

Module Action Note

徐铮

2025.6.27

目录

1	Order and Modules	2
1.1	Gorenstein Order and Modules	2
1.2	Finitely Presented Torsion-Free Modules	2
2	Module Isogenies	4
2.1	Module Isogenies	4
2.2	Polarized and Isogenies	6
3	Symmetric Monoidal Category	7
4	Module Action	8
4.1	Power Objects in an Abelian Category (Definition of Module Action)	8
4.2	Module Action on Oriented Abelian Varieties	10
4.3	Projective Module Action on Abelian Varieties (Keep Abelian Varieties)	11
4.4	Module Action on Dimension 1 (Not require projective module)	12
4.5	Polarization of Module Action on Abelian Varieties	14
5	Copower Objects of Module Actions (Another Action: Tensor)	18
6	Computing Module Action	19
6.1	Computing Module Action: Kernel Approach	19
6.2	Computing Module Action: Clapoti Approach	20
6.3	Computing Action on Isogenies	20
7	Module Action For R, \mathcal{O}-bimodule	20
7.1	Supersingular Case: R , \mathcal{O} -bimodule	20
7.2	Special Case: Weil's Restriction	21
7.3	Scholten's Construction: From Bottom to Top	22
8	Supersingular Isogeny Path Problem and Module Action Inversion	24
9	\otimes-MIKE: Tensor Module Isogeny Key Exchange	26

1 Order and Modules

1.1 Gorenstein Order and Modules

In this section, we assume the order R is an order in quadratic imaginary field with discriminant Δ_R , the quadratic imaginary field is $K = R \otimes_{\mathbb{Z}} \mathbb{Q}$.

Let \mathcal{O}_K be the maximal order of K , and S be an order such that $R \subseteq S \subseteq \mathcal{O}_K$, we denote the conductor of R relative to S by $f_{S/R} = [S : R]$, and the conductor ideal is defined as $\mathfrak{f}_{S/R} = f_{S/R}S$. Moreover, we have $\sqrt{\Delta_R} = f_{S/R}\sqrt{\Delta_S}$, $R = \mathbb{Z} + f_{S/R}S$.

If R is Gorenstein, then every torsion free R -module is reflexive (i.e. $M^{\vee\vee} \cong M$).

Let M be a finitely generated torsion free R -module, we have the exact sequence:

$$0 \longrightarrow M \longrightarrow V \longrightarrow T \longrightarrow 0$$

where V is $\text{Env}(M)$, the vector space over K , T is torsion R -module.

Then there exists a long exact sequence:

$$\cdots \longrightarrow \text{Tor}_2^R(K/R, T) \longrightarrow \text{Tor}_1^R(K/R, M) \longrightarrow \text{Tor}_1^R(K/R, V) \longrightarrow \text{Tor}_1^R(K/R, T) \longrightarrow \cdots$$

For T is torsion R -module, we have $\text{Tor}_2^R(K/R, T) = 0$. Furthermore, since V is vector space over K , K is flat R -module, we have $\text{Tor}_1^R(K/R, V) = 0$. Overall, we obtain $\text{Tor}_1^R(K/R, M) = 0$.

From the exact sequence $0 \rightarrow R \rightarrow K \rightarrow K/R \rightarrow 0$, we have the long exact sequence:

$$\cdots \longrightarrow \text{Tor}_1^R(K/R, M) \longrightarrow R \otimes_R M \longrightarrow K \otimes_R M \longrightarrow \cdots$$

Since $\text{Tor}_1^R(K/R, M) = 0$, we have $M \hookrightarrow K \otimes_R M$. We define the rank of M in vector space $V = K \otimes_R M$ by the dimension of V ($\dim_K(V)$).

1.2 Finitely Presented Torsion-Free Modules

1. R is Dedekind domain:

- A finitely presented R -module is torsion-free if and only if it is projective.
- Every finitely presented projective R -module is isomorphic to a finite direct sum of invertible ideals.

2. R is an order in imaginary quadratic field:

- Let M be a finitely generated torsion free R -module of rank g . Then there is a decomposition $M \cong I_1 \oplus I_2 \oplus \cdots \oplus I_g$, where $R \subseteq \mathcal{O}(I_1) \subseteq \mathcal{O}(I_2) \subseteq \cdots \subseteq \mathcal{O}(I_g) \subseteq K$, $\mathcal{O}(I) = \{x \in K \mid xI \subseteq I\}$ (I is invertible in $\mathcal{O}(I)$).
- Furthermore, the isomorphism class of M only depend on $\mathcal{O}(I_i)$, class of $I_1 I_2 \cdots I_g$, which is an invertible $\mathcal{O}(I_g)$ -ideal.

3. R is maximal order in quaternion algebra:

- A finitely presented left R -module is torsion-free if and only if it is projective.

- Every finitely presented projective left R -module is isomorphic to a finite direct sum of left ideals.
- A finitely presented projective left \mathcal{O} -module of rank at least 2 is free.

Remark 1 It means there exists a basis $\{x_1, \dots, x_g\}$ of $V = M \otimes_R K$ such that $M = I_1 x_1 \oplus I_2 x_2 \oplus \dots \oplus I_g x_g$, where $K = M \otimes \mathbb{Q}$ and I_i are ideals in R .

Defintion 1 (Conductor) M is defined as above, we define the conductor of M relative to R as $f_{M/R} = f_{\mathcal{O}(I_g)/R}$, which we call conductor gap.

We say M is horizontal if $f_{M/R} = 1$, in this case, M is projective R -module (for M is sum of invertible ideals of R , and invertible ideals are projective).

Theorem 1 $M_2 \subseteq M_1$ are finitely generated torsion free R module and have the same rank, then $\#M_1/M_2 = \#M_2^\vee/M_1^\vee$.

Proof. If R is dedekind domain or maximal order in quaternion algebra, then M_1, M_2 are projective.

Consider the exact sequence $0 \rightarrow R \rightarrow K \rightarrow K/R \rightarrow 0$, we have the long exact sequence:

$$0 \longrightarrow \text{Hom}_R(M, R) \longrightarrow \text{Hom}_R(M, K) \longrightarrow \text{Hom}_R(M, K/R) \longrightarrow \text{Ext}_R^1(M, R) \longrightarrow \text{Ext}_R^1(M, K) \longrightarrow \dots$$

Since K is injective R -module, then $\text{Ext}_R^1(M, K) = 0$. Moreover, if M is torsion, $\text{Hom}_R(M, K) = 0$, so $\text{Hom}_R(M, K/R) \cong \text{Ext}_R^1(M, R)$.

For $T = M_1/M_2$ is torsion R -module, from the exact sequence $0 \rightarrow M_2 \rightarrow M_1 \rightarrow M_1/M_2 \rightarrow 0$, we have the long exact sequence:

$$0 \longrightarrow \text{Hom}_R(M_1/M_2, R) = (M_1/M_2)^\vee \longrightarrow \text{Hom}_R(M_1, R) = M_1^\vee \longrightarrow \text{Hom}_R(M_2, R) = M_2^\vee \longrightarrow \text{Ext}_R^1(M_1/M_2, R) \longrightarrow \text{Ext}_R^1(M_1, R) \longrightarrow \dots$$

Since M_1 is torsion free, then M_1 is projective, we have $\text{Ext}_R^1(M_1, R) = 0$, and for $\text{Hom}_R(M_1/M_2, R) = 0$, we get that $\text{Ext}_R^1(M_1/M_2, R) \cong \text{Hom}_R(M_2, R)/\text{Hom}_R(M_1, R)$.

Finally, we obtain $\text{Hom}_R(M_1/M_2, K/R) \cong \text{Ext}_R^1(M_1/M_2, R) \cong \text{Hom}_R(M_2, R)/\text{Hom}_R(M_1, R) = M_2^\vee/M_1^\vee$.

Moreover, since M_1/M_2 is isomorphic to product of R/I , for any R/I , we have:

$$\begin{aligned} \Phi : \text{Hom}_R(R/I, K/R) &\rightarrow I^{-1}/R \\ \varphi &\rightarrow \varphi(1+I) + R \end{aligned}$$

For $I(\varphi(1+I)) \subseteq \varphi(I) \subseteq R$, we have $\varphi(1+I) \in I^{-1}$, which means Φ is well-defined.

If $\Phi(\varphi) = 0$, then $\varphi(1+I) \in R$, for any $\bar{r} \in R/I$, $\varphi(r+I) \in R$, which means $\varphi = 0$. Hence, Φ is injective.

For any $\bar{a} \in I^{-1}$, we define $\varphi_a \in \text{Hom}_R(R/I, K/R)$ by $\varphi_a(\bar{r}) = \bar{a}r$, then φ_a is well-defined, and $\Phi(\varphi_a) = \varphi_a(1+I) = \bar{a}$. It shows Φ is surjective.

From above, we have $\text{Hom}(R/I, K/R) \cong I^{-1}/R$, then $\#\text{Hom}_R(R/I, K/R) = \#I^{-1}/R = \#R/I$.

Hence, $\#\text{Hom}_R(M_1/M_2, K/R) = \#M_1/M_2$, and $\#M_1/M_2 = \#M_2^\vee/M_1^\vee$.

If R is an order in imaginary quadratic field, then we have any finitely generated R module isomorphic to direct sum of ideals in R . Hence we can reduce the case to ideals. For any R -ideal I , we have $\text{Hom}_R(I, R) \cong I^{-1}$.

$$\begin{aligned} \varphi : I^{-1} &\rightarrow \text{Hom}_R(I, R) \\ a &\rightarrow \varphi_a \quad \varphi_a : b \rightarrow ab \end{aligned}$$

If $\varphi_a = 0$, it implies $ab = 0$ for any $b \in I$, then $a = 0$, φ is injective; for any $f \in \text{Hom}_R(I, R)$, we choose $a = b^{-1}f(b)$ which is independent of choice of b ($b^{-1}f(b) = c^{-1}f(c)$). Therefore, a is the preimage of f , and φ is surjective.

Now we consider two R -ideals $I_1 \subseteq I_2$, we have $I_1^\vee/I_2^\vee \cong I_1^{-1}/I_2^{-1}$. Hence, $\#I_2/I_1 = \#(R/I_1)/(R/I_2) = \#(I_1^{-1}/R)/(I_2^{-1}/R) = \#I_1^{-1}/I_2^{-1} = \#I_1^\vee/I_2^\vee$. \square

2 Module Isogenies

2.1 Module Isogenies

Defintion 2 (Module Isogenies) Let $\varphi : M_2 \rightarrow M_1$ be a morphism between finitely generated torsion free R -module, the following are equivalent:

- φ is a monomorphism with finite cokernel $M_1/\varphi(M_2)$
- φ is a monomorphism and M_1, M_2 have the same rank
- φ has finite cokernel and M_1, M_2 have the same rank

If these conditions satisfied, we call φ by module isogeny with degree $\#M_1/\varphi(M_2)$.

We will define the Hermitian modules, where there are some R -antilinear forms.

For any bilinear map of M corresponds to a morphism between M and M^\vee , we give the corresponding (it should be noted that in this section the bilinear map is R -linear on the left side, R -antilinear on the right side):

let $H : M \times M \rightarrow R$ be a bilinear map, we can define $\varphi_H : M \rightarrow M^\vee = \text{Hom}_{\bar{R}}(M, R)$, which sends x to the morphism $H(x, \cdot)$.

On the contrary, if there is a morphism φ from M to M^\vee , we can define a bilinear map as following:

$$\begin{aligned} H : M \times M &\rightarrow R \\ (x, y) &\rightarrow \varphi(x)(y) \end{aligned}$$

Moreover, if $H(x, y) = \overline{H(y, x)}$, we call H by Hermitian form.

Remark 2 We can also define an Hermitian form of $V = M \otimes_R K$ from H , which denoted by H_K . The Hermitian form $H_K : V \times V \rightarrow K$.

Defintion 3 • **(Non-degenerate and positive-definite)** We say an Hermitian form is non-degenerate if φ_H is monomorphism (i.e. isogeny). If $H(x, x) > 0$ for any $0 \neq x \in M$, we say H is positive-definite. (φ_H is monomorphism iff for any $x \in M$, $H(x, y) = 0$ induced $y = 0$, the non-degenerate of Hermitian form)

- **(Unimodular)** An unimodular positive definite Hermitian module (M, H) is a module M with a Hermitian form H which is positive definite and such that $\varphi_H : M \rightarrow M^\vee$ is isomorphism.
- **(Orthogonal)** Given an Hermitian form $H_K : V \times V \rightarrow K$, we define R -orthogonal of R -lattice $M \subseteq V$ as $M^\perp = \{x \in V \mid H_K(x, y) \in R \ \forall y \in M\}$.
- The Hermitian form H_K called non-degenerate (positive-definite) if H is non-degenerate (positive-definite).
- If H is non-degenerate, there is a isomorphism:

$$\begin{aligned} M^\perp &\rightarrow M^\vee \\ x &\rightarrow H_K(x, \cdot) \end{aligned}$$

Since $M \cong M^{\vee\vee}$, we have $M^{\perp\perp} \cong M$.

- **(Integral)** We say that a non-degenerate Hermitian form $H_K : V \times V \rightarrow K$ is integral on R -lattice $M \subseteq V$ if $M \subseteq M^\perp$. (i.e. H_K can be defined on M , that is $H_M : M \times M \rightarrow R$) Hence $\varphi_{H_M} : M \rightarrow M^\vee$ is $M \hookrightarrow M^\perp \cong M^\vee$. It means (M, H_M) is unimodular iff $M^\perp = M$.

Theorem 2 Now we prove the isomorphism between M^\perp and M^\vee .

Proof.

$$\begin{aligned} \Phi : M^\perp &\rightarrow M^\vee \\ x &\rightarrow H_K(x, \cdot) \end{aligned}$$

If there exist $x, y \in M^\perp$ such that $H_K(x, \cdot) = H_K(y, \cdot)$, then $H_K(x - y, M) = 0$. Since $x - y \in V$, there exists $c \in R$ such $c(x - y) \in M$, then we have $H_K(c(x - y), M) = H(c(x - y), M) = 0$. From the monomorphism of $M \rightarrow M^\vee$, we have $c(x - y) = 0$, which means $x = y$. We obtain Φ is injective.

For any $f \in M^\vee = \text{Hom}(M, R)$, since $M^\vee / \varphi_H(M)$ is finite, there exists $b \in \mathbb{Z}$ such that $bf \in \varphi_H(M)$. It means $bf = H(x, \cdot)$ for some $x \in M$. Therefore, $f = H_K(\frac{1}{b} \otimes x, \cdot)$, the pre-image of f is $\frac{1}{b} \otimes x$.

It should be noted that for any $y \in M$, $f(y) \in R$, then $H_K(\frac{1}{b} \otimes x, y) = \frac{1}{b}H(x, y) = f(y) \in R$, which means $\frac{1}{b} \otimes x \in M^\perp$. Hence, Φ is surjective. \square

Let ψ be a vector space isomorphism between two non-degenerate Hermitian vector space: $(V_1, H_1), (V_2, H_2)$, M_1, M_2 be any lattice of V_1, V_2 and $\psi(M_1) \subseteq M_2$, we have ψ induces an isogeny of module $\psi : M_1 \rightarrow M_2$.

Let ψ' be the adjoint pair of ψ , i.e. $H_2(x, \psi(y)) = H_1(\psi'(x), y)$, for any $x \in M_2, y \in M_1$, it is easily to see $\psi'(M_2^\perp) \subseteq M_1^\perp$. It should be noted that $\psi' : M_2^\perp \rightarrow M_1^\perp$ coincides with the dual isogeny $\hat{\psi}$ from M_2^\vee to M_1^\vee . Hence, we call the isogeny ψ' by adjoint isogeny.

Moreover, if M_1, M_2 are unimodular, which means $M_i = M_i^\perp$, hence the adjoint isogeny ψ' equals to $\hat{\psi}$.

Proposition 1 If M is an integral sublattice of non-degenerate Hermitian space (V, H_K) , $M = \sum_{i=1}^g I_i x_i$, x_i^\perp is the dual basis of (x_1, \dots, x_g) , then we have $M^\perp = \sum_{i=1}^g \overline{(R : I_i)} x_i^\perp$, where $(R : I) = \frac{\bar{I}}{\text{Nrd}(I)}$. Moreover, we have $M^{\perp\perp} = M$.

Proof. It is easily to see that $\sum_{i=1}^g \overline{(R : I_i)} x_i^\perp \subseteq M^\perp$.

We only prove the coefficients of x_1^\perp are in $\overline{(R : I_1)}$. Let a_1 be the coefficients of x_1^\perp in M^\perp , then for any $b_i \in I_i$, we have $H(a_1 x_1^\perp, \sum_{i=1}^g b_i x_i) \in R$, which mean $H(a_1 x_1^\perp, b_1 x_1) \in R$, hence $a_1 \bar{b}_1 \in R$. Since for all $b_1 \in I_1$ we have $a_1 \bar{b}_1 \in R$, we get $a_1 \in \frac{I_1}{\text{Nrd}(I_1)} = \overline{(R : I_1)}$.

From above proof, we have $M^\perp = \sum_{i=1}^g \overline{(R : I_i)} x_i^\perp$.

Since $x_i^{\perp\perp} = x_i$, the coefficients of x_i in $M^{\perp\perp}$ are in $(I^{-1})^{-1} = I$, where $I^{-1} = (R : I) = \frac{\bar{I}}{\text{Nrd}(I)}$. Hence, we have $M^{\perp\perp} = M$. \square

It should be noted that Hermitian modules have orthogonal decomposition: (M_i, H_{M_i}) , where $(M, H_M) = (M_1, H_{M_1}) \oplus (M_2, H_{M_2}) \oplus \dots$, and (M_i, H_{M_i}) are uniquely determined. Moreover, for any module, there is no such property. For instants, I, J are two non-equivalent invertible ideals of R , we have two decompositions: $I \oplus I^{-1}, J \oplus J^{-1}$.

Proposition 2 Let (V, H_K) be a non degenerate hermitian vector space.

