Isogenies

Spring school on abelian varieties
Augsburg, 24th March 2010

This talk is an introduction to the topic of isogenies between abelian varieties. We deal with the point of view of complex tori, line bundles and periods in the first part, and with the algebraic point of view (especially the case of positive characteristic) in the second part.

1. Isogenies of complex tori and periods (30′)

1.1. Definition and lattice-theoretic interpretation (7′). See [BL04, 1.2]

Definition. *If X and Y are complex tori, an isogeny $X \to Y$ is a surjective homomorphism with finite kernel.*

Recall that a homomorphism of complex tori is a holomorphic map mapping zero to zero: it is easy to see that a map is an isogeny iff it is étale. If $X = \mathbb{C}^n/L$, $Y = \mathbb{C}^n/M$, the isogenies $X \to Y$ are given by elements of $GL_n(\mathbb{C})$ mapping L into M. Hence any isogeny has the form $\mathbb{C}^n/L \to \mathbb{C}^n/M$, where L is a sublattice of finite index in M.

Any torus has self-isogenies given by $[n] : x \mapsto nx$.

Definition. *The* degree *of an isogeny f is the order of the finite group* $\ker f$. *The* exponent *of f is the least common multiple of order of elements of* $\ker f$.

Proposition 1. *If $f : X \to X'$ is an isogeny with exponent e, there exists an isogeny g such that $fg = e\mathrm{Id}_{X'}$ and $gf = e\mathrm{Id}_X$.*

A complex torus is said to have *complex multiplication* whenever there is some other element $f \in GL_n(\mathbb{C})$ mapping L into itself.

Elliptic curves with complex multiplication have the form $\mathbb{C}/\mathcal{O}_K$ where K is some number field. Examples: $\left\{y^2 = x^3 - 1\right\}$ ($K = \mathbb{Q}(j)$), $\left\{y^2 = x^3 - x\right\}$ ($K = \mathbb{Q}(i)$).

The set of isogenies $X \to X$ forms a ring: it can be embedded in $\mathrm{Hom}(L, M)$, hence it is free as a $\mathbb{Z}$-module.

Proposition 2. *The localisation of* $\mathrm{End}(X) = \mathrm{Hom}(X, X)$ *with respect to isogenies is* $\mathrm{End}_{\mathbb{Q}}(X) = \mathrm{End}(X) \otimes_{\mathbb{Z}} \mathbb{Q}$.

1.2. Line bundles and isogenies $X \to \hat{X}$ (10′).

Recall that line bundles on a complex torus $X = V/L$ correspond bijectively to canonical factors of automorphy

$$\alpha_{H,\chi}(\lambda, z) = \chi(\lambda) \exp(\pi H(\lambda, z) + \pi/2 \cdot H(\lambda, \lambda))$$

Then the translated automorphy factor by a point v is

$$\alpha_{H,\chi}(\lambda, z + v) = \chi(\lambda) \exp(\pi H(\lambda, v)) \exp(\pi H(\lambda, z) + \pi/2 \cdot H(\lambda, \lambda))$$

We want to identify $\chi_v(\lambda) = \chi(\lambda) \exp(\pi H(\lambda, v))$ with a unit semi-character $L \to \mathbb{S}^1$. For this consider the semi-character

$$\chi_v(\lambda) \exp(-\pi H(v, \lambda)) = \chi(\lambda) \exp(2i\pi \mathrm{Im}\, H(\lambda, v))$$

Proposition 3 (see [BL04, 2.4])**.** *Let L be a holomorphic line bundle on X, H an automorphy factor for L, such that the real symplectic form $E = \mathrm{Im} H$ is integral and nondegenerate (E can be identified with the harmonic 2-form $c_1(L)$).*

Then $\phi_L : x \mapsto {\tau_x}^* L \otimes L^{-1}$ defines a degree $\det E$ *isogeny $X \to \hat{X}$.*

Proof. For the moment by $\hat{X}$ we mean $\mathrm{Hom}(L, \mathbb{S}^1)$. The morphism ϕ_L is given by $v \mapsto \exp(2i\pi \mathrm{Im}\, H(\bullet, v))$: the kernel consists of v such that $E(L, v) \subset \mathbb{Z}$, which has $\det E$ elements. □

1.3. Elliptic curves, arithmetic-geometric mean (8′).

A historical example of isogeny between elliptic curves is given by the work of Gauß on the arithmetic-geometric mean [Cox84, Gra89].

