The geometric interpretation of the Tate pairing and its applications

2025/05/22 — Reading group

Damien Robert

Équipe Canari, Inria Bordeaux Sud-Ouest

Table of Contents

1 The geometric interpretation of the Tate pairing

2 Applications

3 Theory

The Tate pairing

- E_1/k elliptic curve; $P \in E_1(k)$ (exact) ℓ-torsion

  k is any field, ℓ need not be prime, we do not assume $\mu_\ell \subset k$. For simplicity we do restrict to ℓ prime to p throughout.
- $\widetilde{\phi} : E_1 \to E_2 = E_1/\langle P \rangle$; $\phi : E_2 \to E_1$
- The Weil-Cartier pairing $e_\phi : \operatorname{Ker} \widetilde{\phi} \times \operatorname{Ker} \phi \to \mu_\ell$ induces an isomorphism $\psi : \mu_\ell \to \operatorname{Ker} \phi$, $\zeta \mapsto P'$, the unique point that satisfies $e_\phi(P, P') = \zeta$.

Definition/Theorem

If $Q \in E_1(k)$, the Tate pairing $T_\phi(P, Q)$ is the unique element $t \in k^*/k^{*,\ell}$ such that there exists an isomorphism $\psi_Q : \{x \in \overline{k} \mid x^\ell = t\} \to \phi^{-1}(Q)$ where

1. ψ_Q is Galois equivariant: $\psi_Q \circ \sigma = \sigma \circ \psi_Q$ for all $\sigma \in \operatorname{Gal}(\overline{k}/k)$
2. If $x' = x\zeta$ where $\zeta \in \mu_\ell$, then $\psi_Q(x') = \psi_Q(x) + \psi(\zeta)$.

- Condition 1 states that ψ_Q is an isomorphism of Galois sets / an isomorphism of k-schemes
- Condition 2 gives compatibilities between the fibers and $\operatorname{Ker} \phi$
- Example: $Q \in \phi(E_2(k)) \Leftrightarrow T_\phi(P, Q) \in k^{*,\ell}$, in which case we have $\#\mu_\ell(k)$ rational preimages.
- Exercice: prove existence and unicity

  Hint: use Hilbert 90. Why do we need both conditions for unicity?
- t is unique, but not ψ_Q (Exercice: how many ψ_Q can there be?)

Insert a frame about the Weil-Cartier pairing

- $\phi : A_1 \to A_2, \widehat{\phi} : \widehat{A}_2 \to \widehat{A}_1$
- Weil-Cartier: $e_\phi : \operatorname{Ker} \phi \times \operatorname{Ker} \widehat{\phi} \to \mathbb{G}_m$
- Compatible with isogenies: $e_{\phi_3 \circ \phi_2 \circ \phi_1}(P, Q) = e_{\phi_2}(\phi_1(P), \widehat{\phi}_3(P))$ whenever these are well defined.
- Biduality: if $i : A_1 \to \widehat{\widehat{A}}_1$ is the biduality morphism, $e_{\widehat{\phi}}(Q, i(P)) = e_\phi(P, Q)^{-1}$
- So as a (horrible) abuse of notation, I'll use

$$e_{\widehat{\phi}}(P, Q) := e_{\widehat{\phi}}(Q, i(P))^{-1} = e_\phi(P, Q)$$

The case of a larger kernel

- $\widehat{\phi} : \widehat{A}_1 \to \widehat{A}_2; \phi : A_2 \to A_1, Q \in A_1(k)$
- $P \in \widehat{K} := \operatorname{Ker} \widehat{\phi}$ of exact order ℓ; $K' := \langle P \rangle^{\perp} \subset K := \operatorname{Ker} \phi$ (for the Weil-Cartier pairing e_{ϕ})
- K' acts on K. The orbits are in bijection with μ_{ℓ}
- K' acts on $\phi^{-1}(Q)$. The orbits are in bijection with $\{x \in \overline{k} \mid x^{\ell} = T_{\phi}(P, Q)\}$
- Galois equivariant and compatible with the Weil-Cartier pairing as before

Proof: ϕ factors out through K' as $\phi = \phi_1 \circ \phi_2$, where $\operatorname{Ker} \phi_2 = K'$ and $\operatorname{Ker} \widehat{\phi}_1 = \langle P \rangle$; and $\phi^{-1}(Q)/K' \simeq \phi_1^{-1}(Q)$. (+ Compatibility of Weil-Cartier pairing with isogenies.)

- Only depends on P, not on $\widehat{K}$ (as long as $P \in \widehat{K}$)
- In particular, $T_{\phi}(P, Q) = T_{\ell}(P, Q)$.

- If $P_1, \dots, P_m \in \widehat{K}(k)$, then the Tate pairings $T_{\phi}(P_i, Q)$ gives information on $\phi^{-1}(Q)$ modulo $\langle P_1, \dots, P_m \rangle^{\perp}$.
- If we have rational generators $P_1, \dots, P_m$ of $\widehat{K}$, the $T_{\phi}(P_i, Q)$ allows to recover the full Galois structure on $\phi^{-1}(Q)$.

Example: The multiplication by $[\ell]$ on an elliptic curve

- $\phi = [\ell] : E \to E$
- (P_1, P_2) basis of $E[\ell], P_1, P_2, Q \in E(k)$ (so $\mu_\ell \subset k$)
- $t_1 = T_\ell(P_1, Q), t_2 = T_\ell(P_2, Q)$

Proposition

t_1, t_2 are the unique elements in $k^* / k^{*,\ell}$ such that there exists a rational / Galois equivariant isomorphism

$$\psi_{Q_1,Q_2} : \{x_1, x_2 \in \bar{k} \mid x_1^\ell = t_1, x_2^\ell = t_2\} \to [\ell]^{-1}(Q)$$

such that $\psi_{Q_1,Q_2}(x_1\zeta_1, x_2\zeta_2) = \psi_{Q_1,Q_2}(x_1, x_2) + T$ where $T \in E[\ell]$ is the unique point that satisfies $e_\ell(P_1, T) = \zeta_1, e_\ell(P_2, T) = \zeta_2$.

- t_1, t_2 give informations on the Galois structure of $[\ell]^{-1}Q$
- They are trivial if and only if $Q \in [\ell]E(k)$
- If $k = \mathbb{F}_q, \mu_\ell \subset \mathbb{F}_q$, then $Q \in [\ell]E(\mathbb{F}_q)$ iff $T_\ell(P, Q)$ for all $P \in E[\ell](\mathbb{F}_q)$
  no need to assume that the full ℓ-torsion is rational (see below)!

