# On isogenies between abelian varieties

2013/08/13 — Microsoft Research

Gaëtan Bisson, Romain Cosset, Alina Dudeanu, Dimitar Jetchev, David Lubicz, **Damien Robert**

# Outline

# Polarised abelian varieties over $\mathbb{C}$

## Definition

A complex abelian variety $A$ of dimension $g$ is isomorphic to a compact Lie group $V/\Lambda$ with

- A complex vector space $V$ of dimension $g$;
- A $\mathbb{Z}$-lattice $\Lambda$ in $V$ (of rank $2g$);

such that there exists an Hermitian form $H$ on $V$ with $E(\Lambda,\Lambda)\subset\mathbb{Z}$ where $E=\operatorname{Im}H$ is symplectic.

- Such an Hermitian form $H$ is called a polarisation on $A$. Conversely, any symplectic form $E$ on $V$ such that $E(\Lambda,\Lambda)\subset\mathbb{Z}$ and $E(ix,iy)=E(x,y)$ for all $x,y\in V$ gives a polarisation $H$ with $E=\operatorname{Im}H$.
- Over a symplectic basis of $\Lambda$, $E$ is of the form.

$$\begin{pmatrix} 0 & D_\delta \\ -D_\delta & 0 \end{pmatrix}$$

  where $D_\delta$ is a diagonal positive integer matrix $\delta=(\delta_1,\delta_2,\ldots,\delta_g)$, with $\delta_1\mid\delta_2\mid\cdots\mid\delta_g$.
- The product $\prod\delta_i$ is the degree of the polarisation; $H$ is a principal polarisation if this degree is $1$.

# Principal polarisations

- Let $E_0$ be the canonical principal symplectic form on $\mathbb{R}^{2g}$ given by $E_0((x_1,x_2),(y_1,y_2)) = {}^t x_1 \cdot y_2 - {}^t y_1 \cdot x_2$;
- If $E$ is a principal polarisation on $A = V/\Lambda$, there is an isomorphism $j : \mathbb{Z}^{2g} \to \Lambda$ such that $E(j(x), j(y)) = E_0(x,y)$;
- There exists a basis of $V$ such that $j((x_1,x_2)) = \Omega x_1 + x_2$ for a matrix $\Omega$;
- In particular $E(\Omega x_1 + x_2, \Omega y_1 + y_2) = {}^t x_1 \cdot y_2 - {}^t y_1 \cdot x_2$;
- The matrix $\Omega$ is in $\mathfrak{H}_g$, the Siegel space of symmetric matrices $\Omega$ with $\mathrm{Im}\,\Omega$ positive definite;
- In this basis, $\Lambda = \Omega\mathbb{Z}^g + \mathbb{Z}^g$; and $H$ is given by the matrix $(\mathrm{Im}\,\Omega)^{-1}$.

# Action of the symplectic group

- Every principal symplectic form (hence symplectic basis) on $\mathbb{Z}^{2g}$ comes from the action of $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{Sp}_{2g}(\mathbb{Z})$ on $(\mathbb{Z}^{2g}, E_0)$;
- This action gives a new equivariant bijection $j_M : \mathbb{Z}^{2g} \to \Lambda$ via $j_M((x_1, x_2)) = (A\Omega x_1 + Bx_2, C\Omega x_1 + Dx_2)$;
- Normalizing this embedding via the action of $(C\Omega + D)^{-1}$ on $\mathbb{C}^g$, we get that $j_M((x_1, x_2)) = \Omega_M x_1 + x_2$ with $\Omega_M = (A\Omega + B)(C\Omega + D)^{-1} \in \mathfrak{H}_g$;
- The moduli space of principally polarised abelian varieties is then isomorphic to $\mathfrak{H}_g / \mathrm{Sp}_{2g}(\mathbb{Z})$.

# Isogenies

Let $A = V/\Lambda$ and $B = V'/\Lambda'$.

## Definition

An isogeny $f : A \to B$ is a bijective linear map $f : V \to V'$ such that $f(\Lambda) \subset \Lambda'$. The kernel of the isogeny is $f^{-1}(\Lambda')/\Lambda \subset A$ and its degree is the cardinal of the kernel.

## Remark

*Up to a renormalization, we can always assume that* $V = V' = \mathbb{C}^g$, $f = \mathrm{Id}$ *and the isogeny is simply* $\mathbb{C}^g/\Lambda \to \mathbb{C}^g/\Lambda'$ *for* $\Lambda \subset \Lambda'$.

# The dual abelian variety

**Definition**

If $A = V/\Lambda$ is an abelian variety, its dual is $\widehat{A} = \mathrm{Hom}_{\overline{\mathbb{C}}}(V, \mathbb{C})/\Lambda^*$. Here $\mathrm{Hom}_{\overline{\mathbb{C}}}(V, \mathbb{C})$ is the space of antilinear forms and $\Lambda^* = \{f \mid f(\Lambda) \subset \mathbb{Z}\}$ is the orthogonal of $\Lambda$.

- There is a canonical polarisation on $A \times \widehat{A}$ (the Poincaré bundle):

$$(x, f) \mapsto f(x).$$

- If $H$ is a polarisation on $A$, its dual $H^*$ is a polarisation on $\widehat{A}$. Moreover, there is an isogeny $\Phi_H : A \to \widehat{A}$:

$$x \mapsto H(x, \cdot)$$

  of degree $\deg H$. We note $K(H)$ its kernel.
- If $f : A \to B$ is an isogeny, then its dual is an isogeny $\widehat{f} : \widehat{B} \to \widehat{A}$ of the same degree.

# Isogenies and polarisations

## Definition

- An isogeny $f : (A, H_1) \to (B, H_2)$ between polarised abelian varieties is an isogeny such that
$$f^* H_2 := H_2(f(\cdot), f(\cdot)) = H_1.$$
- By abuse of notations, we say that $f$ is an $\ell$-isogeny between principally polarised abelian varieties if $H_1$ and $H_2$ are principal and $f^* H_2 = \ell H_1$.

An isogeny $f : (A, H_1) \to (B, H_2)$ respect the polarisations iff the following diagram commutes

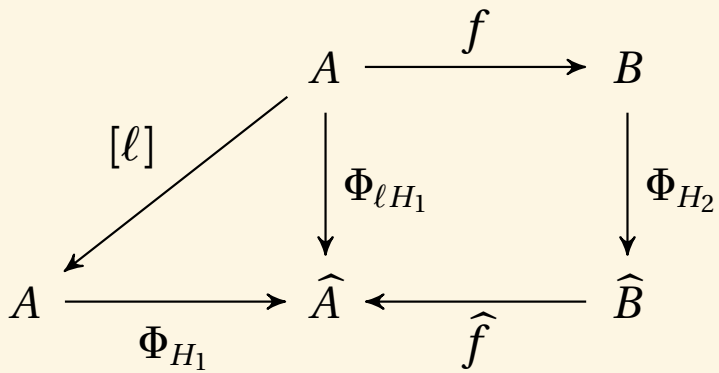
$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow{\scriptstyle \Phi_{H_1}} & & \downarrow{\scriptstyle \Phi_{H_2}} \\ \widehat{A} & \xleftarrow[\widehat{f}]{} & \widehat{B} \end{array}$$

# Isogenies and polarisations

## Definition

- An isogeny $f : (A, H_1) \to (B, H_2)$ between polarised abelian varieties is an isogeny such that
$$f^* H_2 := H_2(f(\cdot), f(\cdot)) = H_1.$$
- By abuse of notations, we say that $f$ is an $\ell$-isogeny between principally polarised abelian varieties if $H_1$ and $H_2$ are principal and $f^* H_2 = \ell H_1$.