If $M_2 \hookrightarrow M_1$ is a sublattice isogeny, then $M_1^\perp \hookrightarrow M_2^\perp$ is the dual isogeny. The Weil-Cartier pairing $H \bmod R : M_1/M_2 \times M_2^\perp/M_1^\perp \rightarrow K/R$ is non-degenerate. In particular, $\#M_1/M_2 = \#M_2^\perp/M_1^\perp$.

Moreover, given a lattice $M \subseteq V$, the Weil pairing $H_K \bmod n : M/nM \times M^\perp/nM^\perp \rightarrow R/nR$ is non-degenerate.

Proof. Firstly, we will prove the pairing is well-defined. For any $m_2 \in M_2, m'_2 \in M_2^\perp$, we have $H(m_2, m'_2) \in R$, which implies $H \equiv 0 \pmod{R}$. Similarly to any $m'_1 \in M_1^\perp, m_1 \in M_1$. Hence, H is well-defined.

The reason for H_K is well-defined same as H .

Secondly, we will prove the non-degenerate of H . If there exists $m'_2 \in M_2^\perp$ such that for any $m_1 \in M_1$, $H(m_1, m'_2) \in R$, then $m'_2 \in M_1^\perp$.

If there exists $m_1 \in M_1$ such that for any $m'_2 \in M_2^\perp$, $H(m_1, m'_2) \in R$, since $M_1 = M_1^{\perp\perp}$, then we have $m_1 \in M_1$.

From above, we prove the pairing H is non-degenerate. Similarly to H_K , special case of multiplication isogeny $[n]$. \square

From now on, we will just say unimodular instead of positive definite unimodular Hermitian.

Proposition 3 Let M_1, M_2 be two finitely presented torsion free R -modules whose relative conductor gap are coprime: $\gcd(f_{M_1/R}, f_{M_2/R}) = 1$. Then $M_1 \otimes_R M_2$ and $\text{Hom}_R(M_1, M_2)$ are torsion free, and $\text{Tor}_1^R(M_1, M_2) = 0$.

Proof. Since for any multiplicative subset S of R , we have $S^{-1}(\text{Tor}_1^R(M_1, M_2)) \cong \text{Tor}_1^{S^{-1}R}(S^{-1}M_1, S^{-1}M_2)$. We choose $S = R \setminus \mathfrak{p}$, where \mathfrak{p} is the prime ideal of R , then we consider the localization of R at \mathfrak{p} .

Since $\gcd(f_{M_1/R}, f_{M_2/R}) = 1$, we have \mathfrak{p} is not in the decomposition of M_1 or M_2 , which means $M_{1,\mathfrak{p}}$ or $M_{2,\mathfrak{p}}$ is direct sums of $R_{\mathfrak{p}}$, hence free $R_{\mathfrak{p}}$ -module (when \mathfrak{p} is coprime to I , $I_{\mathfrak{p}} = R_{\mathfrak{p}}$).

Assume $M_{1,\mathfrak{p}}$ is free $R_{\mathfrak{p}}$ -module, we have $M_{1,\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} M_{2,\mathfrak{p}} \cong M_{2,\mathfrak{p}}^n$, $\text{Hom}_{R_{\mathfrak{p}}}(M_{1,\mathfrak{p}}, M_{2,\mathfrak{p}}) \cong M_{2,\mathfrak{p}}^n$ are torsion free $R_{\mathfrak{p}}$ -modules, $\text{Tor}_1^{R_{\mathfrak{p}}}(M_{1,\mathfrak{p}}, M_{2,\mathfrak{p}}) = 0$.

Therefore, $(M_1 \otimes_R M_2)_{\mathfrak{p}}, (\text{Hom}_R(M_1, M_2))_{\mathfrak{p}}$ are torsion free and $\text{Tor}_1^R(M_1, M_2)_{\mathfrak{p}} = 0$ for any prime ideal \mathfrak{p} .

For commutative algebra, we have $M_1 \otimes_R M_2, \text{Hom}_R(M_1, M_2)$ are torsion free and $\text{Tor}_1^R(M_1, M_2) = 0$. \square

Example 1 If $(M_1, H_1), (M_2, H_2)$ are unimodular Hermitian modules, we have:

$(M_1 \oplus M_2, H_1 \oplus H_2)$ is also a unimodular Hermitian module. If $\gcd(f_{M_1/R}, f_{M_2/R}) = 1$, then $(M_1 \otimes_R M_2, H_1 \otimes_R H_2)$ is also a unimodular Hermitian module.

2. If we define $H_K(x, y) = x\bar{y}$ and $I \subseteq K$ is a fractional R -ideal, then $(I^\perp, H/\text{Nrd}(I))$ is a unimodular Hermitian module, where $I^\perp = \frac{I}{\text{Nrd}(I)} = \overline{(R : I)}$.

Proof. We only prove the unimodular property.

Since $(M_1 \oplus M_2)^\vee \cong M_1^\vee \oplus M_2^\vee$, $(M_1 \otimes_R M_2)^\vee \cong M_1^\vee \otimes_R M_2^\vee$, and $M_i \cong M_i^\vee$, then we have $M_1 \oplus M_2 \cong (M_1 \oplus M_2)^\vee$, $M_1 \otimes_R M_2 \cong (M_1 \otimes_R M_2)^\vee$.

Since $I^\perp = I/\text{Nrd}(I)$, and $I \cong I^\vee$, then we have $I^\perp \cong (I^\perp)^\vee$. \square

2.2 Polarized and Isogenies

Given a finitely presented torsion free R -module M , we say an Hermitian form H on $V = M \otimes_R K$ is a polarization if $M^\perp \subseteq M$ (or H_K is integral on M^\perp). In this case, we say (M, H) is a polarized module. The degree of this polarization is defined to be $\#M/M^\perp$. (This means H is a non-degenerate Hermitian form over M^\perp .)

Moreover, a polarized isogeny $\varphi : (M_2, H_2) \rightarrow (M_1, H_1)$ between two polarized modules is an isogeny $M_2 \hookrightarrow M_1$ such that $\varphi^* H_1 = H_2$, where $\varphi^* H_1(x, y) = H_1(\varphi(x), \varphi(y))$. It should be noted that, in this case, $\varphi^\perp = \varphi^{-1}$.

Generally, an n -isogeny $\varphi : (M_2, H_2) \rightarrow (M_1, H_1)$ between two polarized Hermitian modules is a polarized isogeny $\varphi : (M_2, nH_2) \rightarrow (M_1, H_1)$ i.e. $\varphi^* H_1 = nH_2$.

Let $H : M \times M \rightarrow R$ be a non-degenerate form, if M_1 is a submodule of M such that $H|_{M_1 \times M_1} = 0$, we call M_1 isotropic submodule of M .

Proposition 4 (Isotropic Kernels) Let H be a positive definite Hermitian form on V of dimension g , and M_1 a polarized lattice of V .

- Any polarised submodule $M_2 \subseteq M_1$ gives a polarised isogeny $(M_2, H) \rightarrow (M_1, H)$, with dual isogeny $(M_1^\perp, H) \rightarrow (M_2^\perp, H)$, both induced by the natural inclusions $M_1^\perp \subseteq M_2^\perp \subseteq M_2 \subseteq M_1$. We call $\psi : M_2 \hookrightarrow M_1$ a polarized isogeny for H , and define its degree as $\#M_1/M_2$. This is also the degree of the adjoint isogeny.
- There is a bijection between polarized isogenies for H and isotropic submodules for $H : M_1/M_1^\perp \times M_1/M_1^\perp \rightarrow K/R$, which maps $(M_2, H) \rightarrow (M_1, H)$ such that $M_1^\perp \subseteq M_2^\perp \subseteq M_2$ to M_2^\perp/M_1^\perp . (for any isotropic submodule M/M_1^\perp of M_1/M_1^\perp , we have $M = (M^\perp)^\perp$, and $M_1^\perp \subseteq M \subseteq M_1$. Since $H|_{M \times M}$ is trivial, we have $M \subseteq M^\perp$, and then $M_1^\perp \subseteq M \subseteq M^\perp \subseteq M_1$, which means $(M^\perp, H) \rightarrow (M_1, H)$ is a polarized isogeny.)

From the following diagram, we have $d_1 = d_2 d^2$, where d_i is the degree of $M_i \rightarrow M_i^\perp$, d is the degree of $M_2 \rightarrow M_1$.

$$\begin{array}{ccc}
M_1^\perp & \xrightarrow{d_1} & M_1 \\
\downarrow d & & \uparrow d \\
M_2^\perp & \xrightarrow{d_2} & M_2
\end{array}$$

- If (M_1, H) is unimodular, then the R -orthogonal of M_1 for $\frac{1}{n}H$ is $nM_1^\perp = nM_1$. From above correspondence, the isotropic submodule M_2 of M_1 satisfied $nM_1 = nM_1^\perp \subseteq nM_2^\perp \subseteq M_2 \subseteq M_1$ corresponds to isotropic submodules for Weil pairing $M_1/nM_1 \times M_1/nM_1 \rightarrow \frac{1}{n}R/R$.

Moreover, if $(M_2, \frac{1}{n}H)$ is unimodular ($M_2 = nM_2^\perp$), and there exists an isotropic submodule M such that nM^\perp contains nM_2^\perp , then $nM_1 \subseteq nM_2^\perp = M_2 \subseteq nM^\perp \subseteq M \subseteq M_1$. Since $\#M_1/M_2 = \#nM_2^\perp/nM_1$, we have if $M \neq M_2$, $\#M_1/M < \#nM^\perp/nM_1$, which means nM^\perp is not an isotropic submodule. Therefore, nM_2^\perp is maximal isotropic submodule.

On the contrary, if nM_2^\perp is a maximal isotropic submodule, we have $nM_1 \subseteq nM_2^\perp \subseteq M_2 \subseteq M_1$. Moreover, if $(M_2, \frac{1}{n}H)$ is not unimodular, then $nM_2^\perp \subsetneq M_2$. There exists a submodule M' (polarized) such that $nM_2^\perp \subseteq n(M')^\perp \subseteq M' \subseteq M_2$, which is a contraction. Hence, we have $(M_2, \frac{1}{n}H)$ is unimodular.

Since $M_1 \cong \bigoplus_{i=1}^g I_i x_i$, we have $\#M_1/nM_1 = n^{2g}$. For $\#M_1/M_2 = \#nM_2^\perp/nM_1$, we have $\#M_1/M_2 = n^g$.

Example 2 (Kani's Construction for Hermitian Modules)

$$\begin{array}{ccc}
M_0 & \xrightarrow{\psi_1} & M_1 \\
\downarrow \psi_2 & & \downarrow \psi'_2 \\
M_2 & \xrightarrow{\psi'_1} & M_{12}
\end{array}$$

In the above commutative diagram, $\psi_1 : (M_0, H_0) \rightarrow (M_1, H_1)$, $\psi'_1 : (M_2, H_2) \rightarrow (M_{12}, H_{12})$ are n_1 -isogeny and $\psi_2 : (M_0, H_0) \rightarrow (M_2, H_2)$, $\psi'_2 : (M_1, H_1) \rightarrow (M_{12}, H_{12})$ are n_2 -isogeny. Then $\Psi = \begin{pmatrix} \psi_1 & \hat{\psi}'_1 \\ -\psi_2 & \hat{\psi}'_2 \end{pmatrix} : (M_0 \oplus M_{12}, H_0 \oplus H_{12}) \rightarrow (M_1 \oplus M_2, H_1 \oplus H_2)$ is $n_1 + n_2$ -isogeny.

Similarly, if (M, H_M) is unimodular, there is always a n -isogeny on (M^4, H_M^4) (resp. on (M^2, H_M^2)) if $n = x\bar{x} + y\bar{y}$, $x, y \in R$; resp. on (M, H_M) if $n = x\bar{x}$, $x \in R$.

$$\begin{array}{c}
x : (M, H_M) \rightarrow (M, H_M) \\
m \rightarrow xm
\end{array}$$

Hence $x^*H_M(m, m') = H_M(xm, xm') = \text{Nrd}(x)H_M(m, m')$, and $x^*H_M = nH_M$ which means x is n -isogeny on (M, H_M) . Similarly to the case (M^2, H_M^2) , (M^4, H_M^4) .

3 Symmetric Monoidal Category

Definition 4 (Closed Symmetric Monoidal Category) A closed symmetric monoidal category \mathfrak{C} is a symmetric monoidal category that for any object $Y \in \mathfrak{C}$, the functor $Y \otimes -$ is the tensor product of Y ; the right adjoint functor $[Y, -]_{\mathfrak{C}}$ called an internal Hom out of Y .

From the right adjoint, we have $\text{Hom}_{\mathfrak{C}}(c, [c_1, c_2]_{\mathfrak{C}}) = \text{Hom}_{\mathfrak{C}}(c \otimes c_1, c_2)$.

Let $(\mathfrak{C}, \otimes, 1)$ be a symmetric monoidal category, \mathfrak{D} is another category, a symmetric monoidal action is a categorification of the notion of action, i.e. it is a functor $\cdot : \mathfrak{C} \times \mathfrak{D} \rightarrow \mathfrak{D}$, which respect the “obvious coherence conditions”. Equivalently, an action is given by a monoidal functor from $\mathfrak{C} \rightarrow \text{End}(\mathfrak{D})$.

Assume now that \mathfrak{C} is closed symmetric monoidal, and let \mathfrak{D} be a category enriched in \mathfrak{C} , which means that we see the hom objects $\text{Hom}_{\mathfrak{D}}(d_1, d_2)$ as living in \mathfrak{C} rather than in Set .

Defintion 5 Given $c \in \mathfrak{C}$, $d \in \mathfrak{D}$, the power object $[c, d]_{\mathfrak{C}} \in \mathfrak{D}$ is the unique object such that

$$\mathrm{Hom}_{\mathfrak{D}}(d', [c, d]_{\mathfrak{C}}) = \mathrm{Hom}_{\mathfrak{C}}(c, \mathrm{Hom}_{\mathfrak{D}}(d', d))$$

for all $d' \in \mathfrak{D}$.

The copower object $c \otimes_{\mathfrak{C}} d$ is the unique object such that

$$\mathrm{Hom}_{\mathfrak{D}}(c \otimes_{\mathfrak{C}} d, d') = \mathrm{Hom}_{\mathfrak{C}}(c, \mathrm{Hom}_{\mathfrak{D}}(d', d))$$

for all $d' \in \mathfrak{D}$.

In other words, $[c, d]_{\mathfrak{C}}$ is defined as a presheaf on \mathfrak{D} , that is $[c, d]_{\mathfrak{C}} : X \in \mathfrak{D} \rightarrow \mathrm{Hom}_{\mathfrak{D}}(X, [c, d]_{\mathfrak{C}}) = \mathrm{Hom}_{\mathfrak{C}}(c, \mathrm{Hom}_{\mathfrak{D}}(X, d))$. It is easily to see that $[c, d]_{\mathfrak{C}}$ exists if this presheaf is representable.

It should be noted that $c \cdot d = [c, d]_{\mathfrak{C}}$ gives a contravariant symmetric monoidal action; $c \cdot d = c \otimes_{\mathfrak{C}} d$ gives a covariant symmetric monoidal action.

4 Module Action

4.1 Power Objects in an Abelian Category (Definition of Module Action)

Let \mathcal{A} be an abelian category, A is an object of \mathcal{A} , we have an orientation by ring R (i.e. there is a morphism $R \rightarrow \mathrm{End}_{\mathcal{A}}(A)$).

Theorem 3 (Existence of Power Object) If $A \in \mathcal{A}$ is R -oriented, M is a finitely presented R -module, the power object $[M, A]_R$ exists in \mathcal{A} ($\mathrm{Hom}_{\mathcal{A}}(X, [M, A]_R) = \mathrm{Hom}_R(M, \mathrm{Hom}_{\mathcal{A}}(X, A))$). Moreover, the contravariant functor $[-, A]_R$ is functorial and left exact.

Proof. Since M is finitely presented, there exists an exact sequence $R^m \rightarrow R^n \rightarrow M \rightarrow 0$, where $R^m \rightarrow R^n$ can be written as right-multiplication by some matrix $X \in M_{m,n}(R)$.

For $i : R \rightarrow \mathrm{End}(A)$, we have the left-multiplication by matrix X from $A^n \rightarrow A^m$. Let B be the kernel of $A^n \rightarrow A^m$, we have an exact sequence $0 \rightarrow B \rightarrow A^n \rightarrow A^m$.

For any $X \in \mathcal{A}$, we have $0 \rightarrow \mathrm{Hom}(X, B) \rightarrow \mathrm{Hom}(X, A^n) \cong \mathrm{Hom}(X, A)^n \rightarrow \mathrm{Hom}(X, A^m) \cong \mathrm{Hom}(X, A)^m$ is also an exact sequence. On the other hand, acting $\mathrm{Hom}_R(-, \mathrm{Hom}(X, A))$ to $R^m \rightarrow R^n \rightarrow M \rightarrow 0$, we have

$$0 \rightarrow \mathrm{Hom}_R(M, \mathrm{Hom}(X, A)) \rightarrow \mathrm{Hom}(X, A)^n \rightarrow \mathrm{Hom}(X, A)^m$$

Hence, we obtain $\mathrm{Hom}(X, B) \cong \mathrm{Hom}_R(M, \mathrm{Hom}(X, A))$. In this case, we choose B as $[M, A]_R$.

If $0 \rightarrow M_1 \rightarrow M_2 \rightarrow M_3$ is an exact sequence of finitely presented left R -modules, then for each $X \in \mathcal{A}$,

$$0 \longrightarrow \mathrm{Hom}_R(M_1, \mathrm{Hom}(X, A)) \longrightarrow \mathrm{Hom}_R(M_2, \mathrm{Hom}(X, A)) \longrightarrow \mathrm{Hom}_R(M_3, \mathrm{Hom}(X, A))$$

is exact. This implies that the sequence of representing objects

$$0 \longrightarrow [M_1, A] \longrightarrow [M_2, A] \longrightarrow [M_3, A]$$

is exact. That is, the functor $[-, A]$ is left exact. □

Remark 3 There are some properties about power object we defined above.

