Abstract In this talk the definition of polarization of abelian variety and Weil paring will be given. After introducing some proposition of Weil paring, we will show the Zarhin’s trick about principal polarization.

1 Notation

Let $X$ and $Y$ be abelian varieties over a base scheme $\text{Spec } k$ with dimension $g$, where $k$ is a field. Denote $X^t := \text{Pic}^0_{X/k}$ be the dual of $X$.

2 Polarization

Lemma 2.1. Let $f : X \to Y$ be a homomorphism. Let $M$ be a line bundle on $Y$ and define $L := f^*M$. Then $\varphi_L : X \to X^t$ equals the composition.

$$
X \xrightarrow{f} Y \xrightarrow{\varphi^M} Y^t \xrightarrow{f^t} X^t
$$

If $f$ is an isogeny and $M$ is non-degenerate then $L$ is non-degenerate too, and $\text{rank}(K(L)) = \text{deg}(f)^2 \times \text{rank}(K(M))$. Recall that a line bundle $L$ is non-degenerate if $K(L)$ is finite.

Lemma 2.2. Let $X$ be an abelian variety over a field $k$, let $\lambda : X \to X^t$ be a homomorphism, and consider the line bundle $M := (id, \lambda)^* \mathcal{P}_X$ on $X$. Then $\varphi_M = \lambda + \lambda^t$. In particular, if $\lambda$ is symmetric then $\varphi_M = 2\lambda$.

Proof. From Lemma 2.1 it is known:

$$
\varphi_M = (id, \lambda)^t \circ \varphi_{\mathcal{P}_X} \circ (id, \lambda),
$$
associated with the fact:

\[ \varphi_{\mathcal{P}_X} : X \times X' \to X' \times X^{\nu} \]

\[ (x, \xi) \to (\xi, \kappa_X(x)) \]

we see that \( \varphi_M = \lambda + \lambda^t \).

\[ \Box \]

**Proposition 2.3.** Let \( X \) and \( \lambda \) be above, then TFAE

(i) \( \lambda \) is symmetric

(ii) there exists a field extension \( k \subset K \) and a line bundle \( L \) on \( X_K \) such that \( \lambda_K = \varphi_L \)

(iii) there exists a finite separable field extension \( k \subset K \) and a line bundle \( L \) on \( X_K \) such that \( \lambda_K = \varphi_L \)

**Proof.** Clearly that (iii) implies (i) and (ii).

Now if \( \lambda \) is symmetric, denote \( M := (id, \lambda)^* \mathcal{P}_X \) and \( N := M^2 \). Since we have \( X[2] \subset X[4] \) as totally isotropic subspace. With Corollary (8.11) in [B.E], there exist line bundle \( L \) on \( X_k \) such that \( N \) is the pull back of \( L \) along \( X_k \), then \( 4\lambda_k = \varphi[2]\ast L = 4\varphi_L \). Considering that \( [4]_X \) is an epimorphism, and \( [4]_X \circ \lambda = \lambda \circ [4]_X \), it follows that \( \lambda_k = \varphi_L \). (ii) is right with \( K = k \).

In order to have (ii) implies (iii), since \( P(\lambda) := \varphi^{-1}(\lambda) \) is closed subscheme of \( Pic_{X/k} \), where \( \varphi : Pic_{X/k} \to Hom_{AV}(X, X^t) \). For any line bundle \( L \) on \( X_k \), it defines a isomorphism of \( k \)-schemes \( (X^t)_k \simeq P(\lambda)_k \) by \( x \to [t_x^*L] \), then \( P(\lambda)_k \) is a geometrically integeral \( k \)-scheme, so (iii) satisfied.

With this proposition, one can finish the unfinished part of Wessel about the exact sequence:

\[ 0 \to Pic^0_{X/k} \to Pic_{X/k} \to Hom^{sym}_{AV}(X, X^t) \to 0. \]

Moreover, if \( \lambda \) above is also isogeny, there are more can be said.

**Proposition 2.4.** Let \( \lambda : X \to X^t \) be symmetric homomorphism, \( M := (id, \lambda)^* \mathcal{P}_X \). Let \( k \subset K \) be a field extension and let \( L \) be a line bundle on \( X_K \) with \( \lambda_K = \varphi_L \), then

(i) \( \lambda \) is isogeny \( \iff \) \( L \) is non-degenerate \( \iff \) \( M \) is non-degenerate.

(ii) if \( \lambda \) is isogeny then \( L \) is effective iff \( M \) is effective.
L is ample ⇐⇒ M ample.