Proposition 4. *Let a and b be positive real numbers, and α and γ denote their arithmetic and geometric mean. Then*

$$\int_0^\infty \frac{dx}{2\sqrt{x(x + a^2)(x + b^2)}} = \int_0^\infty \frac{dx}{2\sqrt{x(x + \gamma^2)(x + \alpha^2)}}$$

The value of this integral is exactly $\pi/AGM(a, b)$ where AGM *denotes the* arithmetic-geometric mean.

Let

$$A = (\frac{a + b}{2})^2 \qquad G = ab$$

Consider the following elliptic curves:

$$E_1 = \left\{y^2 = x(x + a^2)(x + b^2)\right\} \qquad E_2 = \left\{Y^2 = X(X + A)(X + G)\right\}$$

and the morphism $f : E_2 \to E_1$ given in projective coordinates by

$$[X : Y : 1] \mapsto [x : y : z] = [Y^2 : Y(X^2 + 2AX + AG) : (X + A)^2]$$

Rewrite E_1 as $\left\{y^2 = x((x-G)^2+4Ax)\right\}$ and note that

$$\begin{aligned} x - Gz &= Y^2 - G(X+A)^2 = (X+A)(X(X+G) - G(X+A)) \\ &= (X+A)(X^2 - AG) \end{aligned}$$

Then check that

$$\begin{aligned} &\frac{x((x-Gz)^2 + 4Axz)}{Y^2(X+A)^2} \\ &= (X^2 - AG)^2 + 4AY^2 \\ &= (X^2 - AG)^2 + 4AX(X+A)(X+G) \\ &= (X^2 + AG)^2 - 4AGX^2 + 4AX(X^2 + AG + (A+G)X) \\ &= (X^2 + AG)^2 + 4AX(X^2 + AG) + 4A^2X^2 = \frac{y^2 z}{Y^2(X+A)^2} \end{aligned}$$

Let ω be the canonical 1-form $\omega = \frac{d(x/z)}{2(y/z)}$. Then

$$\omega = \frac{dx}{2y} - \frac{xdz}{2yz}$$

$$\frac{1}{X} + \frac{1}{X+G} - \frac{1}{X+A} = \frac{X^2 + 2AX + AG}{Y^2}$$

$$\begin{aligned} f^*\omega &= \frac{2YdY}{2Y(X^2 - 2AX + AG)} - \frac{2Y^2(X-A)dX}{2Y(X-A)^2(X^2 - 2AX + AG)} \\ &= \frac{Y}{X^2 - 2AX + AG}\left(\frac{dY}{Y} - \frac{dX}{X-A}\right) \\ &= \frac{Y}{X^2 - 2AX + AG} \times \frac{1}{2}\left(\frac{dX}{X} + \frac{dX}{X+G} - \frac{dX}{X+A}\right) = \frac{dX}{2Y} \end{aligned}$$

Proposition 5. *The morphism defined above is an isogeny of degree 2.*

Proof. The morphism is clearly étale since it pulls back a non-vanishing 1-form to a non-vanishing 1-form. □

The very fast convergence of the computations can be interpreted as the rapid growth of $j(\tau)$ when $\tau = i \cdot 2^k \tau_0$ (write $j(it) = \sum_k j_k \exp(-2k\pi t)$).

2. Isogenies between abelian varieties (20′)

2.1. Definitions, algebraic version (9′).

Reference: [vdGM, ch. V].

Proposition 6. *Let X and Y be abelian varieties, and $f : X \to Y$ be a morphism of group schemes. The following conditions are equivalent:*

1. *f is surjective and* $\dim X = \dim Y$*;*
2. $\ker f$ *is finite, and* $\dim X = \dim Y$*;*
3. *f is finite, flat, and surjective.*

A morphism satisfying these conditions is called an isogeny.

