Ernst Kani

ICAWAG' 93

AIN SHAMS UNIVERSITY
FACULTY OF SCIENCE
DEPARTMENT OF MATHEMATICS
ABBASSIA, CAIRO, EGYPT

Heights on Abelian Varieties and the Theorem of Mordell-Weil

§1. Naive Heights

Let K be a number field, $\bar{K}$ its alg. closure

V/K a smooth projective variety over K

$\mathcal{H}(V) = \{h : V(\bar{K}) \to \mathbb{R}\}$ set of real-valued functions on $V(\bar{K})$
($\bar{K}$-rat'l pts of V)

$\bar{\mathcal{H}}(V) = \mathcal{H}(V)/$bounded functions

$B(h, L, c) := \{P \in V(L) : h(P) \leq c\}$, for $h \in \mathcal{H}(V)$, $K \subset L \subset \bar{K}$, $c \in \mathbb{R}$.

Recall (cf. Jannsen's talk): there is a homo. (of ab. groups)

$$h_V : \mathrm{Pic}(V) \to \bar{\mathcal{H}}(V)$$
$$\mathcal{L} \mapsto h_{\mathcal{L}} = h_{V,\mathcal{L}}$$ note: set of functions

such that:

1) for any morphism $f : V \to W$ and $\mathcal{L} \in \mathrm{Pic}(W)$ we have
$$h_{f^*\mathcal{L}} = h_{\mathcal{L}} \circ f ;$$

2) for $V = \mathbb{P}^n_K$, $\mathcal{L} = \mathcal{O}(1)$ we have
$$h_{\mathcal{L}} = \text{class containing the naive height on } \mathbb{P}^n_K$$

From these properties follows:

3) (Finiteness property) $\mathcal{L}$ ample $\Rightarrow$ for each $h \in h_{\mathcal{L}}$ and L/K finite we have that $\# B(h, L, c) < \infty$, $\forall c \in \mathbb{R}$.

ICAWAG' 93

AIN SHAMS UNIVERSITY
FACULTY OF SCIENCE
DEPARTMENT OF MATHEMATICS
ABBASSIA, CAIRO, EGYPT

§2. Abelian varieties

Def. An abelian variety A/K is a proj. (smooth) algebraic group variety.

Thus: $\exists$ morphisms $m : A \times A \to A$ (multiplication)
$i : A \to A$ (inverse)
$0 \in A(K)$ (identity)

satisfying the group axioms.

Ex. 1) $A = E$ elliptic curve (mult: chord/tangent method)

2) $A = J_C$, Jacobian of a curve C

3) $(K=\mathbb{C})$ a torus $\mathbb{C}^g/\Lambda \hookrightarrow \mathbb{P}^N_{\mathbb{C}}$.

Basic facts: 1) Each ab. var. is commutative
$A(L)$ is a comm. gp.

2) $f : A_1 \to A_2$ morph of ab. var's $\Rightarrow f = h + f(0)$ where h is a homomorphism; moreover $h(A_1)$ is an ab. subvariety of A_2.

3) Each ab. var. is a quotient of Jacobians of curves.

4) $A(\bar{K})$ is divisible
$A[n](\bar{K})$ is finite

ICAWAG' 93

AIN SHAMS UNIVERSITY
FACULTY OF SCIENCE
DEPARTMENT OF MATHEMATICS
ABBASSIA, CAIRO, EGYPT

§3. Statement of the Theorem

Theorem 1. (Tate) Let A/K be an ab. var. Then there is a unique lift

$$\begin{tikzcd} \mathrm{Pic}(A) \arrow[r, "\hat{h}_A"] \arrow[dr, "h_A"'] & \mathcal{H}(A) \arrow[d] \\ & \tilde{\mathcal{H}}(A) \end{tikzcd} \qquad (\mathcal{L} \mapsto \hat{h}_{A,\mathcal{L}}$$

of h_A (i.e. $\hat{h}_{\mathcal{L}} \in h_{\mathcal{L}}$) such that for each $\mathcal{L} \in \mathrm{Pic}(A)$ we have

$$\hat{h}_{A,\mathcal{L}}(P) = \langle P, P \rangle_{\mathcal{L}} + \langle P \rangle_{\mathcal{L}}$$

where $\langle \, , \, \rangle_{\mathcal{L}} : A(\bar{K}) \times A(\bar{K}) \to \mathbb{R}$ is a symm. bi-additive map,
$\langle \, \rangle_{\mathcal{L}} : A(\bar{K}) \to \mathbb{R}$ is a homo.
} uniquely determined by $\hat{h}_{\mathcal{L}}$