Note that a line bundle on $X$ is ample iff it is non-degenerate and effective. With the proposition above, we have the definition of polarization:

**Definition 2.1.** Let $X$ be an abelian variety over a field $k$. A polarization of $X$ is an isogeny $\lambda: X \to X^t$ that satisfies the equivalent conditions below:

(i) $\lambda$ is symmetric isogeny and the line bundle $(id, \lambda)^*P_X$ on $X$ is ample;

(ii) $\lambda$ is symmetric isogeny and the line bundle $(id, \lambda)^*P_X$ on $X$ is effective;

(iii) there exists a field extension $k \subset K$ and an ample line bundle $L$ on $X_K$ such that $\lambda_K = \varphi_L$;

(iv) there exists a finite separable field extension $k \subset K$ and a ample line bundle $L$ on $X_K$ such that $\lambda_K = \varphi_L$.

Moreover, if a polarization is an isomorphism, then we call it a principal polarization.

**Example 2.1.** [Mil] For $E$ an elliptic curve over a field $k$ with $char k = 0$, then $NS(E) = \mathbb{Z}$, for each integer $d$, there is a unique polarization of degree $d^2$; it is $\varphi_L$ where $L = \mathcal{O}_E(D)$ for $D$ any effective divisor of degree $d$.

**Proof.** Since $deg \varphi = rank K(L) = rank \{x \mid t_x^*L \simeq L\}$. Assume that $D = \sum_{i=1}^d P_i$, we only need to calculate $rank \{x \mid t_x^*L \simeq L\} = rank \{x \mid t_x^*D \sim D\}$, which means

$$\sum_{i=1}^d [P_i - x] \sim \sum_{i=1}^d P_i$$

( $\iff$ ) $\sum_{i=1}^d [P_i - x] - \sum_{i=1}^d P_i \sim 0$

( $\iff$ ) $[d]x = O$, $O$ is the zero element in the group $E$. ($E \simeq Pic^0(E)$)

Then $x \in E[d]$ combine with the fact that $|E[d]| = d^2$, we are done. 

A new notation will be introduced in the following proposition which will be useful in the proof of Zarhin’s Trick.

**Proposition 2.5.** Let $f: X \to Y$ be an isogeny. If $g := Y \to Y^t$ is a polarization of $Y$, then $f^*g = f^t \circ g \circ f$ is a polarization of $X$ of degree $\text{degree}(f^*g) = \text{deg}(f)^2 \cdot \text{deg}(g)$. 

3
The proof is trivial after combine the Lemma 2.1 and the equivalent definition of polarization.

In Wessel’s talk we discussed commutator paring and its proposition, similarly we will define Weil pairing which will play a vital role in proving Zarhin’s Trick.

**Definition 2.2.** Define pairing:

\[ e_f : \ker(f) \times \ker(f^t) \to \mathbb{G}_m \]

to be perfect linear pairing given by \( e_f(x, y) = y(x) \) by identifying \( \ker(f^t) \simeq \ker(f)^P \), in particular, if \( f := [n]_X \), then the paring become

\[ e_n : X[n] \times X^t[n] \to \mu_n \]
called Weil paring. More over if \( \lambda : X \to X^t \) be a homomorphism. Define

\[ e^\lambda_n : X[n] \times X[n] \to \mu_n \]
to be \( e^\lambda_n(x_1, x_2) = e_n(x_1, \lambda(x_2)) \).

**Remark 2.6.** For \( L \) a line bundle, we have \( e_{\varphi L} = e^L \), where the \( e^L \) is commutative pairing of theta group.

**Proposition 2.7.** Let \( f : X \to Y \) be an isogeny of abelian varieties. Let \( \kappa_X : X \to X^{\text{tt}} \) be the canonical isomorphism.

(i) For any \( k \)-scheme \( T \) and points \( x \in \ker(f)(T) \) and \( \eta \in \ker(f^t)(T) \) we have the relation

\[ e_f(\eta, \kappa_X(x)) = e_f(x, \eta)^{-1}; \]

(ii) for any integer \( n \geq 1 \), the diagram

\[
\begin{array}{ccc}
X[n] \times Y^t[n] & \xrightarrow{id \times f^t} & X[n] \times X^t[n] \\
\downarrow f \times id & & \downarrow e_n \\
Y[n] \times Y^t[n] & \xrightarrow{e_n} & \mu_n
\end{array}
\]

is commutative, i.e. for any \( T \) as a \( k \)-scheme, \( x \in X[n](T), \eta \in Y^t[n](T) \) then \( e_n(f(x), \eta) = e_n(x, f^t(\eta)) \);
(iii) for \( g : Y \to Z \) be isogenies, and define \( h := g \circ f : X \to Z \). Then the diagrams:

\[
\begin{array}{ccc}
\ker(f) \times \ker(f^t) & \xrightarrow{e_f} & \mathbb{G}_m \\
\downarrow i & & \downarrow f & & \downarrow i \\
\ker(h) \times \ker(h^t) & \xrightarrow{e_h} & \mathbb{G}_m
\end{array}
\]

