A Survey of Local and Global Pairings on Elliptic Curves and Abelian Varieties

Joseph H. Silverman

Brown University

Pairing 2010
Yamanaka Hot Spring, Japan
December 13–15, 2010

What is a Pairing?

Abstractly, a **Pairing** is a *bilinear map* on an *abelian group* M taking values in some other abelian group R,

$$\langle \cdot\,, \cdot \rangle : M \times M \longrightarrow R.$$

There are many abelian groups we might consider

- $\mathbb{Z}$, or more generally $\mathbb{Z}^d$.
- $\mathbb{Z}/m\mathbb{Z}$, a cyclic group of order m, or generally $(\mathbb{Z}/m\mathbb{Z})^d$.
- $\mathbb{F}_p$ with addition as the group law, or generally $\mathbb{F}_p^d$.
- $\mathbb{F}_p^*$ with multiplication as the group law.
- $\boldsymbol{\mu}_m$, the group of m^{th}-roots of unity.
- $E(\mathbb{F}_p)$, the group of $\mathbb{F}_p$-points on an elliptic curve, or more generally $E(K)$ for any field K.
- $A(K)$, the group of points an an abelian variety.
- $E[m]$, the group of points of order m on an elliptic curve, or more generally $A[m]$.

Bilinearity

A pairing

$$\langle \cdot\,, \cdot \rangle : M \times M \longrightarrow R.$$

is a **Bilinear** map. This means that

$$\langle x + y, z \rangle = \langle x, z \rangle + \langle y, z \rangle,$$
$$\langle x, y + z \rangle = \langle x, y \rangle + \langle x, z \rangle.$$

A pairing is the same as a homomorphism

$$\phi : M \longrightarrow \mathrm{Hom}(M, R)$$

from M to the group of homomorphisms from M to R. Thus if we are given a pairing $\langle \cdot\,, \cdot \rangle$, we can define ϕ by

$$\phi(x)(y) = \langle x, y \rangle.$$

And if we are given a homomorphism ϕ, we can define a pairing by

$$\langle x, y \rangle = \phi(x)(y).$$

How To Define and Compute a Pairing

Typically M has a basis $\mathbf{e}_1, \ldots, \mathbf{e}_d$. This means that every element $\mathbf{v}$ of M can be written uniquely as a sum

$$\mathbf{v} = v_1\mathbf{e}_1 + v_2\mathbf{e}_2 + \cdots + v_d\mathbf{e}_d.$$

(The coordinates $v_1, \ldots, v_d$ of $\mathbf{v}$ might be in $\mathbb{Z}$ or $\mathbb{Z}/m\mathbb{Z}$ or $\mathbb{F}_p$, for example.)
Then we can define a pairing by choosing a matrix of numbers $(c_{ij})_{1\le i,j\le d}$ and setting

$$\left\langle \sum_{i=1}^{d} u_i\mathbf{e}_i, \sum_{i=1}^{d} v_i\mathbf{e}_i \right\rangle = \sum_{i=1}^{d}\sum_{j=1}^{d} u_i v_j c_{ij}.$$

Every pairing $\langle \cdot\,, \cdot \rangle$ is given by a formula of this sort, where

$$c_{ij} = \langle \mathbf{e}_i, \mathbf{e}_j \rangle.$$

So there are many many different pairings on M.

In Practice, How Do We Compute a Pairing?

In order to compute $\langle \mathbf{u}, \mathbf{v} \rangle$ as $\sum\sum u_i v_j c_{ij}$, we need to write $\mathbf{u}$ and $\mathbf{v}$ in terms of the basis $\mathbf{e}_1, \ldots, \mathbf{e}_d$.

But writing an element of M as a linear combination of the basis elements $\mathbf{e}_1, \ldots, \mathbf{e}_d$ is equivalent to solving a (multi-dimensional) discrete logarithm problem in M.

In order for a pairing to be useful for cryptography, we want to be able to compute the pairing efficiently without writing elements in terms of a known basis.

Among the many possible pairings on M, we want to find one that is natural (or **functorial**). Equivalently we want to find a functorial isomorphism

$$M \xrightarrow{\sim} \mathrm{Hom}(M, R)$$

whose definition does not depend on choosing a basis for M.