Cor. 1) $\hat{h}_A$ is a homomorphism: $\hat{h}_{A,\mathcal{L}\otimes\mathcal{L}'} = \hat{h}_{A,\mathcal{L}} + \hat{h}_{A,\mathcal{L}'}$

2) If $f : A \to B$ is a homo. of ab. var's, then
$$\hat{h}_{f^*\mathcal{L}} = \hat{h}_{\mathcal{L}} \circ f$$

3) If $i^*\mathcal{L} \simeq \mathcal{L}$ is symmetric then $\langle \, \rangle_{\mathcal{L}} = 0$, i.e. $\hat{h}_{\mathcal{L}}$ is a quadratic form.

4) If $\mathcal{L}$ is ample and symmetric then
$$\hat{h}_{\mathcal{L}}(P) \geq 0 \quad \text{and} \quad \hat{h}_{\mathcal{L}}(P) = 0 \iff P \in A(\bar{K})_{tor}.$$
and $\{P \in A(L) : \hat{h}_{\mathcal{L}}(P) \leq C\}$ is finite.

ICAWAG' 93

AIN SHAMS UNIVERSITY
FACULTY OF SCIENCE
DEPARTMENT OF MATHEMATICS
ABBASSIA, CAIRO, EGYPT

§4. Quadratic functions on ab. groups

Let $\mathcal{A}$, $\mathcal{B}$ be (abstract) ab. groups

$f : \mathcal{A} \to \mathcal{B}$ a map.

Define

$\Delta f : \mathcal{A} \times \mathcal{A} \to \mathcal{B}$ ("1st difference")

$$\Delta f(x,y) = f(x+y) - f(x) - f(y)$$

and $\Delta_2 f : \mathcal{A} \times \mathcal{A} \times \mathcal{A} \to \mathcal{B}$

$$\Delta_2 f(x,y,z) = f(x+y+z) - f(x+y) - f(x+z) - f(y+z) + f(x) + f(y) + f(z)$$

Def. f is a quadratic (resp. linear) function if $\Delta_2 f \equiv 0$ (resp. if $\Delta f \equiv 0$)

Ex. 1) f linear $\Leftrightarrow$ f

2) $f = q(x,x) + l(x)$ is quadratic if $q(x,y) : \mathcal{A} \times \mathcal{A} \to \mathcal{B}$ is symm. bi-additive and l is linear.

Lemma 1: If $\mathcal{B} = \mathbb{R}$, then every quadr. function $f : \mathcal{A} \to \mathbb{R}$ has a unique decomposition

$$f = q_f + l$$

where l is linear and q_f is a quadratic form, i.e.

ICAWAG' 93

AIN SHAMS UNIVERSITY
FACULTY OF SCIENCE
DEPARTMENT OF MATHEMATICS
ABBASSIA, CAIRO, EGYPT

$q_f(x) = b_f(x,x)$ where b_f is symm. bi-additive.

Pf. Easy.

Def. A function $f : A \to \mathbb{R}$ is quasi-quadratic if $\Delta_2 f$ is bounded (on $A \times A \times A$).

Lemma 2 (Tak). If f is quasi-quadratic then $\exists !\ \hat{f} : A \to \mathbb{R}$ such that 1) $\hat{f}$ is quadratic

2) $f = f + O(1)$.

Pf. Uniqueness is clear, for a bounded quadratic function is constant.

Existence: check that

$$b(x,y) = \frac{1}{2} \lim_{n\to\infty} \Delta f(2^n x, 2^n y)/4^n$$

converges and is biadditive. Similarly,

$$l(x) = \lim_{n\to\infty} [f(2^n x) - q(2^n x)]/2^n$$

converges and is linear, where $q(x) = \frac{1}{2} b(x,x)$. Finally, one checks that

$$f = q + l + O(1)$$

and so the assertion follows.

