The geometric interpretation of the Tate pairing and its applications

Damien Robert

The geometric interpretation of the Tate pairing and its applications

DAMIEN ROBERT

Abstract. While the Weil pairing is geometric, the Tate pairing is arithmetic: its value depends on the base field considered. Nevertheless, the étale topology allows to interpret the Galois action in a geometric manner. In this paper, we discuss this point of view for the Tate pairing: its natural geometric interpretation is that it gives étale μ_n-torsors. While well known to experts, this interpretation is perhaps less known in the cryptographic community.

As an application, we explain how to use the Tate pairing to study the fibers of an isogeny, and we prove a conjecture by Castryck and Decru on multiradical isogenies.

1. Introduction

This paper serves two purpose: first provide a geometric interpretation of the Tate pairing, namely as étale μ_n-torsors, and secondly use this interpretation to study fibers of isogenies.

As an application, we give a short proof of a conjecture by Castryck and Decru on multiradical isogenies [CD21, Conjecture 1]. This conjecture is recalled in Section 2, and proven in Section 5, see Theorem 5.18.

Along the way, we review the theory of twists and torsors in Section 3, then explain how to define the Tate-Cartier pairing on an arbitrary abelian scheme A/S in Section 4, this allows us to prove the version "in family" of this conjecture. We also give the general compatibility of the Tate pairing with isogenies in Proposition 4.6, as we haven't been able to find the general formula in the literature.

It is actually quite fun to reprove all the standard theory (bilinearity, non degeneracy, change of base field) of the Tate pairing over finite fields from the torsor point of view. We explain some of this in Section 4.5: the proof of non degeneracy and bilinearity from the torsor point of view does offer some insights compared to the standard proofs, especially in the case where $\mu_n \not\subset \mathbb{F}_q$, see Remark 4.3.

There are several different versions of the Tate pairing. When K is a complete local field, and A/K an abelian variety, Tate defines a pairing $H^i(K, A^\vee) \times H^{1-i}(K, A) \to H^2(K, \mathbb{G}_m) = \mathbb{Q}/\mathbb{Z}$ [Mil06, § I.3]. Instead, we will use the variant (the "Tate-Lichtenbaum-Frey-Ruck" pairing) introduced in [FR94] in the context of DLP and cryptography of elliptic curves, that we will denote by $e_{T,n}$ and which takes value in $H^1(k, \mu_n)$, i.e., gives μ_n-torsors. This is essentially the torsion version of the global pairing defined above, and is induced by the cup product action on cohomology coming from the Weil pairing $e_{W,n}$. In this paper we will call it the Tate pairing, or sometimes the Tate-Cartier pairing $e_{T,f}$ when we look at a general isogeny f (hence the cup product induced by the Weil-Cartier pairing $e_{W,f}$ of f) rather than just the multiplication by $[n]$.

In the context of cryptography, an essential feature of the Tate pairing $e_{T,n}$ on an abelian variety $A/\mathbb{F}_q$ defined over a finite field is that it is non-degenerate if $\mu_n \subset \mathbb{F}_q$. This needs not be the case if $\mu_n \not\subset \mathbb{F}_q$ (but see Theorem 4.22), nor when the base field k is not a finite

Date: May 25, 2023.

field. Over a general base scheme S, we do have a weak version of non degeneracy under certain conditions, see Corollary 5.2. We argue that even if we do not have a strong form of non degeneracy in these more general contexts, the Tate pairing is still useful. The high level overview may be stated as follows: the Weil pairing allows to understand the kernel $\mathrm{Ker}\, f$ of an isogeny f, the Tate pairing to understand its fibers $f^{-1}(P)$. See Proposition 5.1 and Remarks 5.3 and 5.8 for more precise statements.

Thanks to the powerful machinery of étale cohomology [AGV72], it is not more difficult to work over a general scheme[1] S as a base (provided that n is invertible on S). We adopt this point of view in this text. As mentionned above, this allows to naturally provide statements "in family", or to prove that formulas obtained over a generic fiber are valid over points where they have good reduction (see Example 5.20). The reader who is only interested in abelian varieties over fields can without harm take $S = \mathrm{Spec}\, k$ throughout, and use Galois cohomology (see Example 3.7 and Remark 3.10).