The Weil and Lichtenbaum–Tate Pairings

The Weil pairing

$$\langle \cdot\,, \cdot \rangle_{\text{Weil}} : E[m] \times E[m] \longrightarrow \boldsymbol{\mu}_m$$

and the Lichtenbaum–Tate pairing

$$\langle \cdot\,, \cdot \rangle_{\text{LT}} : E[m](\mathbb{F}_q) \times E(\mathbb{F}_q)/mE(\mathbb{F}_q) \longrightarrow \boldsymbol{\mu}_m$$

have become very important in cryptography (as witnessed by this *fourth* annual conference on Pairings!).

But the usual definition of these pairings is very mysterious. To compute them, we create a function on the elliptic curve E with certain zeros and poles and evaluate the function at various points on the curve.

One of the goals of this talk is to show you that these pairings are actually very natural (functorial), and in particular, to explain why they do not depend on choosing a particular basis for $E[m]$ or E/mE.

“Hom” and “Ext”

Homomorphism Groups

The set of homomorphisms from one abelian group to another,

$$\mathrm{Hom}(M, Q),$$

is itself naturally a group. Thus if $f, g \in \mathrm{Hom}(M, Q)$, then

$$(f+g) \in \mathrm{Hom}(M, Q), \qquad (f+g)(x) = f(x) + g(x).$$

A homomorphism of groups

$$\phi : M \to N$$

gives a natural homomorphism of Hom groups in the opposite direction,

$$\phi^* : \mathrm{Hom}(N, Q) \longrightarrow \mathrm{Hom}(M, Q),$$

where

$$\phi^*(f) : M \to Q, \qquad x \mapsto f\big(\phi(x)\big).$$

Failure of Surjectivity

If $\phi : M \to N$ is a *surjective* homomorphism of groups, then it is easy to see that the induced homomorphism

$$\phi^* : \mathrm{Hom}(N, Q) \longrightarrow \mathrm{Hom}(M, Q),$$

is *injective*.
But if $\phi : M \to N$ is an *injective* homomorphism of groups, then the induced homomorphism

$$\phi^* : \mathrm{Hom}(N, Q) \longrightarrow \mathrm{Hom}(M, Q),$$

might not be *surjective*.
Example. The injective homomorphism

$$\phi : \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}/p^2\mathbb{Z}, \qquad x \longmapsto px$$

induces the zero homomorphism

$$\phi^* : \mathrm{Hom}(\mathbb{Z}/p^2\mathbb{Z}, \mathbb{Z}/p\mathbb{Z}) \longrightarrow \mathrm{Hom}(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p\mathbb{Z}),$$

i.e., $\phi^*(f) = 0$ for every f.

Measuring the Failure of Surjectivity

The failure of surjectivity is measured by another group, called the **Ext Group**. (Ext is short for "Extension".)

The elements of $\mathrm{Ext}(M, Q)$ are represented by maps

$$f : M \times M \to Q$$

satisfying the following rather complicated relation:

$$f(x, y) - f(x, y + z) + f(x + y, z) - f(y, z) = 0$$
$$\text{for all } x, y, z \in M.$$

Two such maps f_1 and f_2 are considered to be the same if there is a map (not necessarily a homomorphism)

$$g : M \to Q$$

so that the difference $f_1 - f_2$ looks like

$$f_1(x, y) - f_2(x, y) = g(x + y) - g(x) - g(y).$$

Notice that if g is a homomorphism, then $f_1 = f_2$.

How "Ext" Extends "Hom"

Let

$$0 \to M \xrightarrow[\text{injective}]{\phi} N \xrightarrow[\text{surjective}]{\psi} P \to 0$$

be an exact sequence of abelian groups. This means that ϕ is injective, ψ is surjective, and

$$\psi(y) = 0 \quad \text{if and only if} \quad y = \phi(x) \text{ for some } x \in M.$$

Applying $\mathrm{Hom}(\,\cdot\,, Q)$, we get a new sequence, but it is no longer exact due to the failure of surjectivity. The Ext groups correct this problem.

The Hom-Ext Sequence. There is an exact sequence

$$0 \longrightarrow \mathrm{Hom}(P,Q) \longrightarrow \mathrm{Hom}(N,Q) \longrightarrow \mathrm{Hom}(M,Q) \hookrightarrow \mathrm{Ext}(P,Q) \longrightarrow \mathrm{Ext}(N,Q) \longrightarrow \mathrm{Ext}(M,Q).$$

Dual Abelian Varieties and the Weil Pairing

The Dual of an Abelian Variety

The Weil pairing on an elliptic curve E is a pairing

$$E[m] \times E[m] \longrightarrow \boldsymbol{\mu}_m.$$

The usual definition of the Weil pairing is unenlightening because in general on an abelian variety A, the Weil pairing is actually a pairing between A and its dual $\hat{A}$,

$$A[m] \times \hat{A}[m] \longrightarrow \boldsymbol{\mu}_m.$$

We will consider two definitions of the dual abelian variety. The first is as an Ext group.