- $[R, A]_R$ and A represent the presheaf $\mathrm{Hom}_{\mathcal{A}}(-, A)$ on \mathcal{A} because the presheaf from A is

$$f_A : X \in \mathcal{A} \rightarrow \mathrm{Hom}_{\mathcal{A}}(X, A)$$

the presheaf from $[R, A]_R$ is

$$f_{[R, A]_R} : X \in \mathcal{A} \rightarrow \mathrm{Hom}_{\mathcal{A}}(X, [R, A]_R) = \mathrm{Hom}_R(R, \mathrm{Hom}_{\mathcal{A}}(X, A)) = \mathrm{Hom}_{\mathcal{A}}(X, A)$$

We have $[R, A]_R = A$.

- It is clear from the functorial definition, $[-, A]_R$ commutes with direct sums. For M is finitely presented, we have the exact sequence $R^m \rightarrow R^n \rightarrow M \rightarrow 0$, by acting $[-, A]_R$, we obtain the exact sequence $0 \rightarrow [M, A]_R \rightarrow A^n \rightarrow A^m$.

The map $\psi : R^m \rightarrow R^n$ can be represented by right multiplication by a matrix $N \in M_{m \times n}(R)$, and the same matrix acts by left multiplication to $\varphi = [\psi, A]_R : A^n \rightarrow A^m$, which means $[M, A]_R = \ker(\varphi)$ is the kernel of action of N .

We want to define a symmetric monoidal action, which means $[M, A]_R$ is R -oriented. We will denote these oriented morphisms by $\text{Hom}_{\mathcal{A}_R}(A, B)$ or even $\text{Hom}_R(A, B)$, dropping the orientations i_A, i_B from the notation by simplicity.

Theorem 4 (Existence of Power Object with R -orientation) Let R be a commutative ring, and \mathcal{A}_R be the R -oriented category of \mathcal{A} : objects are given by (A, i_A) with $A \in \mathcal{A}_R$ and $i_A : R \rightarrow \text{End}_{\mathcal{A}}(A)$ is R -orientation, and morphisms $(A, i_A) \rightarrow (B, i_B)$ are morphisms $A \rightarrow B$ in \mathcal{A} respecting the orientations on A and B . For any $f : (A, i_A) \rightarrow (B, i_B)$, $r \in R$, we have the following commutative diagram:

$$\begin{array}{ccc} A & \xrightarrow{i_A(r)} & A \\ \downarrow f & & \downarrow f \\ B & \xrightarrow{i_B(r)} & B \end{array}$$

Given such an oriented morphism, its kernel and cokernel have a canonical orientation. So \mathcal{A}_R is an abelian category, naturally enriched in R -modules ($\text{Hom}_{\mathcal{A}_R}$ is R -module).

Given a finitely presented R -module M , and $(A, i_A) \in \mathcal{A}_R$, the power object $[M, A]_R$ from the above Theorem has a natural R -orientation so lives in \mathcal{A}_R , and it gives the power object in this enriched category: $\text{Hom}_{\mathcal{A}_R}(X, [M, A]_R) = \text{Hom}_R(M, \text{Hom}_{\mathcal{A}_R}(X, A))$ for all $X \in \mathcal{A}_R$.

The functor $[-, -]_R : R\text{-modules} \times \mathcal{A}_R \rightarrow \mathcal{A}_R$ is right exact on the left and left exact on the right, and it commutes with direct sums.

Proof. From above we have $[M, A]_R$ is kernel of $\varphi : A^n \rightarrow A^m$, for R is commutative, then R is commutative with matrix N , which means φ is R -orientation and the kernel $[M, A]_R$ is also R -orientation.

For any $X \in \mathcal{A}_R$, $\text{Hom}_{\mathcal{A}_R}(X, A)$ is R -module, we have:

$$\begin{array}{ccccccc} 0 & \longrightarrow & \text{Hom}_{\mathcal{A}_R}(X, [M, A]_R) & \longrightarrow & \text{Hom}_{\mathcal{A}_R}(X, A)^n & \longrightarrow & \text{Hom}_{\mathcal{A}_R}(X, A)^m \\ & & \downarrow & & \downarrow = & & \downarrow = \\ 0 & \longrightarrow & \text{Hom}_R(M, \text{Hom}_{\mathcal{A}_R}(X, A)) & \longrightarrow & \text{Hom}_{\mathcal{A}_R}(X, A)^n & \longrightarrow & \text{Hom}_{\mathcal{A}_R}(X, A)^m \end{array}$$

The first row is acting $\text{Hom}_{\mathcal{A}_R}(X, -)$ on $[M, A]_R \rightarrow A^n \rightarrow A^m$; the second row is acting $\text{Hom}_R(-, \text{Hom}_{\mathcal{A}_R}(X, A))$ on $R^m \rightarrow R^n \rightarrow M$.

Then, $\text{Hom}_{\mathcal{A}_R}(X, [M, A]_R) = \text{Hom}_R(M, \text{Hom}_{\mathcal{A}_R}(X, A))$.

The exactness properties follow from the functorial definition and the exactness property of the Hom functor in R -modules and abelian category. \square

From above, we have the symmetric monoidal contravariant action from finitely presented R -module to R -oriented objects in \mathcal{A} , which we denote by $M \cdot A = [M, A]_R$.

It is easily to see that $M \cdot N \cdot A = (M \otimes_R N) \cdot A = (N \otimes_R M) \cdot A = N \cdot M \cdot A$.

Proposition 5 (Base Change) $R \subseteq S \subseteq \text{End}_{\mathcal{A}}(A)$, where S is a right R -module, for any finitely represented R -module M , we have $[M, A]_R = [S \otimes_R M, A]_S$.

Proof. Since $\text{Hom}_{\mathcal{A}}(X, [M, A]_R) = \text{Hom}_R(M, \text{Hom}_{\mathcal{A}}(X, A))$, and $\text{Hom}_R(M, \text{Hom}_{\mathcal{A}}(X, A)) = \text{Hom}_S(S \otimes_R M, \text{Hom}_{\mathcal{A}}(X, A))$, we have $\text{Hom}_{\mathcal{A}}(X, [M, A]_R) = \text{Hom}_S(S \otimes_R M, \text{Hom}_{\mathcal{A}}(X, A))$.

Futhermore, for adjoint pair of S , we have $\text{Hom}_S(S \otimes_R M, \text{Hom}_{\mathcal{A}}(X, A)) = \text{Hom}_{\mathcal{A}}(X, [S \otimes_R M, A]_S)$.

It means the presheaf $X \rightarrow \text{Hom}_{\mathcal{A}}(X, [M, A]_R)$ can be represented by $[M, A]_R$ and $[S \otimes_R M, A]_S$. Hence, $[M, A]_R = [S \otimes_R M, A]_S$. \square

Proposition 6 1. Let $\psi : M_2 \rightarrow M_1$ be a morphism of finitely presented R -module, and take presentations: $R^{m_2} \rightarrow R^{n_2} \rightarrow M_2 \rightarrow 0$, $R^{m_1} \rightarrow R^{n_1} \rightarrow M_1 \rightarrow 0$. Since R is projective R -module, we have the following commutative diagram:

$$\begin{array}{ccccccc} R^{m_1} & \longrightarrow & R^{n_1} & \longrightarrow & M_1 & \longrightarrow & 0 \\ \uparrow & & \uparrow & & \uparrow & & \\ R^{m_2} & \longrightarrow & R^{n_2} & \longrightarrow & M_2 & \longrightarrow & 0 \end{array}$$

If $A \in \mathcal{A}_R$, $A_1 = M_1 \cdot A$, $A_2 = M_2 \cdot A$, we have the following commutative diagram:

$$\begin{array}{ccccccc} 0 & \longrightarrow & A_1 & \longrightarrow & A^{n_1} & \longrightarrow & A^{m_1} \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & A_2 & \longrightarrow & A^{n_2} & \longrightarrow & A^{m_2} \end{array}$$

2. Let $\phi : A_1 \rightarrow A_2$ be an oriented morphism of objects in \mathcal{A}_R , and M a finitely presented R -module. Take a presentation $R^m \rightarrow R^n \rightarrow M \rightarrow 0$, and consider the commutative diagram:

$$\begin{array}{ccccccc} 0 & \longrightarrow & M \cdot A_1 & \longrightarrow & A_1^n & \longrightarrow & A_1^m \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & M \cdot A_2 & \longrightarrow & A_2^n & \longrightarrow & A_2^m \longrightarrow 0 \end{array}$$

where the vertical arrows $A_1^n \rightarrow A_2^n$ (and $A_1^m \rightarrow A_2^m$) are given by the diagonal of ϕ .

Then there is a unique dotted arrow making the diagram commutative, this is $M \cdot \phi : M \cdot A_1 \rightarrow M \cdot A_2$.

4.2 Module Action on Oriented Abelian Varieties

We recall that an abelian variety over k is a smooth proper group scheme A/k . The commutativity condition is then automatic. Equivalently, A/k is an abelian variety whenever it is a proper group scheme, which is geometrically connected (equivalently, since 0 is k -rational point, A/k is connected over k) and geometrically reduced (equivalently A is geometrically reduced at 0). If k is perfect, then this result also holds using “reduced” instead of “geometrically reduced”. From now on, we will assume that k is perfect to avoid pathologies; in practice for our applications $k = \mathbb{F}_q$ will be a finite field.

Moreover, if M is a finitely presented R -module, then $M \cdot A = [M, A]_R$ is just a commutative proper group scheme, not abelian variety. For example, $M = R/nR$, $M \cdot A = A[n]$.

Proposition 7 Let X be an R -oriented proper k -group scheme and M be a finitely presented R -module, k' be a k -algebra, then $X(k')$ has a natural action from R , $M \cdot X(k') \cong [M, X(k')]_R$.

Proof. Since there exists exact sequence $R^m \rightarrow R^n \rightarrow M \rightarrow 0$, then we have another exact sequence

$$0 \rightarrow [M, X] \rightarrow X^n \rightarrow X^m. \text{ By the rational points of } k', \text{ we have } 0 \rightarrow M \cdot X(k') \rightarrow X(k')^n \rightarrow X(k')^m.$$

By $[-, X(k')]_R$, we also have the exact sequence $0 \rightarrow [M, X(k')]_R \rightarrow [R^n, X(k')]_R \rightarrow [R^m, X(k')]_R$, since $[R^n, X(k')]_R \cong X(k')^n$, we have $M \cdot X(k') \cong [M, X(k')]_R$. \square

Proposition 8 (Dimension of Module Action) Assume that R is a domain, finitely presented as a \mathbb{Z} -module. If X is an R -oriented commutative proper group scheme, and M a finitely presented R -module, then $M \cdot X = [M, X]_R$ is a commutative proper group scheme of dimension $\text{rank}(M) \dim(A)$. In particular, if M is of torsion (i.e. is finite as a set), $[M, X]_R$ is a finite scheme.

Proof. Since the commutative proper group scheme is abelian category, we have the kernel of $A^n \rightarrow A^m$ is also a commutative proper group scheme. Hence, $[M, X]_R$ is a commutative proper group scheme.

It remains to compute the dimension of $M \cdot X$.

We first prove the case X is abelian variety A .

If M is finite, we have M is quotient of $(R/nR)^m$ for some $n, m \in \mathbb{N}_+$. For R/nR has representation $R \rightarrow R \rightarrow R/nR$, we have $[R/nR, A]_R = A[n]$. Hence, $[M, A]_R \subseteq A[n]^m$, which is finite.

If $r = \text{rank}(M) > 0$, we have $0 \rightarrow R^r \rightarrow M \rightarrow T \rightarrow 0$, where T is torsion, hence there is an exact sequence by acting $[-, A]_R$, that is $0 \rightarrow [T, A]_R \rightarrow [M, A]_R \rightarrow [R^r, A]_R = A^r$. Since $[T, A]_R$ is finite, we have $\dim([M, A]_R) \leq \dim(A^r) = \dim(A) \cdot \text{rank}(M)$.

Since R is finitely presented as \mathbb{Z} -module, there exists $n \in \mathbb{N}_+$ such that $nT = 0$. Then the multiplication $n : R^r \rightarrow R^r$ factor through $R^r \hookrightarrow M \rightarrow R^r$. By acting $[-, A]_R$, we have $A^r \rightarrow [M, A]_R \rightarrow A^r$ is n -multiplication, which is surjective (isogeny between abelian varieties). It means $\dim(A^r) = \dim(A) \text{rank}(M) \leq \dim([M, A]_R)$.

From above, we have $\dim([M, A]_R) = \dim(A) \text{rank}(M)$.

For X is a general proper reduced group scheme, X^0 is its connected component at 0. X^0 is abelian variety of the same dimension as X , and X/X^0 is finite group of components. Hence, we have $0 \rightarrow M \cdot X^0 \rightarrow M \cdot X$. Since there exists a positive integer N such that $NX/X^0 = 0$. Therefore, we have the multiplication $N : X \rightarrow X$ factor through $X \rightarrow X^0 \hookrightarrow X$, by $[M, -]_R$, we have $[M, X]_R \rightarrow [M, X^0]_R \hookrightarrow [M, X]_R$ is $M \cdot [N]$. So the rank of $[M, X^0]_R$ and $[M, X]_R$ are same, which shows $[M, X]_R/[M, X^0]_R$ is finite, and $\dim([M, X]_R) = \dim([M, X^0]_R) = \dim(X^0) \text{rank}(M)$. \square

Definition 6 Given an oriented abelian variety A and a finitely presented torsion free module M , we say that M is compatible with A if $M \cdot A$ is still an abelian variety. Given an isogeny $\psi : M_2 \hookrightarrow M_1$, and an isogeny $\phi : A_1 \rightarrow A_2$, we say that ψ is compatible with ϕ if $\phi \cdot \psi : M_1 \cdot A_1 \rightarrow M_2 \cdot A_2$ is still an isogeny of abelian varieties (in particular, we require that $M_i \cdot A_i$ is an abelian variety). We say that ψ is compatible with A if ψ is compatible with $\text{Id}_A : A \rightarrow A$, in that case the kernel is given by $M_1/M_2 \cdot A$ by right exactness. And similarly for the compatibility of M with $\phi : A_1 \rightarrow A_2$.

Proposition 9 (Induced by Module Isogeny = Abelian Varieties Isogeny) If A is an oriented abelian variety, and $\psi : M_2 \hookrightarrow M_1$ is a monomorphism, with each M_i compatible with A , then $\psi \cdot A : M_1 \cdot A \twoheadrightarrow M_2 \cdot A$ is an epimorphism with kernel $(M_1/M_2) \cdot A$. In particular, if furthermore $M_2 \hookrightarrow M_1$ is an isogeny, then $\psi \cdot A$ is an isogeny.

If $\phi : A_1 \twoheadrightarrow A_2$ is an oriented epimorphism with kernel U , and M is compatible with each A_i , then $M \cdot \phi : M \cdot A_1 \twoheadrightarrow M \cdot A_2$ is an epimorphism with kernel $M \cdot U$. In particular, if ϕ is furthermore an isogeny, $M \cdot \phi$ is an isogeny.

With the notations of Definition above, for an isogeny ψ to be compatible with ϕ , it suffices that each M_i is compatible with each A_j .

Proof. Since we have $0 \rightarrow M_2 \rightarrow M_1 \rightarrow M_1/M_2 \rightarrow 0$, then $0 \rightarrow M_1/M_2 \cdot A \rightarrow M_1 \cdot A \rightarrow M_2 \cdot A$. The image of $M_1 \cdot A \rightarrow M_2 \cdot A$ denoted by B , which is also an abelian variety. We have $\dim(B) = \dim(A)(\text{rank}(M_1) - \text{rank}(M_1/M_2)) = \dim(A) \text{rank}(M_2) = \dim(M_2 \cdot A)$, which means $B = M_2 \cdot A$.

Moreover, if $M_2 \rightarrow M_1$ is an isogeny, then $\text{rank}(M_1) = \text{rank}(M_2)$, and $\dim(M_1 \cdot A) = \dim(M_2 \cdot A)$, which means $M_1 \cdot A \rightarrow M_2 \cdot A$ is also an isogeny (surjective and finite kernel).

The rest is similar. \square

4.3 Projective Module Action on Abelian Varieties (Keep Abelian Varieties)

Here $M^\vee = \text{Hom}_R(M, R)$.

Theorem 5 If $A \in \mathfrak{Ab}_R$ is an oriented abelian variety, and M is a finitely presented projective module, then $M \cdot A$ is still an abelian variety. And we have a canonical isomorphism $(M \cdot A)^\vee \simeq M^\vee \cdot A^\vee$.

If $\psi : M_2 \rightarrow M_1$ is an isogeny between projective modules, $\psi \cdot A$ is an isogeny, and the dual module isogeny $\hat{\psi} : M_1^\vee \rightarrow M_2^\vee$ gives the dual isogeny $\hat{\psi} \cdot A^\vee : M_2^\vee \cdot A^\vee \rightarrow M_1^\vee \cdot A^\vee$.

Proof. Since M is finitely presented projective module, we have $R^n = M \oplus M'$. Then we have $[R^n, A]_R = A^n = M \cdot A \oplus M' \cdot A$. Hence $M \cdot A$ is a quotient of A^n , which means $M \cdot A$ is abelian variety.

If A is R -oriented, $i : R \rightarrow \text{End}(A)$ is the orientation, we define $i^\vee : R \rightarrow \text{End}(A^\vee)$ by $i^\vee(r) = \widehat{i(r)}$, and if $F : A^n \rightarrow A^m$ is a matrix M of elements in R , then $F^\vee : A^{\vee,m} \rightarrow A^{\vee,n}$ is given by the transpose matrix M^T .

If the projective module M is given by $p : R^n \rightarrow M$, then M^\vee is given by $R^{\vee,n} = R^n = M^\vee \oplus M'^\vee$. Hence, $M^\vee \cdot A^\vee$ is given by $A^{\vee,n} = M^\vee \cdot A^\vee \oplus M'^\vee \cdot A^\vee$ and the projection $p^\vee \cdot A^\vee : A^{\vee,n} \rightarrow M^\vee \cdot A^\vee$.

