Isogeny Club: Module Action

Zheng Xu

2025-6-13

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. $M^{\vee\vee} \cong M$).

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

Then there exists a long exact sequence:

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

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

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

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

Since $\mathrm{Tor}_1^R(K/R, M) = 0$, 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 ($\dim_K(V)$).

2. Consider the exact sequence $0 \to R \to K \to K/R \to 0$, we have the long exact sequence:

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

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

3. Assume $T = M_1/M_2$ is torsion R-module, where M_1 is torsion free modules, M_2 is submodule of M_1. From the exact sequence $0 \to M_2 \to M_1 \to M_1/M_2 \to 0$, we have the long exact sequence:

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

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

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

The proof is false in Robert's article.

Recently, Robert sends an e-mail to modify the requirement of R to Bass order. It is easily to see the Dedekind domains and maximal orders in quaternion algebra are Bass order. However, the order in quadratic order may not Bass order, he modify the requirement to an order $\mathcal{O}$ of complex multiplication with maximal real multiplication, then $\mathcal{O}$ is Bass.

Torsion-Free Modules

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.

R is an order in imaginary quadratic field case:

- 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 $\mathcal{O}(I)$).
- Futhermore, 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.

R is maximal order in quaternion algebra case:

- 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 $\{x_1, \cdots, x_g\}$ of $V = M \otimes_R K$ such that $M = I_1 x_1 \oplus I_2 x_2 \oplus \cdots \oplus I_g x_g$, where $K = M \otimes \mathbb{Q}$ and I_i are ideals in R.*

Defintion 1. *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).

Module Isogenies

Defintion 2. *Let $\varphi : M_2 \to M_1$ 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 $\#M_1/\varphi(M_2)$.

If $\varphi : M_2 \hookrightarrow M_1$ is an isogeny, we have an exact sequence: $0 \to M_1^\vee \to M_2^\vee \to \operatorname{Ext}^1_R(M_1/M_2, R)$.
Hence $\varphi^\vee : M_1^\vee \to M_2^\vee$ is an isogeny with cokernel in $\operatorname{Ext}^1_R(M_1/M_2, R) \cong \operatorname{Hom}_R(M_1/M_2, K/R)$.
if R is Bass order M_1, M_2 are projective R- modules, then $\operatorname{Ext}^1_R(M_1, R) = 0$, which means
$\#M_2^\vee/M_1^\vee = \#\operatorname{Ext}^1_R(M_1/M_2, R) = \#\operatorname{Hom}_R(M_1/M_2, K/R) = \#M_1/M_2$.
The last equality is from M_1/M_2 is isomorphic to product of R/I, for any R/I, we have:

$$\Phi : \operatorname{Hom}_R(R/I, K/R) \to I^{-1}/R$$
$$\varphi \to \varphi(1+I) + R$$

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 $\varphi_a \in \operatorname{Hom}_R(R/I, K/R)$ 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 $\operatorname{Hom}(R/I, K/R) \cong I^{-1}/R$, then $\#\operatorname{Hom}_R(R/I, K/R) = \#I^{-1}/R = \#R/I$.
Hence, $\#\operatorname{Hom}_R(M_1/M_2, K/R) = \#M_1/M_2$.

Hermitian Modules

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 $H : M \times M \to R$ be a bilinear map, we can define $\varphi_H : M \to M^\vee = \mathrm{Hom}_{\bar{R}}(M, R)$, 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:

$$H : M \times M \to R$$
$$(x, y) \to \varphi(x)(y)$$

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 $H_K : V \times V \to K$.*

- (**Non-degenerate and positive-definite**) We say an Hermitian form is non-degenerate if φ_H is monmorphism (i.e. isogeny). If $H(x, x) > 0$ for any $0 \neq x \in M$, we say H is positive-definite. (φ_H is monmorphism 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 $\varphi_H : M \to M^\vee$ is isomorphism.
- (**Orthogonal**) Given an Hermitian form $H_K : V \times V \to K$, we define R-orthogonal of R-latice $M \subseteq V$ as $M^\perp = \{x \in V \mid H_K(x, y) \in R \quad \forall y \in M\}$.
- 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:

  $$M^\perp \to M^\vee$$
  $$x \to H_K(x, \cdot)$$

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

Remark 3. *Now we prove the isomorphism between $M^\perp$ and $M^\vee$.*

Proof.

$$\Phi : M^\perp \to M^\vee$$
$$x \to H_K(x, \cdot)$$

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 $M \to M^\vee$, we have $c(x - y) = 0$, which means $x = y$. We obtain Φ is injective.

For any $f \in M^\vee = \mathrm{Hom}(M, R)$, 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. □

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 $\psi : M_1 \to M_2$.

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 $\psi' : M_2^\perp \to M_1^\perp$ 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 $(x_1,\cdots,x_g)$, then we have $M^{\perp}=\sum_{i=1}^{g}\overline{(R:I_i)}x_i^{\perp}$, where $(R:I)=\frac{\bar{I}}{\mathrm{Nrd}(I)}$. 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 $H(a_1x_1^{\perp},\sum_{i=1}^{g} b_ix_i)\in R$, which mean $H(a_1x_1^{\perp},b_1x_1)\in R$, hence $a_1\overline{b_1}\in R$. Since for all $b_1\in I_1$ we have $a_1\overline{b_1}\in R$, we get $a_1\in\frac{I_1}{\mathrm{Nrd}(I_1)}=\overline{(R:I_1)}$.