Definition. The **Dual** of an abelian variety A is the group

$$\hat{A} = \mathrm{Ext}(A, \mathbb{C}^*).$$

The group $\hat{A}$ is itself an abelian variety! (The field $\mathbb{C}$ may be replaced by other fields.)

We will see later than an elliptic curve is its own dual.

The Weil Pairing

We start with the exact sequence

$$0 \longrightarrow A[m] \longrightarrow A \xrightarrow{P \mapsto mP} A \longrightarrow 0$$

and apply $\mathrm{Hom}(\,\cdot\,, \mathbb{C}^*)$. This reverses the direction of the arrows and gives an exact sequence

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{Hom}(A[m], \mathbb{C}^*) & \xrightarrow{\delta} & \mathrm{Ext}(A, \mathbb{C}^*) & \xrightarrow{m} & \mathrm{Ext}(A, \mathbb{C}^*) \\
 & & \| & & \| & & \| \\
0 & \longrightarrow & \mathrm{Hom}(A[m], \boldsymbol{\mu}_m) & \xrightarrow{\delta} & \hat{A} & \xrightarrow{m} & \hat{A}
\end{array}$$

The bottom line says that δ gives an isomorphism

$$\mathrm{Hom}(A[m], \boldsymbol{\mu}_m) \cong \hat{A}[m].$$

This give a perfect pairing (the **Weil Pairing**)

$$e_m : A[m] \times \hat{A}[m] \cong A[m] \times \mathrm{Hom}\big(A[m], \boldsymbol{\mu}_m\big) \longrightarrow \boldsymbol{\mu}_m.$$

The Picard Group

To get a formula for the Weil pairing, we use a second description of $\hat{A}$ in terms of the **Picard Group**,

$$\mathrm{Pic}^0(A) = \frac{\{\text{Divisors algebraically equivalent to } 0\}}{\{\text{Divisors linearly equivalent to } 0\}}.$$

We identify $\mathrm{Pic}^0(A)$ with $\mathrm{Ext}(A, \mathbb{C}^*)$ as follows.

- Let $[D] \in \mathrm{Pic}^0(A)$.
- For $P \in A$, let $T_P : A \to A$ be $T_P(Q) = Q + P$.
- Then $T_P^* D - D$ is the divisor of a function $F_{D,P}$.

From $[D] \in \mathrm{Pic}^0(A)$ we create an element of $\mathrm{Ext}(A, \mathbb{C}^*)$,

$$A \times A \longrightarrow \mathbb{C}^*, \quad (P, Q) \longrightarrow F_{D,P}(Q)/F_{D,P}(O).$$

The resulting map

$$\mathrm{Pic}^0(A) \xrightarrow{\sim} \mathrm{Ext}(A, \mathbb{C}^*) \quad \text{is an isomorphism.}$$

Example: The Picard Group of an Elliptic Curve

A *divisor* on an elliptic curve is a formal sum of points

$$D = \sum n_i(Q_i).$$

D is *algebraically equivalent to* 0 if it has degree 0. Then the points in the divisor

$$T_P^* D - D = \sum n_i(Q_i - P) - \sum n_i(Q_i)$$

sum to O on E, so $T_P^* D - D$ is the divisor of a function,

$$T_P^* D - D = \operatorname{div}(F_{D,P}).$$

We can identify E with its Picard group via the map

$$E \longrightarrow \operatorname{Pic}^0(E), \qquad Q \longrightarrow \big[(Q) - (O)\big].$$

This map is an isomorphism of E with its dual $\hat{E}$. So when working with the Weil pairing on an elliptic curve, there is no need to ever mention the dual of E.