$f : (A, H_1) \to (B, H_2)$ is an $\ell$-isogeny between principally polarised abelian varieties iff the following diagram commutes



# Jacobians

- Let $C$ be a curve of genus $g$;
- Let $V$ be the dual of the space of holomorphic differentials of the first kind on $C$;
- Let $\Lambda \simeq H^1(C, \mathbb{Z}) \subset V$ be the set of periods (integration of differentials on loops);
- The intersection pairing gives a symplectic form $E$ on $\Lambda$;
- Let $H$ be the associated hermitian form on $V$;

$$H^*(w_1, w_2) = \int_C w_1 \wedge w_2;$$

- Then $(V/\Lambda, H)$ is a principally polarised abelian variety: the Jacobian of $C$.

**Theorem (Torelli)**

$\operatorname{Jac} C$ *with the associated principal polarisation uniquely determines* $C$.

**Remark (Howe)**

*There exists an hyperelliptic curve* $H$ *of genus* $3$ *and a quartic curve* $C$ *such that* $\operatorname{Jac} C \simeq \operatorname{Jac} H$ *as non polarised abelian varieties!*

# Projective embeddings

## Proposition

*Let $\Phi : A = V/\Lambda \hookrightarrow \mathbb{P}^{m-1}$ be a projective embedding; Then the linear functions $f$ associated to this embedding are $\Lambda$-automorphics:*

$$f(x+\lambda) = a(\lambda, x) f(x) \quad x \in V, \lambda \in \Lambda;$$

*for a fixed automorphy factor $a$:*

$$a(\lambda+\lambda', x) = a(\lambda, x+\lambda') a(\lambda', x).$$

## Theorem (Appell-Humbert)

*All automorphy factors are of the form*

$$a(\lambda, x) = \pm e^{\pi(H(x,\lambda) + \frac{1}{2} H(\lambda,\lambda))}$$

*for a polarisation $H$ on $A$.*

# Theta functions

- Let $(A, H_0)$ be a principally polarised abelian variety: $\mathbb{C}$: $A = \mathbb{C}^g/(\Omega\mathbb{Z}^g + \mathbb{Z}^g)$ with $\Omega \in \mathfrak{H}_g$.
- All automorphic forms corresponding to a multiple of $H_0$ come from the theta functions with characteristics:

$$\vartheta \begin{bmatrix} a \\ b \end{bmatrix} (z, \Omega) = \sum_{n \in \mathbb{Z}^g} e^{\pi i\, {}^t(n+a)\Omega(n+a) + 2\pi i\, {}^t(n+a)(z+b)} \qquad a, b \in \mathbb{Q}^g$$

- Automorphic property:

$$\vartheta \begin{bmatrix} a \\ b \end{bmatrix} (z + m_1\Omega + m_2, \Omega) = e^{2\pi i({}^t a \cdot m_2 - {}^t b \cdot m_1) - \pi i\, {}^t m_1 \Omega m_1 - 2\pi i\, {}^t m_1 \cdot z} \vartheta \begin{bmatrix} a \\ b \end{bmatrix} (z, \Omega).$$

# Theta functions of level $n$

- Define $Z(\overline{n}) = \mathbb{Z}^g / n\mathbb{Z}^g$ and $\vartheta_i = \vartheta \begin{bmatrix} 0 \\ \frac{i}{n} \end{bmatrix} (., \frac{\Omega}{n})$; this is a basis of the automorphic functions for $H = nH_0$ (theta functions of level $n$);
- This is the unique basis such that in the projective coordinates:

$$\begin{array}{ccc} A & \longrightarrow & \mathbb{P}^{n^g-1}_{\mathbb{C}} \\ z & \longmapsto & (\vartheta_i(z))_{i \in Z(\overline{n})} \end{array}$$

  the translation by a point of $n$-torsion is normalized by

$$\vartheta_i(z + \frac{m_1}{n}\Omega + \frac{m_2}{n}) = e^{-\frac{2\pi i}{n}\, {}^t i \cdot m_1} \vartheta_{i+m_2}(z).$$

- $(\vartheta_i)_{i \in Z(\overline{n})} = \begin{cases} \text{coordinates system} & n \geqslant 3 \\ \text{coordinates on the Kummer variety } A/\pm 1 & n = 2 \end{cases}$
- $(\vartheta_i)_{i \in Z(\overline{n})}$: basis of the theta functions of level $n$
  $\Leftrightarrow A[n] = A_1[n] \oplus A_2[n]$: symplectic decomposition.
- Theta null point: $\vartheta_i(0)_{i \in Z(\overline{n})} =$ modular invariant.

# The differential addition law ($k = \mathbb{C}$)

$$\Big(\sum_{t\in Z(\bar{2})} \chi(t)\vartheta_{i+t}(x+y)\vartheta_{j+t}(x-y)\Big).\Big(\sum_{t\in Z(\bar{2})} \chi(t)\vartheta_{k+t}(0)\vartheta_{l+t}(0)\Big) =$$

$$\Big(\sum_{t\in Z(\bar{2})} \chi(t)\vartheta_{-i'+t}(y)\vartheta_{j'+t}(y)\Big).\Big(\sum_{t\in Z(\bar{2})} \chi(t)\vartheta_{k'+t}(x)\vartheta_{l'+t}(x)\Big).$$

where $\chi \in \hat{Z}(\bar{2}), i, j, k, l \in Z(\overline{n})$

$$(i', j', k', l') = A(i, j, k, l)$$

$$A = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

# Cryptographic usage of isogenies

- Transfer the Discrete Logarithm Problem from one Abelian variety to another;
- Point counting algorithms ($\ell$-adic or $p$-adic) $\Rightarrow$ Verify an abelian varietyis secure;
- Compute the class field polynomials (CM-method) $\Rightarrow$ Construct a secure abelian variety;
- Compute the modular polynomials $\Rightarrow$ Compute isogenies;
- Determine $\mathrm{End}(A)$ $\Rightarrow$ CRT method for class field polynomials;
- Speed up the arithmetic;
- Hash functions and cryptosystems based on isogeny graphs.

# The isogeny theorem

## Theorem

- *Let* $\varphi : Z(\overline{n}) \to Z(\overline{\ell n}), x \mapsto \ell.x$ *be the canonical embedding.*
  *Let* $K = A_2[\ell] \subset A_2[\ell n]$.
- *Let* $(\vartheta_i^A)_{i \in Z(\overline{\ell n})}$ *be the theta functions of level* $\ell n$ *on* $A = \mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g)$.
- *Let* $(\vartheta_i^B)_{i \in Z(\overline{n})}$ *be the theta functions of level* $n$ *of* $B = A/K = \mathbb{C}^g/(\mathbb{Z}^g + \frac{\Omega}{\ell}\mathbb{Z}^g)$.
- *We have:*

$$(\vartheta_i^B(x))_{i \in Z(\overline{n})} = (\vartheta_{\varphi(i)}^A(x))_{i \in Z(\overline{n})}$$

