BUNTES

Maria Ines
Nov 3, 2017

Weil Pairings

Recall: Weil Pairings on Elliptic Curves

E/k an elliptic curve, $m \geq 2$
If $\mathrm{char}(k) = p > 0$, $(m, p) = 1$.

The Weil e_m-pairing $e_m : E[m] \times E[m] \longrightarrow \mu_m$ is defined as follows:

- Fix $T \in E[m]$, then there exists $f \in \bar{k}(E)$ such that $\mathrm{div}(f) = m(T) - m(0)$.
- Fix $T' \in E[m]$ with $mT' = T$ and $g \in \bar{k}(E)$ such that
$$\mathrm{div}(g) = [m]^*(T) - [m]^*(0) = \sum_{R \in E[m]} ((T' + R) - (R))$$

Then $\mathrm{div}(f \circ [m]) = \mathrm{div}(g^m) \Rightarrow f \circ [m] = c \cdot g^m$
By rescaling by c, we can assume $f \circ [m] = g^m$.

- For $S \in E[m]$, $X \in E$,
$$g(X+S)^m = f([m]X + [m]S) = f([m]X) = g(X)^m.$$

$$\frac{g(\cdot + S)}{g(\cdot)} : E \longrightarrow \mathbb{P}^1$$

Can only take finitely many distinct values, thus is not surjective and therefore constant.

So we define $e_m : E[m] \times E[m] \longrightarrow \mu_m$

$$(S, T) \longmapsto \frac{g_T(X+S)}{g_T(X)}$$

- e_m is compatible:

$$e_{mm'}(a, a')^{m'} = e_m(m'a, m'a') \qquad \forall a, a' \in E[mm']$$

- So for any $\ell \neq \mathrm{char}(k)$ prime, we can combine e_{ℓ^n} pairings in an ℓ-adic Weil pairing on $T_\ell E$:

$$e : T_\ell E \times T_\ell E \longrightarrow T_\ell \mu = \mathbb{Z}_\ell(1).$$

Weil Pairings on Abelian Varieties

Let A/k be an abelian variety and assume $k = \bar{k}$.
We construct a Weil e_m-pairing

$$e_m : A[m] \times A^\vee[m] \longrightarrow \mu_m$$

$$(a, a') \longmapsto \frac{(g \circ t_a)(x)}{g(x)} = \frac{g(x+a)}{g(x)}$$

- Fix $a \in A[m]$, $a' \in A^\vee[m]$

Say a' corresponds to some line bundle $\mathcal{L}$ and a divisor D.
Then $\mathcal{L}^m$ and $m_A^* \mathcal{L}$ are trivial, so there exist $f, g \in k(A)$ such that

$$\mathrm{div}(f) = mD, \quad \mathrm{div}(g) = m_A^* D$$

Again, we have $\cdot \operatorname{div}(f \circ m_A) = \operatorname{div}(g^m)$

$\cdot\ g(x+a)^m = g(x)^m$

Prop: The Weil e_m-pairing has the following properties:

(a) e_m is bilinear: $\begin{cases} e_m(a_1+a_2, a') = e_m(a_1, a')\, e_m(a_2, a') \\ e_m(a, a_1'+a_2') = e_m(a, a_1')\, e_m(a, a_2') \end{cases}$

(b) e_m is nondegenerate: $\cdot$ if $e_m(a, a') = 0 \ \ \forall a \in A[m]$, $a' = 0$

$\cdot$ if $e_m(a, a') = 0 \ \ \forall a' \in A^\vee[m]$, $a = 0$

(c) e_m is compatible: $e_{mm'}(a, a')^{m'} = e_m(m'a, m'a') \quad \forall a \in A[mm']$

$\forall a' \in A^\vee[mm']$

$(mm', \operatorname{char}(k)) = 1.$

Note: If k is not algebraically closed, e_m is also Galois-invariant.