Proof. To prove that $1 \implies 2$, we use the theorem of generic flatness: if Y is irreducible and reduced, and $f : X \to Y$ is a morphism of finite type, then f is flat over some open subset $U \subset Y$. If f is a surjective morphism of abelian varieties, any fibre is isomorphic to $\ker f$, which is then finite (by the dimension formula for flat morphisms).

To prove that $3 \implies 1$, since f is already known to be surjective, it only remains to show that $\dim X = \dim Y$, which follows from the dimension formula.

For $2 \implies 3$, note that f is proper with finite fibers, hence f is finite, and since X and Y are regular, f is flat. Surjectivity follows from the fact that $\dim X = \dim Y$. □

Definition. *The degree of an isogeny $f : X \to Y$ is the degree $[K(X) : K(Y)]$.*

Proposition 7. *An isogeny is* separable *iff it is étale, or if* $\ker f$ *is an étale group scheme.*

Proposition 8. *Any isogeny of degree prime to the characteristic of the base field is separable.*

2.2. Positive characteristic and Frobenius morphism.

Proposition 9. *An isogeny is* purely inseparable *(i.e. injective and gives residue fields the structure of inseparable extensions) iff $k(X)$ is purely inseparable over $k(Y)$, or iff* $\ker f$ *is a connected group scheme.*

Recall that the absolute Frobenius F is given on coordinate rings by the p-th power morphism: if X is a S-scheme, where S is a characteristic p scheme, the absolute Frobenius $X \to X$ is not a S-morphism, since it can be written

$$(s, x \in X_s) \to (s^p, x^p \in X_{s^p}).$$

The *relative Frobenius morphism* is thus defined as the fiber product $(\pi, F) : X \to X^{(p)} = S \times_{F,S,\pi} X$, which could be written

$$(s, x \in X_s) \to (s, x^p \in X_s^{(p)} = X_{s^p} \neq X_s).$$

It is no longer an endomorphism of X.

$$\begin{tikzcd}
& X^{(p)} \arrow[dd, dashed] \arrow[dr] & \\
X \arrow[ur, "F_S"] \arrow[rr, "F"'] \arrow[dd, "\pi"'] & & X \arrow[dd, "\pi"] \\
& S \arrow[dl, equal] \arrow[dr, "F"] & \\
S \arrow[rr, "F"'] & & S
\end{tikzcd}$$

Let R be a k-algebra, where k is a ring of characteristic p, and $R^{(p)} := k \otimes_{F,k} R$, where $F : k \to k$ is the absolute Frobenius map. The k-algebra structure of $k \otimes_F R$ is given by

$$\lambda \cdot (a \otimes x) = (\lambda a) \otimes x$$

$$(\lambda^p a) \otimes x = a \otimes (\lambda x)$$

The relative Frobenius morphism $F_k : R^{(p)} \to R$ is given by $\lambda \otimes x \mapsto \lambda x^p$, which is a morphism of k-algebras.

Proposition 10. *If $X = \operatorname{Spec} R$, then $X^{(p)} = \operatorname{Spec} R^{(p)}$ and $F_{\operatorname{Spec} k}$ is induced by the morphism F_k.*

Proposition 11. *The Frobenius homomorphism $X \to X^{(p)} = X \times_F \operatorname{Spec} k$ is a purely inseparable isogeny of degree p^g.*

2.3. **The Verschiebung homomorphism (11′).**

The Verschiebung operator on Witt vectors

$$W(\mathbb{Z}/p\mathbb{Z}) = \{(a_0, a_1, \dots), a_i \in \mathbb{Z}/p\mathbb{Z}\}$$

is defined by

$$V : (a_0, a_1, \dots) \mapsto (0, a_0, a_1, \dots)$$

and under the isomorphism $W(\mathbb{Z}/p\mathbb{Z}) \simeq \mathbb{Z}_p$ given by

$$(a_i) \to \sum \tilde{a}_i p^i$$

(here $\tilde{a}_i$ is the unique root of unity which is $\equiv a_i \pmod p$, the *Teichmüller representative*), it is easily seen that $V(x) = p \cdot x$. But the universal formulae defining Witt p-vectors involve non-linear parts which give the formula

$$p \cdot x = V(Fx) = F(Vx)$$

where F is the Frobenius automorphism.