## Example

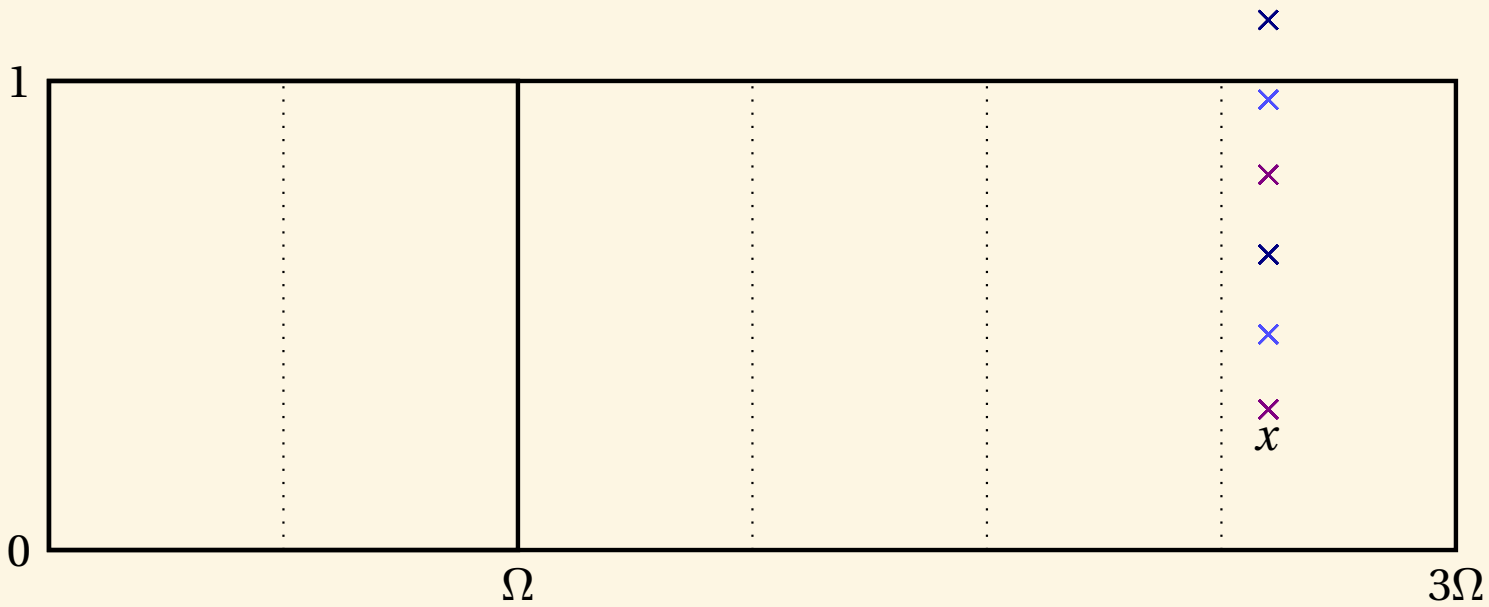
$f : (x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}) \mapsto (x_0, x_3, x_6, x_9)$ is a 3-isogeny between elliptic curves.

# An example with $g = 1$, $n = 2$, $\ell = 3$

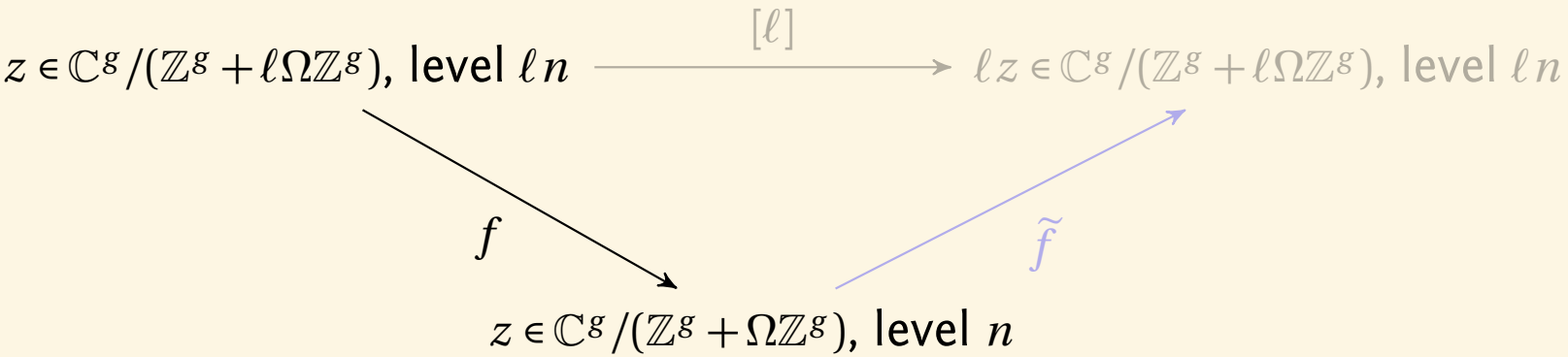
$$z \in \mathbb{C}^g/(\mathbb{Z}^g + \ell\Omega\mathbb{Z}^g), \text{ level } \ell n \xrightarrow{[\ell]} \ell z \in \mathbb{C}^g/(\mathbb{Z}^g + \ell\Omega\mathbb{Z}^g), \text{ level } \ell n$$

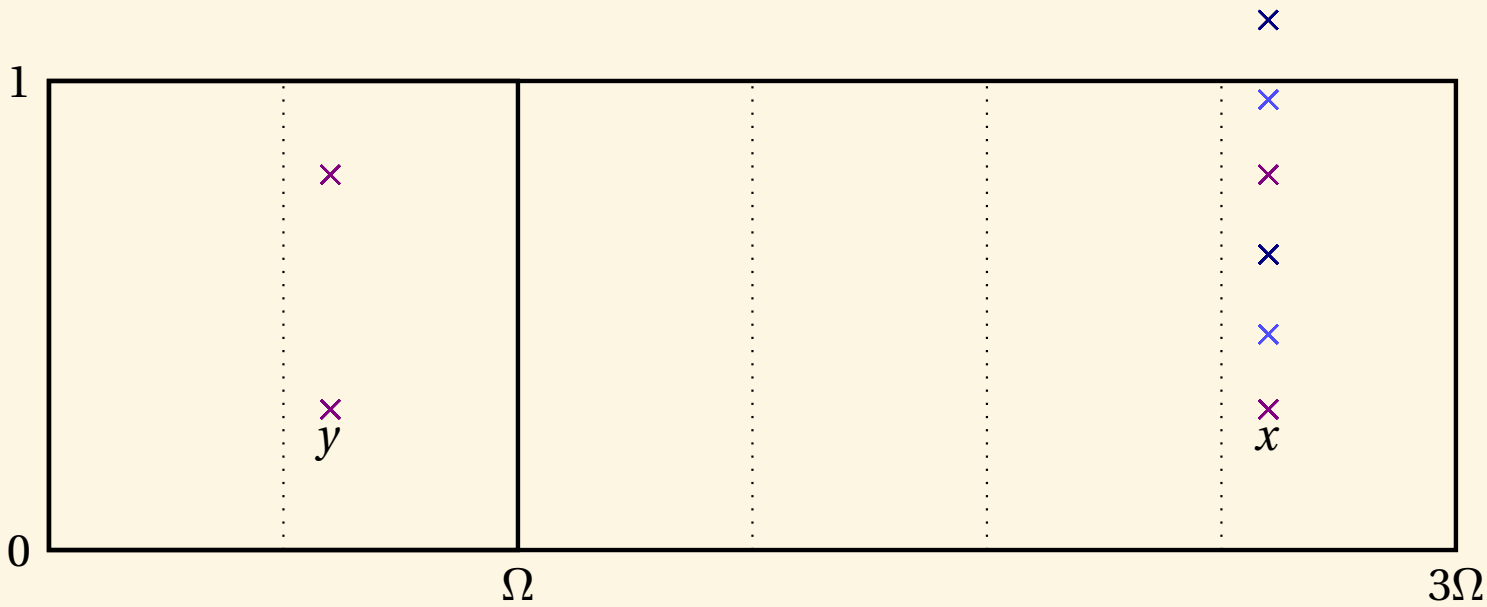
$$f \searrow \qquad \nearrow \tilde{f}$$

$$z \in \mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g), \text{ level } n$$