\[
\begin{array}{ccc}
\ker(g) \times \ker(g^t) & \xrightarrow{e_g} & \mathbb{G}_m \\
\end{array}
\]

commute, where the label \( i \) are the inclusion homomorphisms, i.e. for any \( T \) a \( k \)-scheme, \( x \in \ker(f)(T) \) and \( \eta \in \ker(h^t)(T) \) then \( e_f(x, g^t(\eta)) = e_h(i(x), \eta) \), for \( x' \in \ker(h)(T) \) and \( \xi \in \ker(g^t)(T) \), then \( e_g(f(x'), \xi) = e_h(x', i(\xi)) \).

**Proof.** (ii) Identify \( Y^t[n] \) with \( Y[n]^D := \text{Hom}(Y[n], \mathbb{G}_m) \) we have

\[
e_n(f(x), \eta) = \eta \cdot f(x) = e_n(x, f^t(\eta))
\]

by the property of \( f^t \).

(iii)

\[
e_{g \circ f}(i(x), \eta) = \eta(i(x)) = g^t(\eta)(x) = e_f(x, g^t(\eta))
\]

this gives the first equality. For the second one, considering the \( f^t \circ g^t \) and apply the first equality to it with (i), it gives:

\[
e_{g \circ f}(x', \xi)^{-1} = e_{f^t \circ g^t}(\xi, \kappa_X(x')) = e_{g^t}(\xi, f(x')) = e_g(f(x'), \xi)^{-1}
\]

which ends the proof.

**Proposition 2.8.** Let \( \lambda : X \to X^t \) be a symmetric isogeny, and let \( f : X \to Y \) be an isogeny. There exist a symmetric isogeny \( \nu : Y \to Y^t \) such that the diagram

\[
\begin{array}{ccc}
X & \xrightarrow{\lambda} & X^t \\
\downarrow f & & \downarrow f^t \\
| & & | \\
Y & \xrightarrow{\nu} & Y^t
\end{array}
\]

commute if and only if \( \ker(f) \subset \ker(\lambda) \) and is totally isotropic with respect to the pairing \( e_\lambda : \ker(\lambda) \times \ker(\lambda) \to \mathbb{G}_m \). If \( \nu \) exists then it is unique. Moreover, \( \nu \) is polarization iff \( \lambda \) is polarization.
Remark 2.9. The proof of existence comes from Wessel’s last talk that if $M := (\text{id} \times \lambda) \ast \mathcal{P}_X$, Then $\text{Ker}(f) \times \text{Ker}(f)$ define an action on $M$ which gives us a line bundle $M = (f \times f)^* N$. Then $N$ on $Y \times Y$ induces a homomorphism $\nu$ such that $N = (\text{id} \times \nu)^* \mathcal{P}_Y$, the polarization part comes from the Lemma 2.1.

Finally, we can try to prove the Zarhin’s Trick after we introducing some notation from Matrix with integral coefficients.

Definition 2.3. Let $\alpha = (a_{ij})$ be an $r \times s$ matrix with integral coefficients. Define a homomorphism $[\alpha]_X : X^s \to X^r$ respect to $\alpha = (a_{ij})$ as follow:

$$[\alpha]_X(x_1, \ldots, x_s) = (a_{11}x_1 + a_{12}x_2 + \ldots + a_{1s}x_s, \ldots, \sum_{j=1}^s a_{ij}x_j, \ldots, a_{r1}x_1 + \ldots + a_{rs}x_s)$$

Remark 2.10. (i) $r=s=1$, this is just the multiplication by $n$ maps. The matrix $(1,1)$ gives the group law on $X$.

(ii) $[\beta]_X \circ [\alpha]_X = [\beta \cdot \alpha]_X$, if $[\beta]_X$ is associated to an $l \times r$ matrix $\beta = (b_{ij})$.

(iii) $f : X \to Y$ a homomorphism of AVs, then for any $r \times s$ integral matrix $\alpha_{ij}$,

$$\left( f, \ldots, f \right) [\alpha]_X = [\alpha]_Y \left( f, \ldots, f \right)$$

Lemma 2.11. For $X$ an abelian variety with dimension $g$,

(i) Let $\alpha = (a_{ij}) \in M_r(\mathbb{Z})$, then the homomorphism $[\alpha]_X$ has degree $\deg[\alpha] = \det(\alpha)^{2g}$.

(ii) Let $\beta$ be an $r \times s$ integral matrix. then $([\beta]_X)^t = [\beta^t]_{X^t}$. Where the $\beta^t$ denote the transpose of the matrix $\beta$.