We emphasize that, despite our use of somewhat technical jargon due to our choice of working over a base scheme rather than a field, all our proofs are very natural and simple. See for instance Remarks 5.8 and 5.19 where we reformulate the proofs of Proposition 5.1 and Theorem 5.18 in more elementary terms.

1.1. **Outline:** In Section 2, we briefly review the conjecture by Castryck and Decru on multiradical isogenies.

In Section 3, we review the theory of torsors and how to interpret the first cohomology group in terms of torsors. This is well known and we do not make any claim of originality. We spend a bit of time detailing how to interpret the group structure on the first cohomological group in terms of torsors in the hope of making this operation as concrete as possible.

Then in Section 4 we explain how the Weil-Cartier pairing allows to define a Tate-Cartier pairing on an abelian scheme. There is no difficulty in extending the usual definition over a finite field to a scheme. What is more interesting is to reinterpret and reprove the standard properties of the Tate pairing in terms of torsors. In particular, we give explicit formula over a field in Section 4.4 and then reprove the non degeneracy over a finite field in Section 4.5, and various other standard properties of the Tate pairing over a finite field. As explained in the introduction, for our applications over a general field k we cannot assume that $\mu_n \subset k^*$, so we need to be careful with our statements.

We finally give applications in Section 5. We show how various properties of elliptic curves which are usually proven using the explicit addition formula admit a simpler conceptual proof using the geometric interpretation of the Tate pairing, which allows to extend them to abelian varieties. Indeed, as explained in Section 5.1, the Tate pairing allows to understand the Galois structure of the fibers of an isogeny. This allows us to determine criterion for divisibility in Section 5.2, determine the level of an isogenous elliptic curve on an isogeny volcano in Section 5.3, and to prove the multiradical isogeny conjecture in Section 5.4.

1.2. **Thanks:** I benefited from helpful conversations with Baptiste Morin on étale cohomology. All errors in this text are mine.

[1]For simplicity, we will always assume that S is Noetherian, or at least qcqs with finitely many connected components.

2. Multiradical isogenies

Let $(A, \mathcal{L})$ be a principally polarised abelian variety of dimension g over a field k, and $f : A \to B$ an n-isogeny[2] with $K = \operatorname{Ker} f$ of rank g in $A[n]$, and n invertible in k. Assume a basis $(P_1, \dots, P_g)$ of $\operatorname{Ker} f$ is given over k.

Definition 2.1 (Non backtracking isogenies)**.** A non (partially) backtracking isogeny relative to f is an n-isogeny $g : B \to C$ with kernel of rank g and such that $\operatorname{Ker} g \cap \operatorname{Ker} \tilde{f} = 0$ where $\tilde{f} : B \to A$ is the dual (or rather contragredient[3]) isogeny of f.

It is not hard to check that there are exactly $n^{g(g+1)/2}$ non backtracking isogenies over $\overline{k}$ [CD21, Lemma 2]. This also will be a consequence of Theorem 5.18. Let $\widetilde{\mathcal{J}_f}$ be the moduli of all non backtracking kernels on B.

Lemma 2.2. $\widetilde{\mathcal{J}_f} \simeq \mathcal{L}_f := \{(P'_1, \dots, P'_g) \mid \tilde{f}(P'_i) = P_i$ *and the* P'_i *span an isotropic subgroup of* $B[n]$ *for the Weil pairing* $\}$.

Proof. Let $K' = \operatorname{Ker} g$ be the kernel of a non backtracking n-isogeny. Then K' is isotropic for the Weil pairing $e_{W,n}$ on $B[n]$. Since $K' \cap \operatorname{Ker} \tilde{f} = 0, \tilde{f}$ induces a bijection between K' and $\tilde{f}(B[n]) = K$. So there is a unique basis $(P'_1, \dots, P'_g)$ of K' satisfying the conditions of the Lemma.