The Verschiebung operator can actually be defined for any commutative flat group scheme (see [vdGM] for an exposition). Since the construction is local on the base, we suppose the base has the form $S = \operatorname{Spec} k$, where k is a commutative $\mathbb{Z}/p\mathbb{Z}$-algebra.

Theorem 12. *Let G be a flat commutative group scheme over a base S, and $F : G \to G^{(p)} = G \times_F S$ the relative Frobenius homomorphism.*

Then the morphism $g \to p \cdot g = g + \cdots + g$ can be factored as

$$G \xrightarrow{F} G^{(p)} \xrightarrow{V} G$$

where V is called the Verschiebung *operator, such that $VF = FV = p \cdot \mathrm{Id}_G$.*

If G is an abelian variety, V is a degree p^g isogeny.

The basic idea is the following: write the p-th power as the composition

$$G \xrightarrow{\Delta} \operatorname{Sym}^p G \xrightarrow{\sum} G$$

Here $\operatorname{Sym}^p G$ is the p-th symmetric power of G: when $G = \operatorname{Spec} R$, $\operatorname{Sym}^p G$ is $\operatorname{Spec}((R^{\otimes p})^{\mathfrak{S}_p})$. The morphism $\sum$ is induced by the p-fold coproduct $R \to R^{\otimes p}$ is $\mathfrak{S}_p$ invariant, and Δ is the embedding of the diagonal.

The key ingredient is proving that Δ factors through the relative Frobenius morphism. Note that Δ is expressed in terms of coordinate ring by the morphism $\delta : R^{\otimes p} \to R$ given by

$$a_1 \otimes \cdots \otimes a_p \mapsto a_1 \cdots a_p.$$

Lemma 13. *Let N denote the map $\boldsymbol{x} \mapsto \sum_{\sigma \in \mathfrak{S}_p} \boldsymbol{x}^\sigma$. Then the image of N is an ideal in $(R^{\otimes p})^{\mathfrak{S}_p}$. There is a well-defined natural morphism $\gamma : R^{(p)} \to (R^{\otimes p})^{\mathfrak{S}_p}/\mathrm{Im} N$ such that $\delta\gamma$ coincides with the k-linear Frobenius map $R^{(p)} \to R$.*

Proof. We first check that δ factors through $(R^{\otimes p})^{\mathfrak{S}_p}/\mathrm{Im} N$: it follows from the fact that $\delta(\boldsymbol{x}^\sigma) = \delta(\boldsymbol{x})$ for any $\sigma \in \mathfrak{S}_p$.

Let γ be the map

$$(\lambda, x) \mapsto \lambda(x \otimes \cdots \otimes x)$$

then γ is semi-linear with respect to x, that is

$$\gamma(\lambda, ax+by) = a^p\gamma(\lambda,x) + b^p\gamma(\lambda,y)$$

and linear with respect to λ. It thus correctly defines a map $\gamma : R^{(p)} \to (R^{\otimes p})^{\mathfrak{S}_p}$. Of course $\delta\gamma(\lambda,x) = \lambda x^p = F_k(\lambda\otimes x)$. □

Proposition 14. *If X is flat over S, the canonical closed subscheme $X^{[p]} = \Delta(X) \subset \mathrm{Sym}^p X$ is naturally isomorphic to $X^{(p)}$, and γ induces an isomorphism between $R^{(p)}$ and $(R^{\otimes p})^{\mathfrak{S}_p}/\mathrm{ImN}$, where $R = \mathcal{O}(X)$.*

Proof. If X is flat over S, then R is a direct limit of finitely generated flat (hence free) k-modules. Note that for any k-module M,

$$\gamma_M : (\lambda, m) \mapsto \lambda(m\otimes\cdots\otimes m)$$

still defines a morphism $k\otimes_F M \to (M^{\otimes p})^{\mathfrak{S}_p}$: if γ_M is an isomorphism for any free module M, then γ is also an isomorphism.