# An example with $g = 1$, $n = 2$, $\ell = 3$



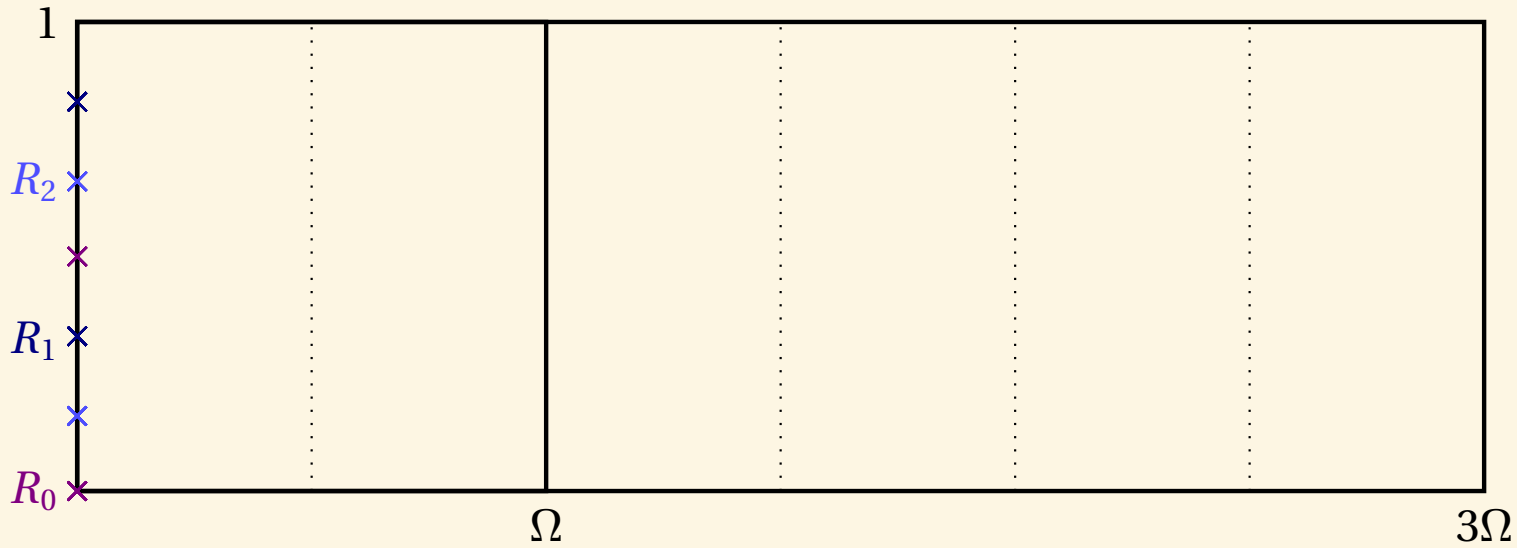



# An example with $g=1$, $n=2$, $\ell=3$

$$z \in \mathbb{C}^g/(\mathbb{Z}^g + \ell\Omega\mathbb{Z}^g), \text{ level } \ell n \xrightarrow{[\ell]} \ell z \in \mathbb{C}^g/(\mathbb{Z}^g + \ell\Omega\mathbb{Z}^g), \text{ level } \ell n$$

$$f \searrow \qquad \nearrow \widetilde{f}$$

$$z \in \mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g), \text{ level } n$$

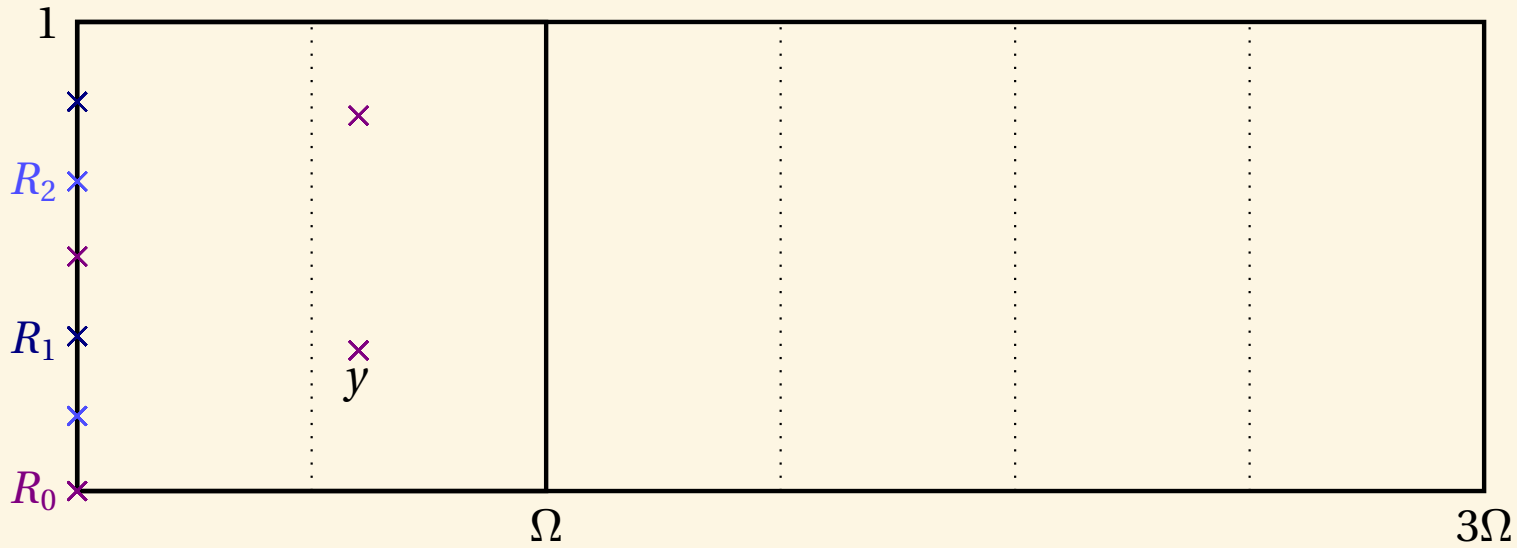


# An example with $g=1$, $n=2$, $\ell=3$

$$z \in \mathbb{C}^g/(\mathbb{Z}^g + \ell\Omega\mathbb{Z}^g), \text{ level } \ell n \xrightarrow{[\ell]} \ell z \in \mathbb{C}^g/(\mathbb{Z}^g + \ell\Omega\mathbb{Z}^g), \text{ level } \ell n$$

$$f \searrow \qquad \nearrow \widetilde{f}$$

$$z \in \mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g), \text{ level } n$$