Conversely, if the (P'_i) satisfy the condition, then they span a subgroup K' of $B[n]$ of cardinal at least n^g since $\#K = n^g$, but the isotropy condition ensures that the cardinal is exactly n^g. Hence $\tilde{f}$ induces a bijection between K' and K, so $K' \cap \operatorname{Ker} \tilde{f} = 0$. Then the isogeny g of kernel K' is a non backtracking isogeny. □

The conjecture by Castryck and Decru [CD21, Conjecture 1] is that there are explicit algebraic formulas expressing the locus $\mathcal{L}_f$ in terms of radicals $e_{T,n}(P_i, P_j)^{1/n}$, where $e_{T,n}$ denotes the n-Tate pairing and $1 \le i \le j \le n$. More precisely, there is an isomorphism defined over k between $\mathcal{L}_f$ and the scheme given by the radical formulas $\{x_{ij}^n = e_{T,n}(P_i, P_j)\}$ for $1 \le i \le j \le g$. This scheme is our first example of torsor: it is a $\mu_n^{g(g+1)/2}$-torsor in the étale topology. They also conjecture that these formulas vary in family, i.e., are valid for an abelian scheme A/S (this is the "good reduction" aspect of their conjecture). Notably by looking at the universal abelian stack $\mathfrak{A}/\mathcal{A}_g^1(n)$ with a marked maximal isotropic basis of rank g in $\mathfrak{A}[n]$, we obtain a universal formula. In this paper we prove these conjectures.

Note that Lemma 2.2 holds for an abelian scheme A/S too if we are provided with a basis $P_1, \dots, P_g$ of $\operatorname{Ker} f$ over S. Indeed since everything is flat over S, we can test isomorphisms fibrally, hence the isogeny g is non backtracking if and only if it is non backtracking on each geometric fibers.

This conjecture was already proven (except the case of "good reduction") for elliptic curves in [CDV20; CDHV22], and applications for isogeny based cryptography are given in [CDV20; CD21; CDHV22]. We will first give in Section 4 the interpretation of the Tate pairings above as étale μ_n-torsors. As mentioned in the introduction, this is of course well known to expert, but probably less known in the cryptographic community. Then in Section 5 we explain how, using this interpretation, the conjecture essentially follows by unraveling the definitions. The reader only interested to the proof can look at Theorem 3.8 and Definitions 3.12, 3.15 and 4.2 for the definition of the Tate pairing as a μ_n-torsor, then skip directly to Section 5. Or even go directly to Remark 5.19 for a direct proof when over a field.

[2] Which means that there is a principal polarisation $\mathcal{M}$ on B such that $f^*\mathcal{M} \simeq \mathcal{L}^n$.

[3] If $f : (A, \mathcal{L}) \to (B, \mathcal{M})$ with $\mathcal{L}$ and $\mathcal{M}$ principal polarisations with associated isogenies $\Phi_{\mathcal{L}} : A \to \widehat{A}$, $\Phi_{\mathcal{M}} : B \to \widehat{B}$, and $f^*\mathcal{M} = \mathcal{L}^n$, we define the contragredient isogeny $\tilde{f}$ by $\tilde{f} := \Phi_{\mathcal{L}}^{-1} \circ \hat{f} \circ \Phi_{\mathcal{M}}$.

3. Torsors

3.1. **Torsors and twists.** We briefly review the general theory of torsors and twists. As usual, the reference for all this is [Stacks], see also [Mil16, §III.4; Gir71].

Definition 3.1. A twist of an object X/S is an object Y/S which is locally isomorphic to X.

Here locally means with respect to some (Grothendieck) topology τ on S. When S is a scheme, standard topologies for the study of twists include the fppf, étale and Zariski topology. In this paper we will mostly use the étale topology. Indeed the étale topology over a field k is essentially the geometric interpretation of Galois theory [Gro71]. In the following we will always assume that τ is coarser than the fppf topology (and in practice we will take the étale topology).

One needs to be careful that we consider twists of X/S in some category (where the local isomorphisms need to be in this category), and that if X/S belong to two different categories, it may have different twists in these categories.

Example 3.2.

- A line bundle is a twist of the affine line $\mathbb{A}^1_S$ for the Zariski topology.
- A twist E'/k of an elliptic curve E/k over a field k is a twist of E (in the category of elliptic curves) for the étale topology: E' becomes isomorphic to E over some étale extension of k.
- If $S = \operatorname{Spec} k$ is a field and $\xi_1, \xi_2 \in k^*$, the schemes $x^n = \xi_1$, $x^n = \xi_2$ (i.e., $\operatorname{Spec}(k[x]/(x^n - \xi_i))$ become isomorphic over the extension $k((\xi_1/\xi_2)^{1/n})$, but they are not isomorphic over k unless ξ_1/ξ_2 is an n-th power over k already. Since $k((\xi_1/\xi_2)^{1/n})$ is a flat extension of k, they are twists for the fppf topology, and also for the étale topology if n is inversible on k.