On the other hand, for the projection $p \cdot A : M \cdot A \rightarrow A^n$, we have $A^{\vee,n} = (M \cdot A)^\vee \oplus (M' \cdot A)^\vee$ and the projection $(p \cdot A)^\vee : A^{\vee,n} \rightarrow (M \cdot A)^\vee$.

Since $(p \cdot A)^\vee = p^\vee \cdot A^\vee$ (by action of transpose), we have $(M \cdot A)^\vee = M^\vee \cdot A^\vee$.

We obtain dual $\hat{\psi} \cdot A^\vee$ from above proposition.

(For there is an exact sequence $0 \rightarrow M' \rightarrow R^n \rightarrow M \rightarrow 0$, we have $0 \rightarrow M^\vee \rightarrow R^n \rightarrow M'^\vee \rightarrow 0$, by acting $[-, A^\vee]$, we have $0 \rightarrow M'^\vee \cdot A^\vee \rightarrow A^{\vee,n} \rightarrow M^\vee \cdot A^\vee \rightarrow 0$ (generalized $\text{Ext}=0$).

On the other hand, acting $[-, A]$ on the origin exact sequence, we have $0 \rightarrow M \cdot A \rightarrow A^n \rightarrow M' \cdot A \rightarrow 0$. Then there is an exact sequence for dual: $0 \rightarrow (M' \cdot A)^\vee \rightarrow A^{\vee,n} \rightarrow (M \cdot A)^\vee \rightarrow 0$.

$$\begin{array}{ccccccc} 0 & \longrightarrow & M'^\vee \cdot A^\vee & \longrightarrow & A^{\vee,n} & \xrightarrow{p} & M^\vee \cdot A^\vee \longrightarrow 0 \\ & & \downarrow & & \downarrow \cong & & \downarrow \\ 0 & \longrightarrow & (M' \cdot A)^\vee & \longrightarrow & A^{\vee,n} & \xrightarrow{p} & (M \cdot A)^\vee \longrightarrow 0 \end{array} \quad)$$

□

4.4 Module Action on Dimension 1 (Not require projective module)

Proposition 10 Let $R = \mathbb{Z}$ or an order in imaginary quadratic field or a maximal order of $B_{p,\infty}$ (where we set R is endomorphism ring of an elliptic curve E). M is finitely presented torsion-free module, then we have $A = M \cdot E$ is an abelian variety isogenous to product of E . Moreover, $[-, E]$ is exact. $[I, E] \cong E/E[I]$, $[R/I, E] \cong E[I]$.

Proof. If $M \cdot E$ is an abelian variety, from the proof of Proposition 8, we have $A = M \cdot E \rightarrow E^r$ is surjective and $M \cdot E, E^r$ have the same rank, hence $A \rightarrow E^r$ is an isogeny.

It remains to prove A is an abelian variety.

If R is \mathbb{Z} or maximal order of $B_{p,\infty}$, we have finitely presented torsion-free R module M is projective module, by Theorem 5, we have $M \cdot E$ is an abelian variety.

So suppose that R is a quadratic order. Let c be the conductor. Let ℓ denote a prime. If $\ell \nmid c$, then the semi-local ring $R \otimes \mathbb{Z}_{(\ell)}$ is a Dedekind domain, but a semi-local Dedekind domain is a principal ideal domain, so $M \otimes \mathbb{Z}_{(\ell)}$ is free of rank r over $R \otimes \mathbb{Z}_{(\ell)}$, and $M/\ell M$ is free of rank r over $R/\ell R$.

We claim that A is smooth. This is automatic if $\text{char } k = 0$. Since $p \nmid c$, so by the above, M/pM is free of rank r over R/pR . Applying $[M, -]$ to

$$0 \rightarrow \text{Lie } E \rightarrow E(k[\epsilon]/(\epsilon^2)) \rightarrow E(k) \rightarrow 0$$

yields

$$0 \rightarrow [M, \text{Lie } E]_R \rightarrow A(k[\epsilon]/(\epsilon^2)) \rightarrow A(k) \rightarrow 0.$$

Thus

$$\text{Lie } A \simeq [M, \text{Lie } E]_R \simeq [M/pM, \text{Lie } E]_{R/pR} \simeq (\text{Lie } E)^r.$$

In particular, $\dim \text{Lie } A = r = \dim(M \cdot E)$, so A is smooth.

Since A is also proper, it is an extension of a finite étale commutative group scheme Φ by an abelian variety B (i.e. there is an exact sequence $0 \rightarrow B \rightarrow A \rightarrow \Phi \rightarrow 0$). The constructed surjection $A \rightarrow E^r$ with

finite kernel restricts to a homomorphism $B \rightarrow E^r$ with finite kernel, and it must still be surjective since $\dim(E^r) = \dim(A) = \dim(B)$; thus B is isogenous to E^r . From Tate's Theorem, for each prime ℓ ,

$$\#A(\bar{k})[\ell] = \#E(\bar{k})[\ell]^r \# \Phi[\ell]$$

On the other hand,

$$A(\bar{k})[\ell] = [M, E(\bar{k})]_R[\ell] = [M/\ell M, E(\bar{k})]_{R/\ell R}[\ell]$$

If $\ell \nmid c$, then $M/\ell M$ is free of rank r over $R/\ell R$, so

$$\#A(\bar{k})[\ell] = \#E(\bar{k})[\ell]^r$$

Now suppose that $\ell \mid c$; in particular, $\ell \neq p$. Then $R/\ell R \simeq \mathbb{F}_\ell[e]/(e^2)$ where $R = \mathbb{Z}[e]$. From $R/\ell R$ is an Artin local ring, the indecomposable module of $R/\ell R$ are \mathbb{F}_ℓ and $R/\ell R$, then every $(R/\ell R)$ -module is a direct sum of copies of \mathbb{F}_ℓ and $\mathbb{F}_\ell[e]/(e^2)$. We have the homomorphisms

$$\frac{R}{\ell R} \rightarrow \frac{\text{End } E}{\ell(\text{End } E)} \rightarrow \text{End } (E(\bar{k})[\ell])$$

are injective (We may require $\text{End}(E)/R$ is torsion-free). On the other hand, $\#E(\bar{k})[\ell] = \ell^2 = \#(R/\ell R)$. The previous three sentences imply that $E(\bar{k})[\ell]$ is free of rank 1 over $R/\ell R$ (If not, $E(\bar{k})[\ell] \cong \mathbb{F}_\ell \times \mathbb{F}_\ell$, which means e acts trivial on $E(\bar{k})[\ell]$. However, $R/\ell R \hookrightarrow \text{End}(E(\bar{k})[\ell])$). The equality $\#\text{Hom}_{R/\ell R}(N, R/\ell R) = \#N$ holds for $N = \mathbb{F}_\ell$ and $N = \mathbb{F}_\ell[e]/(e^2)$, so it holds for every finite $(R/\ell R)$ -module N , and in particular for $M/\ell M$. Thus it implies

$$\#A(\bar{k})[\ell] = \#(M/\ell M) = \#(R/\ell R)^r = \#E(\bar{k})[\ell]^r;$$

the first equality holds for considering $E(\bar{k})[\ell]$ as a free module of $R/\ell R$, the middle equality holds since M and R^r are torsion-free \mathbb{Z} -modules of the same rank.

Hence we have $\#\Phi[\ell] = 1$ for all ℓ , so Φ is trivial. Thus $A = B$, an abelian variety.

For any $M \hookrightarrow P$ where P is projective module, then we have $0 \rightarrow [P/M, E] \rightarrow [P, E] \rightarrow [M, E]$. Since $[P, E], [M, E]$ are abelian varieties, we have the image of $[P, E]$ is subvariety of $[M, E]$.

However, from the dimensions of $[P, E], [M, E], [P/M, E]$, we have the dimension of image of $[P, E]$ equals to dimension of $[M, E]$, which means $[P, E] \rightarrow [M, E]$ is surjective. Hence $[-, E]$ is exact.

(For any module N , there exists projective module P such that $0 \rightarrow K \rightarrow P \rightarrow N \rightarrow 0$,

then $0 \rightarrow [N, E] \rightarrow [P, E] \rightarrow [K, E] \rightarrow \text{Ext}^1(N, E) \rightarrow \text{Ext}^1(P, E) = 0$. Since $[P, E] \rightarrow [K, E]$ is surjective, we have $\text{Ext}^1(N, E) = 0$ for any N , which means $[-, E]$ is exact.)

Assume I is generated by a_1, \dots, a_s , we have an exact sequence $R^s \rightarrow R \rightarrow R/I \rightarrow 0$, where $R^s \rightarrow R$ sends $(r_1, \dots, r_s) \rightarrow r_1 a_1 + \dots + r_s a_s$. Hence, by acting $[-, E]$, we have $0 \rightarrow [R/I, E] \rightarrow E \rightarrow E^s$, where the last map is: $(a_1, \dots, a_s) : E \rightarrow E^s$, and the kernel this map is $\ker(a_1) \cap \dots \cap \ker(a_s) = E[I]$. It means $[R/I, E] = E[I]$.

By the exact sequence $0 \rightarrow I \rightarrow R \rightarrow R/I \rightarrow 0$, we have $0 \rightarrow [R/I, E] = E[I] \rightarrow E \rightarrow [I, E] \rightarrow 0$, which means $[I, E] = E/E[I] = E_I$. \square

Proposition 11 The functor $[-, E]$ is fully faithful.

Proof. The ring R is \mathbb{Z} , a quadratic order, or a maximal quaternionic order. Since every finitely presented torsion-free left R -module is a finite direct sum of nonzero left R -ideals. Thus, we will prove for any two nonzero R -ideals I and J , there is the natural isomorphism map

$$\text{Hom}_R(J, I) \rightarrow \text{Hom}([I, E]_R, [J, E]_R)$$

If $R = \mathbb{Z}$, this is trivial. If R is a quadratic order, this is the elliptic curve case of the isomorphism given in (48) in Kani Proposition 17. If R is a maximal quaternionic order, then by finitely presented torsion-free left R -modules are projective, i.e., direct summands of finitely presented free left R -modules; since $[-, E]$ is fully faithful when restricted to free modules, it is also fully faithful on projective modules. \square

Remark 4 If R is \mathbb{Z} , $J = \langle m \rangle$, $I = \langle n \rangle$, $[I, E]_R = E/E[I] = E/E[n]$, $[J, E] = E/E[m]$. The map:

$$\begin{aligned} \Psi : \text{Hom}_R(J, I) &\rightarrow \text{Hom}(E/E[n], E/E[m]) \\ \varphi : m &\rightarrow tn \rightarrow \varphi_t \frac{n}{m} : P \rightarrow tQ \text{ where } mQ = nP \end{aligned}$$

If R is an order in imaginary quadratic field, we have $\text{Hom}(E_I, E_J) \cong \bar{J}I$ by

$$\begin{aligned} \Phi : \text{Hom}_R(E_I, E_J) &\rightarrow \bar{J}I \\ \varphi &\rightarrow \varphi \circ \varphi_{\bar{J}I} \text{ where } \varphi_{\bar{J}I} \text{ is the isogeny from } E_J \text{ to } E_I \text{ corresponds to } \bar{J}I \end{aligned}$$

Moreover, there is an isomorphism between $\bar{J}I$ and $\text{Hom}_R(J, I)$:

$$\begin{aligned} \Psi : \bar{J}I &\rightarrow \text{Hom}_R(J, I) \\ x &\rightarrow \varphi_x : r \rightarrow \frac{rx}{\text{Nrd}(J)} \end{aligned}$$

The inverse of Ψ can be obtained as following: for any $\varphi \in \text{Hom}_R(J, I)$, $x \in J, x \neq 0$, we assume $\varphi(x) = y$, then for another $x' \in J$, we have $\varphi(xx') = x' \varphi(x) = x \varphi(x')$, which means $x'y = x \varphi(x')$, hence $\varphi(x') = x^{-1}yx'$. It shows φ is induced by $\text{Nrd}(J)x^{-1}y$. Overall, $\text{Hom}(E_I, E_J) \cong \bar{J}I \cong \text{Hom}_R(J, I)$.

Theorem 6 It should be noted that $M \rightarrow M \cdot E$ is an antiequivalence of category between torsion-free finitely presented R -modules and R -oriented abelian varieties which is R -isogenous to product of E (which denoted by $\mathfrak{Ab}_{E,R}$).

The inverse is $A \rightarrow \text{Hom}(A, E)$. Since $\text{Hom}([M, E], E) \cong \text{Hom}([M, E], [R, E]) \cong \text{Hom}_R(R, M) \cong M$.

4.5 Polarization of Module Action on Abelian Varieties

Definition 7 (Polarization) A polarization is a morphism $\lambda = \Phi_{\mathcal{L}}$ induced by a line bundle \mathcal{L} .

If λ is an isogeny, we call λ is non-degenerate. If \mathcal{L} is ample, we say λ is positive(polarized); moreover, if λ is an isomorphism, we say λ is a principal polarization.

Now we assume R is commutative domain, (A, λ_A) is a PPAV with R -oriented. Moreover, we assume $R \rightarrow \text{End}(A)$ is monomorphism, $K = R \otimes \mathbb{Q}$ is either totally real field or CM field, in the first case, the Rosati involution is identity; in the second case, the Rosati involution is the canonical Galois involution. (i.e. $\lambda_A \circ i(\bar{r}) = \widehat{i(r)} \circ \lambda_A$)

Assume $(M, H_M), (N, H_N)$ are projective modules with non-degenerate Hermitian polarization, and $\iota : M \hookrightarrow N$. For polarization, we have an isogeny $\lambda : M^\vee \rightarrow M$, $\lambda' : N^\vee \rightarrow N$. Moreover, we define $H_M : M^\perp \times M^\perp \rightarrow R$ by $H_M(m, m') = H_M(m, \lambda(m'))$

In this case, we have $\lambda' = \iota \circ \lambda \circ \iota^\vee : N^\vee \rightarrow M^\vee \rightarrow M \rightarrow N$. Since ι is an embedding, we have

$$\begin{aligned} H_{\lambda'}(x, y) &= H_{\lambda'}(x, \lambda'(y)) \\ &= H_{\lambda'}(x, \iota \circ \lambda \circ \iota^\vee(y)) \\ &= H_\lambda(\iota^\vee(x), \lambda \circ \iota^\vee(y)) \\ &= H_\lambda(x \circ \iota, \lambda(y \circ \iota)) \\ &= H_\lambda(x \circ \iota, y \circ \iota) \end{aligned}$$

If H_λ is Hermitian, then for any $x, y \in N^\vee$, we have $H_\lambda(x \circ \iota, y \circ \iota) = \overline{H_\lambda(y \circ \iota, x \circ \iota)}$. Hence, $H_{\lambda'}(x, y) = \overline{H_{\lambda'}(y, x)}$. If $H_{\lambda'}$ is Hermitian, since ι can be extended to an isomorphism $M \otimes_R K \rightarrow K^n$, for any $f, g \in M^\vee$,

by tensor K , we have $\text{Hom}_R(M, R) \otimes_R K \cong \text{Hom}_K(M \otimes K, K)$. Since ι is an isomorphism, then f can be written as $f' \circ \iota$ for some $f' \in \text{Hom}_K(K^n, K) \cong K^n$. It shows $H_\lambda(f, g) = H_\lambda(f' \circ \iota, g' \circ \iota) = H_{\lambda'}(f', g')$, from the Hermitian property of $H_{\lambda'}$, we obtain H_λ is Hermitian.

Similarly to prove the equivalence of positive definite between H_λ and $H_{\lambda'}$.

For proving the following theorem, we need some lemmas.

Lemma 1 The Riemann form induced by line bundle is skew-symmetric.

Proof. Mumford [Abelian Varieties p.187-188, Theorem 1] □

Lemma 2 The bilinear form $(x, y) \rightarrow e_\ell(x, \lambda(y))$ which induced by $\lambda : A \rightarrow A^\vee$ and $x, y \in T_\ell(A)$ (Tate module) is skew-symmetric iff $2\lambda = \lambda_{\mathcal{L}}$ for some line bundles \mathcal{L} .

Proof. Mumford [Abelian Varieties p.187-188, Theorem 2] □

Lemma 3 If \mathcal{L} is an line bundle on abelian variety A , there exists some line bundles \mathcal{L}' such that $\mathcal{L} = \mathcal{L}'^n$ iff $A[n] \subseteq K(\mathcal{L})$, where $K(\mathcal{L})$ is the kernel of $\lambda_{\mathcal{L}} : A \rightarrow A^\vee$.

Proof. Mumford [Abelian Varieties p.213, Theorem 3] □

Theorem 7 Let M be finitely presented R -module. The form $H_M : M \times M \rightarrow R$ is Hermitian form iff $\lambda : M \cdot A \rightarrow (M \cdot A)^\vee$ can be induced by a line bundle \mathcal{L} .

Proof. For there exists $0 \rightarrow M \rightarrow R^n$, we have $f : A^n \rightarrow M \cdot A$ is an isogeny. Let $\lambda : M \cdot A \rightarrow (M \cdot A)^\vee$ be an isogeny, we define $\lambda' = \hat{f}\lambda f$. Now we will prove λ is induced by an line bundle iff λ' is.

If $\lambda : M \cdot A \rightarrow (M \cdot A)^\vee$ can be induced by line bundle \mathcal{L} , then the polarization λ' of A^n can be induced by $f^*(\mathcal{L})$.

On the other hand, if the polarization λ' of A^n can be induced by \mathcal{L}' , from Lemma 1, we have $e_\ell(x, \lambda'(y))$ is skew-symmetric. It is easily to see $e_\ell(x, \lambda(y))$ is also skew-symmetric.

where $\lambda' = \hat{f}\lambda f$, and we assume $f(x') = x, f(y') = y$, then

$$\begin{aligned} e_\ell(x, \lambda(y)) &= e_\ell(f(x'), \lambda f(y')) \\ &= e_\ell(x', \hat{f}\lambda f(y')) \\ &= e_\ell(x', \lambda'(y')) \\ &= -e_\ell(\lambda'(y'), x') \\ &= -e_\ell(\lambda f(y'), f(x')) \\ &= -e_\ell(\lambda(y), x) \end{aligned}$$

Therefore, from Lemma 2, we have $\lambda = 2\lambda_{\mathcal{L}_1}$ for some line bundles \mathcal{L}_1 .

