

## 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  $K$

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

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

$B(h, L, c) := \{P \in V(L) : h(P) \leq c\}$ , 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)

$$h_V: \text{Pic}(V) \rightarrow \bar{\mathcal{H}}(V)$$

$$\mathcal{L} \mapsto h_{\mathcal{L}} = h_{V, \mathcal{L}} \quad \leftarrow \text{use: set of functions}$$

such that:

1) for any morphism  $f: V \rightarrow W$  and  $\mathcal{L} \in \text{Pic}(W)$  we have

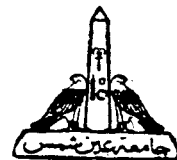
$$h_{f^* \mathcal{L}} = h_{\mathcal{L}} \circ f;$$

2) for  $V = \mathbb{P}_K^n$ ,  $\mathcal{L} = \mathcal{O}(1)$  we have

$$h_{\mathcal{L}} = \text{class containing the naive height on } \mathbb{P}_K^n$$

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

## §2. Abelian varieties

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

Thus:  $\exists$  morphisms  $m: A \times A \rightarrow A$  (multiplication)  
 $i: A \rightarrow A$  (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  $C$   
 $(K = \mathbb{C})$

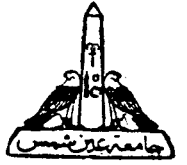
3) a torus  $\mathbb{C}^g / \Lambda \hookrightarrow \mathbb{P}_{\mathbb{C}}^N$

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

2)  $f: A_1 \rightarrow A_2$  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

### § 3. Statement of the Theorem

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

$$\hat{h}_A: \text{Pic}(A) \rightarrow \mathcal{H}(A) \quad (\alpha \mapsto \hat{h}_{A,\alpha})$$

$$\begin{array}{ccc} & \searrow h_A & \downarrow \\ & & \mathcal{H}(A) \end{array}$$

(i.e.  $\hat{h}_\alpha \circ h_\alpha$ )

of  $h_{AV}$  such that for each  $\mathcal{L} \in \text{Pic}(A)$  we have

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

where  $\langle \cdot, \cdot \rangle_{\mathcal{L}}: A(\bar{K}) \times A(\bar{K}) \rightarrow \mathbb{R}$  is a <sup>symm.</sup> bi-additive map, } uniquely determined by  $\hat{h}_{\mathcal{L}}$   
 $\langle \cdot \rangle_{\mathcal{L}}: A(\bar{K}) \rightarrow \mathbb{R}$  is a hemo. }

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  $f: A \rightarrow B$  is a hemo. of ab. var's, then

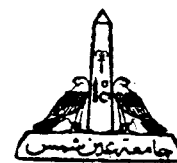
$$\hat{h}_{f^*\mathcal{L}} = \hat{h}_{\mathcal{L}} \circ f$$

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

4) If  $\mathcal{L}$  is ample and symmetric then

$$\hat{h}_{\mathcal{L}}(P) \geq 0 \quad \text{and} \quad \hat{h}_{\mathcal{L}}(P) = 0 \Leftrightarrow P \in A(\bar{K})_{\text{tor.}}$$

and  $\{P \in A(\bar{K}) : \hat{h}_{\mathcal{L}}(P) \leq C\}$  is finite.



### §4. Quadratic functions on ab. groups

Let  $A, B$  be (abstract) ab. groups

$f: A \rightarrow B$  a map.

Define

$$\Delta f: A \times A \rightarrow B \quad (\text{"1st difference"})$$

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

and  $\Delta_2 f: A \times A \times A \rightarrow B$

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

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

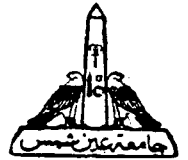
Ex. 1)  $f$  linear  $\Leftrightarrow f$

2)  $f = q(x, x) + l(x)$  is quadratic if  $q(x, y): A \times A \rightarrow B$   
 $\forall$  <sup>symm.</sup> bi-additive and  $l$  is linear.

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

$$f = q_f + l$$

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



ICAWAG' 93

$q_f(x) = b_f(x, x)$  where  $b_f$  is <sup>symm.</sup> bi-additive.

Pf. Easy.