Definition 3.3. Given an fppf algebraic group space G/S, an algebraic space X/S with an action of G is a torsor for the topology τ if X/S is τ-locally isomorphic to G (with its canonical action by itself) in the category of G-spaces. In other words, a torsor is a twist of G/S.

Remark 3.4 (Representability)**.** Even if G/S is a scheme, G-torsors for the fppf (or étale topology) need not be schemes, they are only algebraic spaces in general. Many criteria for representability by schemes are given in [Ray70], see also [Mil16, III Theorem 4.3] for a summary. This will be the case in the following situations:

- If G/S is affine, by effectivity of fppf descent of quasi-coherent sheaves;
- If G/S is quasi-affine, by effectivity of fppf descent for quasi-affine morphisms [Stacks, Tag 0247];
- If G/S is smooth and separated and $\dim S \leq 1$ (in particular if $S = \operatorname{Spec} k$ is a field);
- If G/S is smooth and proper with geometrically connected fibers and G is regular;

As a particular case, G-torsors will be represented by schemes when:

- A/S is an abelian scheme and S is either regular or of dimension ≤ 1. Note however that over a general base, Raynaud proves that an abelian algebraic space A/S is represented by a scheme, but its torsors need not be, see [Ray70] for some examples.
- G/k is a group scheme[4] such that the neutral point 0_G is geometrically reduced over k (because G/k is always separated as the diagonal is the base change of the identity section which is assumed to be rational, and if 0_G is geometrically reduced then G/k is smooth by [GD64, IV.15.6.10.(iii)]).

[4] A quasi-separated algebraic group space is a scheme [Art69].

If X/S is a torsor, then it is a formally principal homogeneous space[5]: the action of G is free and transitive. Equivalently, a formally principal homogeneous space is a G-space, i.e., a space X/S with an action by G, such that the natural map $G \times_S X \to X \times_S X$ is an isomorphism (this can be checked fpqc locally).

Note that if X/S is a (formally) principal homogeneous space, it is isomorphic to G (i.e., it is trivial) if and only if it admits a global section. Indeed, the action of G on this global section induces an isomorphism of G with X over S. So X/S is a torsor in the topology τ if and only if it admits sections τ-locally, and it is the trivial torsor if and only if it admits a global section.

Lemma 3.5. *If G/S is fppf, then fppf-torsors are the same as fppf (formally) principal homogeneous spaces. If G/S is smooth, then fppf-torsors are already étale torsors and they are the same as smooth (formally) principal homogeneous spaces. If G/S is étale, then fppf torsors are already étale torsors and are the same as étale (formally) principal homogeneous spaces.*

Proof. If X/S is a τ-torsor with τ coarser than the fpqc topology, then since G/S is fppf and X/S is locally isomorphic to G, X/S is fppf. By the same reasoning, if G/S is smooth or étale, then a G-torsor X/S will also be smooth or étale because these notions are also fpqc-local on the base [GD64, p. IV.17.7.3].

Conversely, if X/S is an fppf G-formally principal homogeneous space, then it is an fppf torsor. Indeed X/S always admits sections over itself: the diagonal map $X \to X \times_S X$ is such a section, so since X/S is fppf, X/S admits sections fppf-locally, hence is an fppf torsor. Likewise, if X/S is smooth (resp. étale), then it admits sections smooth-locally (resp. étale locally), so is a smooth (resp. étale) torsor. But in fact a smooth morphism always admits étale local sections since it is Zariski locally given by an étale morphism over $\mathbb{A}^n/U$. So if X/S is a smooth fppf torsor, it admits section étale locally, so it is an étale torsor. □

If G/S is a group space, the category of fppf G-torsors above S is classified by the algebraic stack $\mathcal{B}G = [S/G]$ [Stacks, Tag 0CQJ], in particular torsors are stable by base change and satisfy descent under an fppf morphism.

Example 3.6.