A Formula for the Weil Pairing

As we've seen, the Weil pairing comes from an isomorphism

$$\mathrm{Hom}(A[m], \boldsymbol{\mu}_m) \xrightarrow{\sim} \mathrm{Ext}(A, \mathbb{C}^*)[m] = \hat{A}[m].$$

We have also seen that $\hat{A}$ can be identified with $\mathrm{Pic}^0(A)$, so we get a perfect pairing

$$e_m : A[m] \times \mathrm{Pic}^0(A)[m] \longrightarrow \boldsymbol{\mu}_m.$$

Tracing through the definitions of the various maps leads to the usual definition of the Weil pairing in terms of functions with certain divisors evaluated at certain points. Further, for elliptic curves we have an isomorphism

$$E \longrightarrow \mathrm{Pic}^0(E), \qquad Q \longrightarrow \big[(Q) - (O)\big],$$

and using this identification leads to the familiar definition of the Weil pairing for elliptic curves.

Cohomological Pairings

Two Important Pairings

Two other important pairings on abelian varieties are the **Lichtenbaum–Tate pairing**,

$$\langle \cdot\,,\, \cdot \rangle_{\mathrm{LT}} : A(K)/mA(K) \times \hat{A}[m](K) \longrightarrow K^*/K^{*m},$$

and the **Cassels–Tate pairing** on the Shafarevich–Tate group Ш,

$$\langle \cdot\,,\, \cdot \rangle_{\mathrm{CT}} : Ш(A/K) \times Ш(\hat{A}/K) \longrightarrow \mathbb{Q}/\mathbb{Z}.$$

In order to define that LT and CT pairings functorially, one uses the Weil pairing as a building block. (Due to time constraints, I will probably discuss only the Lichtenbaum–Tate pairing in this talk.)

Another important tool used to define the LT and CT pairings is called *Galois cohomology*.

A Primer on Galois Cohomology

We look at a Galois group G that acts on an abelian group M.

Key Example: Let E be an elliptic curve defined over a finite field $\mathbb{F}_p$. Then the Galois group G of the algebraic closure $\bar{\mathbb{F}}_p$ of $\mathbb{F}_p$ acts on the points of E having coordinates in $\bar{\mathbb{F}}_p$.

Similarly, G acts on $E[m]$, the points of order m in $E(\bar{\mathbb{F}}_p)$.

Often we are interested in the set of elements of M that are fixed by every element of G, which is denoted by

$$H^0(G, M) = \{x \in M : \sigma(x) = x \text{ for all } \sigma \in G\}.$$

Continuing with our example from above,

$$H^0\big(G, E(\bar{\mathbb{F}}_p)\big) = E(\mathbb{F}_p),$$
$$H^0\big(G, E[m]\big) = E(\mathbb{F}_p)[m].$$

Failure of Surjectivity

If we have an exact sequence of abelian groups

$$0 \to M \xrightarrow[\text{injective}]{\phi} N \xrightarrow[\text{surjective}]{\psi} P \to 0,$$

and if G acts on M, N, and P, then it is easy to check that we get an exact sequence

$$0 \to H^0(G, M) \xrightarrow[\text{injective}]{} H^0(G, N) \to H^0(G, P),$$

but the final map might not be surjective.

There is another group that extends the H^0 exact sequence, in the same way that the Ext group extends the Hom exact sequence:

$$H^1(G, M) = \frac{(\text{group of 1-cocyles})}{(\text{group of 1-coboundaries})}.$$

Extending the Exact Sequence with H^1

A **1-cocycle** is a map

$$\xi : G \longrightarrow M \quad \text{satisfying} \quad \xi(\sigma\tau) = \sigma\big(\xi(\tau)\big) + \xi(\sigma) \quad \text{for all } \sigma, \tau \in G.$$

A **1-coboundary** is a map of the form

$$\eta : G \longrightarrow M, \quad \eta(\sigma) = \sigma(a) - a,$$

for some $a \in M$.

The H^0–H^1 Sequence. There is an exact sequence

$$0 \longrightarrow H^0(G, M) \xrightarrow{\delta} H^0(G, N) \longrightarrow H^0(G, P) \hookrightarrow H^1(G, M) \longrightarrow H^1(G, N) \longrightarrow H^1(G, P)$$

The map δ is called the **connecting homomorphism**.