Since $2\lambda = \lambda_{\mathcal{L}_1}$, then for any $P \in (M \cdot A)[2]$, $\lambda_{\mathcal{L}_1}(P) = 2\lambda(P) = 0$. From Lemma 3, there exist \mathcal{L} such that $\mathcal{L}_1 = \mathcal{L}^2$.

From above, $\lambda_{\mathcal{L}_1} = 2\lambda = 2\lambda_{\mathcal{L}}$, then λ is induced by \mathcal{L} .

Overall, the polarization λ of $M \cdot A$ is induced by an line bundle iff the polarization λ' of A^n is induced by an line bundle.

For we have proven that the equivalence of Hermitian between H_λ and $H_{\lambda'}$. It remains to prove $H_{\lambda'}$ is Hermitian iff $\lambda : A^n \rightarrow A^{n,\vee}$ can be induced by a line bundle, where λ is induced from $\lambda' : R^{n,\vee} \rightarrow R^n$.

Now let $\lambda_1 : A^n \rightarrow A^{n,\vee}$ induced from $\lambda' : R^{n,\vee} \rightarrow R^n$, for we have the isomorphism Φ between $R^{n,\vee}$ and R^n , where $(f_1, \dots, f_n) \rightarrow (f_1(1), \dots, f_n(1))$, then $\lambda_2 : A^n \rightarrow A^{n,\vee}$ can be induced from Φ . Let $M = \lambda' \Phi^{-1} : R^n \rightarrow R^n$, then $M \in M_n(R)$. For the Rosati involution of endomorphism M (denoted by φ_M) is $\lambda_2^{-1} \circ \widehat{\varphi_M} \circ \lambda_2$ which

corresponds to matrix $\Phi^{-1}M^*\Phi$. From the property of Rosati involution, we have the Rosati involution corresponds to matrix M^+ which is the conjugate transpose of M .

Hence $M^+ = \Phi^{-1}M^*\Phi$. For M corresponds to $\lambda_2^{-1} \circ \lambda_1$, then $M = M^+$ iff $\lambda_2^{-1} \circ \lambda_1$ equals to its Rosati involution. From

$$\begin{aligned} \text{NS}(A) \otimes \mathbb{Q} &\rightarrow \text{End}(A) \otimes \mathbb{Q} \\ \mathcal{L} &\rightarrow \lambda^{-1} \circ \lambda_{\mathcal{L}} \end{aligned}$$

gives correspondence between $\text{NS}(A) \otimes \mathbb{Q}$ and elements in $\text{End}(A) \otimes \mathbb{Q}$ which fixed by Rosati involution, we have $M = M^+$ iff λ_1 can be induced by an line bundle \mathcal{L} . \square

Lemma 4 Let $f : A \rightarrow B$ be an isogeny and \mathcal{L} be a line bundle on B . Then \mathcal{L} is ample if and only if $f^*(\mathcal{L})$ is ample.

Lemma 5 Let $\lambda : M^\vee \rightarrow M$ be injective such that H_λ is Hermitian. Then there exists a free R -module $M \xrightarrow{\iota} N = \bigoplus_{i=1}^n Re_i$ and integers $(\ell_i)_{1 \leq i \leq n}$ such that if $\lambda' = \iota\lambda\iota^\vee$, then $H_{\lambda'} : N^\vee \times N^\vee \rightarrow R$ satisfies $H_{\lambda'}(e_i^\vee, e_j^\vee) = \ell_i\delta_{ij}$.

Proof. Since λ is injective, the hermitian form H_λ is non-degenerate. We can find a basis (α_i) of $V^\vee = K \otimes M^\vee$ of vectors of M^\vee which is orthogonal for H_λ , i.e., $H_\lambda(\alpha_i, \lambda(\alpha_j)) = \ell_i\delta_{ij}$ with $\ell_i \in \mathbb{Z}$.

Consider $N' = \bigoplus_{i=1}^n R\alpha_i \subseteq M^\vee$ and then $N = N'^\vee \supseteq (M^\vee)^\vee \simeq M$. Denote by $\iota : M \rightarrow N$ the injection and (e_i) the dual basis of (α_i) . We get that

$$H_{\lambda'}(e_i^\vee, e_j^\vee) = H_{\lambda'}((\alpha_i^\vee)^\vee, (\iota\lambda\iota^\vee)(\alpha_j^\vee)^\vee) = H_\lambda(\alpha_i, \lambda(\alpha_j)) = \ell_i\delta_{ij}.$$

\square

Theorem 8 As notations above, $\lambda_1 : M^\vee \rightarrow M$, H_M is Hermitian, $\lambda : M \cdot A \rightarrow (M \cdot A)^\vee$, there exists an isogeny $f : A^n \rightarrow M \cdot A$, integers ℓ_1, \dots, ℓ_n , $D \in \text{End}(A^n) : (x_1, \dots, x_n) \rightarrow (\ell_1 x_1, \dots, \ell_n x_n)$ and a commutative diagram:

$$\begin{array}{ccc} A^n & \xrightarrow{\lambda' \circ D} & A^{n,\vee} \\ \downarrow f & & \uparrow \tilde{f} \\ M \cdot A & \xrightarrow{\lambda} & (M \cdot A)^\vee \end{array}$$

where $\lambda'' : A^n \rightarrow A^{n,\vee}$ induced from R^n -action. Moreover, λ is a polarization if and only if $\ell_i > 0$ for all i , or equivalently if and only if H_λ is positive definite.

Proof. From Lemma 5, we choose $\iota : M \rightarrow N = \bigoplus_{i=1}^n Re_i$ and $u : N \rightarrow R^n$ by sending $(r_i e_i)$ to (r_i) .

Then $u \circ \iota$ induced $f : A^n \rightarrow M \cdot A$. Since H_λ is Hermitian, there exists a line bundle \mathcal{L} on $M \cdot A$ such that $\lambda = \varphi_{\mathcal{L}}$. Since $\lambda'' \circ D$ is the pullback of λ by f , from Lemma 4, the isogeny λ is a polarization if and only if $\lambda'' \circ D$ is a polarization.

$$\begin{array}{ccc} A^n & \xrightarrow{\lambda'' \circ D} & A^{n,\vee} \\ \downarrow u \cdot A & & \uparrow \widehat{u \cdot A} \\ N \cdot A & \xrightarrow{\lambda'} & (N \cdot A)^\vee \\ \downarrow \iota \cdot A & & \uparrow \widehat{\iota \cdot A} \\ M \cdot A & \xrightarrow{\lambda} & (M \cdot A)^\vee \end{array}$$

Moreover, $\lambda'' \circ D$ is a polarization of A^n if and only if $\ell_i > 0$ for all i . (For $\text{NS}(A) \otimes \mathbb{Q} \rightarrow \text{End}(A) \otimes \mathbb{Q}$ gives the correspondence between ample line bundles and positive-definite matrix) Also, we can conclude that H_λ is positive definite if and only if $H_{\lambda''} = \text{diag}(\ell_1, \dots, \ell_g)$ is, and we have the final equivalence. \square

Theorem 9 Let (A, λ_A) be a principally polarized abelian variety, and R a CM order as above.

Let (M, H_M) be a projective module with a non-degenerate Hermitian polarization H_M . Then we have an autodual isogeny $(M, H_M) \cdot \lambda_A : M \cdot A \rightarrow (M \cdot A)^\vee$. This autodual isogeny is induced by an ample line bundle (i.e. is a polarization) iff H_M is definite positive, and it gives a principal polarization on $M \cdot A$ iff (M, H_M) is furthermore unimodular.

Let $\psi : M_2 \hookrightarrow M_1$ be an isogeny of projective R -modules, and $\phi = \psi \cdot A : M_1 \cdot A \rightarrow M_2 \cdot A$ be the induced isogeny of oriented abelian varieties. Then the dual module isogeny $M_1^\vee \rightarrow M_2^\vee$ gives the dual isogeny $M_2^\vee \cdot A^\vee \rightarrow M_1^\vee \cdot A^\vee$, and the contragredient isogeny $\hat{\phi}$ corresponds to the action of the adjoint of $\psi : \hat{\psi} : (M_1, H_1) \rightarrow (M_2, H_2)$. In particular, a n -similitude $(M_2, H_2) \rightarrow (M_1, H_1)$ between unimodular projective modules induces a n -isogeny $M_1 \cdot A \rightarrow M_2 \cdot A$.

Proof. We define the orientation on A^\vee by $i^\vee(r) = \widehat{i(\bar{r})}$. We use $M^\vee = \text{Hom}_{\bar{R}}(M, R)$ instead $\text{Hom}_R(M, R)$ and obtain the same result of Theorem 5. It should be noted that if $\gamma : A^n \rightarrow A^m$ given by matrix N , then the dual morphism $A^{\vee, m} \rightarrow A^{\vee, n}$ is given by the conjugate-transpose $F^+ = \overline{F^T}$.

Since H_M is non-degenerate Hermitian polarization, we have $M^\perp \cong M^\vee$, and for non-degenerate on M^\vee , we have $H_M : M^\vee \cong M^\perp \rightarrow M$ is an isogeny. By Theorem 5, we have an isogeny $M \cdot A \rightarrow M^\vee \cdot A \cong M^\vee \cdot A^\vee \cong (M \cdot A)^\vee$.

The last statement on the dual and contragredient isogeny follows from our matrix computation. \square

Remark 5 (n -isogeny) If $\psi : (M_2, H_2) \hookrightarrow (M_1, H_1)$ is n -isogeny, then $f : M_1 \cdot A \rightarrow M_2 \cdot A$ is an isogeny induced from ψ . Moreover, since $\psi^* H_1 = n H_2$, by acting $[-, A]_R$, we have $f^* \lambda_1 = n \lambda_2$, which is the definition of n -isogeny f . Hence, it implies that n -isogeny of R -module induced n -isogeny of abelian varieties.

Theorem 10 (Special Case of Theorem 9) Let $A \in \mathfrak{Ab}_{E, R}$, A can thus be written as $A = M \cdot E$ for some torsion-free R -module M . Then $A^\vee = M^\vee \cdot E$, a symmetric morphism $\phi : A \rightarrow A^\vee$ (equivalently a morphism induced by a line bundle \mathcal{L} on A) respecting the orientation corresponds to an Hermitian R -form H_M on M^\vee , ϕ is an isogeny (i.e. \mathcal{L} is non degenerate) iff H_M is non degenerate, and ϕ is a polarisation (i.e. \mathcal{L} is an ample line bundle) iff H_M is positive definite.

Finally, a principally polarised abelian variety $(A, \lambda_A) \in \mathfrak{Ab}_{E, R}$ corresponds to a unimodular positive definite Hermitian module (M, H_M) .

Proof. As the proof of Theorem 9. \square

Remark 6 In particular, if $M_1 \hookrightarrow M$, $M_2 \hookrightarrow M$ are two module isogenies, corresponding to abelian variety isogenies $A \rightarrow A_1$, $A \rightarrow A_2$ where $A = M \cdot E$, $A_i = M_i \cdot E$, then the push-forward isogeny $A \rightarrow A_{12}$ with kernel $K_1 + K_2$ corresponds to the module isogeny $M_1 \cap M_2 \hookrightarrow M$, and the isogeny $A \rightarrow A'_{12}$ with kernel $K_1 \cap K_2$ corresponds to the module isogeny $M_1 + M_2 \hookrightarrow M$.

For $M_1 \cap M_2 \hookrightarrow M$, $M_2 \hookrightarrow M$ are module isogenies, then we have $M \cdot E \rightarrow M_1 \cdot E$ can be factored from $M \cdot E \rightarrow M_1 \cdot E \rightarrow (M_1 \cap M_2) \cdot E$. It means $K_1 = \ker(M \cdot E \rightarrow M_1 \cdot E) \subseteq \ker(M \cdot E \rightarrow (M_1 \cap M_2) \cdot E)$, similarly to M_2 , hence, $K_1 + K_2 \subseteq \ker(M \cdot E \rightarrow (M_1 \cap M_2) \cdot E)$. Compared to degree of module isogeny, we have $K_1 + K_2 = \ker(M \cdot E \rightarrow (M_1 \cap M_2) \cdot E)$.

Similarly to the case of $M \cdot E \rightarrow (M_1 + M_2) \cdot E$.

Remark 7 How to compute the module and Hermitian form? Given (A, λ_A) a polarized abelian variety in $\mathfrak{Ab}_{E, R}$, the module between E and A is $\text{Hom}(A, E)$. It remains to determine the Hermitian form of M .

Since $A^\vee = M^\vee \cdot E$, for any $x, y \in M^\vee$, we have $R \rightarrow M^\vee$, $r \rightarrow rx$ or ry . By acting to E , it induced $x \cdot E, y \cdot E : A^\vee \rightarrow E$. Moreover, the dual of $y \cdot E : A^\vee \rightarrow E$ is $y^\vee \cdot E : E \rightarrow A$. It means $x \cdot E \circ \lambda_A \circ y^\vee \cdot E : E \rightarrow A \rightarrow A^\vee \rightarrow E$ is an oriented endomorphism $\gamma : E \rightarrow E$.

Since R is a primitive orientation on E , we have $\gamma \in R$ and $H(x, y) = \gamma$.

Next, we want to prove the module action is independent on base curve E .

Lemma 6 Let $E' \in \mathfrak{Ab}_{E, R}$ be another primitively R -oriented elliptic curve. Let $I = \text{Hom}_R(E', E)$, this is an invertible ideal. Then $M \cdot E' = M \cdot I \cdot E = (M \otimes_R I)E$ and if $A \in \mathfrak{Ab}_{E, R}$, $\text{Hom}(A, E) = I \text{Hom}(A, E')$.

Proof. Since $\text{Hom}(A, E) \cong \text{Hom}([M, E], [R, E]) = \text{Hom}_R(R, M) \cong M$, and $I \text{Hom}(A, E') \cong I \text{Hom}([M, E], [I, E]) \cong I \text{Hom}_R(I, M)$, we can prove $\text{Hom}_R(I, M) \cong I^{-1}M$ as above, thus $\text{Hom}(A, E) = I \text{Hom}(A, E')$. \square

We can also define the tensor product $A_1 \otimes_E A_2$ by $(M_1 \otimes_R M_2) \cdot E$, where $A_1 = M_1 \cdot E$, $A_2 = M_2 \cdot E$.

Now we consider $A \in \mathfrak{Ab}_{E,R}$, where $A = M_A \cdot E$, $M_A = \text{Hom}(A, E)$. We define the conductor of A to R is the conductor of M_A to R . From above Lemma, it does not depend on choice of E (for I is invertible, then the conductor of I_g and $I_g \otimes I$ are same). If the conductor is 1, the module M_A is projective. If M is also a torsion free finitely presented R module, we say M and A is Tor-independent if M, M_A are Tor-independent (i.e. conductors are primitive).

For example, $M \cong I_1 \oplus \cdots \oplus I_g$, then $A = M \cdot E = \prod_{i=1}^g E_i$, where $E_i = I_i \cdot E$. Moreover, the conductor of E_i dividing the conductor of E_{i+1} . The conductor of A equals to the conductor of E_g .

Table 1: Module Isogenies and Abelian Varieties Isogenies

	Module Isogenies	Abelian Varieties Isogenies
Form	$M_2 \hookrightarrow M_1$	$M_1 \cdot A \rightarrow M_2 \cdot A$
Conditions	two of: monomorphism, same rank, finite cokernel	two of: surjective, same dimension, finite kernel
Dual	$M^\vee = \text{Hom}_{\bar{R}}(M, R)$	$A^\vee = \text{Pic}^0(A)$
Polarized	$H_M : M^\vee \hookrightarrow M$	$\lambda_M = H_M \cdot A : M \cdot A \rightarrow M^\vee \cdot A = (M \cdot A)^\vee$
λ exists	H_M Hermitian	λ_M induced from line bundle
λ is an isogeny ((A, λ) is polarized)	H_M positive-definite	λ_M induced from ample line bundle
λ is isomorphism ((A, λ) is principally polarized)	H_M unimodular	λ_M has degree 1
n -isogeny	$M_2 \hookrightarrow M_1$ is n -isogeny	$M_1 \cdot A \rightarrow M_2 \cdot A$ is n -isogeny

5 Copower Objects of Module Actions (Another Action: Tensor)

Theorem 11 Let $A \in \mathfrak{Ab}_{E,R}$ and M a torsion free finitely presented R -module. If M and A are Tor-independent, then M is compatible with A : the power object $M \cdot A$ is in $\mathfrak{Ab}_{E,R}$, and in particular is still an abelian variety. The copower object $M \otimes_R A$ also exist in $\mathfrak{Ab}_{E,R}$.

Proof. Since $M \cdot A = (M \otimes M_A) \cdot E$, and M, A are Tor-independent, then $M \otimes M_A$ is torsion-free and finitely presented, hence $M \cdot A \in \mathfrak{Ab}_{E,R}$.

For $M \otimes A$ and the adjoint of copower, we have

$$\text{Hom}(M \otimes A, E) \cong \text{Hom}_R(M, \text{Hom}(A, E)) \cong \text{Hom}(A, [M, E]) \cong \text{Hom}([M_A, E], [M, E]) \cong \text{Hom}_R(M, M_A)$$

Hence $M \otimes A$ is induced from $\text{Hom}_R(M, M_A)$, that is $\text{Hom}_R(M, M_A) \cdot E = M \otimes A$. \square

Specially, if A is horizontal (conductor is 1), then for any torsion-free finitely presented M , we have $M \cdot A \in \mathfrak{Ab}_{E,R}$. Also, if M is projective, $M \cdot A$ is also in $\mathfrak{Ab}_{E,R}$.