The reduced Tate pairing

- If $t = T_\ell(P, Q)$ and $x^\ell = t$, then
$$\Xi = \Xi_t : \sigma \in \mathrm{Gal}(\bar{k}/k) \mapsto \frac{\sigma(x)}{x}$$
gives a cocycle with value in μ_ℓ
- Well defined up to a coboundary
- Explains how $\mathrm{Gal}(\bar{k}/k)$ acts on $\phi^{-1}(Q)$: if $Q_0 = \psi_Q(x)$ so that $\phi(Q_0) = Q$, then
$$\sigma(Q_0) = Q_0 + \psi(\Xi(\sigma))$$
- Reformulation (which also works for larger kernels $P \in \widehat{K}$): $\xi(\sigma) = e_\phi(P, \sigma(Q_0) - Q_0) \in \mu_\ell$
- If $\mu_\ell \subset k$, Ξ is a morphism $\mathrm{Gal}(\bar{k}/k) \to \mu_\ell$ and does not depends on the choice of x
- Hilbert 90: $t \in k^*/k^{*,\ell} \mapsto \Xi_t \in H^1(k, \mu_\ell)$ is an isomorphism

- If $k = \mathbb{F}_q$, the cocyle Ξ is uniquely determined by its value on π_q
- $\Xi(\pi_q) = \frac{\pi_q(x)}{x} = t^{\frac{q-1}{\ell}}$ is the reduced Tate pairing:
$$t_\phi(P, Q) = T_\phi(P, Q)^{(q-1)/\ell}$$
- Well defined in $\mu_\ell/(\pi_q - 1) \simeq H^1(\mathbb{F}_q, \mu_\ell)$. $\#\mu_\ell/(\pi_q - 1) = \#\mathbb{F}_q^*/\mathbb{F}_q^{*,\ell} = \#\mu_\ell(\mathbb{F}_q)$
- If $\mu_\ell \subset \mathbb{F}_q$, the reduced Tate pairing is well defined in μ_ℓ

Properties of the Tate pairing

$\widehat{\phi} : \widehat{A}_1 \to \widehat{A}_2; \phi : A_2 \to A_1$, Ker ϕ of exponent L, $Q \in A_1(k)$; $T_\phi : \widehat{K}(k) \times A_1(k) \to k^*/k^{*,L}$.

Bilinearity:

- Bilinear on the right

  Given Q_1, Q_2, combine ψ_{Q_1}, ψ_{Q_2}. This crucially relies on compatibility of ψ_{Q_i} and ψ.

- Bilinear on the left (by bilinearity of the Weil pairing)

  If P_1 is of nm-torsion and $P_2 = mP_1$, naive bilinearity is

  $$T_{nm}(P_2, Q) = T_{nm}(P_1, Q)^m$$

  seen in $k^*/k^{*,nm}$.
  We can also see $T_{nm}(P_2, Q)$ as $T_m(P_2, Q) \in k^*/k^{*,n}$. We have a natural map $H^1(k, \mu_n) \to H^1(k, \mu_{nm})$ associated to the inclusion $\mu_n \hookrightarrow \mu_{nm}$; it corresponds via the isomorphism $H^1(k, \mu_n) \simeq k^*/k^{*,n}$ to $i : k^*/k^{*,n} \to k^*/k^{*,nm}, [x] \mapsto [x^m]$. It is not injective in general, so we lose some information if we see $T_{nm}(P_2, Q) = i(T_m(P_2, Q)) \in k^*/k^{*,mn}$ rather than $T_m(P_2, Q) \in k^*/k^{*,n}$.

  We also have a map $\mu_{nm} \twoheadrightarrow \mu_n, \zeta \mapsto \zeta^m$, which induces $H^1(k, \mu_{nm}) \to H^1(k, \mu_n)$, hence $p : k^*/k^{*,nm} \to k^*/k^{*,n}$, given by $[x] \mapsto [x]$.
  Refined bilinearity is

  $$T_m(P_2, Q) = p(T_{nm}(P_1, Q)) \in k^*/k^{*,n}.$$

  We recover naive bilinearity via $i(T_m(P_2, Q)) = ip(T_{nm}(P_1, Q)) = T_{nm}(P_1, Q)^m \in k^*/k^{*,nm}$.

  If $\mu_{nm} \subset k$, then $i : k^*/k^{*,n} \to k^*/k^{*,nm}$ is injective, and we can ignore this subtlety.

Properties of the Tate pairing

$\widehat{\phi} : \widehat{A}_1 \to \widehat{A}_2; \phi : A_2 \to A_1$, Ker ϕ of exponent L, $Q \in A_1(k); T_\phi : \widehat{K}(k) \times A_1(k) \to k^*/k^{*,L}$.

Non degeneracy:

- Non degeneracy on the left if $\widehat{K}(k) = \widehat{K}(\overline{k})$:

$$T_\phi(P,Q) = 1 \forall P \in \widehat{K} \Leftrightarrow Q \in \phi(E_2(k))$$

Non degeneracy properties over a finite field $k = \mathbb{F}_q$:

- If P of order ℓ, and $[x] \in \mathbb{F}_q^*/\mathbb{F}_q^{*,\ell}$, then there exists $Q \in A_1(\mathbb{F}_q)$ such that $T_\phi(P,Q) = [x]$

⇒ Non degeneracy on the right:
if $\mu_\ell(\mathbb{F}_q) \neq 1$, there exists $Q \in A_1(\mathbb{F}_q)$ such that $T_\phi(P,Q) \neq 1 \in \mathbb{F}_q^*/\mathbb{F}_q^{*,\ell}$.
(Direct proof: use that $\#A_2(\mathbb{F}_q) = \#A_1(\mathbb{F}_q)$)

- If $\mu_L \subset \mathbb{F}_q$, non degeneracy on the left also holds even if $\widehat{K}(\mathbb{F}_q) \neq \widehat{K}(\overline{\mathbb{F}}_q)$:
if $T_\phi(P,Q) = 1 \in \mathbb{F}_q^*/\mathbb{F}_q^{*,L}$ for all $P \in \widehat{K}(\mathbb{F}_q)$, then $Q \in \phi(A_2(\mathbb{F}_q)$.

Computing the Tate pairing

$P \in E_1(k), \widetilde{\phi} : E_1 \to E_2 = E_1/\langle P \rangle, Q \in E_1(k)$.

Not easy a priori: how to compute $T_\phi(P,Q)$?

Theorem/Definition

$$T_\phi(P,Q) = T_\ell(P,Q) = f_{\ell,P}(Q)$$

where $f_{\ell,P}$ is the normalised Miller function with divisor $(\ell)(P) - (\ell)(0_E)$.

- Can be computed in $O(\log \ell)$ operations in k
- Does not require to build ϕ nor E_2!