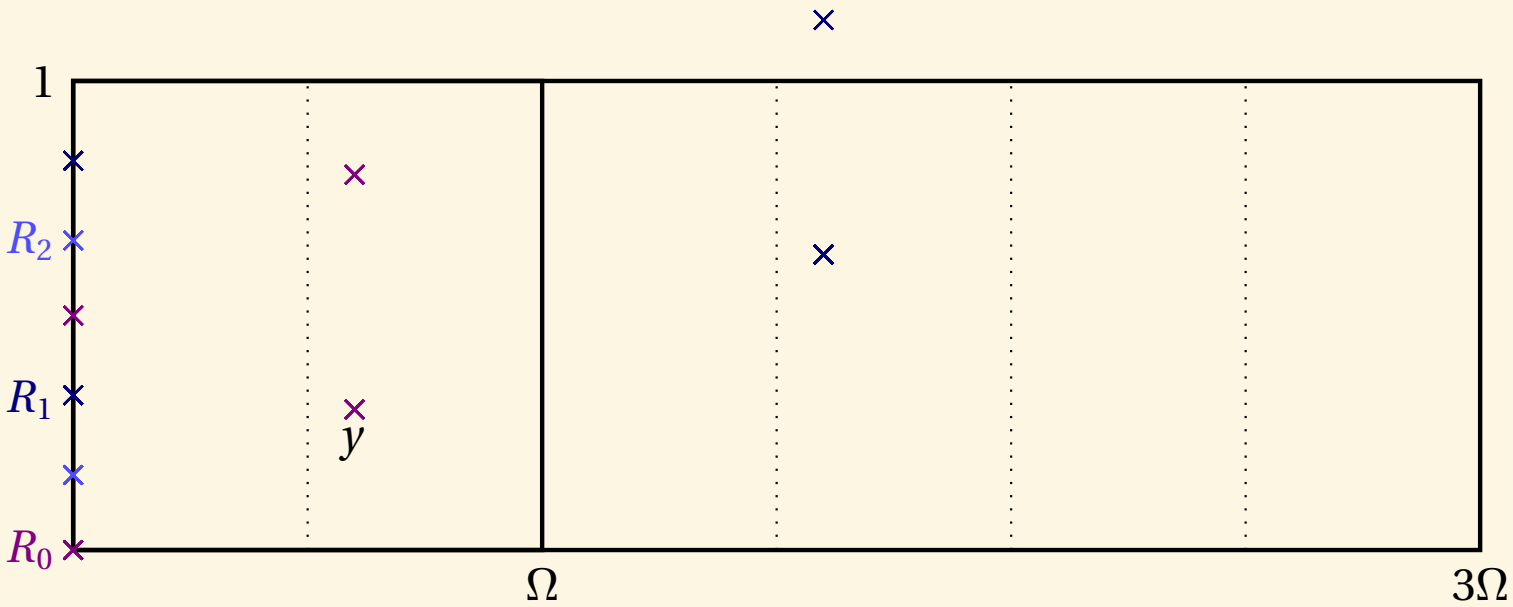


# An example with $g = 1$, $n = 2$, $\ell = 3$

$$z \in \mathbb{C}^g/(\mathbb{Z}^g + \ell\Omega\mathbb{Z}^g), \text{ level } \ell n \xrightarrow{[\ell]} \ell z \in \mathbb{C}^g/(\mathbb{Z}^g + \ell\Omega\mathbb{Z}^g), \text{ level } \ell n$$

$$f \searrow \qquad \nearrow \widetilde{f}$$

$$z \in \mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g), \text{ level } n$$

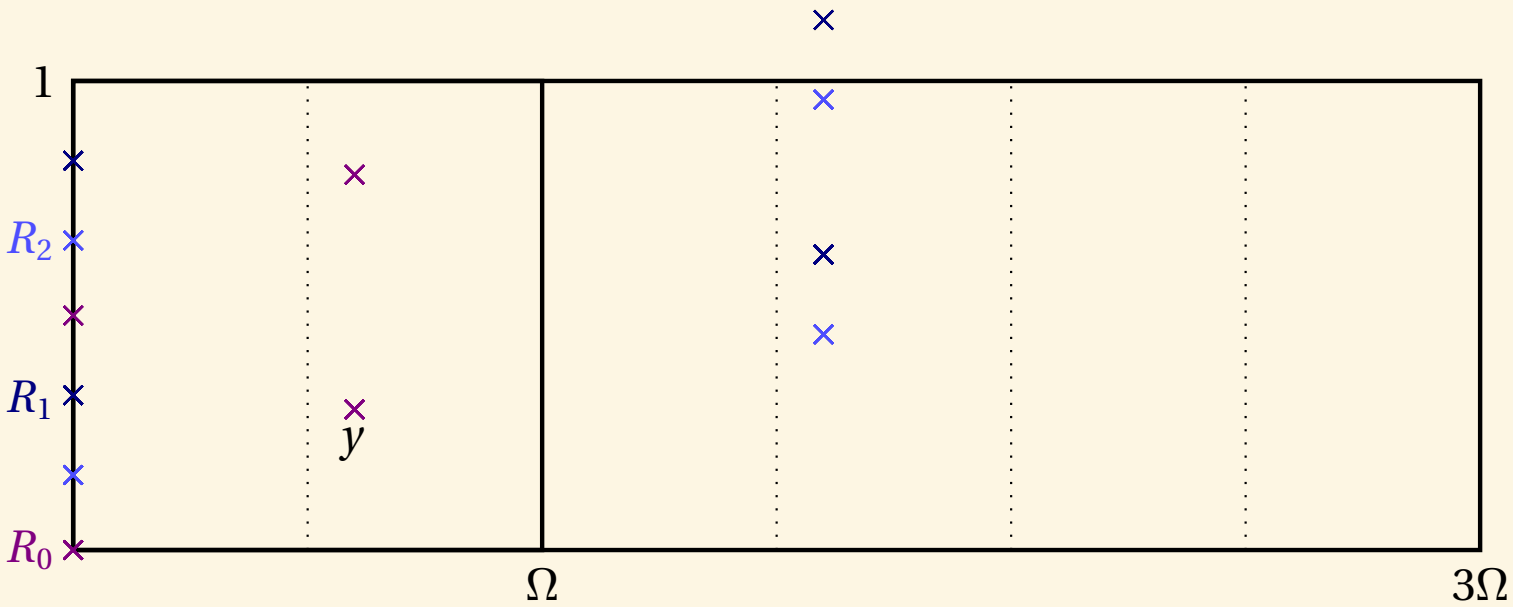


# An example with $g = 1$, $n = 2$, $\ell = 3$

$$z \in \mathbb{C}^g/(\mathbb{Z}^g + \ell\Omega\mathbb{Z}^g), \text{ level } \ell n \xrightarrow{[\ell]} \ell z \in \mathbb{C}^g/(\mathbb{Z}^g + \ell\Omega\mathbb{Z}^g), \text{ level } \ell n$$

$$f \searrow \qquad \nearrow \widetilde{f}$$

$$z \in \mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g), \text{ level } n$$