Let $\lambda_A : A \rightarrow A^\vee$ be a symmetric morphism in $\mathfrak{Ab}_{E,R}$, $\Phi_H : M \rightarrow M^\vee$ induced by a Hermitian form, then by functoriality, we get a morphism $M \cdot A \rightarrow M^\vee \cdot A^\vee$, this morphism is symmetric. We denote the corresponding morphism as $H \cdot \lambda_A$.

Theorem 12 Let $A \in \mathfrak{Ab}_{E,R}$, assume that M is compatible with A , then M^\vee is compatible with A^\vee , and $M^\vee \cdot A^\vee = (M \cdot A)^\vee$.

If λ_A is a polarization on A , and H_M is a positive-definite Hermitian form on M^\vee , then $H_M \cdot \lambda_A$ is a polarization on $M \cdot A$. In particular, if λ_A is a principal polarization and H_M is unimodular on M , then $(M \cdot A, H_M \cdot \lambda_A)$ is a principally polarized abelian variety.

Given a principal polarization λ_A on A as above, assume that $\psi : (M_2, H_2) \rightarrow (M_1, H_1)$ is an n -similitude, and M_i is compatible with A . Then $\phi = \psi \cdot A : (M_1 \cdot A, H_1 \cdot \lambda_A) \rightarrow (M_2 \cdot A, H_2 \cdot \lambda_A)$ is an n -isogeny, which we often write simply as $M_1 \cdot A \rightarrow M_2 \cdot A$. Moreover, the dual of isogeny ϕ corresponds to the action of adjoint $(M_1, H_1) \rightarrow (M_2, H_2)$.

Proof. Since $M \cdot A = (M \otimes M_A) \cdot E$, then $(M \cdot A)^\vee = ((M \otimes M_A) \cdot E)^\vee = (M \otimes M_A)^\vee \cdot E = (M^\vee \otimes M_A^\vee) \cdot E = M^\vee \cdot A^\vee$.

The Hermitian form $H_M \cdot \lambda_A$ is induced from $M \otimes M_A \rightarrow (M \otimes M_A)^\vee$. For modules M, M_A correspond to positive-definite Hermitian form (unimodular), we have $M \otimes M_A$ correspond to positive-definite Hermitian form (unimodular).

We have prove $M_1 \cdot A \rightarrow M_2 \cdot A$ is an isogeny. For $\psi^* H_1 = n H_2$, by tensor M_A , we have $\psi^* H_1 \cdot \lambda_A = n H_2 \cdot \lambda_A$.

□

6 Computing Module Action

6.1 Computing Module Action: Kernel Approach

M is a module, $m \in M$, we have $R \rightarrow M$ by $r \rightarrow rm$. Then there is $m : M \cdot A \rightarrow A$. If we can compute this map for any m , we say $M \cdot A$ is effective.

Proposition 12 Let $M_2 \hookrightarrow M_1$ be an isogeny. Let $A \in \mathfrak{Ab}_R$ be compatible with this isogeny. By assumption, the corresponding morphism $M_1 \cdot A \rightarrow M_2 \cdot A$ is an isogeny. The kernel of this isogeny is given by $(M_1/M_2) \cdot A = (M_1 \cdot A)[M_2]$, i.e., the intersection of the kernels of all morphisms $m : M_1 \cdot A \rightarrow A$ with $m \in M_2$; conversely, if $m \in M_1$ vanishes on this kernel, then m belongs to M_2 .

Proof. Since M_2 is finitely presented, we have an exact sequence $R^m \rightarrow R^n \rightarrow M_2 \rightarrow 0$. Hence we have an monomorphism $[M_2, A] \rightarrow A^n$, which can be written as $(m_1, \dots, m_n) : [M_2, A] \rightarrow A^n$, where m_1, \dots, m_n generate M_2 .

Now we consider $R^n \rightarrow M_2 \hookrightarrow M_1$, which induced $M_1 \cdot A \rightarrow M_2 \cdot A \rightarrow A^n$. Therefore, the kernel of $M_1 \cdot A \rightarrow M_2 \cdot A$ equals to the kernel of $M_1 \cdot A \rightarrow A^n$. Since $M_2 \subseteq M_1$, $R^n \rightarrow M_2 \hookrightarrow M_1$ is same as $R^n \rightarrow M_2$ with different target, the isogeny $M_1 \cdot A \rightarrow A^n$ can be written as $(m_1, \dots, m_n) : M_1 \cdot A \rightarrow A^n$, which means $\ker(M_1 \cdot A \rightarrow M_2 \cdot A) = (M_1 \cdot A)[M_2]$.

Conversely, if $m : M_1 \cdot A \rightarrow A$ is zero on $(M_1 \cdot A)[M_2]$, then m descends to $M_2 \cdot A \rightarrow A = \text{Hom}(M_2 \cdot A, A) = M_2$, which means $m \in M_2$. □

Remark 8 How to understand $[M_2, A] \rightarrow A^n$ is (m_1, \dots, m_n) . For $m_i \in M_2 = \text{Hom}(M_2 \cdot A, A)$ and $f : R^n \rightarrow M_2$ by acting $(m_1, \dots, m_n)^T$ on R^n , which means for any $(r_1, \dots, r_n) \in R^n$, $f((r_1, \dots, r_n)) = (r_1, \dots, r_n) \cdot (m_1, \dots, m_n)^T$, therefore, $g : M_2 \cdot A \rightarrow A^n$ is also by acting the transpose of $(m_1, \dots, m_n)^T$ on $M_2 \cdot A$. i.e. for any $P \in M_2 \cdot A$, $g(P) = (m_1, \dots, m_n)(P) = (m_1(P), \dots, m_n(P))$.

For example, let $(I, H/\text{Nrd}(I)) \rightarrow (R, H)$ be a $\text{Nrd}(I)$ -similitude, which is compatible with A . Then isogeny $A \rightarrow I \cdot A$ has kernel $(R/I) \cdot A = A[I] = \{x \in A \mid \gamma(x) = 0, \forall \gamma \in I\}$.

Corollary 13 Let (A, λ_A) be a principally polarized abelian variety in \mathfrak{Ab}_R , and $\psi : (M_2, H_2) \rightarrow (M_1, H_1)$ be an n -isogeny compatible with A . If $M_1 \cdot A$ has an effective module orientation, n is smooth, and the n -torsion on $M_1 \cdot A$ is accessible, then we can effectively compute the n -isogeny $\phi : M_1 \cdot A \rightarrow M_2 \cdot A$.

Proof. We know that the kernel of ϕ lies in $(M_1 \cdot A)[n]$, which is given by the intersection of the kernels of the morphisms $m_i : M_1 \cdot A \rightarrow A$, where m_1, \dots, m_s are the generators of $\psi(M_2) \subset M_1$. By assumption, we can compute m_i and recover these kernels through some discrete logarithm problems. Once we have the kernel, we can apply an isogeny algorithm to compute the isogeny. □

Corollary 14 If (M, H_M) is a unimodular module of rank g , and we can find an n -isogeny $(R^g, H_R^g) \rightarrow (M, H_M)$ compatible with a principally polarized abelian variety (A, λ_A) , where n is smooth and the n -torsion on A is accessible, then we can effectively compute $(M, H_M) \cdot (A, \lambda_A)$.

Proof. By the dual, we certainly have an effective module orientation on $(R^g, H_R^g) \cdot (A, \lambda_A) = (A^g, \lambda_A^g)$, where λ_A^g is the product polarization: for an element $m \in R^g$ (represented as a column vector of elements in R), the

corresponding morphism $m : A^g \rightarrow A$ corresponds to the morphism induced by the row vector m^T and the orientation on A . So we apply the above corollary. \square

6.2 Computing Module Action: Clapoti Approach

Theorem 15 Suppose that we have n_1 and n_2 isogeny, with n_1 coprime to n_2 and $n_1 + n_2$ powersmooth, between two unimodular Hermitian modules $(M_2, H_2), (M_1, H_1)$, and that we know $M_1 \cdot A$ and its module action. Then the two corresponding isogenies $M_1 \cdot A \rightarrow M_2 \cdot A$ are efficiently computable.

Proof. Taking the contragredient of the n_2 -isogeny, we have a $n_1 n_2$ -isogeny $\psi : (M_1, H_1) \rightarrow (M_1, H_1)$, which splits as $M_1 \rightarrow M_2 \rightarrow M_1$, a n_2 -isogeny followed by a n_1 -isogeny, or as $M_1 \rightarrow M'_2 \rightarrow M_1$, a n_1 -isogeny followed by a n_2 -isogeny. We have $M'_2 = \psi(M_1) + n_2 M_1 \subset M_1$. Assume first that $n_1 + n_2$ is powersmooth. The Kani construction gives us a $(n_1 + n_2)$ -isogeny $(M_1^2, H_1^2) \rightarrow (M_2, H_2) \oplus (M'_2, H'_2)$, which we can compute efficiently, because the module orientation is effective on $M_1^2 \cdot A = (M_1 \cdot A)^2$, since it is on $M_1 \cdot A$. The corresponding $(n_1 + n_2)$ -isogeny $(M_1 \cdot A)^2 \rightarrow (M_2 \cdot A) \oplus (M'_2 \cdot A)$ allows us to recover both $M_2 \cdot A$ and the two n_i -isogenies $(M_1 \cdot A) \rightarrow (M_2 \cdot A)$. \square

6.3 Computing Action on Isogenies

Now for any isogeny $\phi : A_1 \rightarrow A_2$, unimodular M , we want to compute $M \cdot \phi : M \cdot A_1 \rightarrow M \cdot A_2$. We will assume $M \cdot A_1$ is effective.

Proposition 13 Let $\phi : A_1 \rightarrow A_2$ be an n -isogeny between ppavs in \mathfrak{Ab}_R with kernel K . Let M be an R -module compatible with ϕ . Then the kernel of $M \cdot \phi : M \cdot A_1 \rightarrow M \cdot A_2$ is given by $\{x \in M \cdot A_1 \mid m(x) \in K, \forall m \in M : M \cdot A_1 \rightarrow A_1\}$. In particular, if M is unimodular and we know $M \cdot A_1$, n is smooth and the n -torsion on $M \cdot A_1$ is accessible, we can compute the n -isogeny $M \cdot \phi$ efficiently via its kernel.

Proof. Take a surjection $R^n \rightarrow M$ and consider the commutative diagram induced by functoriality:

$$\begin{array}{ccc} A_1^n & \xrightarrow{\text{diag}(\phi)} & A_2^n \\ \uparrow (m_1, \dots, m_n) & & \uparrow (m_1, \dots, m_n) \\ M \cdot A_1 & \xrightarrow{M \cdot \phi} & M \cdot A_2 \end{array}$$

The commutativity shows that $\text{Ker}(M \cdot \phi) = \{x \in M \cdot A_1 \mid m(x) \in K, \forall m \in M : M \cdot A_1 \rightarrow A_1\}$. \square

Proposition 14 Assume that we have an efficient representation of $\phi : A_1 \rightarrow A_2$, and that we also know both $M \cdot A_1$ and $M \cdot A_2$ and the module action of M on them. Then we can recover an efficient representation of $M \cdot \phi$.

Proof. We can evaluate $\phi(P)$ on ℓ -torsion points in A_1 with small ℓ . Since we also can compute $M \cdot A_1 \hookrightarrow A_1^n$, $M \cdot A_2 \hookrightarrow A_2^n$, the commutative diagram gives the method to recover the image of $M \cdot \phi$ on ℓ -torsion points in $M \cdot A_1$. This is enough to compute $M \cdot \phi$. \square

7 Module Action For R, \mathcal{O} -bimodule

7.1 Supersingular Case: R, \mathcal{O} -bimodule

Theorem 16 Let E be a maximal supersingular curve E with endomorphism ring \mathcal{O} . Then the functor the functor $A \mapsto \text{Hom}_{\mathbb{F}_{p^2}}(A, E)$ is an antiequivalence between the category of maximal supersingular abelian varieties over \mathbb{F}_{p^2} and finitely presented torsion free left \mathcal{O} -modules, the inverse functor being given by the power object construction $M \rightarrow [M, E]$.

A principal polarisation on $A = M \cdot E$ is represented by an \mathcal{O} -integral unimodular positive definite Hermitian form H_M on M .

Proof. This is a special case of Theorem 6. \square

Remark 9 The dimension 1 case is $M = \text{Hom}_{\mathbb{F}_{p^2}}(E', E)$, this left \mathcal{O} -module corresponds to unimodular polarization $H_M(\varphi_1, \varphi_2) = \varphi_1 \hat{\varphi}_2 \in \mathcal{O}$, where $\varphi_1, \varphi_2 : E' \rightarrow E$.

Moreover, if $\varphi : E \rightarrow E'$ is an isogeny corresponds to left \mathcal{O} -ideal I , then there is an isomorphism $\iota : M \rightarrow I; m \rightarrow m \circ \varphi$. Since $H(\varphi_1 \circ \varphi, \varphi_2 \circ \varphi) = \deg(\varphi) H_M(\varphi_1, \varphi_2)$, we define $H_I(x, y) = \frac{x\bar{y}}{\text{Nrd}(I)}$. In this case, $H_M(\varphi_1, \varphi_2) = H_I(\iota(\varphi_1), \iota(\varphi_2))$.

Proposition 15 Let E be a supersingular curve with endomorphism \mathcal{O} , and suppose that E admits a primitive orientation by a quadratic imaginary ring R . Let M be a R -module, $\mathcal{O} \otimes_R M$ is then a (\mathcal{O}, R) -bimodule, and $[M, E]_R \simeq [\mathcal{O} \otimes_R M, E]_{\mathcal{O}}$ (where the isomorphism forgets the R orientation on $[M, E]$).

Proof. This is a special case of Proposition 5. \square

We can consider the above proposition as R -orientation, that is $E' = M \cdot E = (\mathcal{O} \otimes_R M) \cdot E$, the supersingular elliptic curve E' can be obtain from \mathbb{F}_{p^2} isogeny $\varphi_{\mathcal{O} \otimes_R M}$ or R -orientation isogeny φ_M .

It should be noted that if we consider M as R -module, then $M = \text{Hom}_R([M, E], E)$; however, if we consider $M_{\mathcal{O}}$ as \mathcal{O} -module, we have $M_{\mathcal{O}} = \text{Hom}_{\mathbb{F}_{p^2}}([M, E], E)$. Moreover, M is the R -submodule of $M_{\mathcal{O}}$ that commutes with the R -orientation on $M \cdot E$ and E . If M commutes with the R -orientation on $M \cdot E$ and E , we have $M_{\mathcal{O}} = \mathcal{O} \otimes_R M$. (For $M_{\mathcal{O}}$ action sends E to $[M, E]_R$.) If we have M , we can obtain $M_{\mathcal{O}}$ by $M_{\mathcal{O}} = M \otimes_R \mathcal{O}$. If we have $M_{\mathcal{O}}$, the R -module M is the set of elements m in $M_{\mathcal{O}}$ satisfied $m : E' \rightarrow E$ commutes with the R -orientation.

7.2 Special Case: Weil's Restriction

The Weil's restriction $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)$ is defined as the descent of the abelian surface $E \times E^{\sigma}$ from \mathbb{F}_{p^2} to \mathbb{F}_p (here σ is the Frobenius π_p), under the Galois action $(P_1, P_2) \mapsto (\sigma(P_2), \sigma(P_1))$. In particular, if E/\mathbb{F}_p is an elliptic curve defined over \mathbb{F}_p , then $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)/\mathbb{F}_p$ is a twist of E^2/\mathbb{F}_p .

In particular, on $E^2(\mathbb{F}_{p^2})$, while the standard Frobenius from E^2/\mathbb{F}_p is $(P, Q) \rightarrow (\sigma(P), \sigma(Q))$, the one induced by $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)/\mathbb{F}_p$ is $(P, Q) \rightarrow (\sigma(Q), \sigma(P))$.

If E/\mathbb{F}_p is supersingular, it has $(p+1)$ points over \mathbb{F}_p , so $E^2(\mathbb{F}_p)$ has $(p+1)^2$ points, while $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)(\mathbb{F}_p) \simeq E(\mathbb{F}_{p^2})$ also has $(p+1)^2$ points. In particular, $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)$ is isogeneous to E_0^2 , and $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)$ belongs to our category $\mathfrak{A}_{E_0, R}$, so is of the form $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E) = (M, H_M) \cdot E_0$. More generally, if A/\mathbb{F}_{p^2} is a maximal supersingular abelian variety of dimension g , the Frobenius endomorphism on $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(A)/\mathbb{F}_p$ satisfy $\pi^2 = -p$, hence $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(A)$ is standard supersingular, so is isogeneous to E_0^{2g} .

Theorem 17 Let E_0/\mathbb{F}_p be primitively oriented by $R = \mathbb{Z}[\sqrt{-p}]$ and $\text{End}(E_0) \cong \mathcal{O}_0$. Let $(M_{\mathcal{O}}, H_{\mathcal{O}}) = \text{Hom}_{\mathbb{F}_{p^2}}(E, E_0)$, and $(M_R, H_R) = \text{Hom}_{\mathbb{F}_p}(W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E), E_0)$, so that $E = (M_{\mathcal{O}}, H_{\mathcal{O}}) \cdot E_0$ and $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E) = (M_R, H_R) \cdot E_0$ by the antiequivalence of categories. Then $\mathcal{O}_0 \otimes_R (M_R, H_R) = (M_{\mathcal{O}}, H_{\mathcal{O}}) \oplus (M_{\mathcal{O}}^{\sigma}, H_{\mathcal{O}}^{\sigma})$, where $M_{\mathcal{O}}^{\sigma}$ is the given by the Galois conjugation by σ , i.e. $M_{\mathcal{O}}^{\sigma} = \pi_{E_0} M_{\mathcal{O}} \pi_E^{-1}$.