Corollary: There exists a bilinear, non-degenerate (Galois-invariant) pairing

$$e : T_\ell A \times T_\ell A^\vee \longrightarrow T_\ell \mu$$
$$((a_n), (a_n')) \longmapsto (e_{\ell^n}(a_n, a_n'))$$

For a homomorphism $\lambda : A \longrightarrow A^\vee$, we define

$$e_m^\lambda : A[m] \times A[m] \longrightarrow \mu_m$$
$$(a, a') \longmapsto e_m(a, \lambda(a'))$$

$$e^\lambda : T_\ell A \times T_\ell A \longrightarrow T_\ell \mu$$
$$(a, a') \longmapsto e(a, \lambda(a'))$$

Notation: If $\lambda = \lambda_k$, $e^k := e^\lambda$.

Prop 13.2: For a homomorphism $\alpha: A \longrightarrow B$,

(a) $e(a, \alpha^\vee(b)) = e(\alpha(a), b) \quad \forall\, a \in T_e A,\ b \in T_e B$

(b) $e^{\alpha^\vee \circ \lambda \circ \alpha}(a, a') = e^\lambda(\alpha(a), \alpha(a'))$

for $a, a' \in T_e A$, $\lambda \in \mathrm{Hom}(B, B')$.

(c) $e^{\alpha^* h}(a, a') = e^h(\alpha(a), \alpha(a'))$, $\quad a, a' \in T_e A$, $h \in \mathrm{Pic}(B)$

(d) The map

$$\begin{array}{ccc} \mathrm{Pic}\, A & \longrightarrow & \mathrm{Hom}(\wedge^2 T_e A,\ T_{\ell\mu}) \\ h & \longmapsto & e^h \end{array}$$

is a homomorphism.

(In particular, e^h is skew-symmetric).

Proof: (a) $a = (a_n) \in T_e A$, $\quad b = (b_n) \in T_e B^\vee$

Fix a divisor D on B representing b_n, and $g \in k(B)$ such that $\mathrm{div}(g) = (\ell_B^n)^* D$.

Then $\alpha^* D$ represents $\alpha^\vee(b_n)$ (since $\alpha^\vee(h) = \alpha^* h$), so

$$\mathrm{div}(g \circ \alpha) = \alpha^* \mathrm{div}(g) = \alpha^* (\ell_B^n)^* D = (\ell_A^n)^* \alpha^* D$$

So

$$\begin{aligned} e_{\ell^n}(\alpha(a_n), b_n) &= \frac{g(x + \alpha(a_n))}{g(x)} \\ &= \frac{g(\alpha(y) + \alpha(a_n))}{g(\alpha(y))} \\ &= e_{\ell^n}(a, \alpha^\vee(b_n)) \end{aligned}$$

Since this quotient is constant, can take any x, so assume $x = \alpha(y)$

(b) $\begin{aligned} e^{\alpha^\vee \circ \lambda \circ \alpha}(a, a') &= e(a, \alpha^\vee \circ \lambda \circ \alpha(a')) \\ &= e(\alpha(a), \lambda \circ \alpha(a')) \\ &= e^\lambda(\alpha(a), \alpha(a')) \end{aligned}$ $\Big\}$ by (a)

(c) Note $\lambda_{\alpha^* \circ L} = \alpha^\vee \circ \lambda_L \circ \alpha$ and apply (b)

(d) Follows from $\lambda_{L \otimes L'} = \lambda_L + \lambda_{L'}$. □

Example: Let $A/\mathbb{C}$ be an abelian variety.

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathcal{O}_A \xrightarrow{e^{2\pi i(\cdot)}} \mathcal{O}_A^\times \longrightarrow 0$$

induces

$$H^1(A(\mathbb{C}), \mathbb{Z}) \longrightarrow H^1(A(\mathbb{C}), \mathcal{O}_A) \longrightarrow H^1(A(\mathbb{C}), \mathcal{O}_A^\times)$$

$$\longrightarrow H^2(A(\mathbb{C}), \mathbb{Z}) \longrightarrow H^2(A(\mathbb{C}), \mathcal{O}_A)$$