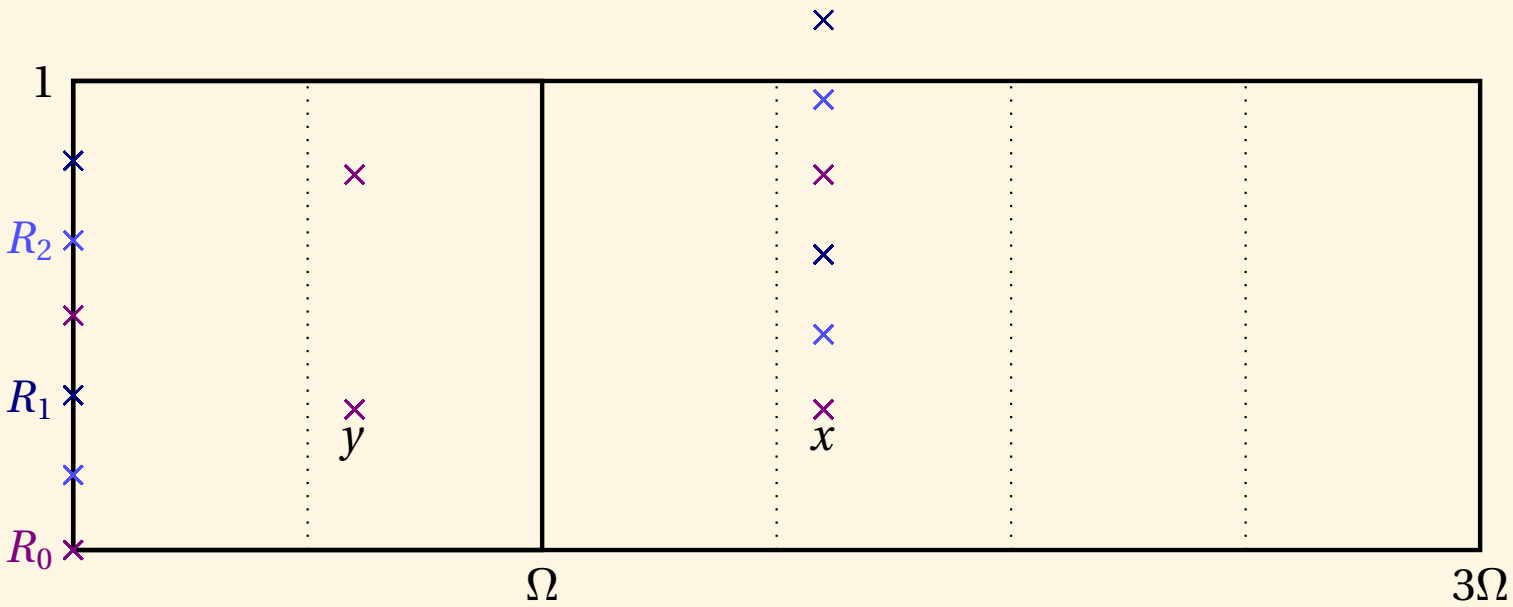


# An example with $g=1$, $n=2$, $\ell=3$

$$z \in \mathbb{C}^g/(\mathbb{Z}^g + \ell\Omega\mathbb{Z}^g), \text{ level } \ell n \xrightarrow{[\ell]} \ell z \in \mathbb{C}^g/(\mathbb{Z}^g + \ell\Omega\mathbb{Z}^g), \text{ level } \ell n$$

$$f \searrow \qquad \nearrow \widetilde{f}$$

$$z \in \mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g), \text{ level } n$$



# Changing level

**Theorem (Koizumi–Kempf)**

*Let $F$ be a matrix of rank $r$ such that ${}^tFF = \ell \operatorname{Id}_r$. Let $X \in (\mathbb{C}^g)^r$ and $Y = F(X) \in (\mathbb{C}^g)^r$. Let $j \in (\mathbb{Q}^g)^r$ and $i = F(j)$. Then we have*

$$\vartheta \begin{bmatrix} 0 \\ i_1 \end{bmatrix} (Y_1, \frac{\Omega}{n}) \dots \vartheta \begin{bmatrix} 0 \\ i_r \end{bmatrix} (Y_r, \frac{\Omega}{n}) = \sum_{\substack{t_1,\dots,t_r \in \frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g \\ F(t_1,\dots,t_r)=(0,\dots,0)}} \vartheta \begin{bmatrix} 0 \\ j_1 \end{bmatrix} (X_1 + t_1, \frac{\Omega}{\ell n}) \dots \vartheta \begin{bmatrix} 0 \\ j_r \end{bmatrix} (X_r + t_r, \frac{\Omega}{\ell n}),$$

*(This is the isogeny theorem applied to $F_A : A^r \to A^r$.)*

- If $\ell = a^2 + b^2$, we take $F = \left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right)$, so $r = 2$.
- In general, $\ell = a^2 + b^2 + c^2 + d^2$, we take $F$ to be the matrix of multiplication by $a + bi + cj + dk$ in the quaternions, so $r = 4$.

# The isogeny formula

$$\ell \wedge n = 1, \quad B = \mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g), \quad A = \mathbb{C}^g/(\mathbb{Z}^g + \ell\Omega\mathbb{Z}^g)$$

$$\vartheta^B_b := \vartheta \begin{bmatrix} 0 \\ \frac{b}{n} \end{bmatrix} \left(\cdot, \frac{\Omega}{n}\right), \quad \vartheta^A_b := \vartheta \begin{bmatrix} 0 \\ \frac{b}{n} \end{bmatrix} \left(\cdot, \frac{\ell\Omega}{n}\right)$$

## Proposition

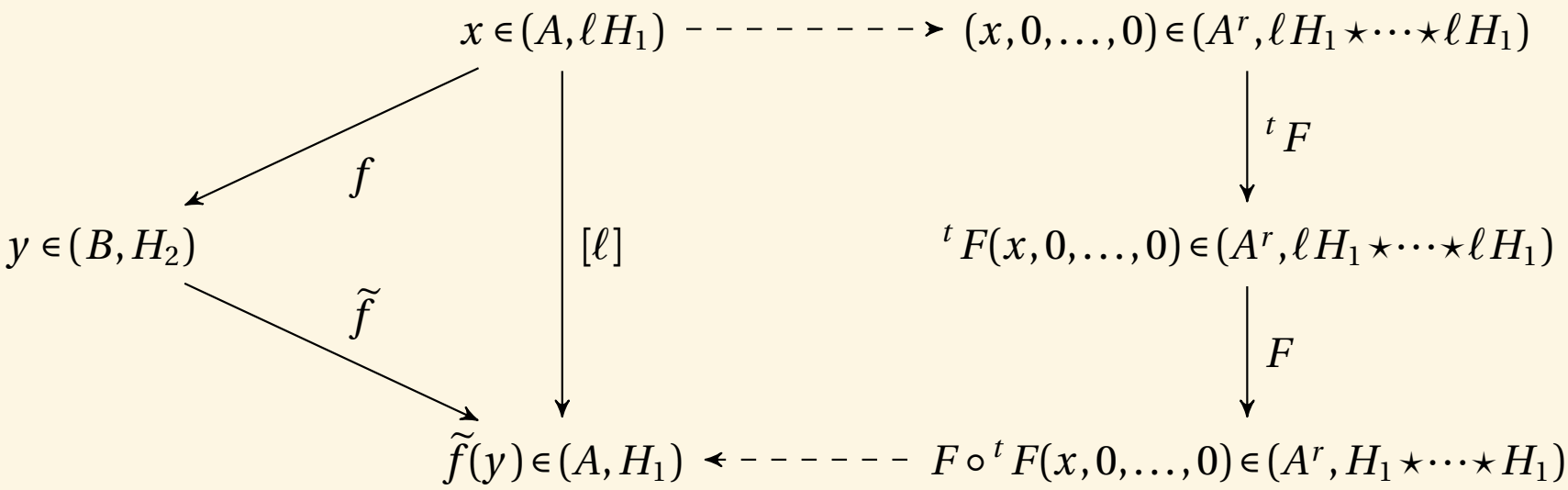
*Let $F$ be a matrix of rank $r$ such that ${}^tFF = \ell\,\mathrm{Id}_r$. Let $X$ in $(\mathbb{C}^g)^r$ and $Y = XF^{-1} \in (\mathbb{C}^g)^r$. Let $i \in (Z(\overline{n}))^r$ and $j = iF^{-1}$. Then we have*

$$\vartheta^A_{i_1}(Y_1)\dots\vartheta^A_{i_r}(Y_r) = \sum_{\substack{t_1,\dots,t_r \in \frac{1}{\ell}\mathbb{Z}^g/\mathbb{Z}^g \\ (t_1,\dots,t_r)F=(0,\dots,0)}} \vartheta^B_{j_1}(X_1+t_1)\dots\vartheta^B_{j_r}(X_r+t_r),$$