Example 1: The Kummer Sequence for $\bar{K}^*$

Let K be a field, let $\bar{K}$ be an algebraic closure of K, and let $\boldsymbol{\mu}_m \subset \bar{K}^*$ be the group of m^{th}-roots of unity. Then there is an exact sequence

$$1 \longrightarrow \boldsymbol{\mu}_m \longrightarrow \bar{K}^* \xrightarrow{z \to z^m} \bar{K}^* \longrightarrow 1.$$

Taking the subgroups fixed by G gives

$$\begin{array}{ccccccc} H^0(G,\bar{K}^*) & \xrightarrow{z\to z^m} & H^0(G,\bar{K}^*) & \xrightarrow{\delta} & H^1(G,\boldsymbol{\mu}_m) & \longrightarrow & H^1(G,\bar{K}^*) \\ \| & & \| & & \| & & \| \\ K^* & \xrightarrow{z\to z^m} & K^* & \xrightarrow{\delta} & H^1(G,\boldsymbol{\mu}_m) & \longrightarrow & 1. \end{array}$$

$H^1(G,\bar{K}^*) = 1$ is called Hilbert's Theorem 90.

We get an isomorphism that will be used later:

$$K^*/(K^*)^m \xrightarrow{\sim} H^1(G,\boldsymbol{\mu}_m).$$

Example 2: The Kummer Sequence for Abelian Varieties

Let A/K be an abelian variety. Multiplication-by-m gives an exact sequence

$$0 \longrightarrow A[m] \longrightarrow A(\bar{K}) \xrightarrow{P \to mP} A(\bar{K}) \longrightarrow 0.$$

Taking the subgroups fixed by G gives

$$\begin{array}{ccccccc}
H^0\big(G, A(\bar{K})\big) & \xrightarrow{z \to z^m} & H^0\big(G, A(\bar{K})\big) & \xrightarrow{\delta} & H^1\big(G, A[m]\big) & \longrightarrow & H^1\big(G, A(\bar{K})\big) \\
\| & & \| & & \| & & \| \\
A(K) & \xrightarrow{P \to mP} & A(K) & \xrightarrow{\delta} & H^1\big(G, A[m]\big) & \longrightarrow & H^1\big(G, A(\bar{K})\big)
\end{array}$$

For abelian varieties the group $H^1\big(G, A(\bar{K})\big)$ is not trivial, but we at least get an injective map

$$A(K)/mA(K) \xrightarrow{\delta} H^1\big(G, A[m]\big).$$

The Lichtenbaum–Tate Pairing

We now use the Weil pairing and the two Kummer sequences to construct the Lichtenbaum–Tate pairing.
Let $P \in A(K)$ and $Q \in \hat{A}[m](K)$. Using

$$\delta : A(K)/mA(K) \longrightarrow H^1\big(G, A[m]\big),$$

we get a 1-cocycle

$$\delta_P : G \longrightarrow A[m], \qquad \sigma \longmapsto \delta_P(\sigma).$$

We use the point $Q \in \hat{A}[m](K)$ and the Weil pairing to turn this into a 1-cocycle with values in $\boldsymbol{\mu}_m$,

$$G \longrightarrow \boldsymbol{\mu}_m, \qquad \sigma \longmapsto e_m\big(\delta_P(\sigma), Q\big).$$

This is an element of $H^1(G, \boldsymbol{\mu}_m)$, and the Kummer sequence for $\bar{K}^*$ says that $H^1(G, \boldsymbol{\mu}_m)$ equals K^*/K^{*m}.
This defines the Lichtenbaum–Tate pairing,

$$\big\langle \cdot\,, \cdot \big\rangle_{\mathrm{LT}} : A(K)/mA(K) \times \hat{A}[m](K) \longrightarrow K^*/K^{*m}.$$

The Néron–Tate Canonical Height Pairing

The Height of an Algebraic Number

The **height** of a rational number is the number of bits it takes to store the number,

$$h\left(\frac{a}{b}\right) = \log_2|a| + \log_2|b|.$$

More generally, consider an algebraic number α of degree d. It is the root of a polynomial

$$a_0X^d + a_1X^{d-1} + \cdots + a_d \in \mathbb{Z}[X]$$
$$\text{with } \gcd(a_0, a_1, \ldots, a_d) = 1.$$

Then the **height of α** is

$$h(\alpha) = \log_2|a_0| + \log_2|a_1| + \cdots + \log_2|a_d|.$$

Theorem. There are only finitely many numbers of bounded degree and height. In other words,

$$\left\{\alpha \in \bar{\mathbb{Q}} : \deg(\alpha) < D \text{ and } h(\alpha) < H\right\} \text{ is a finite set.}$$

Heights on Elliptic Curves and Abelian Varieties

Height functions are used extensively when studying points on elliptic curves and abelian varieties.