ICAWAG' 93

AIN SHAMS UNIVERSITY
FACULTY OF SCIENCE
DEPARTMENT OF MATHEMATICS
ABBASSIA, CAIRO, EGYPT

§5. The Theorem of the Cube

This is:

Theorem 2. Let A be an abelian variety and V/k be any variety. Then for any $\mathcal{L} \in \mathrm{Pic}(A)$ the function

(geom. integral)

$$\begin{aligned} {}^*\mathcal{L} : \mathrm{Mor}(V, A) &\longrightarrow \mathrm{Pic}(V) \\ f &\longmapsto f^*\mathcal{L} \end{aligned}$$

is quadratic.

Rmk. By definition this means: for $f, g, h : V \to A$

$$\Delta_2({}^*\mathcal{L})(f, g, h) \simeq \mathcal{O}_X$$

$$\parallel$$

$$(f+g+h)^*\mathcal{L} \otimes (f+g)^*\mathcal{L}^{-1} \otimes (f+h)^*\mathcal{L}^{-1} \otimes (g+h)^*\mathcal{L}^{-1} \otimes f^*\mathcal{L} \otimes g^*\mathcal{L} \otimes h^*\mathcal{L}$$

Pf. [Mu], p.58.

Basic technique: base change & cohomology

ICAWAG' 93

AIN SHAMS UNIVERSITY
FACULTY OF SCIENCE
DEPARTMENT OF MATHEMATICS
ABBASSIA, CAIRO, EGYPT

§6. Proof of Theorem 1:

By Lemma 2 (and Lemma 1) it is enough to show that $h_{\mathcal{L}}$ is quasi-quadratic.

For this, let $p_i : A^3 \to A$ denote the i^{th} projection.

$$h_{p_i^*\mathcal{L}} = h_{\mathcal{L}} \circ p_i + O(1) \qquad \text{(as functions on } A(K)^3)$$

$$h_{(p_i+p_j)^*\mathcal{L}} = h_{\mathcal{L}} \circ (p_i+p_j) + O(1) \qquad \text{etc.}$$

we see that

$$\Delta_2 h_{\mathcal{L}} = h_{\Delta_2(*\mathcal{L})(p_1, p_2, p_3)} + O(1).$$

By the theorem of the cube, $\mathcal{D} := \Delta_2(*\mathcal{L})(p_1, p_2, p_3) \simeq \mathcal{O}_{A^3}$, so $h_{\mathcal{D}} = O(1)$, which proves that $h_{\mathcal{L}}$ is quasi-quadratic. //

Pf. of Cor: 1), 2) immediate

3) Write $\hat{h}_{\mathcal{L}} = q + l$. By hypothesis: $\hat{h}_{\mathcal{L}}(-x) \overset{\text{and } 2)}{=} \hat{h}_{i^*\mathcal{L}}(x) = \hat{h}_{\mathcal{L}}(x)$, so $q(x) + l(x) = q(-x) + l(-x) = q(x) - l(x) \Rightarrow l(x) = 0$.

4) Wlog $\mathcal{L}$ very ample, so $\mathcal{L} = \varphi^*\mathcal{O}(1)$ for $\varphi : A \hookrightarrow \mathbb{P}^n$.

Then $h_{\mathcal{L}}$ is bounded below, hence so is the quadr. form $\hat{h}_{\mathcal{L}} = \langle\, , \rangle_{\mathcal{L}}$, $\Rightarrow \hat{h}_{\mathcal{L}} \geq 0$. Moreover, if $\hat{h}_{\mathcal{L}}(P) = 0$ then $\hat{h}_{\mathcal{L}}(nP) = 0 \ \forall n \in \mathbb{Z}$ $\Rightarrow \{nP\}$ finite set (finiteness property) $\Rightarrow P \in A(\bar{K})_{\text{tor}}$.

ICAWAG' 93

AIN SHAMS UNIVERSITY
FACULTY OF SCIENCE
DEPARTMENT OF MATHEMATICS
ABBASSIA, CAIRO, EGYPT

§7. Application: Theorem of Mordell-Weil.

This is:

Theorem 3. Let A/K be an ab. var over a number field K
Then $A(K)$ is a finitely generated group.