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 $I^{-1}=(R:I)=\frac{\bar{I}}{\mathrm{Nrd}(I)}$. Hence, we have $M^{\perp^{\perp}}=M$. □

It should be noted that Hermitian modules have orthogonal decomposition: (M_i,H_{M_i}), where $(M,H_M)=(M_1,H_{M_1})\oplus(M_2,H_{M_2})\oplus\cdots$, 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 $H \mod R: M_1/M_2\times M_2^{\perp}/M_1^{\perp}\to K/R$ 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 $H_K \mod n: M/nM\times M^{\perp}/nM^{\perp}\to R/nR$ 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 $[n]$. □

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 $\mathrm{Hom}_R(M_1,M_2)$ are torsion free, and $\mathrm{Tor}_1^R(M_1,M_2)=0$.*

Proof. Since for any multiplicative subset S of R, we have $S^{-1}(\mathrm{Tor}_1^R(M_1,M_2))\cong\mathrm{Tor}_1^{S^{-1}R}(S^{-1}M_1,S^{-1}M_2)$. We choose $S=R\backslash\mathfrak{p}$, 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 $M_{1,\mathfrak{p}}\otimes_{R_{\mathfrak{p}}}M_{2,\mathfrak{p}}\cong M_{2,\mathfrak{p}}^n$, $\mathrm{Hom}_{R_{\mathfrak{p}}}(M_{1,\mathfrak{p}},M_{2,\mathfrak{p}})\cong M_{2,\mathfrak{p}}^n$ are torsion free $R_{\mathfrak{p}}$-modules, $\mathrm{Tor}_1^{R_{\mathfrak{p}}}(M_{1,\mathfrak{p}},M_{2,\mathfrak{p}})=0$.

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

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

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

1. *$(M_1\oplus M_2,H_1\oplus H_2)$ 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 $(I^{\perp},H/\mathrm{Nrd}(I))$ is a unimodular Hermitian module, where $I^{\perp}=\frac{I}{\mathrm{Nrd}(I)}=\overline{(R:I)}$.*

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

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

Let $H : M \times M \to R$ 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 $(M_2, H) \to (M_1, H)$, with dual isogeny $(M_1^\perp, H) \to (M_2^\perp, H)$, 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 $H : M_1/M_1^\perp \times M_1/M_1^\perp \to K/R$, which maps $(M_2, H) \to (M_1, H)$ 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 $(M^\perp, H) \to (M_1, H)$ is a polarized isogeny.)*

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

$$\begin{tikzcd} M_1^\perp \arrow[r, "d_1"] \arrow[d, "d"] & M_1 \\ M_2^\perp \arrow[r, "d_2"] & M_2 \arrow[u, "d"'] \end{tikzcd}$$

- *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 $M_1/nM_1 \times M_1/nM_1 \to \frac{1}{n}R/R$.*

  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 country, 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)**.**

$$\begin{tikzcd} M_0 \arrow[r, "\psi_1"] \arrow[d, "\psi_2"] & M_1 \arrow[d, "\psi_2'"] \\ M_1 \arrow[r, "\psi_1'"] & M_{12} \end{tikzcd}$$

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

$$x : (M, H_M) \to (M, H_M)$$
$$m \to xm$$

Hence $x^*H_M(m,m') = H_M(xm,xm') = \mathrm{Nrd}(x)H_M(m,m')$, 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).

Symmetric Monoidal Category

Defintion 3 (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 $Y \otimes_{\mathfrak{C}} -$ 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 $\mathrm{Hom}_{\mathfrak{C}}(c,[c_1,c_2]_{\mathfrak{C}}) = \mathrm{Hom}_{\mathfrak{C}}(c \otimes_{\mathfrak{C}} c_1, c_2)$.

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 $\cdot : \mathfrak{C} \times \mathfrak{D} \to \mathfrak{D}$, which respect the "obvious coherence conditions". Equivalently, an action is given by a monoidal functor from $\mathfrak{C} \to \mathrm{End}(\mathfrak{D})$.

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 $\mathrm{Hom}_{\mathfrak{D}}(d_1,d_2)$ as living in $\mathfrak{C}$ rather than in Set.

Defintion 4. *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 $[c,d]_{\mathfrak{C}} : X \in \mathfrak{D} \to \mathrm{Hom}_{\mathfrak{D}}(X,[c,d]_{\mathfrak{C}}) = \mathrm{Hom}_{\mathfrak{C}}(c,\mathrm{Hom}_{\mathfrak{D}}(X,d))$. 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.

Power Objects in an Abelian Category

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

Theorem 1 (Existence of Power Object)**.** *If $A \in \mathscr{A}$ is R-oriented, M is a finitely presented R-module, the power object $[M,A]_R$ exists in $\mathscr{A}$ ($\mathrm{Hom}_{\mathscr{A}}(X,[M,A]_R) = \mathrm{Hom}_R(M,\mathrm{Hom}_{\mathscr{A}}(X,A))$). Moreover, the contravariant functor $[-,A]_R$ is functorial and left exact.*

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

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

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

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

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

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

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 4. *There are some properties about power object we defined above.*

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

$$f_A : X \in \mathscr{A} \to \mathrm{Hom}_{\mathscr{A}}(X,A)$$

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

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

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* $R^m \to R^n \to M \to 0$*, by acting* $[-,A]_R$*, we obtain the exact sequence* $0 \to [M,A]_R \to A^n \to A^m$.

  The map $\psi : R^m \to R^n$ *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* $\varphi = [\psi,A]_R : A^n \to A^m$*, 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 $\mathrm{Hom}_{\mathscr{A}_R}(A,B)$ or even $\mathrm{Hom}_R(A,B)$, dropping the orientations i_A, i_B from the notation by simplicity.

