of $\psi-(\varphi)_{\ell\in N}$ is a multiple of ℓ. Write $\psi-(\varphi)_{\ell\in N}=(\varphi_\ell)_{\ell\in N}$. Note that T_ℓ sends ψ_ℓ to ϕ_ℓ, the kernel of ψ_ℓ and then of φ is finite. Then φ is an isogeny.

It remains to show that $(\deg\varphi,N)=1$. Suppose $\ell\in N$ satisfies $\ell|\deg\varphi$. Then $B[\ell]\cap\mathrm{Ker}(\varphi)$ has an element x other than 0. Hence

$$\psi_\ell(x)=\varphi(x)+\varphi_\ell(x)=0$$

and therefore

$$\phi_\ell(x)=T_\ell(\psi_\ell)(x)=0$$

Since ϕ_ℓ is an isomorphism, $x=0$, a contradiction. ■

Lemma 1.4.5. There are only finitely many isomorphism classes of $\mathbb{Z}_\ell[G_K]$-invariant lattices in $T_\ell(A)\otimes_{\mathbb{Z}_\ell}\mathbb{Q}_\ell$.

Proof. This is Jordan-Zassenhaus theorem. ■

Proposition 1.4.6. There exist an integer $n\geq1$ depending only on N and $A_1,\cdots,A_n$ which are isogeous to A, such that for any B isogenous to A, there exists $i=i(B)$ such that there is an isogeny

$$\phi:B\to A_i$$

with $(\deg(\phi),N)=1$.

Proof. This proposition follows from the above two lemmas immediately. ■

Now we come to the main step.

Theorem 1.4.7. Let A be a principally polarized Abelian variety over K with semi-stable reduction. Then there exists a finite set N of prime numbers, depending on A, such that, for any isogeny $\varphi:B\to A$ with $(\deg(\varphi),N)=1$, then

$$h(B)=h(A)$$

If this theorem holds, then

$$\{h(B)|\ B\text{ is isogenous to }A\}=\{h(A_1),\cdots,h(A_n)\}$$

Therefore 1.4.3 holds true.

Proof. Choose two different prime number p and ℓ such that $K/\mathbb{Q}$ is unramified at p and ℓ, in addition for each place $v|p\ell$ the Abelian variety A has good reduction at v.

For each $1 \leq h \leq 2g \cdot [K:\mathbb{Q}]$, we define the polynomials

$$P_h(T) = \det\left(T \cdot \mathrm{id} - \mathrm{Frob}_p | \bigwedge^h \mathrm{Ind}_{G_K}^{G_\mathbb{Q}} T_\ell(A)\right)$$

Indeed, the representation $\mathrm{Ind}_{G_K}^{G_\mathbb{Q}} T_\ell B$ is the Tate module of the Weil restriction $\mathrm{Res}_{K/\mathbb{Q}} B$. Then the polynomials are exactly the character polynomials of Frob_p on an Abelian variety over $\mathbb{Q}$. Then every P_h has integral coefficients and has roots with absolute values equal to $p^{h/2}$. Also, these polynomials do not depend on the prime ℓ.

Define N as follows: A prime number p' is in N if one of the following conditions is satisfied

(i) $p' \in \{2, p\}$.

(ii) $K/\mathbb{Q}$ is ramified at p'.

(iii) there exists some places $v|p'$ such that the Abelian variety A has bad reduction at v.

(iv) for $h \in [0, 2g[K:\mathbb{Q}]]$ and $j \in [0, g[K:\mathbb{Q}]]$ such that $j \neq \dfrac{h}{2}$ the prime p' divides one of the numbers $P_h(\pm p^j)$.

Note that N does not depend on ℓ. We may choose ℓ in the following sense.

Let $\phi : B \to A$ be an isogeny such that $(\deg \phi, N) = 1$. By factorizing ϕ we may assume that $\deg \phi = \ell^n$. Let $\mathrm{Ker}(\phi) = G$, then $\ell^n \cdot G = 0$.

We can construct a new isogeny

$$B \to B/\mathrm{Ker}(G[\ell]) \to B/\mathrm{Ker}(G[\ell^2]) \to \cdots \to B/\mathrm{Ker}(G[\ell^n]) \cong A$$

where $B/G[\ell^i]$ denote the categorical quotient for the action induced by $G[\ell^i] \to B$. Hence we may assume that $G[\ell] = G$, i.e., ℓ kills G.

Let χ_ℓ be the ℓ-adic cyclotomic character.

Let V be the $\mathbb{F}_\ell$-representation $T_\ell(B)/\ell T_\ell(B)$. Let W be the representation $\mathrm{Ind}_{G_K}^{G_\mathbb{Q}} V$. Note that $G \subseteq V$. Let $U = \mathrm{Ind}_{G_K}^{G_\mathbb{Q}} G$. Consider the representation $\chi : \det(G) \to (\mathbb{Z}/\ell\mathbb{Z})^*$ and $\chi_0 : \det(U) \to (\mathbb{Z}/\ell\mathbb{Z})^*$.

The semi-stable condition implies I_v acts on G as unipotent action. Hence $\det(G)$ is trivial. Hence, $\det(g)$ acts as $\epsilon : G_\mathbb{Q} \to G_\mathbb{Q}/G_K \to \{\pm 1\}$, which is the sign character. Then $\chi_0 = \chi\epsilon$. This is unramified outside ℓ. By the Kronecker-Weber theorem, χ must be a power of the ℓ-adic cyclotomic character. Say χ_ℓ^d.

Then by mod ℓ, $\chi_0(\mathrm{Frob}_p) = \pm p^d$. But it is a zero of P_h for $h = n[K:\mathbb{Q}]$. Then $\ell | P_h(\pm p^d)$. Then $d = \dfrac{[n \cdot [K:\mathbb{Q}]]}{2}$.

A theory of Raynaud states that $|s^*(\Omega^1_{\mathcal{G}/\mathcal{O}_K})| = \ell^d$. Then

$$h(A) - h(B) = 0$$

■

1.5 Proof of [Mor]

I gave up, see Milne's note for details. Maybe someday I will resume this note.