- Let $\xi \in k^*$, then the scheme $x^n = \xi$ has a natural action multiplicative action by μ_n. It is a torsor over k in the fppf topology, and even in the étale topology if n is prime to the characteristic p of k. In particular the twists $x^n = \xi_1$ and $x^n = \xi_2$ from Example 3.2 are not only twists in the category of schemes, but also in the category of schemes with a μ_n-action.
- The archetypical example of a torsor is a quotient: if a fppf group G/S acts freely on a space $X \to S$, then the quotient X/G (in the category of fppf sheaves) is an algebraic space [Ryd13] and $X \to X/G$ is a G-torsor above S. Conversely given a G-torsor $X \to Y$ above S, then Y is isomorphic to X/G.
- If A/k is an abelian variety and $p : X \to A$ a finite étale cover, then X is an abelian variety provided that $p^{-1}(0_A)$ has a rational point in X, and in this case p is a separable isogeny. This is the Serre-Lang theorem, see [EGM12, Theorem 10.36]. In this case, p is a Galoisian étale cover with abelian Galois group $\ker p$, and $p : X \to A = X/\operatorname{Ker} p$ is a $\operatorname{Ker} p$-torsor. As an application, $\pi^1_{\text{etale}}(A_{k^{\text{sep}}}, 0_A) = \varprojlim A[n](k^{\text{sep}}) = T(A)$ is

[5] Also called pseudo-torsor in [Stacks, Tag 0497]; in the terminology of [DA70] a principal homogeneous space is a torsor for the fpqc topology.

the Tate module, hence $H^1_{\text{etale}}(A_{k^{\text{sep}}}, \mathbb{Z}_\ell) = \text{Hom}(\pi^1_{\text{etale}}(A_{k^{\text{sep}}}, 0_A), \mathbb{Z}_\ell) = T_\ell A^\vee$ [EGM12, § 10.38 and 10.39].

Example 3.7 (The case of a field)**.** If $S = \text{Spec}\, k$ is a field, a connected finite étale cover is a finite separable field extension k'/k. An fppf cover is any non empty scheme of finite type $Y \to k$, in particular an inseparable field extension k'/k is an fppf cover but not an étale cover.

If G/k is a group scheme then an fppf G-torsor $X \to k$ is a scheme X/k of finite type with an action by G such that the induced action of $G(\bar{k})$ on $X(\bar{k})$ is free and transitive. If G/k is smooth, X/k is a torsor in the étale topology, and will be trivialised over k^{sep} already.

The link between twists, torsors and cohomology is given by:

Theorem 3.8. *Let X/S be an algebraic space, and $G = \text{Aut}_S(X)$. Then twists of X/S in the τ-topology correspond bijectively to G-torsors in the τ-topology, whose isomorphism classes are classified by $H^1_\tau(S, G)$.*

Proof. We will only need the second assertion, which is proven in [Stacks, Tag 03AG].

Note that in the category of G-spaces, $\text{Aut}_S(G) = G$, so the first assertion of Theorem 3.8 applied to G-torsors become the tautological statement that a G-torsor is a twist of G (by definition) is a G-torsor (by Theorem 3.8).

To show the first assertion, it thus suffices to show that twists of X/S are classified by $H^1_\tau(S, G)$ (in particular this also proves the second statement). Given a twist Y/S and a cover $U = \bigcup U_i \to S$ in the τ-topology where Y is locally isomorphic to X over each U_i, then these isomorphisms need not coincide on $U_i \cap U_j$ but they differ by an element $g_{ij} \in G = \text{Aut}_S(X)$. The g_{ij} define a cocycle on the Cech cohomology group $\check{H}^1(U, S)$, and conversely a cocycle define a twist of Y locally isomorphic to X on the U_i. We conclude by the Cech to derived spectral sequence [Stacks, Tag 03OW], which shows that the Cech cohomology on X gives sheaf cohomology for $i = 0, 1$ [AGV72, V Corollaire 3.4; Fu11, Corollary 5.6.3]. □

Example 3.9.