Theorem 2 (Existence of Power Object with R-orientation)**.** *Let* R *be a commutative ring, and* $\mathscr{A}_R$ *be the* R*-oriented category of* $\mathscr{A}$*: objects are given by* (A,i_A) *with* $A \in \mathscr{A}_R$ *and* $i_A : R \to \mathrm{End}_{\mathscr{A}}(A)$ *is* R*-orientation, and morphisms* $(A,i_A) \to (B,i_B)$ *are morphisms* $A \to B$ *in* $\mathscr{A}$ *respecting the orientations on* A *and* B*. For any* $f : (A,i_A) \to (B,i_B)$*,* $r \in R$*, we have the following commutative diagram:*

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

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

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

The functor $[-,-]_R : R-\textbf{\textit{modules}} \times \mathscr{A}_R \to \mathscr{A}_R$ *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 $\varphi : A^n \to A^m$, 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 $X \in \mathscr{A}_R$, $\mathrm{Hom}_{\mathscr{A}_R}(X,A)$ is R-module, we have:

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

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

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

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

From above, we have the symmetric monoidal contravariant action from finitely presented R-module to R-oriented objects in $\mathscr{A}$, 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)* $R \subseteq S \subseteq \mathrm{End}_{\mathscr{A}}(A)$*, 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 $\mathrm{Hom}_{\mathscr{A}}(X,[M,A]_R) = \mathrm{Hom}_R(M, \mathrm{Hom}_{\mathscr{A}}(X,A))$, and $\mathrm{Hom}_R(M,\mathrm{Hom}_{\mathscr{A}}(X,A)) = \mathrm{Hom}_S(S\otimes_R M, \mathrm{Hom}_{\mathscr{A}}(X,A))$, we have $\mathrm{Hom}_{\mathscr{A}}(X,[M,A]_R) = \mathrm{Hom}_S(S\otimes_R M, \mathrm{Hom}_{\mathscr{A}}(X,A))$.

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

It means the presheaf $X \to \mathrm{Hom}_{\mathscr{A}}(X,[M,A]_R)$ can be represented by $[M,A]_R$ and $[S\otimes_R M, A]_S$. Hence, $[M,A]_R = [S\otimes_R M, A]_S$. ☐

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

$$\begin{tikzcd} R^{m_1} \arrow[r] & R^{n_1} \arrow[r] & M_1 \arrow[r] & 0 \\ R^{m_2} \arrow[r] \arrow[u] & R^{n_2} \arrow[r] \arrow[u] & M_2 \arrow[r] \arrow[u] & 0 \end{tikzcd}$$

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

$$\begin{tikzcd} 0 \arrow[r] & A_1 \arrow[r] \arrow[d, dashed] & A^{n_1} \arrow[r] \arrow[d] & A^{m_1} \arrow[d] \\ 0 \arrow[r] & A_2 \arrow[r] & A^{n_2} \arrow[r] & A^{m_2} \end{tikzcd}$$

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

$$\begin{tikzcd} 0 \arrow[r] & M\cdot A_1 \arrow[r] \arrow[d, dashed] & A_1^n \arrow[r] \arrow[d] & A_1^m \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & M\cdot A_2 \arrow[r] & A_2^n \arrow[r] & A_2^m \arrow[r] & 0 \end{tikzcd}$$

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

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

The 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, $M = R/nR$, $M\cdot A = A[n]$.

Lemma 1. *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 $R^m \to R^n \to M \to 0$, then we have another exact sequence $0 \to [M,X] \to X^n \to X^m$. By the rational points of k', we have $0 \to M\cdot X(k') \to X(k')^n \to X(k')^m$.

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

Proposition 7. *(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 $rank(M)\dim(A)$. 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 $A^n \to A^m$ 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 $n, m \in \mathrm{N}_+$. For R/nR has representation $R \to R \to R/nR$, we have $[R/nR, A]_R = A[n]$. Hence, $[M, A]_R \subseteq A[n]^m$, which is finite.

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

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

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

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 $0 \to M \cdot X^0 \to M \cdot X$. Since there exists a positive integer N such that $NX/X^0 = 0$. Therefore, we have the multiplication $N : X \to X$ factor through $X \to X^0 \hookrightarrow X$, by $[M, -]_R$, we have $[M, X]_R \to [M, X^0]_R \hookrightarrow [M, X]_R$ 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 $\dim([M, X]_R) = \dim([M, X^0]_R) = \dim(X^0) rank(M)$. □

Defintion 5. *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 $\phi : A_1 \to A_2$, we say that ψ is compatible with ϕ if $\phi \cdot \psi : M_1 \cdot A_1 \to M_2 \cdot A_2$ 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 $\mathrm{Id}_A : A \to A$, 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 $\phi : A_1 \to A_2$.*

Proposition 8. *(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 $0 \to M_2 \to M_1 \to M_1/M_2 \to 0$, then $0 \to M_1/M_2 \cdot A \to M_1 \cdot A \to M_2 \cdot A$. The image of $M_1 \cdot A \to M_2 \cdot A$ denoted by B, which is also an abelian variety. We have $\dim(B) = \dim(A)(rank(M_1) - rank(M_1/M_2)) = \dim(A) rank(M_2) = \dim(M_2 \cdot A)$, which means $B = M_2 \cdot A$.

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

The rest is similar. □

Projective Module Action on Abelian Varieties (Abelian variety after module action is also abelian variety)

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

Theorem 3. *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 $\psi : M_2 \to M_1$ is an isogeny between projective modules, $\psi \cdot A$ is an isogeny, and the dual module isogeny $\hat{\psi} : M_1^\vee \to M_2^\vee$ gives the dual isogeny $\hat{\psi} \cdot A^\vee : M_2^\vee \cdot A^\vee \to M_1^\vee \cdot A^\vee$.