Note: $H^1(A(\mathbb{C}), \mathcal{O}_A^\times) \simeq \operatorname{Pic} A$

$$\frac{H^1(A(\mathbb{C}), \mathcal{O}_A)}{H^1(A(\mathbb{C}), \mathbb{Z})} \simeq A^\vee(\mathbb{C}) = \operatorname{Pic}^0(A)$$

$\Rightarrow$ We get an exact sequence

$$0 \longrightarrow NS(A) \longrightarrow H^2(A(\mathbb{C}), \mathbb{Z}) \longrightarrow H^2(A(\mathbb{C}), \mathcal{O}_A)$$
$$\lambda \longmapsto E^\lambda$$

where

$$NS(A) = \operatorname{Pic} A / \operatorname{Pic}^0 A$$

Then we can regard E^λ as a skew-symmetric 2-form on $H_1(A(\mathbb{C}), \mathbb{Z})$

Mumford (pg 237) proves

$$E^\wedge : H_1(A(\mathbb{C}), \mathbb{Z}) \times H_1(A(\mathbb{C}), \mathbb{Z}) \longrightarrow \mathbb{Z} \ni n$$

$$\downarrow \qquad\qquad \downarrow \qquad\quad \downarrow$$

$$T_\ell(A) \times T_\ell(A) \longrightarrow T_\ell\mu \ni \zeta^n$$

$$\zeta = (e^{2\pi i/\ell^n})_n$$

So $e^\lambda(a, a') = \zeta^{-E^\wedge(a, a')}$.

Results about Polarisations

Let $k = \bar{k}$, $p = \mathrm{char}(k) \geq 0$.

Thm 13.4: Let $\alpha : A \longrightarrow B$ be an isogeny of degree prime to $\mathrm{char}(k)$ and $\lambda \in NS(A)$.

Then, $\lambda = \alpha^*(\lambda')$, for $\lambda' \in NS(B)$

$\iff \forall \ell \mid \deg(\alpha)$, ℓ prime, there exists a skew-symmetric form $f : T_\ell B \times T_\ell B \longrightarrow T_\ell\mu$ such that $e^\lambda(a, a') = f(\alpha(a), \alpha(a'))$, $\forall a, a' \in T_\ell A$.

Proof: Mike 1986, Thm 16.4. □

Corollary 13.5: $\ell \neq \mathrm{char}(k)$

$\lambda \in NS(A)$ is divisible by ℓ^n $\iff$ e^λ is divisible by ℓ^n in $\mathrm{Hom}(\Lambda^2 T_\ell A, T_\ell \mu)$

Proof: Apply Thm 13.4 with $\alpha = \ell^n$.

Lemma 13.7: Let $\mathcal{P}$ be the Poincaré sheaf on $A \times A^\vee$.

Then

$$e^{\mathcal{P}}((a,b),(a',b')) = e(a,b')/e(a',b)$$

$\forall\, a, a' \in T_\ell A, \quad b, b' \in T_\ell A^\vee$.

Proof: Milne 1986, 16.7.

Use $(1+\lambda_\ell)^* \mathcal{P} \cong m^* \mathcal{L} \otimes p^* \mathcal{L}^{-1} \otimes q^* \mathcal{L}^{-1}$. □

Proposition 13.6: Assume $\mathrm{char}(k) \neq \ell, 2$.

Then a homomorphism $\lambda : A \to A^\vee$ is $\lambda = \lambda_{\mathcal{L}}$ for some $\mathcal{L} \in \mathrm{Pic}\, A$ $\iff$ e^λ is skew-symmetric.

Proof: ($\Rightarrow$) ✓

($\Leftarrow$) e^λ is skew-symmetric.

Define $\mathcal{L} := (1 \times \lambda)^* \mathcal{P}$

Then $\forall\, a, a' \in T_\ell A$,

$$e(a, \lambda_{\mathcal{L}}(a')) = e^{\mathcal{L}}(a, a')$$

$$= e^{(1\times\lambda)^*\mathcal{P}}(a, a')$$

$$= e^{\mathcal{P}}((a, \lambda(a)), (a', \lambda(a'))) = \frac{e(a, \lambda(a'))}{e(a', \lambda(a))}$$

(13.2(c)) (Lemma)

$$= \frac{e^\lambda(a,a')}{e^\lambda(a',a)} \overset{\text{skew-symmetric}}{=} e^\lambda(a,a')^2 = e(a, 2\lambda(a')).$$

$\Rightarrow 2\lambda = \lambda_L$ (since e is non-degenerate)

So by Corollary 13.5, $\lambda_L = 2\lambda_{L'}$ for some $L' \in \mathrm{Pic}\, A$.