The height of the point

$$P = (x_P, y_P) \quad \text{on the curve} \quad E : Y^2 = X^3 + AX + B$$

is the height of its coordinates,

$$h(P) = h(x_P) + h(y_P).$$

More generally, we embed an abelian variety A in projective space and define the height of a point $P \in A(\bar{\mathbb{Q}})$ to be the height of the coordinates of P.

Heights and the Group Law

- The group law on an abelian variety gives us a geometric way to combine points.
- The height of a point measures the point's information-theoretic complexity.

It is thus important to understand how the group law interacts with the height.

Theorem. On an elliptic curve,

$$h(nP) = n^2 h(P) + O(1) \quad \text{for all } P \in E(\bar{\mathbb{Q}}),$$

where the $O(1)$ depends only on E and n.

The same result is true on an abelian variety A provided we take a symmetric embedding of A into projective space.

The Canonical Height

The height of nP is more-or-less equal to n^2 times the height of P. It would be nice to get rid of the $O(1)$.

Theorem. The limit

$$\hat{h}(P) = \lim_{n\to\infty} \frac{1}{n^2} h(nP)$$

exists and is called the *Néron–Tate height* (or the *canonical height*) of P.

Theorem. The Néron–Tate height has the following useful properties:

- $\hat{h}(P) = h(P) + O(1)$.
- $\hat{h}(nP) = n^2\hat{h}(P)$.

The first properties says that $\hat{h}$ still contains information-theoretic content, the second says that $\hat{h}$ grows like a quadratic function.

The Canonical Height Pairing

The **Néron–Tate canonical height pairing** is the map

$$\langle \cdot\,,\cdot \rangle_{\mathrm{NT}} : E \times E \longrightarrow \mathbb{R},$$
$$\langle P, Q \rangle_{\mathrm{NT}} = \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q).$$

Theorem. The canonical height pairing is a bilinear form, and it extends to a non-degenerate bilinear form on $A(\bar{\mathbb{Q}}) \otimes \mathbb{R}$.

This means that if $P_1, \ldots, P_r \in A(\bar{\mathbb{Q}})$ are independent modulo torsion, then their regulator

$$\mathrm{Reg}(P_1, \ldots, P_r) = \det\bigl(\langle P_i, P_j \rangle_{\mathrm{NT}}\bigr)_{1 \le i,j \le r}$$

is non-zero. The value of this regulator is an important quantity, appearing in the conjectures of Birch and Swinnerton-Dyer.

Canonical Heights in Cryptography

Height functions have been used in ECC to show that certain potential attacks are not practical. For example, Suzuki and I used heights and other tools to show that a direct index-calculus attack on ECDLP does not work, and heights were used to show the same is true of a reverse index attack.

Indeed, Neal Koblitz gave a talk at ECC 2000 with the title

Miracles of the Height Function
A Golden Shield Protecting ECC

This description of the canonical height pairing is somewhat *ad hoc*. I will now briefly explain why the canonical height pairing is a natural functorial pairing.

The Canonical Height as a Functorial Pairing

Embeddings and Divisors

We have defined the height of a point to be the height of its coordinates.
This means that the height of a point on an abelian variety A depends on how the abelian variety is embedding into projective space $\mathbb{P}^n$.

If we have fixed an embedding

$$A \subset \mathbb{P}^n$$

then the intersection of A with a hyperplane $H \subset \mathbb{P}^n$ is a (very ample) divisor

$$A \cap H \in \mathrm{Div}(A).$$

Conversely, if we have a very ample divisor $D \in \mathrm{Div}(A)$, then by taking functions $f_0, \ldots, f_n$ whose only poles are along D, we get an embedding

$$\phi_D :\longhookrightarrow \mathbb{P}^n.$$

Divisors and Heights

For any very ample divisor $D \in \mathrm{Div}(A)$, we define a height function

$$h_D : A(K) \longrightarrow \mathbb{R}, \qquad h_D(P) = h\big(\phi_D(P)\big).$$

h_D is well-defined up to a bounded function.