Lemma 3: ("Infinite descent"): Suppose $\mathcal{A}$ is an ab. group such that:

1) $\exists m > 1$ s.th $\mathcal{A}/m\mathcal{A}$ is finite
2) $\exists$ quadr. form $h: \mathcal{A} \to \mathbb{R}$ s.th. the set $H_c = \{a \in \mathcal{A} : h(a) \leq c\}$ is finite $\forall c \in \mathbb{R}$.

Then $\mathcal{A}$ is finitely generated.

Proof. Let $a_1, \dots, a_r$ be coset representatives of $\mathcal{A}/m\mathcal{A}$ and put $c = \underset{1 \leq i \leq r}{\mathrm{Max}}\, h(a_i)$.

claim. $\{a_1, \dots, a_r\} \cup H_c$ generates $\mathcal{A}$.

First note that $h \geq 0$, so

(1) $\quad h(x - a_i) = 2h(x) + 2h(a_i) - h(x + a_i) \leq 2h(x) + 2c$.

Moreover,

(2) $\quad h(mx) = m^2 h(x)$.

ICAWAG' 93

AIN SHAMS UNIVERSITY
FACULTY OF SCIENCE
DEPARTMENT OF MATHEMATICS
ABBASSIA, CAIRO, EGYPT

Now let $x \in A$, and write:

$$x = m x_1 + a_{i_1} \qquad x_1 \in A$$
$$x_1 = m x_2 + a_{i_2} \qquad \vdots$$
$$\vdots$$
$$x_n = m x_{n+1} + a_{i_{n+1}}$$
$$\vdots$$

Then $h(x_j) = \frac{1}{m^2} h(m x_j) = \frac{1}{m^2} h(x_{j-1} - a_{i_j}) \le \frac{1}{m^2}[2h(x_{j-1}) + 2c]$

so

$$h(x_n) \le \left(\frac{2}{m^2}\right)^n h(x) + \left(\frac{1}{m^2} + \frac{2}{m^4} + \dots + \frac{2^{n-1}}{m^{2n}}\right) 2c$$

$$\le 2^{-n} h(x) + c$$

For $n \gg 0$, $x_n \in H_{c+1}$ and so the assertion follows.

To apply this, Lemma we need:

<u>Theorem 4</u> (weak Mordell-Weil): $\exists$ finite ext'n $L \supset K$ and int. $m \ge 1$ s.t. $A(L)/m A(L)$ is f.g.

<u>Pf.</u> (sketch) Fix m, choose L s.t. $A[m](\bar{K}) \subset A(L)$ ($\Rightarrow \mu_m \subset L$).

Now use

<u>Fund. Lemma</u>: $L_m = L([m]^{-1} A(L))$ is an ab. ext'n of L of exponent m which is unramified outside a finite set of places of L, hence is finite over L

ICAWAG' 93

AIN SHAMS UNIVERSITY
FACULTY OF SCIENCE
DEPARTMENT OF MATHEMATICS
ABBASSIA, CAIRO, EGYPT

Pf. [Mu], Appendix B

Put $G = Gal(L_m/L)$. Then have injection

$$\varphi : A(L)/mA(L) \hookrightarrow Hom(G, A[m]) \leftarrow \text{finite gp!}$$

given by $\varphi(x)(\sigma) = \sigma y - y$ where $y \in [m]^{-1}(x)$

Note: It is unknown how to characterize the image of φ, so weak MW is not effective (hence also MW is not effective).

Pf. of MW: choose L according to Th. 4', so $A = A(L)$ satisfies (i) of Lemma 3.

Choose an ample divisor $\mathcal{L}_0 \in Pic(A)$ (exists since A proj.)
Then $\mathcal{L} = \mathcal{L}_0 \otimes i^*\mathcal{L}_0$ is symmetric and ample, so $h_{\mathcal{L}}$ satisfies ~~Axiom 2~~.
(ii). Thus by the lemma, $A(L)$ is f.g., hence so is $A(K) \subset A(L)$.

References

[CS] Cornell, Silverman, Arithmetic Geometry. Springer Verlag

[Mu] D. Mumford, Abelian Varieties. Oxford U Press, 1974 (2^{nd} ed'n).