Theorem 2.12. (Zarhin’s Trick) Let $X$ be an abelian variety over a field $k$. Then $X^4 \times (X^t)^4$ carries a principal polarization.

Proof. Suppose there is another abelian variety $Y$ (we will see it is actually $X^4$), a polarization $\mu : Y \to Y^t$ and the endormorphism $\alpha : Y \to Y$, consider the isogeny:

$$f : Y \times Y \to Y \times Y^t$$

$$(y_1, y_2) \mapsto (y_1 - \alpha(y_2), \mu(y_2))$$
with $\text{Ker}(f) = \{(\alpha(y), y) | y \in \text{Ker}(\mu)\}$ and $\deg f = \#\text{Ker}(f) = \#\text{Ker}(\mu) = \deg \mu$. We want to know when the polarization: $\lambda := \mu \times \mu : Y \times Y \to Y^t \times Y^t$ descends to a polarization on $Y \times Y^t$ via the isogeny $f$, i.e:

$$
\begin{align*}
Y \times Y & \xrightarrow{\lambda} Y^t \times Y^t \\
\downarrow f & \quad \uparrow f^t \\
Y \times Y^t & \xrightarrow{\exists \nu \in \text{Ker}(\mu)} Y^t \times Y
\end{align*}
$$

According to Proposition 2.8, such a polarization exists iff

(i) $\text{Ker}(f) \subset \text{Ker}(\lambda)$ and is totally isotropic with respect to the pairing $e_{\lambda}$, i.e.

$$
e_{\lambda}((\alpha(y_1), y_1), (\alpha(y_2), y_2)) = 1, \ \forall \ y_1, \ y_2 \in \text{Ker}(\mu)
\iff e_{\mu}(\alpha(y_1), \alpha(y_2)) \cdot e_{\mu}(y_1, y_2) = 1 \ \forall \ y_1, \ y_2 \in \text{Ker}(\mu) \tag{1}
$$

(ii) $\lambda$ is a polarization of $Y^t \times Y$.

Only part (i) needs to be verified, Since $\alpha(\text{Ker}(\mu)) \subset \text{Ker}(\mu) \iff \exists$ an endormorphism $\beta : Y^t \to Y^t$ such that $\beta \circ \mu = \mu \circ \alpha$ ($\text{Ker}(\mu) \subset \text{Ker}(\mu \circ \alpha)$).

With proposition 2.7 we have

$$
e_{\mu}(\alpha(y_1), \alpha(y_2)) = e_{\mu \circ \alpha}(y_1, \alpha(y_2)) = e_{\beta \circ \mu}(y_1, \alpha(y_2)) = e_{\mu}(y_1, \beta^t \alpha(y_2))
$$

then equation (1) becomes $e_{\mu}(y_1, (1 + \beta^t \alpha)(y_2)) = 1, \ \forall \ y_1, \ y_2 \in \text{Ker}(\mu)$. The fact that $e_{\mu}$ is a perfect pairing means

$$
(1 + \beta^t \alpha)(y_2) = 1, \ \forall \ y_2 \in \text{Ker}(\mu) \tag{2}
$$

Now proper homomorphism $\alpha$ and $\beta$ will be constructed to make $Y \times Y^t$ carries a principal polarization in situation $Y = X^4$: Let

1. $\mu = \varphi^4 := \varphi \times \varphi \times \varphi \times \varphi$, where $\varphi : X \to X^t$ a polarization on $X$. $\alpha = [\alpha]_X$ given by integral matrix (so $\varphi^4 \circ [\alpha]_X = [\alpha]_{X^t} \circ \varphi^4$);
2. \( \beta = [\alpha]_{X^t} \), then \( \beta^t = [\alpha^t]_X \)

3. \([Id_4]\) denote the Identity matrix in \( M_4(\mathbb{Z}) \)

So the condition(2) becomes \([Id_4 + \alpha^t \alpha] \) is trivial on \( Ker(\mu) = Ker(\varphi^4) \). As \( Ker(\varphi) \subset X[m] \) for some \( m \in \mathbb{Z}_+ \), we can end the proof if \([Id_4 + \alpha^t \alpha] \equiv 0 \mod m \) with specific \([\alpha]_X \). From the well know fact that every integer can be write as the sum of four squares. In particular,

\[
m - 1 = a^2 + b^2 + c^2 + d^2, \quad a, b, c, d \in \mathbb{Z}
\]

Let \([\alpha]_X \) be the homomorphism associated with the integral matrix bellow:

\[
M = \begin{bmatrix}
a & -b & -c & -d \\
- b & a & -d & c \\
- c & - d & a & -b \\
- d & - c & b & a
\end{bmatrix}
\]

We are done.

\[\square\]

References