## Corollary

$$\vartheta^A_k(0)\vartheta^A_0(0)\dots\vartheta^A_0(0) = \sum_{\substack{t_1,\dots,t_r \in K \\ (t_1,\dots,t_r)F=(0,\dots,0)}} \vartheta^B_{j_1}(t_1)\dots\vartheta^B_{j_r}(t_r), \quad (j = (k,0,\dots,0)F^{-1} \in Z(\overline{n}))$$

# The Algorithm



# Complexity over $\mathbb{F}_q$

- The geometric points of the kernel live in a extension $k'$ of degree at most $\ell^g - 1$ over $k = \mathbb{F}_q$;
- The isogeny formula assumes that the points are in affine coordinates. In practice, given $A/\mathbb{F}_q$ we only have projective coordinates $\Rightarrow$ we use differential additions to normalize the coordinates;
- Computing the normalization factors takes $O(\log \ell)$ operations in $k'$;
- Computing the points of the kernel via differential additions take $O(\ell^g)$ operations in $k'$;
- If $\ell \equiv 1 \pmod 4$, applying the isogeny formula take $O(\ell^g)$ operations in $k'$;
- If $\ell \equiv 3 \pmod 4$, applying the isogeny formula take $O(\ell^{2g})$ operations in $k'$;

$\Rightarrow$ The total cost is $\widetilde{O}(\ell^{2g})$ or $\widetilde{O}(\ell^{3g})$ operations in $\mathbb{F}_q$.

**Remark**

*The complexity is much worse over a number field because we need to work with extensions of much higher degree.*

# Equations of the Kernel

- We suppose that we have (projective) equations of $K$ in diagonal form over the base field $k$:

$$P_1(X_0, X_1) = 0$$
$$X_2 X_0^d = P_2(X_0, X_1)$$
$$\dots$$
$$X_n X_0^d = P_n(X_0, X_1)$$

- By setting $X_0 = 1$ we can work with affine coordinates. The projective solutions can be written $(x_0, x_0 x_1, \dots, x_0 x_n)$ so $X_0$ can be seen as the normalization factor.
- Note: I don't know how to obtain equations of $K$ without computing the geometric points of $K$ as we don't have modular polynomials in higher dimension (yet).

# Operations on generic points

- We can work in the algebra $\mathfrak{A} = k[X_1]/(P_1(X_1))$, each operation takes $\widetilde{O}(\ell^g)$ operations in $k$ (this is also "true" for number fields).
- A generic point is $\eta = (X_0, X_0X_1, X_0P_2(X_1), \ldots, X_0P_n(X_1))$;
- By computing differential additions over the algebra $\mathfrak{A}$, one can recover a generic normalization $X_0^\ell = \mu \in \mathfrak{A}$;
- We assume here that none of the coordinates of the geometric points are zero, otherwise computing generic differential additions get tricky;
- If we suppose $P_1$ irreducible, the Galois action on $\eta$ give "linearly free generic points".

# The generic algorithm (first version)

- Use the Galois action to compute $g$ "linearly independent generic points" $\eta_1, \ldots, \eta_g$;
- Compute the $\eta_i + \eta_j$ over $\mathfrak{A}$;
- Normalize each of these points;
- Use differential additions to formally compute each points of the kernel;
- Apply the isogeny formula. The result is computed in $\mathfrak{A}$ but will actually be in $k$.

**Remark**

*This look nice, but in fact this is just a fancy way of working over the splitting field of $P_1$. In this case we can as well work directly with the geometric points of $K$ so we gain nothing!*

# Uniform normalization

- Normalizing the basis and using differential additions to compute the rest of the kernel assure that we have a uniform normalization;
- But in the equation

$$\vartheta_k^B(0)\vartheta_0^B(0)\dots\vartheta_0^B(0) = \sum_{\substack{t_1,\dots,t_r \in K \\ (t_1,\dots,t_r)F=(0,\dots,0)}} \vartheta_{j_1}^A(t_1)\dots\vartheta_{j_r}^A(t_r), \quad (j=(k,0,\dots,0)F^{-1} \in Z(\overline{n}))$$

  we only need to normalize uniformly between the points $t_1,\dots,t_r$ (ie do a local normalization);
- When we work with the geometric points, it's better to normalize only the basis and then use differential addition (which is faster than normal addition) than normalize the points in the kernel independently;
- However here since we do a generic normalization we only need to do it once!

# The case $\ell \equiv 1 \pmod 4$

- Let $F = \left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right)$. Let $c = -a/b \pmod \ell$. The points in the kernel of $F$ are of the form $(x, cx)$ for each $x \in K$.
- So we normalize the generic point $\eta$, compute $c.\eta$ and then $R := \vartheta^A_{j_1}(\eta)\vartheta^A_{j_2}(c.\eta) \in \mathfrak{A}$.
- We then just have to compute $\sum_{x \in K} R(x_1) \in k$;
- In the euclidean division $XRP_1' = P_1 Q + S$, the result is given by $Q(0)$;
- This last operation is quasi-linear in the degree of $\mathfrak{A}$.

# The case $\ell \equiv 3 \pmod 4$

- Essentially the same as before, except the tuple in the kernel of $F$ are of the form $(x_1, x_2, ax_1 + bx_2, cx_1 + dx_2)$ for $(x_1, x_2) \in k^2$;
- we have to work on a plane rather than on a line;
- we need two "independent" generic points, so we work in $\mathfrak{A}^{\otimes 2}$;
- we need three normalizations;
- To evaluate the sum of the final polynomial on the couple of points in the kernel we can apply the preceding formula twice.

# Complexity over $k$

An operation in $\mathfrak{A}$ is $\widetilde{O}(\ell^g)$ operations in $k$.

- Computing the generic normalization factor takes $\widetilde{O}(\log \ell)$ operations in $\mathfrak{A}$;
- If $\ell \equiv 1 \pmod 4$, working in the line take $O(\log \ell)$ operations in $\mathfrak{A}$;
- If $\ell \equiv 3 \pmod 4$, working in the plane take $O(\log \ell)$ operations in $\mathfrak{A}^{\otimes 2}$;
- The final reduction step is quasi-linear in the degree of the algebra.

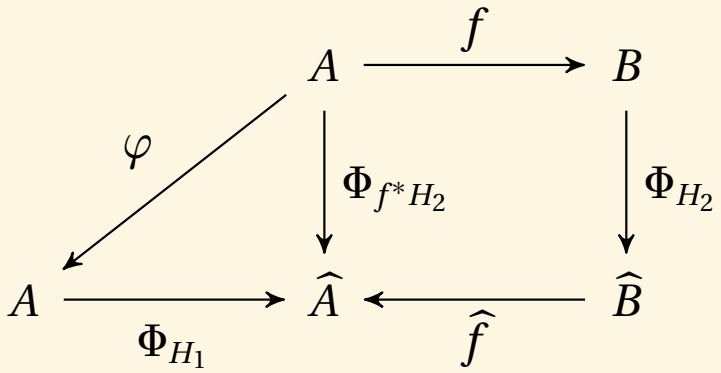
$\Rightarrow$ The total cost is $\widetilde{O}(\ell^g)$ or $\widetilde{O}(\ell^{2g})$ operations in $k$.