So from M_R we recover $M_{\mathcal{O}}$ by unicity of the orthogonal decomposition (it is crucial to have the polarisation H_R here), and conversely given $M_{\mathcal{O}}$ we can recover M_R as the set of elements of $M_{\mathcal{O}} \oplus M_{\mathcal{O}}^{\sigma}$ commuting with the following Galois action: $\sigma \cdot (\alpha, \beta) = (\beta^{\sigma}, \alpha^{\sigma})$, and H_R as the descent of $H_{\mathcal{O}} \oplus H_{\mathcal{O}}^{\sigma}$. This unimodular module (M_R, H_R) is isomorphic to $(M_{\mathcal{O}}, H'_{\mathcal{O}})$ where $H'_{\mathcal{O}}(x, y) = H_{\mathcal{O}}(x, y) + \pi H_{\mathcal{O}}(x, y) \pi^{-1} \in R$, and $\pi = \pi_{E_0} \in \mathcal{O}_0$.

Proof. For $M_R = \text{Hom}_{\mathbb{F}_p}(W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E), E_0)$, $M_{\mathcal{O}} = \text{Hom}_{\mathbb{F}_{p^2}}(E, E_0)$, we have $[\mathcal{O}_0 \otimes_R M_R, E_0]_{\mathbb{F}_{p^2}} \cong [M_R, E_0]_{\mathbb{F}_p}$, since $[M_R, E_0]_{\mathbb{F}_p} = W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)$, the action of $\mathcal{O}_0 \otimes_R M_R$ on E_0 is isomorphic to $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)$. It means $\mathcal{O}_0 \otimes_R M_R \cong \text{Hom}_{\mathbb{F}_{p^2}}(W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E), E_0)$.

By $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E) = E \times E^{\sigma}$, we have

$$\mathcal{O}_0 \otimes_R M_R = \text{Hom}_{\mathbb{F}_{p^2}}(W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E), E_0) = \text{Hom}_{\mathbb{F}_{p^2}}(E, E_0) \oplus \text{Hom}_{\mathbb{F}_{p^2}}(E^{\sigma}, E_0) \cong \text{Hom}_{\mathbb{F}_{p^2}}(E, E_0) \oplus \text{Hom}_{\mathbb{F}_{p^2}}(E^{\sigma}, E_0^{\sigma}) \cong M_{\mathcal{O}} \oplus M_{\mathcal{O}}^{\sigma}$$

This is an orthogonal direct sum because if we consider H_R on $\alpha \in M_\theta$ and $\beta \in M_\theta^\sigma$, the element α (resp. β) corresponds to $\alpha \times 0 : E \times E^\sigma \rightarrow E_0; (P, Q) \rightarrow \alpha(P)$ (resp. $0 \times \beta : (P, Q) \rightarrow \beta(Q)$). Hence, we have $H_{\theta_0 \otimes_R M_R}(\alpha, \beta) = (\alpha \times 0) \circ \widehat{0 \times \beta} = 0$.

Conversely, if we have (M_θ, H_θ) , the elements in M_R is the element of $\text{Hom}_{\mathbb{F}_{p^2}}(W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E), E_0)$ that commute with $\pi = \sigma$. For any $(\alpha, \beta) \in \text{Hom}_{\mathbb{F}_{p^2}}(W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E), E_0) \cong \text{Hom}_{\mathbb{F}_{p^2}}(E, E_0) \oplus \text{Hom}_{\mathbb{F}_{p^2}}(E^\sigma, E_0)$, we have $\sigma((\alpha, \beta)) = (\sigma(\alpha), \sigma(\beta))$, and $(\alpha, \beta) \circ \sigma = (\beta \circ \sigma, \alpha \circ \sigma)$, which means $\beta = \pi_{E_0} \alpha \pi_E^{-1}$.

Hence

$$\begin{aligned} M_\theta &\rightarrow M_R \\ \alpha &\rightarrow (\alpha, \pi_{E_0} \circ \alpha \circ \pi_E^{-1}) \end{aligned}$$

is an isomorphism between M_R and M_θ , and

$$H'_\theta(x, y) = H_\theta(x, y) + H_\theta^\sigma(\pi_{E_0} \circ x \circ \pi_E^{-1}, \pi_{E_0} \circ y \circ \pi_E^{-1}) = x\bar{y} + \pi_{E_0} x \bar{y} \pi_{E_0}^{-1}$$

□

These results can be generalized to abelian varieties.

It should be noted that if E is defined over \mathbb{F}_p , then $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)$ is isomorphic to a twist of E^2 , there are two modules of E^2 , that are $\text{Hom}_{\mathbb{F}_p}(E^2, E_0) \cong I_E^2$ or $I_E \times I_E^\sigma$, where $I_E = \text{Hom}(E, E_0)$. The last module is compatible with the σ -action.

7.3 Scholten's Construction: From Bottom to Top

Lemma 7 Let E_0/\mathbb{F}_p be a supersingular curve with primitive Frobenius orientation, and let $A = M \cdot E_0$. Then M is projective iff $A[2](\mathbb{F}_p) \simeq (\mathbb{Z}/2\mathbb{Z})^g$.

Proof. Let us assume first that $p \equiv 3 \pmod{4}$, so that $R = \mathbb{Z}[\sqrt{-p}]$ is not maximal, and let \mathcal{O}_R be its maximal order.

Let $M = \oplus \mathfrak{a}_i$, then $A[2]$ is isomorphic as a R -module to $M/2M$ (as in the proof of Proposition 10). If $O(\mathfrak{a}) = R$, then $\mathfrak{a}/2\mathfrak{a} \simeq R/2R$, and $\text{Ker}(\pi - 1) \simeq \mathbb{Z}/2\mathbb{Z}$ on $\mathfrak{a} \cdot E_0$, while if $O(\mathfrak{a}) = \mathcal{O}_R$, then $\mathfrak{a}/2\mathfrak{a} \simeq \mathcal{O}_R/2\mathcal{O}_R$, and $\text{Ker}(\pi - 1) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ on $\mathfrak{a} \cdot E_0$.

Since M is a direct sum of g modules \mathfrak{a}_i , and each \mathfrak{a}_i is invertible either in R or in \mathcal{O}_R . Let m be the number of modules invertible in R . Then $A[2](\mathbb{F}_p) \simeq (\mathbb{Z}/2\mathbb{Z})^m \times (\mathbb{Z}/2\mathbb{Z})^{2(g-m)}$.

Hence, M is projective iff $m = g$ iff $A[2](\mathbb{F}_p) \cong (\mathbb{Z}/2\mathbb{Z})^g$.

If $p \equiv 1 \pmod{4}$, $R = \mathcal{O}_R$, and in this case M is automatically projective, and $A[2](\mathbb{F}_p)$ always equal to $(\mathbb{Z}/2\mathbb{Z})^g$. □

We can also prove the R orientation of $A = M \cdot E_0$ extend to an \mathcal{O}_R -orientation iff $A[2](\mathbb{F}_p) = (\mathbb{Z}/2\mathbb{Z})^{2g}$. This can be checked directly: the R orientation extend to an \mathcal{O}_R -orientation iff $\frac{1+\pi}{2}$ is well-defined on A iff $\pi = 1$ on $A[2]$.

If E_0 is on the bottom, E'_0 is on the top, we have the action of M on E_0 is horizontal to $E_0^m \times E_0'^{g-m}$. If $m = 0$, we say $A = M \cdot E_0$ is on the top; if $m = g$, we say $A = M \cdot E_0$ is on the bottom.

It is easily to see $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(A)$ (A is supersingular abelian variety over \mathbb{F}_{p^2}) is module action by projective module: if the dimension of $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(A)$ is g , then $\dim(A) = \frac{g}{2}$ and $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(A)[2](\mathbb{F}_p) = A[2](\mathbb{F}_{p^2}) \cong (\mathbb{Z}/2\mathbb{Z})^g$.

The Weil restriction over \mathbb{F}_p are not Jacobian or product of elliptic curves in general.

It should be noted that the classification of principally polarised abelian surface, due to Weil, is indeed as follows: a principally polarized abelian surfaces over finite field k is either

1. a product of two elliptic curves

2. the Jacobian of an hyperelliptic curve of genus 2

3. the Weil restriction of an elliptic curve defined over an extension k' of degree 2 of k

The third case is often forgotten in the crypto litterature (because it disappears over \bar{k} , a Weil restriction is simple but not absolutely simple).

To solve this problem, we have Scholten's construction:

The method for constructing is gluing by kernel $K = \{(T, \sigma(T)) \in E \times E^\sigma \mid T \in E[2]\}$ on $E \times E^\sigma$.

Proposition 16 Let $p \equiv 3 \pmod{4}$, $R = \mathbb{Z}[\sqrt{-p}]$, \mathcal{O}_R be the maximal order, $I = \langle 2, \pi + 1 \rangle$. For any supersingular curve E , we have the Scholten's construction is given by $I \cdot W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)$.

Proof. Since $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)[I] = W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)[2](\mathbb{F}_p)$, and $\pi(P, Q) = (\sigma(Q), \sigma(P))$, then the kernel of I -acting is $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)[I] = W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)[2](\mathbb{F}_p) = \{(P, \sigma(P)) \in E \times E^\sigma \mid P \in E[2]\}$. \square

For $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)$ can be written as $M \cdot E_0$, then the Scholten's construction $I \cdot W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E) = I \cdot M \cdot E_0 = (M \otimes \mathcal{O}_R) \cdot E$, where $E = I \cdot E_0$ is on the top. Similarly to the case of abelian variety A , that is $W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(A) = I \cdot W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(A)$, and if $A = M \cdot E_0$, we have $W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(A) = I \cdot (M \cdot E_0) = (M \otimes_R \mathcal{O}_R) \cdot_{\mathcal{O}_R} E'_0$, where $E'_0 = I \cdot E_0$ is on the top.

From now on, we write Scholten's construction $I \cdot W_{\mathbb{F}_{p^2}/\mathbb{F}_p}$ by $W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}$.

Lemma 8 Assume that $p \equiv 3 \pmod{4}$. Scholten's construction $W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(A)$ is naturally \mathcal{O}_R -oriented, and in particular it has its full 2-torsion rational, and it even has a rational level 2 theta null point rational if $p \equiv 7 \pmod{8}$.

Proof. By the above discussion, $W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(A)$ comes from an \mathcal{O}_R -module action from E (where $E = I \cdot E_0$), so it is naturally \mathcal{O}_R oriented and has its 2-torsion fully rational.

It remains to check that it has a rational level 2 theta null point. If 2 splits in \mathcal{O}_R (i.e. $p \equiv 7 \pmod{8}$), the decomposition $(2) = \mathfrak{p}_2 \bar{\mathfrak{p}}_2$ gives a symplectic decomposition $B[4] = B[\mathfrak{p}_2^2] \oplus B[\bar{\mathfrak{p}}_2^2]$ for any \mathcal{O}_R -oriented abelian variety, so in particular for $W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(A)$.

This is sufficient for $W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(A)$ to have a rational theta null point. \square

The reason for Scholten's construction rather than Weil restriction is there are rational theta null points over \mathbb{F}_p .

Proposition 17 Let $\mathcal{O}_0 = \text{End}(E_0)$, $\mathcal{O}'_0 = \text{End}(E'_0)$, A/\mathbb{F}_{p^2} be a maximal supersingular abelian variety, and $(M_{\mathcal{O}'}, H_{\mathcal{O}'}) = \text{Hom}_{\mathbb{F}_{p^2}}(A, E'_0)$. Then $W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(A) = (M_{\mathcal{O}'}, H_{\mathcal{O}'}) \cdot_{\mathcal{O}_R} E'_0$, where $M_{\mathcal{O}'}$ is considered as an \mathcal{O}_R -module and $H_{\mathcal{O}'}$ is the Hermitian \mathcal{O}_R -form on $M_{\mathcal{O}'}$ with the same quadratic form as the one given by $H_{\mathcal{O}'}$.

In other words, while the Weil restriction corresponded to forgetting the \mathcal{O}_0 structure on M when $A = M \cdot E_0$ (only keeping the R -structure), Scholten's construction corresponds to forgetting the \mathcal{O}'_0 structure on $M' = M \otimes_R I$ when $A = M' \cdot E'_0$ (only keeping the \mathcal{O}_R structure).

Proof. We have $E'_0 = I \cdot E_0$, then $E'_0 = (\mathcal{O}_0 \otimes_R I) \cdot E_0$, and thus $\text{Hom}_{\mathbb{F}_{p^2}}(E'_0, E_0) = \mathcal{O}_0 \otimes_R I$.

Let $I_0 = \mathcal{O}_0 \otimes_R I$, which is a left \mathcal{O}_0 -module. We have

$$\begin{aligned} \mathcal{O}'_0 &= \text{Hom}(E'_0, E'_0) \\ &= \text{Hom}(I_0 \cdot E_0, I_0 \cdot E_0) \\ &= \text{Hom}_{\mathcal{O}_0}(I_0, I_0) = I_0^\vee \otimes_{\mathcal{O}_0} I_0 \\ &= \text{Hom}_{\mathcal{O}_0}(I \otimes_R \mathcal{O}_0, \mathcal{O}_0) \otimes_{\mathcal{O}_0} \mathcal{O}_0 \otimes_R I \\ &= \text{Hom}_R(I, \mathcal{O}_0) \otimes_R I = I^\vee \otimes_R \mathcal{O}_0 \otimes_R I \\ &= I \otimes_R \mathcal{O}_0 \otimes_R I \end{aligned}$$

Similarly, if $M_{\mathcal{O}} = \text{Hom}_{\mathbb{F}_{p^2}}(A, E_0)$, we have $M_{\mathcal{O}'} = \text{Hom}_{\mathbb{F}_{p^2}}(A, E'_0) = \text{Hom}_{\mathbb{F}_{p^2}}(M_{\mathcal{O}} \cdot E_0, (\mathcal{O}_0 \otimes_R I) \cdot E_0) = \text{Hom}_{\mathcal{O}_0}(\mathcal{O}_0 \otimes_R I, M_{\mathcal{O}}) = (\mathcal{O}_0 \otimes_R I)^\vee \otimes_{\mathcal{O}_0} M_{\mathcal{O}} = I_0^\vee \otimes_{\mathcal{O}_0} M_{\mathcal{O}}$.

However, $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(A) = M \cdot E_0$, where $M = M_{\mathcal{O}}$ as an R -module, and $W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(A) = I \cdot W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(A) = I \cdot M \cdot E_0 = M \cdot E'_0 = (M \otimes_R I) \cdot_{\mathcal{O}_R} E'_0 = M' \cdot_{\mathcal{O}_R} E'_0$, and $M' = I \otimes_R M$.

But as an \mathcal{O}_R -module, we also have $M_{\mathcal{O}'} = I \otimes_R \mathcal{O}_0 \otimes_{\mathcal{O}_0} M_{\mathcal{O}} = M'$.

Now, for the polarisation, since E_0 and E'_0 are linked by a 2-isogeny, the \mathcal{O} -Hermitian form on $M_{\mathcal{O}'}$ and $M_{\mathcal{O}}$ and the R -Hermitian form on M' and M differ by a factor 2 (via the appropriate pullback). But the quadratic form on M is twice the quadratic form on $M_{\mathcal{O}}$, on the other hand the quadratic form on M' seen as a S -module is half the quadratic form on M' seen as a R -module. This means that the pullback of it on M is equal to H_M , whose quadratic form is twice the one induced by $H_{M_{\mathcal{O}}}$ so corresponds to the pullback of $M_{\mathcal{O}'}$. In other words, the quadratic form induced on M' is precisely the one from $M_{\mathcal{O}'}$. \square

Proposition 18 Let E/\mathbb{F}_p be a rational supersingular curve with rational 2-torsion (so E is horizontally isogenous to E'_0), and $A = W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)$. Then $A \simeq E \times E^t$, where E^t is the quadratic twist of E .

Proof. Scholten's construction is given by the quotient of $E \times E^\sigma$ by the kernel $K = \{(T, \sigma(T)), \forall T \in E[2]\}$. But with our hypothesis, $E^\sigma = E$ and $\sigma(T) = T$, hence the kernel is simply $K = \{(T, T), \forall T \in E[2]\}$. Let $\Phi : E^2 \rightarrow E^2, (P, Q) \mapsto (P + Q, P - Q)$, this Φ has the same kernel K , the diagonal of $E[2]$ in E^2 , hence $E^2/K \simeq E^2$ over \mathbb{F}_{p^2} .

Now if we descend Φ to $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)$, the codomain will be $E \times E^t$ over \mathbb{F}_p . We can find it by keeping track of the Galois action, the one on the Weil restriction is given by $\sigma(P, Q) = (\pi(Q), \pi(P))$, and applying Φ to this we get $(\pi(P + Q), -\pi(P - Q))$. So on the codomain the Galois action is the usual one on the first factor and on the second one (by -1) on the second factor. This twist by -1 corresponds to the quadratic twist E^t of E . \square

8 Supersingular Isogeny Path Problem and Module Action Inversion

Definition 8 (Module Inversion) Given principally polarized abelian varieties $(A, \lambda_A), (M \cdot A, H_{M \cdot \lambda_A})$, recover a description of the unimodular Hermitian module (M, H_M) .

Like in the supersingular case, we could ask for variants of this problem where we ask to recover the effective orientation of M on $M \cdot A$, or if we just want to recover partial informations on M , e.g. one element $M \cdot A \rightarrow A$ corresponding to $m \in M$. We could also ask for the relationship, given $M \cdot E_0$, between knowing $\text{End}_R(M \cdot E_0)$ and knowing M (in rank > 1), and so on. We leave it for future work to study the relationship between these variants.

Example 3 If $(A, \lambda_A) = (M, H_M) \cdot (E_0, \lambda_{E_0})$, then $M = \text{Hom}_R(A, E_0)$, and the Hermitian form H_M is given as follows: for m_1, m_2 which we interpret as morphisms $A \rightarrow E_0$, then $m_1 \hat{m}_2$ gives an R -endomorphism of E_0 , hence an element of R , which is $H_M(m_1, m_2)$.

Let E be a supersingular elliptic curve. If we find an isogeny path $\phi : E_0 \rightarrow E$, then we obtain an isogeny $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\phi) : W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_0) \rightarrow W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)$.

$$\begin{aligned} W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\phi) : W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_0) &\rightarrow W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E) \\ (P, Q) &\rightarrow (\varphi(P), \sigma \circ \varphi \circ \sigma^{-1}(Q)) \end{aligned}$$

The Frobenius on left is $(P, Q) \rightarrow (\sigma(Q), \sigma(P))$, after $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\phi)$, the image is $(\varphi(\sigma(Q)), \sigma \circ \varphi \circ \sigma^{-1}(\sigma(P))) = (\varphi(\sigma(Q)), \sigma \circ \varphi(P))$.