$\Rightarrow \lambda = \lambda_{L'}$. □

Dfn: For a polarisation $\lambda : A \longrightarrow A^\vee$, define

$$e^\lambda : \ker(\lambda) \times \ker(\lambda) \longrightarrow \mu_m$$
$$(a, a') \longmapsto e_m(a, \lambda(b))$$

where

m kills $\ker(\lambda)$ and $b \in A$ s.t. $mb = a'$.

Remark: One needs to check this is independent of the choice of m and b.

Note: e^λ is skew-symmetric.

Prop 13.8: $\alpha : A \longrightarrow B$ is an isogeny of degree prime to p, $\lambda : A \longrightarrow A'$ a polarisation. Then

$\lambda = \alpha^* \lambda'$, $\lambda' : B \longrightarrow B^\vee$ a polarisation $\iff$ $\ker(\alpha) \subseteq \ker(\lambda)$, e^λ is trivial on $\ker(\alpha) \times \ker(\alpha)$

Note: If $\lambda = \alpha^* \lambda'$, then

$$\deg(\lambda) = \deg(\lambda') \cdot \deg(\alpha)^2$$

$$\alpha^* \lambda' = \alpha^\vee \circ \lambda' \circ \alpha$$

Corollary 13.10: A is an abelian variety, $\lambda : A \to A^\vee$ is a polarisation with $(\deg(\lambda), p) = 1$.
Then A is isogenous to a principally polarised abelian variety.

Proof: Fix $\ell \mid \deg(\lambda)$ prime.
Choose a subgroup $N \subseteq \ker(\lambda)$ of order ℓ.
Let $\alpha : A \to A/N =: B$
N is cyclic and e^λ is skew-symmetric
$\Rightarrow e^\lambda$ is trivial on $N \times N$.
$\Rightarrow B$ has a polarisation of degree $\deg(\lambda)/\ell^2$
(by Prop 13.8). □

Corollary 13.11: Let λ be a polarisation of A such that $\ker(\lambda) \subseteq A[m]$ for some $(m, p) = 1$.
If there exists $\alpha : A \to A$ such that $\alpha(\ker(\lambda)) \subseteq \ker(\lambda)$ and $\alpha^\vee \circ \lambda \circ \alpha = -\lambda$ on $A[m^2]$, then $A \times A^\vee$ is principally polarised.

Proof: Mike 1986. □

Theorem 13.2 (Zarhin's Trick)

For any abelian variety A, $(A \times A^\vee)^4$ is principally polarised.

Proof: Fix $\lambda : A \to A^\vee$ a polarisation.

Assume $\ker(\lambda) \subseteq A[m]$, $(m, p) = 1$.

There exist $a, b, c, d \in \mathbb{Z}$ such that

$$a^2 + b^2 + c^2 + d^2 = m^2 - 1 \equiv -1 \pmod{m^2}.$$

Then

$$\alpha = \begin{pmatrix} a & -b & -c & -d \\ b & a & d & -c \\ c & -d & a & b \\ d & c & -b & a \end{pmatrix}$$ works.

□

Corollary 13.3: Let k be a finite field.

Then for each $g \in \mathbb{Z}$, there exist only finitely many isomorphism classes of abelian varieties of dim g / k.

Proof: Let A/k be an abelian variety of dimension g.

Then by Thm 13.2, $(A \times A^\vee)^4$ is an abelian variety of dimension $8g$ with a principal polarisation.

By Thm 11.2 $\Rightarrow$ There are only finitely many isomorphism classes of AV's with a principal polarisation of fixed dimension.

Further, $(A \times A^\vee)^4$ has finitely many direct factors. (Thm 15.3).

□