Aside: roots of unity in a finite field

- $\mathbb{F}_q^*/\mathbb{F}_q^{*,\ell} \simeq \mu_\ell/(\pi_q - 1)$ is of cardinal $\ell_0 = \#\mu_\ell(\mathbb{F}_q)$.
- $\ell_0 = \ell \wedge (q-1)$, and $\mu_{\ell_0} = \mu_{\ell_0}(\mathbb{F}_q)$
- Writing $\ell = \ell' \ell_0$, the exponentiation $\mu_\ell \to \mu_{\ell_0}, \zeta \mapsto \zeta^{\ell'}$ induces an isomorphism

$$\mu_\ell/(\pi_q - 1) \simeq \mu_{\ell_0}$$

- The corresponding isomorphism $\mathbb{F}_q^*/\mathbb{F}_q^{*,\ell} \simeq \mathbb{F}_q^*/\mathbb{F}_q^{*,\ell_0}$ is given by $[x] \mapsto [x]$
- If P is of order ℓ, $T_\ell(P,Q) = T_{\ell_0}(\ell' P, Q) \in \mathbb{F}_q^*/\mathbb{F}_q^{*,\ell_0}$
- If ϕ is the isogeny induced by $\langle P \rangle$ and ϕ' the one induced by $\langle \ell' P \rangle$, we see that the Galois structure of the small fiber ${\phi'}^{-1}(Q)$ completely determines the Galois structure of the larger fiber $\phi^{-1}(Q)$.

Questions

- Why "geometric"?
- What are some applications of this interpretation?
- Why is the Tate pairing fast to compute?
- How do we link the geometric interpretation with Miller's algorithm?
- Can we build an isomorphism $\psi_Q : \{x \in \overline{k} \mid x^\ell = T_\ell(P, Q)\} \to \phi^{-1}(Q)$ explicitly?

- What if $\phi : E_2 \to E_1$ is rational, cyclic of order ℓ, $Q \in E_1(k)$, but Ker $\widetilde{\phi}$ has no rational generator P?

  If P lives in an extension k', $t = T_\ell(P, Q)$ is well defined in $k'^* / k'^{*,\ell}$, but changing t by tx^ℓ where $x \in k'$ may change the k-Galois structure of $\{x \mid x^\ell = t\}$!

Table of Contents

1 The geometric interpretation of the Tate pairing

2 Applications

3 Theory

Usual applications of the Tate pairing

- Non degeneracy $\Rightarrow$ pairing based cryptography
- Subgroup membership testing [Koshelev]

- If $A/\mathbb{F}_q$ is an abelian variety, $T_1, \dots, T_r$ a basis of $A[\ell](\mathbb{F}_q)$ where T_i is of order ℓ_i, and $\mu_\ell \subset \mathbb{F}_q$ then by non degeneracy

$$T : A(\mathbb{F}_q)/A[\ell](\mathbb{F}_q) \to \prod_{i=1}^{r} \mu_{\ell_i}, P \mapsto t_\ell(T_i, P)$$

  is an isomorphism. (Reijnders's profiles)
- This allows to probe $\mathbb{Z}_\ell$-torsion information on the subgroup $\langle P_i \rangle$ generated by some sampled points P_i.
- For instance, if ℓ is prime, $\langle P_i \rangle$ generates the ℓ-Sylow of $A(\mathbb{F}_q)$ iff the $T(P_i)$ generate μ_ℓ^r.
- Example: Entangled basis is a special case of this when $E/\mathbb{F}_{p^2}$ is supersingular and $\ell = 2$.
- See [Rei25] paper for more applications and generalisations of the entangled basis algorithm

- Here we only focus only on applications from the geometric interpretation
- It tells us that Tate pairings allow us to probe the Galois structure of the fiber of an isogeny ϕ
- How can we use this information?

Montgomery curves

$P \in E_1[2](k), \widetilde{\phi} : E_1 \to E_2 = E_1/\langle P \rangle, \phi : E_2 \to E_1$

- $E_2[2] = \phi^{-1}(0_{E_1}) \bigcup \phi^{-1}(P)$
- $\phi^{-1}(0_{E_1}) \simeq \mu_2 \simeq \mathbb{Z}/2\mathbb{Z}$ ($p \neq 2$) so we always have at least one rational point of 2-torsion on E_2 generating the dual isogeny
- E_2 has full rational two torsion if and only if $\phi^{-1}(P)$ has rational points, if and only if $T_2(P, P)$ is a square

Sending P to $(0, 0)$, we obtain:

Proposition

Let $E : By^2 = x^3 + Ax^2 + tx$, and $P = (0, 0)$ the point of 2-torsion on it. Then $T_2(P, P) = [t] \in k^*/k^{*,2}$ and t is a square if and only if $E/\langle P \rangle$ has full rational 2-torsion.

Montgomery curves

Proposition

Let $E : By^2 = x^3 + Ax^2 + tx$, *and* $P = (0,0)$ *the point of 2-torsion on it. Then* $T_2(P,P) = [t] \in k^*/k^{*,2}$ *and t is a square if and only if* $E/\langle P \rangle$ *has full rational 2-torsion.*

Conversely, if $t \in k^*$ is any representative of $T_2(P,P)$, then up to a change of $(X:Z)$ variables, translation by P is given by $(X:Z) \mapsto (Z:tX)$ [BRS23, § 6], so:

- If $x = X/Z$, the 2-torsion on E_1 is given by $x = \infty, 0, \alpha, t/\alpha$
- The 4-torsion points P' above P satisfy $x(P') = \pm\sqrt{t}$
- In this model, $E : By^2 = x^3 + Ax^2 + tx$

Example

- If $T_2(P,P)$ is a square, P is of "Montgomery type", and taking $t = 1$ we obtain that E_1 is isomorphic to:
$$By^2 = x^3 + Ax^2 + x, \quad A = -\alpha - 1/\alpha$$
- Otherwise, we recover the Montgomery$^-$-model of [CD20]:
$$By^2 = x^3 + Ax^2 + \xi x$$

$[\xi] = T_2(P,P), \xi \in k^* \setminus k^{*,2}$

Probing the Galois structure of an isogeneous elliptic curve

- $E_1/\mathbb{F}_q, E_1(\mathbb{F}_q) = \langle P_1, P_2 \rangle$ a basis, P_1, P_2 of order n_1, n_2.
- $P \in E_1(\mathbb{F}_q)$ of order ℓ, $\widetilde{\phi} : E_1 \to E_2 = E_1/\langle P \rangle, \phi : E_2 \to E_1$
- Since $\phi(E_2(\mathbb{F}_q)) \subset E_1(\mathbb{F}_q)$, the $\mathbb{F}_q$-Galois structure of the fibers $\phi^{-1}(P_1), \phi^{-1}(P_2)$ encodes the group structure of $E_2(\mathbb{F}_q)$
- Hence the Tate pairings $t_1 = T_\phi(P, P_1), t_2 = T_\phi(P, P_2)$ encode all the information about $E_2(\mathbb{F}_q)$.