Proof. Since M is finitely presented projctive 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, $i : R \to \mathrm{End}(A)$ is the orientation, we define $i^\vee : R \to \mathrm{End}(A^\vee)$ by $i^\vee(r) = \widehat{i(r)}$, and if $F : A^n \to A^m$ is a matrix M of elements in R, then $F^\vee : A^{\vee, m} \to A^{\vee, n}$ is given by the transpose matrix M^T.

If the projective module M is given by $p : R^n \to M$, 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 $p^\vee \cdot A^\vee : A^{\vee, n} \to M^\vee \cdot A^\vee$.

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

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

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

Special Case: Module Action on Dimension 1 Not require projective module in dimension 1

Proposition 9. *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 7, we have $A = M \cdot E \to E^r$ is surjective and $M \cdot E$, E^r have the same rank, hence $A \to E^r$ 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 3, 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 char $k = 0$. Since $p \nmid c$, so by the above, M/pM is free of rank r over R/pR. Applying $[M, -]$ to

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

yields

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

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, $\dim \text{Lie } A = r = \dim(M \cdot A)$, 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 $0 \to B \to A \to \Phi \to 0$). The constructed surjection $A \to E^r$ with finite kernel restricts to a homomorphism $B \to E^r$ with finite kernel, and it must still be surjective since E^r does not have algebraic subgroups of infinite index; thus B is isogenous to E^r. From Tate's Theorem, for each prime ℓ,

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

On the other hand,

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

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

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

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 $\mathbb{F}_\ell$ and $R/\ell R$, then every $(R/\ell R)$-module is a direct sum of copies of $\mathbb{F}_\ell$ and $\mathbb{F}_\ell[e]/(e^2)$. We have the homomorphisms

$$\frac{R}{\ell R} \to \frac{\text{End } E}{\ell(\text{End } E)} \to \text{End } (E(\overline{k})[\ell])$$

are injective (We may require $\text{End}(E)/R$ is torsion-free). On the other hand, $\#E(\overline{k})[\ell] = \ell^2 = \#(R/\ell R)$. The previous three sentences imply that $E(\overline{k})[\ell]$ is free of rank 1 over $R/\ell R$ (If not, $E(\overline{k})[\ell] \cong \mathbb{F}_\ell \times \mathbb{F}_\ell$, which means e acts trivial on $E(\overline{k})[\ell]$. However, $R/\ell R \hookrightarrow \text{End}(E(\overline{k})[\ell])$). 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

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

the fist equality holds for considering $E(\overline{k})[\ell]$ 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 $0 \to [P/M, E] \to [P, E] \to [M, E]$. Since $[P, E], [M, E]$ are abelian varieties, we have the image of $[P, E]$ is subvariety of $[M, E]$ (which means $\dim([M, E]) \geq \dim([P, E])$).

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 $[P, E] \to [M, E]$ is surjective. Hence $[-, E]$ is exact. (For any module N, there exists projective module P such that $0 \to K \to P \to N \to 0$, then $0 \to [N, E] \to [P, E] \to [K, E] \to \mathrm{Ext}^1(N, E) \to \mathrm{Ext}^1(P, E) = 0$. Since $[P, E] \to [K, E]$ is surjective, we have $\mathrm{Ext}^1(N, E) = 0$ for any N, which means $[-, E]$ is exact.)

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

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

Proposition 10. *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

$$\mathrm{Hom}_R(J, I) \to \mathrm{Hom}([I, E]_R, [J, E]_R)$$

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 5. *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:*

$$\Psi : \mathrm{Hom}_R(J, I) \to \mathrm{Hom}(E/E[n], E/E[m])$$
$$\varphi : m \to tn \to \varphi_{t\frac{n}{m}} : P \to tQ \text{ where } mQ = nP$$

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

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

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

$$\Psi : \bar{J}I \to \mathrm{Hom}_R(J, I)$$
$$x \to \varphi_x : r \to \frac{rx}{\mathrm{Nrd}(J)}$$

The inverse of Ψ can be obtained as following: for any $\varphi \in \mathrm{Hom}_R(J, I)$, $x \in J, x \neq 0$, 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 $\mathrm{Nrd}(J)x^{-1}y$. Overall, $\mathrm{Hom}(E_I, E_J) \cong \bar{J}I \cong \mathrm{Hom}_R(J, I)$.

Theorem 4. *It should be noted that $M \to M \cdot E$ 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 $A \to \mathrm{Hom}(A, E)$. Since $\mathrm{Hom}([M, E], E) \cong \mathrm{Hom}([M, E], [R, E]) \cong \mathrm{Hom}_R(R, M) \cong M$.

Defintion 6 (Polarization)**.** *A polarization is a morphism $\lambda = \Phi_{\mathscr{L}}$ induced by a line bundle $\mathscr{L}$.*

If λ is an isogeny, we call λ is non-degenerate. If $\mathscr{L}$ 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 $R \to \mathrm{End}(A)$ 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 $\lambda : M^\vee \to M$, $\lambda' : N^\vee \to N$. Moreover, we define $H_M : M^\perp \times M^\perp \to R$ by $H_M(m, m') = H_M(m, \lambda(m'))$

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

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

So it only changes base and it is easily obtain λ is positive-definite iff λ' is.