For any divisor $D \in \mathrm{Div}(A)$, we write D as a difference

$$D = D_1 - D_2 \quad \text{of very ample divisors,}$$

and then we define

$$h_D : A(K) \longrightarrow \mathbb{R}, \qquad h_D(P) = h_{D_1}(P) - h_{D_2}(P).$$

The **canonical height** on A relative to the (symmetric) divisor D is defined by the usual limit

$$\hat{h}_{A,D} : A(K) \longrightarrow \mathbb{R}, \quad \hat{h}_{A,D}(P) = \lim_{m\to\infty} \frac{1}{m^2} h_{A,D}\big(mP\big).$$

The Poincaré Divisor

The definition of $\hat{h}_{A,D}$ is very nice, but it still depends on choosing a divisor D.

To get a functorial definition, we do not want a pairing of $A(K)$ with itself. Instead, we want a pairing between $A(K)$ and $\hat{A}(K)$.

This functorial definition uses the **Poincaré divisor**

$$\mathcal{P} \in \mathrm{Div}(A \times \hat{A}).$$

Identifying $\hat{A}$ with $\mathrm{Pic}^0(A)$, the Poincaré divisor satisfies:

- $\mathcal{P} \cap \big(A \times \{\xi\}\big) \sim \xi$, for all $\xi \in \hat{A} = \mathrm{Pic}^0(A)$.
- $\mathcal{P} \cap \big(\{P\} \times \hat{A}\big) \sim 0$, for all $P \in A$.

(The Poincaré divisor is unique up to linear equivalence.)

The Canonical Height Pairing

The functorial definition of the canonical height pairing uses the Poincaré divisor on $A \times \hat{A}$.

Theorem. Let A be an abelian variety defined over a number field K. The canonical height on $A \times \hat{A}$ relative to the Poincaré divisor,

$$\hat{h}_{A\times\hat{A},\mathcal{P}} : A(K) \times \hat{A}(K) \longrightarrow \mathbb{R},$$

is a non-degenerate bilinear form.

Here non-degeneracy means that

$$\hat{h}_{A\times\hat{A},\mathcal{P}}(P,Q) = 0 \text{ for all } P \in A \iff Q \in \hat{A}_{\text{tors}},$$
$$\hat{h}_{A\times\hat{A},\mathcal{P}}(P,Q) = 0 \text{ for all } Q \in \hat{A} \iff P \in A_{\text{tors}}.$$

Using the self-duality $E \cong \hat{E}$ of an elliptic curve, we obtain twice the canonical height pairing defined earlier (because $\mathcal{P} = 2(O)$).

The Shafarevich–Tate Group and the The Cassels–Tate Pairing

The Mordell–Weil Theorem

If K is a number field, for example $K = \mathbb{Q}$, then the celebrated Mordell–Weil Theorem says that

$A(K)$ is a finitely generated abelian group.

However, there is currently no algorithm known to compute generators for $A(K)$.

The obstruction to finding an algorithm is a mysterious group that appears in the proof of the Mordell–Weil theorem. It is called the

Shafarevich–Tate group, and is denoted $Ш(A/K)$.

It is conjectured that $Ш(A/K)$ is a finite group, but this is only proven in a small number of cases.

The Shafarevich–Tate Group

One way to define $Ш(A/K)$ is in terms of abelian varieties B/K that are $\bar{K}$-isomorphic to A/K and also $K_{\mathfrak{p}}$-isomorphic to A/K for every $\mathfrak{p}$-adic completion of K, but not necessarily K-isomorphic to A/K. A second definition uses group cohomology,

$$\text{Kernel}\Big(H^1\big(G, A(\bar{K})\big) \longrightarrow \prod_{\mathfrak{p}} H^1\big(G, A(\bar{K}_{\mathfrak{p}})\big)\Big).$$

Cassels and Tate define an alternating bilinar pairing

$$\langle \cdot\,, \cdot \rangle_{\mathrm{CT}} : Ш(A/K) \times Ш(\hat{A}/K) \longrightarrow \mathbb{Q}/\mathbb{Z}.$$

If $Ш(A/K)$ is finite, then the pairing is non-degenerate. There are several equivalent definitions of the Cassels–Tate pairing, but all are complicated. In the article accompanying this talk I have sketched Tates' definition using Galois cohomology and the Weil pairing.

I would like to thank you for your attention.

I would also like to thank the organizers for inviting me to deliver this lecture.

A Survey of Local and Global Pairings on Elliptic Curves and Abelian Varieties

Joseph H. Silverman

Brown University

Pairing 2010
Yamanaka Hot Spring, Japan
December 13–15, 2010