Proposition

- *We have an isomorphism of Galois sets:*

$$\phi^{-1}(E_1(\mathbb{F}_q)) \simeq \{x \in \overline{\mathbb{F}}_q \mid x^\ell = t_1^{a_1} t_2^{a_2}, 0 \leq a_1 < n_1, 0 \leq a_2 < n_2\}/\mathbb{F}_q^*)$$

- *If P_i is of order n_i, as a Galois-set,* $E_2(\mathbb{F}_q) \simeq \{x \in \mathbb{F}_q \mid x^\ell = t_1^{a_1} t_2^{a_2}, 0 \leq a_i < n_i\}$

The isomorphisms ψ_{P_1}, ψ_{P_2} are unique only up to a translation by $T \in \operatorname{Ker} \phi(\mathbb{F}_q)$. Since T is rational, this ambiguity still allows to recover the group structure of $E(\mathbb{F}_q)$.

Probing the ℓ-torsion of an isogeneous elliptic curve

- $P \in E_1(\mathbb{F}_q)$ of order ℓ, $\widetilde{\phi} : E_1 \to E_2 = E_1/\langle P \rangle$, $\phi : E_2 \to E_1$
- $\phi(E_2[\ell]) = \langle P \rangle$ so $E_2[\ell] = \phi^{-1}(\langle P \rangle)$
- The self Tate pairing $t = T_\phi(P, P) \in \mathbb{F}_q^*/\mathbb{F}_q^{*,\ell}$ encodes all the information about the Galois structure of $E_2[\ell]$
- We have an isomorphism of Galois sets:

$$E_2[\ell](\overline{\mathbb{F}}_q)) \simeq \{x \in \overline{\mathbb{F}}_q \mid x^\ell = t^a\}/\mathbb{F}_q^*$$

- For fun, we can also use the reduced Tate pairing

$$\begin{aligned} t_\phi(P, Q) &= t^{(q-1)/\ell} \in \mu_\ell/(\pi_q - 1) \\ &= e_\ell(P, \pi_q Q_0 - Q_0) \text{ where } \ell Q_0 = Q \end{aligned}$$

- Pick a representative $\zeta = \zeta_0^u$ of $t_\phi(P, Q)$ in $\mu_\ell = \langle \zeta_0 \rangle$.
- There exists a basis Q_1, Q_2 of $E_2[\ell](\overline{\mathbb{F}}_q)$ such that
  - $\phi(Q_1) = 0_{E_1}, e_\phi(P, Q_1) = \zeta_0$. We have $\pi_q(Q_1) = qQ_1$ since $\operatorname{Ker} \phi \simeq \mu_\ell$;
  - $\phi(Q_2) = P$, and $\pi_q(Q_2) = Q_2 + uQ_1$
- So the matrix of π_q acting on $E_2[\ell]$ is equivalent to $\begin{pmatrix} q & u \\ 0 & 1 \end{pmatrix}$

Volcanoes

- $E/\mathbb{F}_q$ ordinary, $\ell \mid \#E(\mathbb{F}_q)$, ℓ prime
- The ℓ-isogeny graph forms a volcano structure
- On level 0 (the floor): $E[\ell^\infty](\mathbb{F}_q) = \mathbb{Z}/\ell^f\mathbb{Z}$
- On level 1: $E[\ell^\infty](\mathbb{F}_q) = \mathbb{Z}/\ell^{f-1}\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$
- On level $m < f/2$: $E[\ell^\infty](\mathbb{F}_q) = \mathbb{Z}/\ell^{f-m}\mathbb{Z} \times \mathbb{Z}/\ell^m\mathbb{Z}$
- If we reach level $m = f/2$ (the stability level), then f has to be even, and at all levels $m \geq f/2$:

$$E[\ell^\infty](\mathbb{F}_q) = \mathbb{Z}/\ell^{f/2}\mathbb{Z} \times \mathbb{Z}/\ell^{f/2}\mathbb{Z}$$

- A cyclic descending isogeny stays descending
- A cyclic ascending isogeny stays ascending, until it eventually reach the crater, where it can have horizontal then descending steps.

$\Rightarrow$ If $\phi : E_1 \to E_2$ is a cyclic ℓ^e-isogeny and we know the level of E_1 and E_2, then we know exactly how many ascending/horizontal/descending steps ϕ took.

Pairing the volcano [IJ10]

Proposition

If $P \in E_1[\ell^e](\mathbb{F}_q)$ *and* $\mu_{\ell^e} \subset \mathbb{F}_q$*, then*

$$E_2[\ell^e](\mathbb{F}_q) = \mathbb{Z}/\ell^e\mathbb{Z} \times \mathbb{Z}/\ell^{e-e'}\mathbb{Z}$$

where $\ell^{e'}$ *is the order of* $t_{\ell^e}(P,P)$.

The lower the order of the self Tate pairing, the more rational points of ℓ^e-torsion we have on the codomain, and the higher we are in the volcano:

- If $e' > 0$ then we know that E_2 is at level $e - e'$
- Otherwise, we only know that E_2 is at level $\geq e$

See [Rob23, Example 5.16] for a fully detailed discussion, including the case $\mu_{\ell^e} \not\subset \mathbb{F}_q$.

Example (2-isogenies)

If $P \in E[2]$, $t_2(P,P) = 1 \Leftrightarrow E/\langle P \rangle$ has full rational two torsion $\Leftrightarrow E/\langle P \rangle$ is at level ≥ 1.

A case study: the CSIDH volcano

- $E/\mathbb{F}_p$ supersingular elliptic curve, $p = u2^f - 1$ (u odd), $f \geq 3$ so $p \equiv 7 \pmod 8$.
- The CSIDH volcano is of height 1 (and $\mu_{2^f}(\mathbb{F}_p) = \mu_2$)

Torsion:

- **On the floor**: primitive orientation by $\mathbb{Z}[\pi_p]$
- $E(\mathbb{F}_p) \simeq \mathbb{Z}/(p+1)\mathbb{Z}$, so $E[2^\infty](\mathbb{F}_p) = \mathbb{Z}/2^f\mathbb{Z}$
- If E' is the quadratic twist of E, $E[2^f] = E[2^f](\mathbb{F}_{p^2}) \simeq E[2^f](\mathbb{F}_p) \oplus E'[2^f](\mathbb{F}_p)$

- **On the crater**: primitive orientation by $\mathbb{Z}[\frac{1+\pi_p}{2}]$.
- $E(\mathbb{F}_p) \simeq \mathbb{Z}/\frac{p+1}{2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, so $E[2^\infty](\mathbb{F}_p) = \mathbb{Z}/2^{f-1}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
- $E[2^{f-1}] = E[2^{f-1}](\mathbb{F}_{p^2}) = E[2^{f-1}](\mathbb{F}_p) + E'[2^{f-1}](\mathbb{F}_p)$, with:

$$E[2^{f-1}](\mathbb{F}_p) \cap E'[2^{f-1}](\mathbb{F}_p) = E[2]$$

- $(2) = (2, \frac{\pi-1}{2})(2, \frac{\pi+1}{2}) = \mathfrak{p}_+\mathfrak{p}_-$
- $2^f \mid \pi_p^2 - 1, \mathfrak{p}_+^{f-1}\mathfrak{p}_- \mid \pi_p - 1, \mathfrak{p}_-^{f-1}\mathfrak{p}_+ \mid \pi_p + 1.$

The CSIDH volcano: on the floor

- $E[2^\infty](\mathbb{F}_p) = \mathbb{Z}/2^f\mathbb{Z}$.
- P_0 a generator, $T_0 := 2^{f-1}P_0$.
- T_0 generates the ascending isogeny, and $t_2(T_0, T_0) = 1$ as expected.
- The reduced Tate pairing $t_{2^f}(P_0, P_0) = t_2(T_0, P_0) = -1 \in \mu_2$ is non trivial by non degeneracy, so $E/\langle P_0 \rangle$ is on the floor.
- The isogeny generated by P_0 goes up, goes in the '+' horizontal direction for $f-2$ steps, then goes down again.
- If P_0' a generator of $E'[2^\infty](\mathbb{F}_p)$, the isogeny generated by P_0' goes up, goes in the '-' horizontal direction for $f-2$ steps, then goes down again.