Theorem 5. *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 $(M, H_M) \cdot \lambda_A : M \cdot A \to (M \cdot A)^\vee$. This autodual isogeny is induced by a 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 $\phi = \psi \cdot A : M_1 \cdot A \to M_2 \cdot A$ be the induced isogeny of oriented abelian varieties. Then the dual module isogeny $M_1^\vee \to M_2^\vee$ gives the dual isogeny $M_2^\vee \cdot A^\vee \to M_1^\vee \cdot A^\vee$, and the contragredient isogeny $\hat{\phi}$ corresponds to the action of the adjoint of ψ : $\hat{\psi} : (M_1, H_1) \to (M_2, H_2)$. In particular, a n-similitude $(M_2, H_2) \to (M_1, H_1)$ between unimodular projective modules induces a n-isogeny $M_1 \cdot A \to M_2 \cdot A$.

Proof. We define the orientation on $A^\vee$ by $i^\vee(r) = \widehat{i(\bar{r})}$. We use $M^\vee = \mathrm{Hom}_{\bar{R}}(M, R)$ instead $\mathrm{Hom}_R(M, R)$ and obtain the same result of Theorem 3. It should be noted that if $\gamma : A^n \to A^m$ given by matrix N, then the dual morphism $A^{\vee,m} \to A^{\vee,n}$ 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 : $M^\vee \cong M^\perp \to M$ is an isogeny. By Theorem 3, we have an isogeny $M \cdot A \to M^\vee \cdot A \cong M^\vee \cdot A^\vee \cong (M \cdot A)^\vee$. Moreover, since $M^\vee \to M$ is autodual, we have $M \cdot A \to (M \cdot A)^\vee$ is also autodual.

It remains to prove that this isogeny is induced by an ample line bundle iff H_M is positive definite.

Since M is of rank g, we have an isogeny $M \to R^g$, hence an isogeny $f : A^g \to M \cdot A$. (If $(M \cdot A, H_M)$(resp. (A^g, H_{R^g})) is induced by $\mathscr{L}$ (resp. $\mathscr{L}'$), we have $f^*(\mathscr{L}) = \mathscr{L}'$.) On the other hand, we have H_M is positive-definite iff H_{R^g} is. The question reduces to whether the induced isogeny $A^g \to A^{\vee,g}$ comes from an ample line bundle, so we can assume that $M = R^g$ is free.

On A^g, we have the product polarisation as a principal polarisation. The other polarisations are given by totally positive elements in $NS(A^g)$ which correspond to totally positive symmetric elements in $\mathrm{End}(A^g)$. We also have a canonical product polarisation (R^g, H_R^g) on R^g, and the other positive definite Hermitian forms are also given by totally positive symmetric elements in $\mathrm{End}_R(R^g) = M_g(R) \subset \mathrm{End}_R(A^g)$, by the same arguments as for abelian varieties. The result follows.

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

Theorem 6 (Special Case of Theorem 5)**.** *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 $\phi : A \to A^\vee$ (equivalently a morphism induced by a line bundle $\mathscr{L}$ on A) respecting the orientation corresponds to an Hermitian R-form H_M on $M^\vee$, ϕ is an isogeny (i.e. $\mathscr{L}$ is non degenerate) iff H_M is non degenerate, and ϕ is a polarisation (i.e. $\mathscr{L}$ 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 5. ☐

Remark 6. *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 $\mathrm{Hom}(A, E)$. 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 $R \to M^\vee$, $r \to rx$ or ry. By acting to E, it induced $x \cdot E, y \cdot E : A^\vee \to E$. Moreover, the dual of $y \cdot E : A^\vee \to E$ is $y^\vee \cdot E : E \to A$. It means $x \cdot E \circ \lambda_A \circ y^\vee \cdot E : E \to A \to A^\vee \to E$ is an endomorphism $\gamma : E \to E$.

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

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

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 $A = M_A \cdot E$, $M_A = \mathrm{Hom}(A, E)$. 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.

Theorem 7. *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

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

Hence $M \otimes A$ is induced from $\mathrm{Hom}_R(M, M_A)$. □

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 $\mathfrak{Ab}_{E,R}$.

Remark 7. *In particular, if $M_1 \hookrightarrow M$, $M_2 \hookrightarrow M$ are two module isogenies, corresponding to abelian variety isogenies $A \to A_1$, $A \to A_2$ where $A = M \cdot E$, $A_i = M_i \cdot E$, then the push - forward isogeny $A \to A_{12}$ with kernel $K_1 + K_2$ corresponds to the module isogeny $M_1 \cap M_2 \hookrightarrow M$, and the isogeny $A \to A'_{12}$ with kernel $K_1 \cap K_2$ corresponds to the module isogeny $M_1 + M_2 \hookrightarrow M$.*

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

Theorem 8. *Let $A \in \mathfrak{A}_{E_0,R}$, 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 $\psi : (M_2, H_2) \to (M_1, H_1)$ is an n-similitude, and M_i is compatible with A. Then $\phi = \psi \cdot A : (M_1 \cdot A, H_1 \cdot \lambda_A) \to (M_2 \cdot A, H_2 \cdot \lambda_A)$ is an n-isogeny, which we often write simply as $M_1 \cdot A \to M_2 \cdot A$. Moreover, the dual of isogeny ϕ corresponds to the action of adjoint $(M_1, H_1) \to (M_2, H_2)$.

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 $M \otimes M_A \to (M \otimes M_A)^\vee$. 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 $M_1 \cdot A \to M_2 \cdot A$ is an isogeny. For $\psi^* H_1 = n H_2$, by tensor M_A, we have $\psi^* H_1 \cdot \lambda_A = n H_2 \cdot \lambda_A$. □

Computing Module Action: Kernel Approach

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

Proposition 11. *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 $M_1 \cdot A \to M_2 \cdot A$ 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 $m : M_1 \cdot A \to A$ 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 $R^m \to R^n \to M_2 \to 0$. Hence we have an monomorphism $[M_2, A] \to A^n$, which can be written as $(m_1, \cdots, m_s) : [M_2, A] \to A^n$, where $m_1, \cdots, m_s$ generate M_2.