- For an elliptic curve E/k with $\text{Aut}_k(E) = \mu_2 = \pm 1$, we recover the fact that twists of E are given by μ_2-torsors, i.e., quadratic twists.
- If E/S is an elliptic curve, then E-torsors corresponds to twists of E in the category of E-spaces[6] rather than in the category of elliptic curves. In the former category, as seen in the proof of Theorem 3.8, $\text{Aut}_S(E) = E$. The group $H^1(S, E)$, classifying E-torsors, is also called the Weil-Chatelet group. When $S = \text{Spec}\, K$ is a number field, we also have the closely related Selmer and Tate-Shafarevich groups.
- Since a line bundle is a twist of $\mathbb{A}^1$ whose automorphism group is $\mathbb{G}_m$ we get that $\text{Pic}(S) = H^1_{\text{Zariski}}(S, \mathbb{G}_m)$. By Hilbert 90, $H^1_{\text{Zariski}}(S, \mathbb{G}_m) = H^1_{\text{etale}}(S, \mathbb{G}_m) = H^1_{\text{fppf}}(S, \mathbb{G}_m)$: a twist of $\mathbb{A}^1$ for the fppf topology is in fact a line bundle, i.e., a twist for the Zariski topology.
- The same is true for vector bundles: a vector bundle of rank d is a twist of $\mathbb{A}^d$, so a Gl_d-torsor. Since Gl_d is a special group in the terminology of Serre-Grothendieck, Gl_d-torsors for the fppf topology are already torsors for the Zariski topology [Gro71, IX Proposition 5.1], so a vector bundle of rank d for the fppf topology is already a vector bundle in the Zariski topology.

[6] These will be schemes if $S = \text{Spec}\, k$ is a field by Remark 3.4.

- A Severi-Brauer variety X/k is a twist of $\mathbb{P}^{n-1}/k$. Since $\mathrm{Aut}_k(\mathbb{P}^{n-1}) = \mathrm{PGL}_n(k)$, they are classified by $H^1_\tau(k, \mathrm{PGL}_n(k))$.
- A central simple algebra of rank n^2 is a twist of $M_n(k)$. Since $\mathrm{Aut}_k(M_n(k)) = \mathrm{PGL}_n(k)$, they are also classified by $H^1_\tau(k, \mathrm{PGL}_n(k))$.

Remark 3.10 (Galois cohomology)**.** Let S be a connected scheme and $\bar{s} \in S$ a geometric point. Then Galois theory [Gro71] provides an equivalence between LCC (locally constant constructible) étale sheaves, finite étale covers and $\pi^1_{\text{etale}}(S, \bar{s})$-finite sets [Stacks, Tag oDV4], where $\pi^1_{\text{etale}}(S, \bar{s})$ is the étale fundamental group. For an LCC étale sheaf F, there is a natural map $H^i(\pi^1_{\text{etale}}(S, \bar{s}), F) \to H^i_{\text{etale}}(S, F)$ which is an isomorphism for $i = 0, 1$ [AGV72, §VII.2; Fu11, Proposition 5.7.20][7] ($i = 0$ is Galois theory, and for $i = 1$ this also follows from Theorem 3.8). If $S = \operatorname{Spec} k$ is a field, and $\bar{s}$ corresponds to $k \to \bar{k}$, the étale fundamental group is the Galois group $\mathrm{Gal}(\bar{k}/k)$ and the above map is an isomorphism for all i (k is an algebraic $K(\pi, 1)$-space): étale cohomology is simply Galois cohomology [Stacks, Tag 03QQ].

Remark 3.11 (Twists and Galois action)**.** If X'/S is a twist of an object X/S (in the étale topology), and $T \to S$ is a Galois finite étale cover where X' and X become isomorphic, then the Galois action on $X'(T)$ is a twist of the Galois action on $X(T)$ by the cocycle in $H^1(\pi^1_{\text{etale}}(S, \bar{s}), \mathrm{Aut}_S(X)) = H^1(S, \mathrm{Aut}_S(X))$ representing X' by Theorem 3.8.

3.2. **Torsors and cohomology.** So torsors give a geometric interpretation of the first cohomology group. We will use this to describe the first maps in the long exact sequence of cohomology. We drop the τ in our notations, for now we do not need to assume anything on the topology τ.

Given an exact sequence of fppf *commutative* group spaces over S:

$$0 \to K \xrightarrow{i} G \xrightarrow{\alpha} H \to 0 \tag{1}$$

seen as abelian sheaves, the long exact sequence of cohomology is given by

$$0 \to H^0(S, K) \to H^0(S, G) \to H^0(S, H) \to H^1(S, K) \to H^1(S, G) \to H^1(S, H) \to H^2(S, K) \to \dots \tag{2}$$

If $f : S' \to S$ is a morphism, the preimage functor f^{-1} is exact (it induces a geometric morphism of topoi $\mathrm{Sh}_\tau(S') \to \mathrm{Sh}_\tau(S)$), hence the long exact sequence commutes with the base change to S' (see also [GD64, p. III.0.12.1.6]).