The CSIDH volcano: on the crater

Isogenies:

- $E[2](\mathbb{F}_p) = \{0_E, T_-, T_0, T_+\}$ where:
  - T_0 generates the descending isogeny $\phi_0 : E \to E_0$
  - $E[\mathfrak{p}_\pm] = \langle T_\pm \rangle$ so that $\phi_- : E \to E_-$, $\phi_+ : E \to E_+$ are the two horizontal isogenies
- P_+ a generator of $E[\mathfrak{p}_+^{f-1}]$, it is of order 2^{f-1} and above T_+.
- P_0 a generator of $E_0(\mathbb{F}_p)[2^f]$

Images (up to renormalisation):

- $\phi_+(E[2^{f-1}](\mathbb{F}_p) = \langle \phi_+(P_+) \rangle \oplus \langle \phi_+(T_-) \rangle \simeq \mathbb{Z}/2^{f-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

$$\phi_+(P_+) = 2P_+^{E_+}, \quad \phi_+(2^{f-3}P_+) = T_+^{E_+}$$
$$\phi_+(T_-) = \phi_+(T_0) = T_-^{E_+}, \quad \phi_+(2^{f-3}P_+ + T_-) = T_0^{E_+}.$$

- $\phi_-(E[2^{f-1}](\mathbb{F}_p)) = \langle \phi_-(P_+) \rangle \simeq \mathbb{Z}/2^{f-1}$, so $\phi_-(P_+) = P_+^{E_-}$.
- $\phi_0(P_+) = 2P_0$, and $\widetilde{\phi_0}(P_0) = P_+ + T_0$.

The CSIDH volcano: on the crater

Pairings:

- T_+ is the only point divisible by 2 in $E(\mathbb{F}_p)$, so all pairings $t_2(T_i, T_+)$ are trivial
- T_+, T_- are horizontal, so have trivial self pairings; T_0 goes down, so has non trivial self pairing.
- Only T_+ is in the rational image of $\widetilde{\phi_0}$ (out of T_+, T_-, T_0)
- The isogeny of $\widetilde{\phi_+}$ is of type $-$, so only T_+ is in the rational image
- The isogeny of $\widetilde{\phi_-}$ is of type $+$, so all T_i are in the rational image

Proposition

$$
\begin{array}{llll}
t_2(T_-, T_-) = 1 & t_2(T_-, T_0) = 1 & t_2(T_-, T_+) = 1 & t_2(T_-, P_+) = -1 \\
t_2(T_0, T_-) = -1 & t_2(T_0, T_0) = -1 & t_2(T_0, T_+) = 1 & t_2(T_0, P_+) = 1 \\
t_2(T_+, T_-) = -1 & t_2(T_+, T_0) = -1 & t_2(T_+, T_+) = 1 & t_2(T_+, P_+) = 1
\end{array}
$$

The CSIDH volcano: applications

On the floor:

- P generates the full cyclic rational 2^f-torsion if and only if $t_2(T_0, P) = -1$.
- This is equivalent to $x(P) - x(T_0)$ is not a square

On the crater:

- T_0 is the unique point of 2-torsion with non trivial self pairing
- $t_2(T_0, T_\pm) = \pm 1$, so we can identify T_+, T_-
- A rational point $P \in E[2^\infty](\mathbb{F}_p)$ is of exact order 2^{f-1} $\Leftrightarrow$ it is not in the image of $\widetilde{\phi_-}(E_-(\mathbb{F}_p))$ $\Leftrightarrow t_2(T_-, P) = -1$
- A rational point P of exact order 2^{f-1} generates an horizontal isogeny (hence is P_+) if and only if $t_2(T_+, P) = 1$.

See [DEF+25, Appendix D] for other cool applications!

Evaluating divided endomorphisms

- Assume that $E[\ell] \subset E(\mathbb{F}_q)$
- Then $\pi_q - 1$ is divisible by ℓ

- If $P \in E(\mathbb{F}_q)$, we want to evaluate $\frac{\pi_q - 1}{\ell}(P)$
- Let $P' \in E(\overline{\mathbb{F}}_q)$ such that $\ell P' = P$.
- Then $\frac{\pi_q - 1}{\ell}(P) = (\pi_q - 1)P'$
- Can we compute this without computing P'?

- Pick a basis T_1, T_2 of $E[\ell]$
- We know how π_q acts on P' thanks to the reduced Tate pairings $t_\ell(T_1, P), t_\ell(T_2, P)$!
- Hence we can evaluate $\frac{\pi_q - 1}{\ell}$ without using division points (this requires DLPs in μ_ℓ through)
- See [DEF+25, Appendix D.2] for the details.

Multiradical isogenies

- Let $\phi_1 : A_1 \to A_2$ be an ℓ-isogeny of rank g of ppavs
- $\phi_2 : A_2 \to A_3$ is said to be non (partially) backtracking if $\phi_2 \circ \phi_1$ is still of rank g
- Equivalently: $\ker \phi_2 \cap \operatorname{Ker} \widetilde{\phi}_1 = 0$
- So $\widetilde{\phi}_1$ induces a bijection between $\operatorname{Ker} \phi_2$ and $\operatorname{Ker} \phi_1$.

Proposition

Assume that we have rational generators $P_1, \dots, P_g$ of $\operatorname{Ker} \phi_1$. Then each choice of isotropic $Q_1 \in \widetilde{\phi}_1^{-1}(P_1), \dots, Q_g \in \widetilde{\phi}_1^{-1}(P_g)$ gives a different non backtracking isogeny ϕ_2, via $\operatorname{Ker} \phi_2 = \langle Q_1, \dots, Q_g \rangle$, and they all arise this way.

So there are $\ell^{g(g+1)/2}$ such isogenies.

Theorem (Multiradical isogenies)

There is a rational bijection between these choices and the solutions of $\{x_{ij}^{\ell} = T_\ell(P_i, P_j) \mid i \leq j\}$.