Now we consider $R^n \to M_2 \hookrightarrow M_1$, which induced $M_1 \cdot A \to M_2 \cdot A \to A^n$. Therefore, the kernel of $M_1 \cdot A \to M_2 \cdot A$ equals to the kernel of $M_1 \cdot A \to A^n$. Since $M_2 \subseteq M_1$, the isogeny $M_1 \cdot A \to A^n$ can be written as $(m_1, \cdots, m_s) : M_1 \cdot A \to A^n$, which means $\ker(M_1 \cdot A \to M_2 \cdot A) = (M_1 \cdot A)[M_2]$.

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

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

Corollary 1. *Let (A, λ_A) be a principally polarized abelian variety in $\mathfrak{Ab}_R$, and $\psi : (M_2, H_2) \to (M_1, H_1)$ be an n-similitude compatible with A. If $M_1 \cdot A$ has an effective module orientation, n is smooth, and the n-torsion on A is accessible, then we can effectively compute the n-isogeny $\phi : M_1 \cdot A \to M_2 \cdot A$.*

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 $m_i : M_1 \cdot A \to A$, where $m_1, \ldots, m_s$ 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. $\square$

Corollary 2. *If (M, H_M) is a unimodular module of rank g, and we can find an n-similitude $(R^g, H_R^g) \to (M, H_M)$ 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 $m : A^g \to A$ corresponds to the morphism induced by the row vector m^T and the orientation on A. So we apply the above corollary. $\square$

Computing Module Action: Clapoti Approach

Theorem 9. *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 $M_1 \cdot A \to M_2 \cdot A$ are efficiently computable.*

Proof. Taking the contragredient of the n_2-isogeny, we have a $n_1 n_2$-isogeny $\psi : (M_1, H_1) \to (M_1, H_1)$, which splits as $M_1 \to M_2 \to M_1$, a n_2-isogeny followed by a n_1-isogeny, or as $M_1 \to M_2' \to M_1$, 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 $(M_1^2, H_1^2) \to (M_2, H_2) \oplus (M_2', H_2')$, 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 $(M_1 \cdot A)^2 \to (M_2 \cdot A) \oplus (M_2' \cdot A)$ allows us to recover both $M_2 \cdot A$ and the two n_i-isogenies $(M_1 \cdot A) \to (M_2 \cdot A)$. $\square$

Acting on Isogenies

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

Proposition 12. *Let $\phi : A_1 \to A_2$ 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 $M \cdot \phi : M \cdot A_1 \to M \cdot A_2$ is given by $\{x \in M \cdot A_1 \mid m(x) \in K, \ \forall m \in M : M \cdot A_1 \to A_1\}$. 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 $R^n \to M$ and consider the commutative diagram induced by functoriality:

$$\begin{tikzcd} A_1^n \arrow[r, "diag(\phi)"] & A_2^n \\ M_1 \cdot A_1 \arrow[u, hook] \arrow[r, "M\cdot\phi"] & M \cdot A_2 \arrow[u, hook] \end{tikzcd}$$

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

Proposition 13. *Assume that we have an efficient representation of $\phi : A_1 \to A_2$, 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 pointsin 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 diaram gives the method to recover the image of $M \cdot \varphi$ on ℓ-torsion points in $M \cdot A_1$. This is enough to compute $M \cdot \phi$. $\square$

Supersingular Case

Theorem 10. *Let E be a maximal supersingular curve E with endomorphism ring $\mathcal{O}$. Then the functor the functor $A \mapsto \mathrm{Hom}_{\mathbb{F}_{p^2}}(A, E)$ 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 $M \to [M, E]$.*

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 4. ☐

Remark 8. *The dimension 1 case is $M = \mathrm{Hom}_{\mathbb{F}_{p^2}}(E', E)$, this left $\mathcal{O}$-module corresponds to unimodular polarization $H_M(\varphi_1, \varphi_2) = \varphi_1 \hat{\varphi}_2 \in \mathcal{O}$, where $\varphi_1, \varphi_2 : E' \to E$.*

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

Proposition 14. *Let E be a supersingular curve wth 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. ☐

It should be noted that if we consider M as R-module, then $M = \mathrm{Hom}_R([M, E], E)$; however, if we consider $M_{\mathcal{O}}$ as $\mathcal{O}$-module, we have $M_{\mathcal{O}} = \mathrm{Hom}_{\mathbb{F}_{p^2}}([M, E], E)$. 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 $[M, E]_R$.)

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 $(P, Q) \to (\sigma(P), \sigma(Q))$, the one induced by $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)/\mathbb{F}_p$ is $(P, Q) \to (\sigma(Q), \sigma(P))$.

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^2, and $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)$ belongs to our category $\mathfrak{A}_{E,R}$, 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 11. *Let $E_0/\mathbb{F}_p$ be primitively oriented by $R = \mathbb{Z}[\sqrt{-p}]$ and $\mathrm{End}(E_0) \cong \mathcal{O}_0$. Let $(M_{\mathcal{O}}, H_{\mathcal{O}}) = \mathrm{Hom}_{\mathbb{F}_{p^2}}(E, E_0)$, and $(M_R, H_R) = \mathrm{Hom}_{\mathbb{F}_p}(W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E), E_0)$, 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 $M_R = \mathrm{Hom}_{\mathbb{F}_p}(W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E), E_0)$, $M_{\mathcal{O}} = \mathrm{Hom}_{\mathbb{F}_{p^2}}(E, E_0)$, 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 $\mathcal{O}_0 \otimes M_R \cong \mathrm{Hom}_{\mathbb{F}_{p^2}}(W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E), E_0)$.