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

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

- 1)  $\hat{f}$  is quadratic
- 2)  $f = \hat{f} + O(1)$ .

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

Existence: check that

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

converges and is biadditive. Similarly,

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

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

## §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  $\mathcal{L} \in \text{Pic}(A)$  the function

(geom. integral)  $\uparrow$

$$\begin{array}{ccc} *_{\mathcal{L}} : \text{Mor}(V, A) & \rightarrow & \text{Pic}(V) \\ f & \mapsto & f^* \mathcal{L} \end{array}$$

is quadratic.

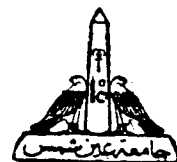
Rmk. By definition this means: for  $f, g, h : V \rightarrow A$

$$\Delta_{\mathcal{L}}^{(f, g, h)} \cong \mathcal{O}_X$$

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

Pf. [Mu], p.58.

Bez technique: base change & cohomology



### §6. Proof of Theorem 1:

By Lemma 2 (and Lemma 1) it is enough to show that  $h_x$  is quasi-quadratic.

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

$$h_{p_i^* x} \approx h_x \circ p_i + O(1) \quad (\text{as functions on } A(K)^3)$$

$$h_{(p_i + p_j)^* x} = h_x \circ (p_i + p_j) + O(1) \quad \text{etc.}$$

we see that

$$\Delta_2 h_x = h_{\Delta_2^*(x)}(p_1, p_2, p_3) + O(1)$$

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

Pf. of Cor: 1), 2) immediate

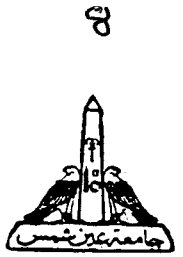
3) Write  $\hat{h}_x = q + l$ . By hypothesis:  $\hat{h}_x(-x) = \hat{h}_{i^* x}(x)$   
 $= \hat{h}_x(x)$ , so  $q(x) + l(x) = q(-x) + l(-x) = q(x) - l(x) \Rightarrow l(x) = 0$ .

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

Then  $h_x$  is bounded below, hence so is the quad. form  $\hat{h}_x = \langle \cdot, \cdot \rangle_x$ ,

$\Rightarrow \hat{h}_x \geq 0$ . Moreover, if  $\hat{h}_x(P) = 0$  then  $\hat{h}_x(uP) = 0 \quad \forall u \in \mathbb{Z}$

$\Rightarrow \{uP\}$  finite set (finiteness property)  $\Rightarrow P \in A(\bar{K})$  for.



### §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  $A$  is an ab. group such that:

- 1)  $\exists m > 1$  s.t.  $A/mA$  is finite
- 2)  $\exists$  quad. form  $h: A \rightarrow \mathbb{R}$  s.t. the set  $H_c = \{a \in A : h(a) \leq c\}$  is finite  $\forall c \in \mathbb{R}$ .

Then  $A$  is finitely generated.

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

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

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,

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





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

$$x = mx_1 + a_{i_1} \quad x_1 \in A$$

$$x_1 = mx_2 + a_{i_2} \quad \vdots$$

$$\vdots$$

$$x_n = mx_{n+1} + a_{i_{n+1}}$$

$$\vdots$$

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

so

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

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

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

To apply this, lemma we need:

Theorem 4' (weak Mordell-Weil):  $\exists$  finite ext'n  $L \supset K$  and int.

with  $h$ .  $A(L)/m A(L) \cong f \cdot g$ .

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

Now use

Fund. Lemma:  $L_m = L([m]^{-1} A(L))$  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  $L$ .



Pf. [Mu], Appendix B

Put  $G = \text{Gal}(L_m/L)$ . Then have injection

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

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

Note: It is unknown how to characterize the image of  $\psi$ , 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  $Z_0 \in \text{Pic}(A)$  (exists since  $A$  proj.)

Then  $\pi^* Z_0 \in \text{Pic}(L)$  is symmetric and ample, so  $L$  satisfies Lemma 2.

(ii). Thus by the lemma,  $A(L)$  is f.g., hence so is  $A(K)A(L)$ .

### References

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

[Mu] D. Mumford, Abelian Varieties. Oxford U Press, 1974 (2<sup>nd</sup> ed'n).