Multiradical isogenies

Proposition

Assume that we have rational generators $P_1, \dots, P_g$ of $\operatorname{Ker} \phi_1$. Then each choice of isotropic $Q_1 \in \widetilde{\phi}_1^{-1}(P_1), \dots, Q_g \in \widetilde{\phi}_1^{-1}(P_g)$ gives a different non backtracking isogeny ϕ_2, via $\operatorname{Ker} \phi_2 = \langle Q_1, \dots, Q_g \rangle$, and they all arise this way.
So there are $\ell^{g(g+1)/2}$ such isogenies.

Theorem (Multiradical isogenies)

There is a rational bijection between these choices and the solutions of $\{x_{ij}^\ell = T_\ell(P_i, P_j) \mid i \leq j\}$.

Proof.

Without the isotropy condition on the Q_i, we know by the geometric interpretation that there is a (rational) bijection Ψ between $T = \{x_{ij}^\ell = T_\ell(P_i, P_j) \mid 1 \leq i, j \leq g\}$ and the set $\{(Q_1, \dots, Q_g) \mid Q_i \in \widetilde{\phi}_1^{-1}(P_i)\}$.
Adding the isotropy condition gives via Ψ^{-1} a (rational) subset $T' \subset T$. Working a bit more, we can prove that the projection map $T \to T''$, $(x_{ij}, 1 \leq i, j \leq g) \mapsto (x_{ij}, 1 \leq i \leq j \leq g)$ restricts to a bijection $T' \simeq T''$, see [Rob23, Theorem 5.19]. Composing all maps, we obtain a rational bijection between the subset of isotropic Q_i and $\{x_{ij}^\ell = T_\ell(P_i, P_j) \mid i \leq j\}$.

□

Making the isomorphism effective

- E_1/k elliptic curve; $P \in E_1(k)$ ℓ-torsion, $\widetilde{\phi}: E_1 \to E_2 = E_1/\langle P \rangle$. $Q \in E_1(k)$,
- We want to build an explicit rational isomorphism

$$\psi_Q : \operatorname{Spec} k[x]/(x^\ell - T_\ell(P,Q)) \to \phi^{-1}(Q).$$

- We will use cubical arithmetic!

- Pick up a cubical point $\widetilde{P}$ above P, possibly over an extension, such that $\ell\widetilde{P} = \widetilde{O}$ (no need for $\widetilde{P}$ to be symmetric here)
- Pick some rational cubical points $\widetilde{Q}, \widetilde{P+Q}$ and compute $\ell\widetilde{P+Q} = \lambda_Q \cdot \widetilde{Q}$
- Cubical theory tells us that λ_Q is rational (even if $\widetilde{P}$ is not) and a representative of $T_\ell(P,Q)$.
- For any λ such that $\lambda^\ell = \lambda_Q$, then replacing $\widetilde{P+Q}$ by $\lambda \cdot \widetilde{P+Q}$ above we get that $\ell\widetilde{P+Q} = \widetilde{Q}$ (and conversely).
- If we work with (cubical) coordinates $X_1, \dots, X_n$ of level n prime to ℓ, then the $X_i(j\widetilde{P+Q})$ gives the (cubical) coordinates of level $n\ell$ of the point in $\phi^{-1}(Q)$ corresponding to λ
- We can use a magic 5×5 matrix to descend from level $n\ell$ to coordinates of level n.
- See [Rob24, § 6.2] and [Rob25]

Table of Contents

1 The geometric interpretation of the Tate pairing

2 Applications

3 Theory

A descent story

- We have a k-rational isogeny $\phi : A_1 \to A_2$ between abelian varieties.
- Goal: We want to recover $A_2(k)$.
- A rational point $Q \in A_2(k)$ may come from a non rational point $P \in A_1(\bar{k})$.
- How can we recover the rational points on A_2 from the geometric points on A_1?

General descent theory:

- If $\phi : X \twoheadrightarrow Y$ is an epimorphism, we can look at the pullback $X \times_Y X \rightrightarrows X$.
- A point $T \to Y$ induces by pullback points $T' \to X$ and $T'' \to X \times_Y X$ and an action $T'' = T' \times_Y X \to T'$ satisfying appropriate gluing condition ("descent data").
- If $T_1 \to T_2$ is a morphism above Y, the pullback gives a morphism $T_1' \to T_2'$ compatible with the descent data $T_i'' \to T_i'$.
- Conversely, if ϕ is a descent epimorphism (e.g. ϕ is fppf), then all morphisms $T_1' \to T_2'$ above X respecting the descent data come from a morphism $T_1 \to T_2$ above Y.
- If ϕ is of effective descent, we can even reconstruct the objects $T \to Y$ from the descent data, without knowing a priori that it already exists.

Torsor galore

- If k_2/k_1 is a Galois field extension of Galois group G, then $\operatorname{Spec} k_2 \to \operatorname{Spec} k_1$ is a G-torsor: $\operatorname{Spec} k_1 \simeq [\operatorname{Spec} k_2/G]$
- $\operatorname{Spec} k_2 \times_{\operatorname{Spec} k_1} \operatorname{Spec} k_2 \simeq \operatorname{Spec} k_2 \times G$
- The two natural maps to $\operatorname{Spec} k_2$ are given by $(x, \sigma) \mapsto x$ and $(x, \sigma) \mapsto \sigma(x)$.
- Given $X, Y/k_1$, the descent data corresponds to the Galois action on X_{k_2} and Y_{k_2} and a map $X_{k_2} \to Y_{k_2}$ descends to k_1 iff it is Galois equivariant.

- Likewise if $\phi : A_1 \to A_2$ is an isogeny over $\overline{k}$ with kernel K, ϕ is a K-torsor: $A_2 = [A_1/K]$.
- $A_1 \times_{A_2} A_1 \simeq A_1 \times K$ with the two natural maps given by $(x, t) \mapsto x$ and $(x, t) \mapsto x + t$.
- $\overline{k}$-points on A_2 corresponds to K-orbits on A_1

The rational points of the isogeneous abelian variety

Putting everything together:

$$\begin{aligned} A_2(k) &\simeq \{P+K \mid P \in A_1(k^{sep}), \sigma(P+K) = P+K \quad \forall \sigma \in \mathrm{Gal}(k^{sep}/k)\} \\ &\simeq \{P \in A_1(k^{\mathrm{sep}}), \sigma(P) - P \in K \quad \forall \sigma \in \mathrm{Gal}(k^{sep}/k)\}/K \end{aligned}$$

- We do not want to work in $A_1(\bar{k})$.
- Switching the roles: if we have an isogeny $\phi' : A_2 \to A_1$, then each rational point P on A_1 corresponds to some Galois stable fiber ${\phi'}^{-1}(P) \subset A_2$.
- We stay in $A_1(k)$, but the corresponding descent data lives in A_2, which we don't know (yet).
- Idea: use duality!
- If $\phi : A_1 \to A_2$, $\widehat{\phi} : \widehat{A}_2 \to \widehat{A}_1$. A point $Q \in \widehat{A}_1$ corresponds to a rational divisor D_Q in A_1 (algebraically equivalent to 0). The fiber $\widehat{\phi}^{-1}(Q) \subset \widehat{A}_2$ corresponds to the divisors D_R in A_2 such that $\phi^* D_R = D_Q$.
- The fiber $\widehat{\phi}^{-1}(Q)$ encodes the descent of D_Q to A_2 through ϕ. We can reexpress this in terms of descent data on A_1!