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

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

This is an orthogonal direct sum because if we consider H_R on $\alpha \in M_{\mathcal{O}}$ and $\beta \in M_{\mathcal{O}}^\sigma$, the element α (resp. β) corresponds to $\alpha \times 1 : E \times E^\sigma \to E_0; (P, Q) \to \alpha(P)$ (resp. $1 \times \beta : (P, Q) \to \beta(Q)$). Hence, we have $H_R(\alpha, \beta) = (\alpha \times 1) \circ \widehat{\beta \times 1} = 0$.

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

Hence

$$M_R \to M_{\mathscr{O}}$$
$$\alpha \to (\alpha, \pi_{E_0} \circ \alpha \circ \pi_E^{-1})$$

is an isomorphism between M_R and $M_{\mathscr{O}}$, and

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

□

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 E^2, there are two modules of E^2, that are $\mathrm{Hom}_{\mathbb{F}_p}(E^2, E_0) \cong I_E^2$ or $I_E \times I_E^{\sigma}$, where $I_E = \mathrm{Hom}(E, E_0)$. The last module is compatible with the σ-action.

Scholten's Construction

Lemma 3. *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 $\mathscr{O}_R$ 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 9). If $O(\mathfrak{a}) = R$, then $\mathfrak{a}/2\mathfrak{a} \simeq R/2R$, and $\mathrm{Ker}(\pi - 1) \simeq \mathbb{Z}/2\mathbb{Z}$ on $\mathfrak{a} \cdot E_0$, while if $O(\mathfrak{a}) = \mathscr{O}_R$, then $\mathfrak{a}/2\mathfrak{a} \simeq \mathscr{O}_R/2\mathscr{O}_R$, and $\mathrm{Ker}(\pi - 1) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ 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 $\mathscr{O}_R$. Let m be the number of modules invertible in R. Then $A[2](\mathbb{F}_p) \simeq (\mathbb{Z}/2\mathbb{Z})^m \times (\mathbb{Z}/2\mathbb{Z})^{2(g-m)}$.

If $p \equiv 1 \pmod 4$, $R = \mathscr{O}_R$, 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 $\mathscr{O}_R$-orientation iff $A[2](\mathbb{F}_p) = (\mathbb{Z}/2\mathbb{Z})^{2g}$. This can be checked directly: the R orientation extend to an $\mathscr{O}_R$-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 $E_0^m \times E_0'^{g-m}$. 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 projecive module: for $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(A)[2](\mathbb{F}_p) = A[2](\mathbb{F}_{p^2}) \cong (\mathbb{Z}/2\mathbb{Z})^g$.

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

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 15. *Let $p \equiv 3 \pmod 4$, $R = \mathbb{Z}[\sqrt{-p}]$, $\mathscr{O}_R$ 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 $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)[I] = W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)[2](\mathbb{F}_p) = \{(P, \sigma(P)) \in E \times E^{\sigma} \mid P \in E[2]\}$. □

For $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)$ can be written as $M \cdot E_0$, then the Scholten's construction $I \cdot W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E) = I \cdot M \cdot E_0 = (M \otimes \mathscr{O}_R) \cdot E$, where $E = I \cdot E_0$ 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 4. *Assume that $p \equiv 3 \pmod 4$. Scholten's construction $W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(A)$ is naturally $\mathscr{O}_R$-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 $\mathscr{O}_R$-module action from E (where $E = I \cdot E_0$), so it is naturally $\mathscr{O}_R$ 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 $\mathscr{O}_R$ (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 $_R$-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. □

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

Proposition 16. *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 $\Phi : E^2 \to E^2, (P,Q) \mapsto (P+Q, P-Q)$, 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. □

Supersignular Isogeny Pah Problem and Module Action Inversion

Defintion 7 (Module Inversion)**.** *Given princiaplly polarized abelian vaeieties (A, λ_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 $M \cdot A \to A$ corresponding to $m \in M$. We could also ask for the relationship, given $M \cdot E_0$, between knowing $\mathrm{End}_R(M \cdot E_0)$ 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 $M = \mathrm{Hom}_R(A, E_0)$, and the Hermitian form H_M is given as follows: for m_1, m_2 which we interpret as morphisms $A \to E_0$, then $\hat{m}_2 m_1$ 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 $\phi : E_0 \to E$, then we obtain an isogeny $W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\phi) : W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_0) \to W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)$. Conversely, if we have some path $\Phi : W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_0) \to W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)$ over $\mathbb{F}_p$, then over $\mathbb{F}_{p^2}$, we get $\Phi : E_0^2 \to E \times E^\sigma$. Now Φ is given by a matrix of isogenies, and at least one of the isogeny $E_0 \to E$ or $E_0 \to E^\sigma$ in this matrix is non-trivial. It follows that, composing with π_p if necessary, we obtain a non-trivial isogeny $E_0 \to E$. 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 12. *Assume that we know $\mathscr{O}_0 = \mathrm{End}(E_0)$. Then the isogeny path problem $E_0 \to E$ 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 11, we have shown that the knowledge of $I = \mathrm{Hom}_{\mathbb{F}_{p^2}}(E, E_0)$ is equivalent to the knowledge of (M, H_M). Since the isogeny path reduces to finding I, the result follows. □

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

Remark 9. *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.*

- *A more precise version of the conjecture is that: first, combining the Weil restriction of supersingular curves over $\mathbb{F}_{p^2}$ with the action of invertible ideals (i.e., rank 1 module actions) does not give all the objects we expect. One reason is that we only get horizontal abelian surfaces by just taking the Weil restriction and the action of invertible ideals.*

  Second, forgetting the polarization, the action on $E_0^2 = W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_0) \cong E_0 \times I^2 \cdot E_0$, and the action on the Picard group of E_0 misses the unpolarized abelian varieties of the form $E_0 \times JE_0$, so we only get a fraction of $1/\#\mathrm{Pic}(R)^2$ of the unpolarized abelian varieties.