Definition 3.12 (Pushforward/Change of structure group of torsors)**.** If $\alpha : G \to H$ is a group morphism (all our morphisms and maps will be above the base scheme S), then to a G-torsor X one can associate a H torsor $Y = \alpha_* X = X \times_G H := (X \times H)/G$, where G acts on $X \times H$ on T-points via: $g \cdot (x, h) = (g.x, h\alpha(g)^{-1})$ and H acts on itself. Hence α_* gives a pushforward map $H^1(S, G) \to H^1(S, H)$.

Lemma 3.13. *The maps $H^1(S, K) \to H^1(S, G) \to H^1(S, H)$ are given by the pushforwards i_* and α_* respectively.*

Proof. This is essentially an unraveling of Theorem 3.8 and the definitions. If X/S is a G-torsor which is trivial over each U_i, where $U = \bigcup U_i \to S$ is a cover, then $\alpha_*(X)$ is a H-torsor which is trivial over each U_i. Furthermore let g_{ij} be the cocycle data on the $U_i \cap U_j$ associated to X, then $\alpha(g_{ij})$ is the cocycle data associate to $\alpha_*(G)$, which is what we wanted. □

[7] These references give the case of a constant sheaf F, but the general case of an LCC sheaf reduces to this case via the Hochschild-Serre spectral sequence [Mil16, Theorem III.2.20].

Remark 3.14 (Quotient)**.** In the situation of Equation (1), then $G \to H$ is a K-torsor above S. If $X \to Y$ is a G-torsor, the pushforward map $X \to \alpha_* X$ can be interpreted as a quotient $X \to X/K$ by Lemma 3.19 below, and $X \to Y$ factorizes as $X \to X/K \to Y$ where $X \to X/K$ is a K-torsor and $X/K \to Y$ a H-torsor.

Definition 3.15 (Preimage/Fiber)**.** Let $\alpha : G \to H$ be a group morphism. Let $P \in H^0(S,H) = H(S)$ be a point, it represents a section $P : S \to H$ of $H \to S$. To this section P one can associate the pullback of P by α: $\alpha^* P : \alpha^{-1}(P) \to G$. The space $\alpha^{-1}(P)$ is called the preimage or fiber of P by α, and it is a $\mathrm{Ker}\,\alpha$-torsor.

Lemma 3.16. *The map $H^0(S,H) \to H^1(S,K)$ is given by $P \in H(S) \mapsto \alpha^{-1}(P)$.*

Proof. Again, this is an unraveling of the definitions. Since $0 \to K \to G \to H \to 0$ is an exact sequence in the category of sheaves for the τ-topology, $\alpha^{-1}(P)$ admits a section over a τ-cover U of S. Since it is clearly a K-principal homogeneous space (we can check this locally), it is a K-torsor, which as mentioned is trivial over U. It is then an exercise to check that the corresponding cocycle is the one given by the connecting morphism $H^0(S,H) \to H^1(S,K)$. □

Remark 3.17 (Gerbes)**.** The map $H^1(S,H) \to H^2(S,K)$ is described similarly. The second cohomology group classify K-gerbes. To a H-torsor Y, one associate the category $\alpha^{-1}Y$ of all G-torsors X such that $\alpha_* X = Y$. This category is a K-gerbe over S (τ-locally on S this category is isomorphic to the category of K-torsors), hence an element of $H^2(S,K)$.

3.3. **Properties of the pushforward map.** We will need various elementary properties of the pushforward map defined in Definition 3.12.

Definition 3.18. Let $\alpha : G \to H$ be a morphism, X/S a G-torsor and Y/S a H-torsor. Via α, Y can be seen as a G-space. A morphism $f : X \to Y$ (of (G,H)-torsors) relative to/above α is a morphism of G-spaces $f : X \to Y$, i.e., a morphism which is compatible with the action on T-points: $f(g.x) = \alpha(g).f(x)$. If α is an isomorphism, the morphism f is automatically an isomorphism too (because it is locally an isomorphism).

If $\alpha = \mathrm{Id}$, then $f : X \to Y$ is simply a morphism of G-torsors, in which case it is automatically an isomorphism.