In a stack no one can hear you scream

- At this point, it is convenient to use the language of stacks.

  Or it's because I had to learn about stacks for a paper, so now I try to mention them everytime…
- An algebraic stack $\mathfrak{X}$ behaves exactly like a scheme/an algebraic space, except that the points $\mathfrak{X}(R)$ form a groupoid rather than just a set
- Hence two maps $T \rightrightarrows \mathfrak{X}$ can be (2)-isomorphic without being equal.
- Let $B\mathbb{G}_m = [k/\mathbb{G}_m]$ be the stacky quotient. $B\mathbb{G}_m$ is the classifying stack of $\mathbb{G}_m$-torsor, hence of line bundles / divisors (up to linear equivalence).

In a stack no one can hear you scream

- Back to our isogeny $\phi : A_1 \to A_2$.
- A (linear class of) divisor D on A_1 corresponds to a map $\Phi_D : A_1 \to B\mathbb{G}_m$.
- D is algebraically equivalent to 0 if and only if this map is invariant (up to isomorphism) by translation by P for all $P \in A_1(\overline{k})$: $t_P^* \Phi_D \simeq \Phi_D$
- Equivalently: this diagram is commutative (up to isomorphism)

$$\begin{array}{ccc} A_1 & \xrightarrow{\quad t_P \quad} & A_1 \\ & {\scriptstyle \Phi_D} \searrow \qquad \swarrow {\scriptstyle \Phi_D} & \\ & B\mathbb{G}_m & \end{array}$$

- $\widehat{A}_1 = \mathrm{Hom}(A_1, B\mathbb{G}_m)$ (morphisms of Picard stacks)
- Descending D to D' on A_2 means finding a map $\Phi_{D'} : A_2 \to B\mathbb{G}_m$ such that the composition $A_1 \xrightarrow{\phi} A_2 \to B\mathbb{G}_m$ is (isomorphic to) the map $\Phi_D : A_1 \to B\mathbb{G}_m$: $\phi^* \Phi_{D'} \simeq \Phi_D$.

$$\begin{array}{ccc} A_1 & \xrightarrow{\quad \phi \quad} & A_2 \\ & {\scriptstyle \Phi_D} \searrow \qquad \swarrow {\scriptstyle \Phi_{D'}} & \\ & B\mathbb{G}_m & \end{array}$$

- Concretely, this consists in picking up for each $P \in \mathrm{Ker}\, \phi(\overline{k})$ a choice of an isomorphism $t_P^* \Phi_D \simeq \Phi_D$, in a compatible way.

Long story short

- $\phi : A_1 \to A_2$ of kernel K
- $Q \in \widehat{A}_1$ corresponds to a divisor D_Q on A_1
- $G(D_Q)$ the theta group:

$$G(D_Q)(\bar{k}) = \{(P, g_{P,Q})\}$$

  where $g_{P,Q}$ induces an isomorphism between D_Q and $t_P^* D_Q$.
- We may see $g_{P,Q}$ as a function with divisor $t_P^* D_Q - D_Q$.
- The fiber $\widehat{\phi}^{-1}(Q) \subset \widehat{A}_2$ is in bijection with K-descent data for D_Q
- These descent data (datum?) correspond exactly to lifts $\widetilde{K}$ of K to $G(D_Q)$.
- This is Galois equivariant: $\widetilde{K}$ corresponds to a rational point $Q' \in \widehat{\phi}^{-1}(Q)$ if and only if it is invariant by Galois.

- Any explicit description of $G(D_Q)$ allows to compute these descent data
- If $X \to A_1 \times \widehat{A}_1$ is the Poincaré biextension, $G(D_Q)$ is the pullback of X to $A_1 \times Q$
- So we can use our favorite biextension arithmetic: Miller's representation, cubical arithmetic, …
- Generic framework to recover the Galois structure of fibers of any isogeny!

Back to elliptic curves

- $P \in E_1(k)$ of order ℓ, $\phi : E_1 \to E_2 = E_1/\langle P \rangle$
- $Q \in E_1(k), D_Q = (Q) - (0_E)$
  Actually it should be $(-Q) - (0_E)$ but everyone is used to the "wrong" divisor $(Q) - (0_E)$ in the literature.
- A lift of $K = \langle P \rangle$ to the theta group $G(D_Q)$ corresponds to a choice of biextension function $g_{P,Q}$ with divisor[1]
$$\operatorname{div} g_{P,Q} = (P) + (Q) - (P+Q) - (0_E)$$
  which is of order ℓ for the biextension group law.
- $\widetilde{K} = \{1, g_{P,Q}, g_{2P,Q}, g_{3P,Q}, \dots\}$

- Let $\mathbf{g}_{P,Q}$ be the biextension function normalised to 1 at 0_{E_1}.
- Then $\mathbf{g}_{\ell P,Q} = f_{\ell,P}(Q)$ where $f_{\ell,P}$ is the normalised Miller function with divisors $\ell(P) - \ell(0_{E_1})$
- The biextension function $\lambda \mathbf{g}_{P,Q}$ is of order ℓ if and only if $\lambda^{-\ell} = f_{\ell,P}(Q)$
- Since $\sigma(\mathbf{g}_{P,Q}) = \mathbf{g}_{P,Q}$, we have $\sigma(\lambda g_{P,Q}) = \sigma(\lambda) g_{P,Q}$
- So the fiber $\widetilde{\phi}^{-1}(Q)$ is Galois-isomorphic to $\{x \mid x^\ell = f_{\ell,P}(Q)\}$.
- This gives Condition 1 of the geometric Tate pairing. For condition 2 we need to work more and use that the biextension arithmetic also gives the Weil pairing.