The Frobenius on right is $(\varphi(P), \sigma \circ \varphi \circ \sigma^{-1}(Q)) \rightarrow (\sigma^2 \circ \varphi \circ \sigma^{-1}(Q), \sigma \circ \varphi(P)) = ([-p] \circ \varphi \circ \sigma^{-1}(Q), \sigma \circ \varphi(P)) = (\varphi \circ \sigma(Q), \sigma \circ \varphi(P))$

Conversely, if we have some path $\Phi : W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_0) \rightarrow W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)$ over \mathbb{F}_p , then over \mathbb{F}_{p^2} , we get $\Phi : E_0^2 \rightarrow E \times E^\sigma$. Now Φ is given by a matrix of isogenies, and at least one of the isogeny $E_0 \rightarrow E$ or $E_0 \rightarrow E^\sigma$ in this matrix is non-trivial. It follows that, composing with π_p if necessary, we obtain a non-trivial isogeny $E_0 \rightarrow E$. We see that the path problem between E_0 and E and the one between $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_0)$ and $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)$ are essentially equivalent.

Theorem 18 Assume that we know $\mathcal{O}_0 = \text{End}(E_0)$. Then the isogeny path problem $E_0 \rightarrow E$ reduces to the rank 2 module inversion problem on E_0 , $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)$.

Proof. From E we can compute its Weil restriction $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)$. Let $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E) = (M, H_M) \cdot E_0$. From Theorem 17, we have shown that the knowledge of $I = \text{Hom}_{\mathbb{F}_{p^2}}(E, E_0)$ is equivalent to the knowledge of (M, H_M) . Since the isogeny path reduces to finding I , the result follows. \square

How to compute M_2 for given isogeny $M_1 \cdot A \rightarrow M_2 \cdot A$. Since $M_2 \hookrightarrow M_1$ and $(M_1 \cdot A)[M_2] = \ker(M_1 \cdot A \rightarrow M_2 \cdot A)$, $nM_1 \subseteq M_2 \subseteq M_1$, we can use $\ker(M_1 \cdot A \rightarrow M_2 \cdot A)$ to test which elements of M_1 belong to M_2 .

Remark 10 We give some heuristics about the security of the rank 2 module inversion:

- We focus on the subcategory $\mathfrak{A}_{E_0, R}$ given by abelian surfaces: that is, supersingular abelian surfaces over \mathbb{F}_p which are isogenous to E_0^g over \mathbb{F}_p . We conjecture that there are about $p^{3/2}$ such abelian surfaces, and that the ℓ -isogeny graph is an expander graph.

The reason for the above conjecture is if $A = W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)$ is the Weil restriction of E , then we do not get another Weil restriction by the action of an invertible ideal (unless E is already defined over \mathbb{F}_p). We note that there are about p Weil restrictions of supersingular curves, and $\approx \sqrt{p}$ invertible ideals, which give $p^{\frac{3}{2}}$ supersingular abelian surfaces isogenous to E_0^2 over \mathbb{F}_p .

- The best known algorithm to solve the supersingular isogeny path problem has a time complexity of $\tilde{O}(\sqrt{p})$. Delf and Galbraith gives a heuristic version, which consists in taking random paths until we hit a supersingular curve over \mathbb{F}_p . We expect to solve the general module inversion problem by using a heuristic algorithm similar to Delf and Galbraith: take random paths until we find an abelian surface A' isogenous to a product polarization, and reduce it to a rank 1 problem, i.e., the Hermitian module corresponding to A' is an orthogonal direct sum of ideals. Then we perform the module inversion on A' and go back to the original A through a smooth path.

Heuristically, it should reach the target in $\tilde{O}(\sqrt{p})$ time (for there are $O(p^{3/2})$ vertices of \mathbb{F}_p -abelian surfaces isogenous to E_0^2 , and the number of product of supersingular elliptic curves is approximately $O(\sqrt{p} \cdot \sqrt{p}) = O(p)$). The rank 1 problem is known to be solvable in heuristic $\tilde{O}(p^{1/4})$ time, or in quantum sub-exponential time. We can also look for a Weil restriction, which we expect to find in $\tilde{O}(\sqrt{p})$ time.

However, since the problem of computing isogenies between E_0 , E and the problem of Weil restriction of them are equivalent, the complexity of both problems is $O(\sqrt{p})$.

- Can we recover M from $\text{End}(M \cdot A)$?

If $A = E_0$ or other primitively oriented elliptic curves and M is an invertible ideal, then $\text{End}(M \cdot A) = R$, so this information is vacuous in that case.

If $A = E_0$, $M \cdot A = W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)$ is the Weil restriction of a supersingular elliptic curve E over \mathbb{F}_{p^2} , then

$\text{End}(A) = \text{Hom}_{\mathbb{F}_p}(W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E), W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)) = \text{Hom}_{\mathbb{F}_{p^2}}(W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E) \times_{\mathbb{F}_p} \mathbb{F}_{p^2}, E) = \text{Hom}_{\mathbb{F}_{p^2}}(E \oplus E^\sigma, E) = \text{End}(E) \oplus \mathfrak{p}$, where \mathfrak{p} is the unique bi-ideal of $\text{End}(E)$ of reduced norm p : $p = \mathfrak{p}^2$ in $\text{End}(E)$. So from $\text{End}(E)$, we obtain $\text{End}(A)$.

Conversely, if we know $\text{End}(A)$, working over \mathbb{F}_{p^2} , we obtain endomorphisms of $E \times E^\sigma$ and we easily get $\text{End}(E)$.

From the knowledge of $\text{End}(E)$, we compute $I = \text{Hom}_{\mathbb{F}_{p^2}}(E, E_0)$. Hence, from Theorem 18, we obtain M such that $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E) = M \cdot E_0$.

9 \otimes -MIKE: Tensor Module Isogeny Key Exchange

If G is a commutative group acting on a set X , there is the well known generalisation of Diffie-Hellmann key exchange given as follows: we fix a base point $x_0 \in X$, Alice and Bob takes secret $a, b \in G$ and publish $a \cdot x_0$ and $b \cdot x_0$ respectively. Their common secret is $(ab) \cdot x_0 = a \cdot (b \cdot x_0)$.

Model for CSIDH(OSIDH) the action of the group $\text{Pic}(R)$ of invertible R -ideals on R -oriented elliptic curves. We argue that we should consider the invertible ideals not as a group, but as the symmetric monoidal category of rank 1 projective modules over R .

Likewise, oriented elliptic curves form a natural category, with morphisms the R -oriented isogenies (and 0). It is easy to see that the usual ideal action is actually (contravariantly) compatible with these morphisms, hence form a symmetric monoidal contravariant action.

Model for SQIsign Assume that it is hard to compute morphisms in \mathcal{O} between two given objects; then Alice has for secret key such a morphism $\varphi : x \rightarrow y$, and for public key the domain and codomain x, y . Bob challenges with an element $b \in \mathfrak{C}$ and Alice responds to the challenge with $b \cdot \varphi : b \cdot x \rightarrow b \cdot y$, since Bob can compute $b \cdot x, b \cdot y$, he can check that the morphism is between the correct domain and codomain. Of course, a difficulty in instantiating such a scheme, is that $b \cdot \varphi$ should not provide information on φ .

Hermitian module key exchange:

$$\begin{array}{ccc} A_0 & \longrightarrow & A_1 = M_1 \cdot A_0 \\ \downarrow & & \downarrow \\ A_2 = M_2 \cdot A_0 & \longrightarrow & A_{12} = (M_1 \otimes M_2) \cdot A_0 \end{array}$$

$(A_0, \lambda_{A_0}) \in \mathfrak{Ab}_R$ has dimension g_0 , M_1, M_2 are finitely presented projective R -module with rank g_1, g_2 , $A_{12} = (M_1 \otimes M_2) \cdot A_0$ has dimension $g_1 g_2 g_0$. If $A_0 \in \mathfrak{Ab}_{E,R}$, the projectivity condition on M_i to torsion free.

The method for Alice to compute $M_1 \cdot A_0$ is to compute a smooth n_1 -isogeny $(M_1, H_1) \rightarrow (R^{g_1}, H_R^{g_1})$, then she obtains $A^{g_1} \rightarrow A_1$ for A^{g_1} is effective. Similarly to Bob.

Hence we have n_1 -isogeny $A_0^{g_1} \rightarrow A_1$ and n_2 -isogeny $A_0^{g_2} \rightarrow A_2$ (we require n_1, n_2 are coprime), then we have the following diagram:

$$\begin{array}{ccc} A_0^{g_1 g_2} & \longrightarrow & A_1^{g_2} \\ \downarrow & & \downarrow \\ A_2^{g_1} & \longrightarrow & A_{12} = (M_1 \otimes M_2) \cdot A_0 \end{array}$$

On the module side, the diagram corresponds to:

$$\begin{array}{ccc} R^{g_1} \otimes_R R^{g_2} & \longrightarrow & M_1 \otimes_R R^{g_2} \\ \downarrow & & \downarrow \\ R^{g_1} \otimes_R M_2 & \longrightarrow & M_1 \otimes_R M_2 \end{array}$$

To compute A_{12} , we can also use Clapoti method, which means $n_1 + n_2$ is smooth. This allows us to relax the smoothness condition on n_1 .

Instantiation on supersingular elliptic curves:

In order to have an efficient module key exchange, we will start on $A_0 = E_0$ an elliptic curve, typically use a supersingular elliptic curve E_0/\mathbb{F}_p (on the bottom of the 2-volcano) to have a good control on its torsion, as in CSIDH, and act by rank 2 module (to prevent Kuperberg).

We will select a prime of the form $u2^e - 1$ with e large, in order to use 2^e -isogenies in higher dimension. So in that case A_1, A_2 are supersingular abelian surfaces over \mathbb{F}_p , and A_{12} is of dimension 4. The key exchange takes $3 \log p$ bit to send the Igusa invariants $J(A_i)$.

It should be noted that if $p \equiv 3 \pmod{4}$, $E_0 : y^2 = x^3 + x$ over \mathbb{F}_p , its twist $E'_0 : y^2 = x^3 - x$ and $IE_0 = E'_0$. By computation, we have $E_0^t = E'_0$ and $E_0'^t = E'_0$. Hence $W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E'_0) = E_0'^2$.

$$\begin{array}{ccc}
E'_0 & \longrightarrow & E_1 \\
\downarrow & & \downarrow \\
E_2 & \longrightarrow & W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_1) \otimes_{E'_0} W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_2) \\
\\
E_0'^4 & \longrightarrow & W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_1)^2 \\
\downarrow & & \downarrow \\
W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_2)^2 & \longrightarrow & W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_1) \otimes_{E'_0} W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_2)
\end{array}$$

For the security, we need E_1, E_2 are randomly chosen. We use the method in SQIsign2D-West, that is one selects a left-ideal I in $\mathcal{O}' = \text{End}(E'_0)$, and computes two equivalent ideals I_1, I_2 with reduced norm d_1, d_2 , computes positive integers u, v such that $ud_1 + vd_2 = 2^e$, $u = u_1^2 + u_2^2$, $v = v_1^2 + v_2^2$, and computes an endomorphism γ of E'_0 with degree uvd_1d_2 , where $\gamma \in \mathcal{O}'$.

We also consider γ as an endomorphism of $E'_0/\mathbb{F}_{p^2} \cong W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E'_0)/\mathbb{F}_p$, therefore, $\gamma \in M_2(\mathcal{O}_R)$. Then γ is an endomorphism of $W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_2)$, since γ is in matrix of R -orientation. Alice then splits using a 8-dimensional isogeny to obtain the dimension four abelian variety A_{12} .

However, in this case, we need compute 8-dimension isogenies, which leads the key-exchange inefficient. When Alice obtains $j(E_2)$ from Bob, she computes $W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_2)$. We assume the secret isogeny of Alice corresponds to left \mathcal{O}' -ideal I_1 , then the embedding $I_1 \hookrightarrow \mathcal{O}'$ is also an \mathcal{O}_R -module isogeny $M_1 \hookrightarrow \mathcal{O}_R^2$ and the degree of this module isogeny equals to the degree of secret isogeny. She computes $K = A_2^2[M_1]$, where $A_2 = W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_2)$. By computing A_2^2/K , she obtains $A_{12} = W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_1) \otimes_{E'_0} W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_2)$. (Here we assume $M_1 \hookrightarrow \mathcal{O}_R^2$ is $m_1 \rightarrow (r_1, r_2)$, then $m_1 \cdot A_2 : (P, Q) \rightarrow r_1P + r_2Q$, the kernel of this map is $\ker(m_1)$ and $\ker(M_1) = \cap \ker(m_1)$.)

Hence, Alice only computes 4-dimensional isogeny. However, if Bob also computes 2^e -isogeny as his secret isogeny, the actions of Alice after Bob leads to $E_0'^4$, then we need the degree of secret isogenies of Alice and Bob are coprime. Moreover, if Alice computes 2^e -isogeny as secret key, Bob computes 3^f -isogeny as secret key, it required the prime p equals to $2^e 3^f - 1 \approx 2^{4\lambda}$, and j -invariant $\approx 2^{8\lambda}$. This double the key size compared to the previous variant.

Theorem 19 Assume that we know $\mathcal{O}_0 = \text{End}(E_0)$. Assume that the rank 2 module action-CDH from Weil restriction of supersingular curves is as hard as the inversion. Assume that the isogeny path problem on E_1, E_2 is as hard as for a uniformly sampled supersingular curve E , and that the best attack against this problem is in $\tilde{O}(\sqrt{p})$.

Then for λ bits of security for \otimes -MIKE, we need to select p with size 2λ . The key exchange which outputs the j -invariant of the E_i then takes 4λ bits for each E_i .

Proof. By assumption action-CDH is as hard as action-inversion, which by Theorem 5.22 is at least as hard as the supersingular isogeny path problem on E_1 or E_2 .

We note that since $2^e \approx p$, there are $\approx p$ possible different 2^e -isogenies for Alice starting from E'_0 over \mathbb{F}_{p^2} , so the assumption that the isogeny path problem between E'_0 and E_1 being as hard as for a random supersingular curve is not made immediately vacuous by a meet in the middle collision. \square

Compare Module Action and Ideal Action

- Invertible ideals form a group, this is very convenient for cryptography. By contrast, projective modules of rank > 1 are not invertible, hence we only have a monoid.

algorithm 1 The \otimes -MIKE key exchange on Alice's side

INPUT: The supersingular curve $E'_0/\mathbb{F}_p : y^2 = x^3 - x$, primitively oriented by \mathcal{O}_R , with $p = u \cdot 2^e - 1$.

OUTPUT: The common secret $J(A_{12})$ in the \otimes -MIKE key exchange from Alice's point of view

- 1: As a precomputation step, compute a basis (P, Q) of $E'_0[2^e]$ and how generators of \mathcal{O}'_0 act on this basis.
 - 2: Alice selects a random kernel $K = \langle uP + vQ \rangle$ of degree 2^e , along with its corresponding ideal I .
 - 3: She computes $E_1 = E/K$, and send $j(E_1)$ to Bob.
 - 4: The \mathcal{O}'_0 -ideal 2^e -similitude $\Phi : I \hookrightarrow \mathcal{O}'_0$ gives (by forgetting the \mathcal{O}'_0 -orientation), a unimodular \mathcal{O}_R -module 2^e -similitude $\psi : M_1 \hookrightarrow \mathcal{O}_R^2$.
 - 5: She selects a model $j(E_2)$ from Bob's model of E_2 .
 - 6: She computes the Scholten construction $A_2 = W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_2)$.
 - 7: She computes the kernel $K' = (A_2^2)[M_1]$, where the action of $m_1 \in M_1$ on A_2^2 is given by, if $\psi(m_1) = (\gamma_1, \gamma_2)$, $(P_1, P_2) \in A_2^2 \mapsto \gamma_1 P_1 + \gamma_2 P_2 \in A_2$, where $\gamma_i P_i$ is computed via the Frobenius orientation.
 - 8: She computes the quotient $A_{12} = (A_2^2)/K'$.
 - 9: She output $J(A_{12})$ where J are dimension 4 modular invariants.
-

- Each action by a projective module of rank g multiplies the dimension by g . Hence, even in rank $g = 2$, we can only act by very few modules before the dimension explodes.
- It follows that the module action is a lot less flexible than the ideal action. However, for security, this drawbacks turn into advantages, preventing Kuperberg's algorithm to apply directly.
- The module action computes 4 or 8-dimensional isogeny, and ideal action computes 1-dimensional isogeny. However, ideal action requires using isogenies of large degree. And a dimension 4 2^u -isogeny, while quite a bit slower than a dimension 1 2^u -isogeny, will be faster than a dimension 1 ℓ -isogeny for $\ell \approx 2^u$ large enough.
- The main drawback is that we have only discussed Alice's side here, while in Bob's side, he needs to compute a dimension 8 2^e -isogeny over \mathbb{F}_p to complete the second part of the key exchange, which will be much more expansive (and annoying to implement) than Alice's dimension 4 counterpart.

Kuperberg's algorithm can't apply for the module action

- First, we have a monoid, rather than a group.
- Secondly, the monoid is not finite, nor even finitely generated (a projective module of rank a prime number ℓ can only be written as a tensor product of another module of rank ℓ and an ideal)
- And finally, each action increases the dimension, so the action acts on an infinite set.

Although we now have good signatures algorithms, like **SQIsign2D** whose security properties reduce to the supersingular isogeny path problem, this is not the case key exchange schemes or public key encryption based on supersingular isogenies.

MIKE is a first step towards this direction, since it requires to publish neither torsion point, nor partial information on the endomorphism rings of E_1, E_2 .

MIKE gets a more inefficient scheme (but still polynomial time with respect to the security parameter), especially on Alice's side, whose security reduces to the action-CDH problem for (the Weil restriction of) random supersingular elliptic curves.