But if M has basis $(e_i)_{i\in I}$, we know a basis of $(M^{\otimes p})^{\mathfrak{S}_p}$, by looking at the various coefficients, and observe that $N(e_J) = \sum_\sigma e_{\sigma(J)}$ gives a basis element of $(M^{\otimes p})^{\mathfrak{S}_p}$ except when $J = (i,i,\dots,i)$, in which case the stabilizer has order divisible by p. The isomorphism γ_M is then explicit. □

About Cartier duality: if G is a finite locally free group scheme, then the group ring of G is a Hopf k-algebra H which is a free module of finite rank over k (up to a localisation).

Then H^* is also a Hopf algebra, by interchanging product and coproduct. Remember the diagram

$$H \xrightarrow{\Sigma^*} (H^{\otimes p})_{\mathfrak{S}_p} \xrightarrow{\Delta^*} H$$

where Σ^* is given by the p-fold Hopf coproduct, and Δ^* is the contraction of tensors. Then the dual maps are the dual of the product of H, which is the coproduct of H^*, and the traditional product on H^*, hence by duality, the Frobenius and Verschiebung operators of G become the Verschibenug and Frobenius operators on G^D.

2.4. **The Verschiebung for elliptic curves.** Let k be a field of characteristic 2, and E a k-ellptic curve with affine equation

$$y^2 + y = x^3 + px + q$$

Then $E^{(2)}$ is the curve over k with equation

$$y^2 + y = x^3 + p^2x + q^2 = (x+p)^3 + px^2 + p^3 + q^2.$$

Let $P = (a,b)$ be a point of E and let us compute $-2P = (x,y)$. The tangent line at P has equation

$$y - b = (a^2+p)(x-a) = a^2x - a^3 + p(x-a)$$

which gives the equations

$$(y^2+y) - (b^2+b) = x^3 - a^3 + p(x-a)$$

$$y^2 - b^2 = x(x^2-a^2)$$

but $(y-b)^2 = (a^2+p)^2(x-a)^2$, hence

$$x = (a^2+p)^2 = a^4+p^2 \qquad y = (a^2+p)^3 + a^3 + pa + b = (a^2+p)^3 + b^2 + q$$

Then 2P is given by corodinates:

$$\begin{aligned} x &= (a^2+p)^2 = a^4+p^2 \\ y &= (a^2+p)^3 + a^3 + pa + b = (a^2+p)^3 + b^2 + q + 1 \end{aligned}$$

This proves that $2P = V(a^2, b^2)$, where V is defined by

$$(A,B) \mapsto (X = A^2 + p^2, Y = (A+p)^3 + B + q + 1)$$

If $(A,B) \in E^{(2)}$, then

$$\begin{aligned} Y^2 + Y &= (A+p)^6 + (A+p)^3 + B^2 + B + q^2 + q \\ &= X^3 + (pA^2 + p^3 + q^2) + (q^2 + q) \\ &= X^3 + p(A^2 + p^2) + q \\ &= X^3 + pX + q \end{aligned}$$

2.5. **Consequences for p-torsion points.** Let X be an abelian variety over a field k of characteristic p. Then the group of p-torsion points $X[p]$ corresponds bijectively to the kernel of the Verschiebung morphism $X^{(p)} \to X$, which is a p-torsion group of rank $f \leq g$.

(When $l \wedge p = 1$, $X[l] \simeq (\mathbb{Z}/l\mathbb{Z})^{2g}$.)

References

[BL04] Christina Birkenhake and Herbert Lange, *Complex abelian varieties*, 2nd ed., Grundlehren der Mathematischen Wissenschaften, vol. 302, Springer-Verlag, Berlin, 2004. MR2062673 (2005c:14001)

[Cox84] David A. Cox, *The arithmetic-geometric mean of Gauss*, Enseign. Math. (2) **30** (1984), no. 3-4, 275–330. MR767905 (86a:01027)

[Car70] Pierre Cartier, *Quelques remarques sur la divisibilite des coefficients binomiaux*, Enseign. Math. (2) **16** (1970), 21–30.

[vdGM] Gerard van der Geer and Ben Moonen, *Abelian varieties*, book in preparation.

[Gra89] Daniel R. Grayson, *The arithogeometric mean*, Arch. Math. (Basel) **52** (1989), no. 5, 507–512, DOI 10.1007/BF01198359. MR998624 (90g:11071)