[1] Technically: $\operatorname{div} g_{P,Q} = (-P-Q) + (0_E) - (-P) - (-Q)$ and $\operatorname{div} f_{\ell,P} = l(0_{E_1}) - l(-P)$

The case of a non rational generator

- The theta group/biextension point of view allow to handle rational kernels with non rational generators.
- Let $P \in E_1(\overline{\mathbb{F}}_q)$ of order ℓ which generate a $\mathbb{F}_q$-rational isogeny $\phi : E_1 \to E_2$ with kernel K.
- We have $\pi_q(P) = mP$ for some m prime to ℓ.
- Let $Q \in E_1(\mathbb{F}_q)$, and $\mathbf{g}_{P,Q}$ be the normalised biextension function.
- If $\lambda^{-\ell} = f_{\ell,P}(Q)$, $g_{P,Q} := \lambda \mathbf{g}_{P,Q}$ generates a lift $\widetilde{K} = \{1, g_{P,Q}, g_{2P,Q}, \dots\}$ of K in $G(D_Q)$.
- This time, $\pi_q(\mathbf{g}_{P,Q})$ is the normalised biextension function $\mathbf{g}_{mP,Q}$ above (mP, Q), so $\pi_q(g_{P,Q}) = \lambda^q \mathbf{g}_{mP,Q}$.
- So $\widetilde{K} = \langle g_{P,Q} \rangle$ is rational (hence corresponds to a rational point in $\widetilde{\phi}^{-1}(Q)$) if and only if $\pi_q(g_{P,Q}) = g_{mP,Q}$.
- Evaluating at 0_{E_1}, this gives an equation $\lambda^q = \lambda^m f_{m,P}(Q)$.
  (The biextension arithmetic gives that $\mathbf{g}_{mP,Q}(0_{E_1}) = f_{mP}(Q)$.)
- More generally, $\sigma(\langle \lambda \mathbf{g}_{P,Q} \rangle) = \langle \lambda' \mathbf{g}_{P,Q} \rangle$ where λ' satisfy $\lambda^q = \lambda'^m f_{m,P}(Q)$.
- This gives the $\mathbb{F}_q$-Galois structure on the solutions $\{\langle \lambda \mathbf{g}_{P,Q} \rangle) \mid \lambda^\ell = T_\ell(P,Q)\}$

Example (The geometric interpretation of the Ate pairing)

Take $P \in E[\ell]$ of eigenvalue q for the Frobenius: $\pi_q(P) = qP$. The action of π_q on the fiber $\widetilde{\phi}^{-1}(Q)$ is described by $\pi_q^{-1}(f_{q,P}(Q))$ where $f_{q,P}(Q))$ is the Ate pairing! (See also [Rob24, Remark 3.21])

Last slide: The geometric interpretation of the Tate pairing

- Secretly the geometric interpretation is about étale μ_ℓ-torsors
- $A_1/k, P \in \widehat{A}_1(k)$ ℓ-torsion, $\widehat{\phi} : \widehat{A}_1 \to \widehat{A}_2 = \widehat{A}_1/\langle P \rangle, \phi : A_2 \to A_1, Q \in A_2(k)$
- P induces an isomorphism $\operatorname{Ker} \phi \simeq \mu_\ell, T \mapsto e_\phi(P, T)$, hence an isomorphism $B \operatorname{Ker} \phi \simeq B\mu_\ell$
- $A_2 \to \operatorname{Spec} k$ is $\operatorname{Ker} \phi$-equivariant (taking the trivial action on $\operatorname{Spec} k$), hence induces a map

$$[A_2 / \operatorname{Ker} \phi] \to B \operatorname{Ker} \phi$$

We have the following pullback diagram:

$$\begin{array}{ccccccc}
\phi^{-1}(Q) & \longrightarrow & \operatorname{Spec} k & & \operatorname{Spec} k & \longleftarrow & \{x^\ell = t\} \\
\downarrow & & \downarrow Q & & \downarrow t & & \downarrow \\
A_2 & \xrightarrow{\phi} & A_1 \simeq [A_2 / \operatorname{Ker} \phi] & & \mathbb{G}_m \simeq [\mathbb{G}_m / \mu_\ell] & \xleftarrow[x \mapsto x^\ell]{} & \mathbb{G}_m \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
\operatorname{Spec} k & \longrightarrow & B \operatorname{Ker} \phi & \xrightarrow{\simeq} & B\mu_\ell & \longleftarrow & \operatorname{Spec} k
\end{array}$$

Last slide: The geometric interpretation of the Tate pairing

We have the following pullback diagram:

$$
\begin{array}{ccccccc}
\phi^{-1}(Q) & \longrightarrow & \operatorname{Spec} k & & \operatorname{Spec} k & \longleftarrow & \{x^\ell = t\} \\
\downarrow & & \downarrow Q & & \downarrow t & & \downarrow \\
A_2 & \xrightarrow{\phi} & A_1 \simeq [A_2 / \operatorname{Ker} \phi] & & \mathbb{G}_m \simeq [\mathbb{G}_m / \mu_\ell] & \xleftarrow[x \mapsto x^\ell]{} & \mathbb{G}_m \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
\operatorname{Spec} k & \longrightarrow & B \operatorname{Ker} \phi & \xrightarrow{\simeq} & B\mu_\ell & \longleftarrow & \operatorname{Spec} k
\end{array}
$$

Definition (The Tate pairing)

- Given a point $Q : \operatorname{Spec} k \to A_1$, the Tate pairing is the map

$$T_\phi(P, Q) : \operatorname{Spec} k \to B\mu_\ell$$

  given by the composition $\operatorname{Spec} k \to A_1 \to B \operatorname{Ker} \phi \to B\mu_\ell$.
- Since $B\mu_\ell(k) = k^* / k^{*,\ell}$, there is a representative t in k^* such that $T_\phi(P, Q) : \operatorname{Spec} k \to B\mu_\ell$ is isomorphic to $t : \operatorname{Spec} k \to B\mu_\ell$, hence gives an isomorphism of μ_ℓ-torsors:

$$\phi^{-1}(Q) \simeq \{x^\ell = t\}$$

Bibliography

[BRS23] R. Barbulescu, D. Robert, and N. Sarkis. "Models of Kummer lines and Galois representations". June 2023 (cit. on p. 16).

[CD20] W. Castryck and T. Decru. "CSIDH on the surface". In: International Conference on Post-Quantum Cryptography. Springer. 2020, pp. 111–129 (cit. on p. 16).

[DEF+25] P. Dartois, J. K. Eriksen, T. B. Fouotsa, A. H. L. Merdy, R. Invernizzi, D. Robert, R. Rueger, F. Vercauteren, and B. Wesolowski. "PEGASIS: Practical Effective Class Group Action using 4-Dimensional Isogenies". Accepted for publication at Crypto 2025. Mar. 2025 (cit. on pp. 25, 26).

[IJ10] S. Ionica and A. Joux. "Pairing the volcano". In: Algorithmic number theory. Springer, 2010, pp. 201–218 (cit. on p. 20).

[Rei25] K. Reijnders. A Note on the Advanced Use of the Tate Pairing. Cryptology ePrint Archive, Paper 2025/477. 2025. url: https://eprint.iacr.org/2025/477 (cit. on p. 14).

[Rob23] D. Robert. "The geometric interpretation of the Tate pairing and its applications". Feb. 2023 (cit. on pp. 20, 28).

[Rob24] D. Robert. "Fast pairings via biextensions and cubical arithmetic". Apr. 2024 (cit. on pp. 29, 38).

[Rob25] D. Robert. "Cubical arithmetic on abelian varieties: introduction and applications". Biextension reading group. Feb. 2025. url: http://www.normalesup.org/~robert/pro/publications/slides/2025-02-Cubical.pdf (cit. on p. 29).