  However, we conjecture that 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 $\mathbb{F}_p$.

- *Under the expander graph assumption, we have a worst - case to average - case reduction, i.e., the average rank 2 module inversion problem is hard if and only if the worst - case is hard. Indeed, if the average case is easy, and* $A = M \cdot E_0$ *is an abelian surface, we can take random smooth isogenies until we get an easy case* $A' = M' \cdot E_0$*. Thanks to the expander graph property, we quickly get a uniform distribution. From* M' *and the path* $A \to A'$*, we recover* M *by computing action.*

  In particular, under the expander graph assumption, the average-case rank 2 module inversion is at least as hard as the supersingular isogeny path problem.

- *The best known algorithm to solve the supersingular isogeny path problem has a time complexity of* $\widetilde{O}(\sqrt{p})$*. 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 $\widetilde{O}(\sqrt{p})$ *time. The rank 1 problem is known to be solvable in heuristic* $\widetilde{O}(p^{1/4})$ *time, or in quantum sub-exponential time. We can also look for a Weil restriction, which we expect to find in* $\widetilde{O}(\sqrt{p})$ *time, and reduce it to the supersingular isogeny path problem, which is also solvable in* $\widetilde{O}(\sqrt{p})$ *time.*

  So we see that unless a better algorithm for the supersingular isogeny path problem is found, considering non - Weil restricted supersingular abelian surfaces over $\mathbb{F}_p$ *does not improve the security.*

Now we assume $A = W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E)$ is the Weil restriction of $E/\mathbb{F}_{p^2}$, and we try to solve the Hermitian module inversion problem for $A = (M, H_M) \cdot E_0$ (where E_0 is a supersingular curve over $\mathbb{F}_p$ with a primitive orientation). We assume that we have chosen an E_0 with a known endomorphism ring $\mathcal{O}_0$, which can always be done under the Generalized Riemann Hypothesis (GRH).

$\otimes$-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-Helmann 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 $\mathrm{Pic}(R)$ 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 $\mathscr{O}$ between two given objects; then Alice has for secret key such a morphism $\varphi : x \to y$, 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 $b \cdot \varphi : b \cdot x \to b \cdot y$, 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.

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.
- 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.

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.

Hermite module key exchange:

$$\begin{tikzcd} A_0 \arrow[r] \arrow[d] & A_1 = M_1 \cdot A_0 \arrow[d] \\ A_2 = M_2 \cdot A_0 \arrow[r] & A_{12} = (M_1 \otimes M_2) \cdot A_0 \end{tikzcd}$$

$(A_0, \lambda_{A_0}) \in \mathfrak{Ab}_R$ 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 $(M_1, H_1) \to (R^{g_1}, H_R^{g_1})$, then she obtains $A^{g_1} \to A_1$ for A^{g_1} is effective. Similarly to Bob.

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

$$\begin{tikzcd} A_0^{g_1 g_2} \arrow[r] \arrow[d] & A_1^{g_2} \arrow[d] \\ A_2^{g_1} \arrow[r] & A_{12} = (M_1 \otimes M_2) \cdot A_0 \end{tikzcd}$$

On the module side, the diagram corresponds to:

$$\begin{tikzcd} R^{g_1} \otimes_R R^{g_2} \arrow[r] \arrow[d] & M_1 \otimes_R R^{g_2} \arrow[d] \\ R^{g_1} \otimes_R M_2 \arrow[r] & M_1 \otimes_R M_2 \end{tikzcd}$$

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 $W_{\mathbb{F}_{p^2}/\mathbb{F}_p} = E_0'^2$.

$$\begin{tikzcd} E_0' \arrow[r] \arrow[d] & E_1 \arrow[d] \\ E_2 \arrow[r] & W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_1) \otimes_{E_0'} W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_2) \end{tikzcd}$$

$$\begin{tikzcd} E_0'^4 \arrow[r] \arrow[d] & W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_1)^2 \arrow[d] \\ W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_2)^2 \arrow[r] & W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_1) \otimes_{E_0'} W_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_2) \end{tikzcd}$$

Theorem 13. *Assume that we know $\mathcal{O}_0 = \mathrm{End}(E_0)$. 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 $\widetilde{O}(\sqrt{p})$.*

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. $\square$

---

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: For instance, she selects $I_1 = \langle 2^e, \alpha \rangle$ with α of reduced norm $2^e o$, o odd, and computes $K = \langle \overline{\alpha} P \rangle$ (assuming $\overline{\alpha} P$ has full order, otherwise switch to $K = \langle \overline{\alpha} Q \rangle$).

4: She computes $E_1 = E/K$, and send $j(E_1)$ to Bob.

5: The $\mathcal{O}_0'$-ideal 2^e-similitude $\Phi : I_1 \hookrightarrow \mathcal{O}_0'$ gives (by forgetting the $\mathcal{O}_0'$-orientation), a unimodular O_R-module 2^e-similitude $\psi : M_1 \hookrightarrow O_R^2$.

6: She selects a model $j(E_2)$ from Bob's model of E_2.

7: She computes the Scholten construction $A_2 = W'_{\mathbb{F}_{p^2}/\mathbb{F}_p}(E_2)$.

8: 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.

9: She computes the quotient $A_{12} = (A_2^2)/K'$.

10: She output $J(A_{12})$ where J are dimension 4 modular invariants.