**Remark**

- *If $k = \mathbb{F}_q$ and $\ell \equiv 3 \pmod 4$, it is actually faster to generate equations of the kernel from the geometric point (costing $\widetilde{O}(\ell^{2g})$) and apply the generic algorithm than to use the isogeny formula directly!*
- *Still not quasi-linear in the degree of the isogeny when $\ell \equiv 3 \pmod 4$!*

# Cyclic isogeny

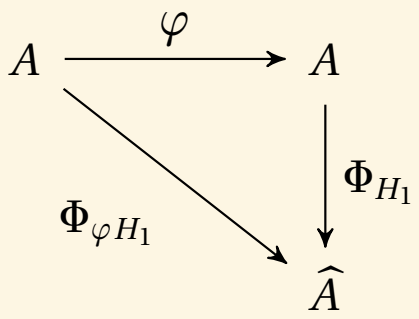
- Let $f : (A, H_1) \to (B, H_2)$ be an isogeny between principally polarised abelian varieties with cyclic kernel of degree $\ell$;
- There exists $\varphi$ such that the following diagram commutes:



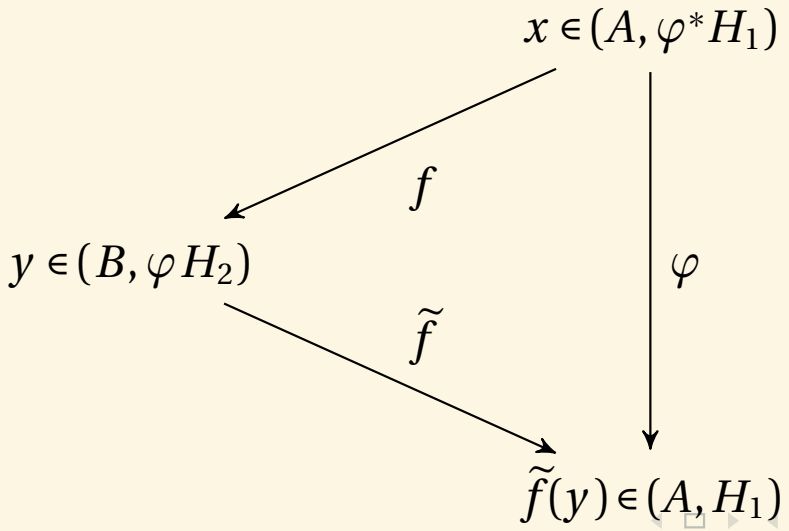

- $\varphi$ is an $(\ell, 0, \ldots, \ell, 0, \ldots)$-isogeny whose kernel is not isotropic for the $H_1$-Weil pairing on $A[\ell]$!
- $\varphi$ commutes with the Rosatti involution so is a real endomorphism ($\varphi$ is $H_1$-symmetric).

# Descending a polarisation via $\varphi$

- The isogeny $f$ induces a compatible isogeny between $\varphi H_1 = f^* H_2$ and $H_2$ where $\varphi H_1$ is given by the following diagram




- $\varphi$ plays the same role as $[\ell]$ for $\ell$-isogenies;
- We then define the $\varphi$-contragredient isogeny $\widetilde{f}$ as the isogeny making the following diagram commute



# $\varphi$-change of level

- $\varphi$ is a totally positive element of a totally positive order $O_{K_0}$;
- A theorem of Siegel show that $\varphi$ is a sum of $m$ squares in $K_0$;
- Clifford's algebras give a matrix $F \in r(K_0)$ such that $\mathrm{diag}(\varphi) = F^* F$;
- We can use this matrix $F$ to change level as before: If $X \in (\mathbb{C}^g)^r$ and $Y = F(X) \in (\mathbb{C}^g)^r$, $j \in (\mathbb{Q}^g)^r$ and $i = F(j)$, we have

$$\vartheta \begin{bmatrix} 0 \\ i_1 \end{bmatrix} (Y_1, \frac{\Omega}{n}) \ldots \vartheta \begin{bmatrix} 0 \\ i_r \end{bmatrix} (Y_r, \frac{\Omega}{n}) =$$

$$\sum_{\substack{t_1,\ldots,t_r \in K(\varphi H_1) \\ F(t_1,\ldots,t_r)=(0,\ldots,0)}} \vartheta \begin{bmatrix} 0 \\ j_1 \end{bmatrix} (X_1 + t_1, \frac{\varphi^{-1}\Omega}{n}) \ldots \vartheta \begin{bmatrix} 0 \\ j_r \end{bmatrix} (X_r + t_r, \frac{\varphi^{-1}\Omega}{n}),$$

**Remark**

- *In general $r$ can be larger than $m$;*
- *The matrix $F$ acts by real endomorphism rather than by integer multiplication;*
- *There may be denominators in the coefficients of $F$.*

# The Algorithm for cyclic isogenies

$$B = \mathbb{C}^g/(\mathbb{Z}^g + \Omega\mathbb{Z}^g), \quad A = \mathbb{C}^g/(\mathbb{Z}^g + \varphi\Omega\mathbb{Z}^n)$$

$$\vartheta_b^B := \vartheta \begin{bmatrix} 0 \\ \frac{b}{n} \end{bmatrix} \left(\cdot, \frac{\Omega}{n}\right), \quad \vartheta_b^A := \vartheta \begin{bmatrix} 0 \\ \frac{b}{n} \end{bmatrix} \left(\cdot, \frac{\varphi\Omega}{n}\right)$$

## Theorem

*Let $X$ in $(\mathbb{C}^g)^r$ and $Y = XF^{-1} \in (\mathbb{C}^g)^r$. Let $i \in (Z(\overline{n}))^r$ and $j = iF^{-1}$.*

$$\vartheta_{i_1}^A(Y_1)\dots\vartheta_{i_r}^A(Y_r) = \sum_{\substack{t_1,\dots,t_r \in K(\varphi H_2) \\ (t_1,\dots,t_r)F=(0,\dots,0)}} \vartheta_{j_1}^B(X_1+t_1)\dots\vartheta_{j_r}^B(X_r+t_r),$$

$$\begin{array}{ccc}
x \in (A, \varphi H_1) & \dashrightarrow & (x,0,\dots,0) \in (A^r, \varphi H_1 \star \cdots \star \varphi H_1) \\
\downarrow f \quad \downarrow \varphi & & \downarrow {}^tF \\
y \in (B, H_2) & & {}^tF(x,0,\dots,0) \in (A^r, \varphi H_1 \star \cdots \star \varphi H_1) \\
\downarrow \widetilde{f} & & \downarrow F \\
\widetilde{f}(y) \in (A, H_1) & \dashleftarrow & F \circ {}^tF(x,0,\dots,0) \in (A^r, H_1 \star \cdots \star H_1)
\end{array}$$

# Hidden details

- We normalize the coordinates by using multi-way additions;
- The real endomorphisms are codiagonalisable, this is important to apply the isogeny theorem;
- If $g=2$, $K_0=\mathbb{Q}(\sqrt{d})$, the action of $\sqrt{d}$ is given by a standard $(d,d)$-isogeny, so we can compute it using the previous algorithm for $d$-isogenies!
- The important point is that this algorithm is such that we can keep track of the projective factors when computing the action of $\sqrt{d}$.

# AVIsogenies

- AVIsogenies: Magma code written by Bisson, Cosset and R.
  http://avisogenies.gforge.inria.fr
- Released under LGPL 2+.
- Implement isogeny computation (and applications thereof) for abelian varieties using theta functions.
- Current release 0.6.