Our basic tool for checking various isomorphisms will be given by:

Lemma 3.19. *If $\alpha : G \to H$ is a morphism, there is a natural map $f : X \to \alpha_* X$ of (G,H)-torsors above α.*

Conversely, if X is a G torsor, Y a H torsor, and $\alpha : G \to H$ a morphism, then if $f : X \to Y$ is a morphism above α, it induces an isomorphism $\alpha_*(X) \to Y$. More precisely, we have a bijection between maps $f : X \to Y$ above α and isomorphisms $\alpha_* X \to Y$.

Proof. The neutral section $0 \to H$ induces a map $X = X \times 0 \to X \times H$ compatible with the action of G, and composing with $X \times H \to (X \times H)/G$ we get a map $X \to \alpha_* X$.

Conversely, given $f : X \to Y$, we have a map $X \times H \to Y$ given on points by $(x,h) \mapsto h.f(x)$, and the compatibility of f with the action shows that the action of G on $X \times H$ factor through this map. Hence this map descends to a morphism of H-torsor $\alpha_* X \to Y$, which as we have seen is automatically an isomorphism. □

Lemma 3.20. *The pushforward is functorial, commutes with base change, direct sums, and sends the trivial G-torsor to the trivial H-torsor. If X is a G-torsor, then $X \times X = \Delta_* X$ is the $G \times G$-torsor induced by the pushforward of the diagonal map $\Delta : G \to G \times G$.*

Proof. Let $\alpha_1 : G_1 \to G_2$, $\alpha_2 : G_2 \to G_3$ are two morphisms and X a G-torsor. Then α_2 induces a map $X \times G_2 \to X \times G_3$ and this map commutes with the action of G_1 induced by α_1 and $\alpha = \alpha_2 \circ \alpha_1$, hence we get a map $\alpha_{1,*}X \to \alpha_* X$. Then by Lemma 3.19, $\alpha_{2,*}\alpha_{1,*}X \simeq \alpha_* X$. Commutativity with base change is similar.

If $\alpha_1 : G_1 \to H_1$, $\alpha_2 : G_2 \to H_2$ are two morphisms and X_1 is a G_1-torsor, X_2 a G_2-torsor, then $X_1 \times X_2$ is a $G_1 \times G_2$-torsor, and the maps $X_1 \to \alpha_{1,*}X_1$ above α_1, $X_2 \to \alpha_{2,*}X_2$ above α_2 induce a map $X_1 \times X_2 \to \alpha_{1,*}X_1 \times \alpha_{2,*}X_2$ above $\alpha_1 \times \alpha_2$, hence $(\alpha_1 \times \alpha_2)_*(X_1 \times X_2) \simeq \alpha_{1,*}X_1 \times \alpha_{2,*}X_2$ by Lemma 3.19.

Finally, the map $\alpha : G \to H$ above itself shows that $\alpha_* G \simeq H$ still by Lemma 3.19, and the diagonal map $X \to X \times X$ above the diagonal map $G \to G \times G$ shows that $\Delta_* X \simeq X \times X$. □

Lemma 3.21. *If we have a commutative diagram of morphisms*

$$\begin{array}{ccc} G_1 & \xrightarrow{\alpha_1} & H_1 \\ \downarrow{\scriptstyle \beta_1} & & \downarrow{\scriptstyle \beta_2} \\ G_2 & \xrightarrow{\alpha_2} & H_2 \end{array}$$

and $f : X_1 \to X_2$ a morphism of (G_1, G_2)-torsors above β_1, then f induces a morphism $g : \alpha_{1,*}X_1 \to \alpha_{2,*}X_2$ of (H_1, H_2)-torsors above β_2.

Proof. From $f : X_1 \to X_2$ we get a morphism $X_1 \times H_1 \to X_2 \times H_2 \to (X_2 \times H_2)/G_2 = \alpha_{2,*}X_2$, and the commutativity of the diagram shows that the action of G_1 on $X_1 \times H_1$ factorizes through this map.

Notice that Lemma 3.19 above is a special case of this with $G_1 = G, G_2 = H_1 = H_2 = H$. Conversely, Lemma 3.21 could be directly deduced from Lemma 3.19 and the isomorphism $\alpha_{2,*}X_2 \simeq \alpha_{2,*}\beta_{1,*}X_1 \simeq \beta_{2,*}\alpha_{1,*}X_1$ given by functoriality. □

Lemma 3.22. *Let $f_1 : G_1 \to G_2$, $f_2 : G_2 \to G_3$ be morphisms. Then if $P_3 \in G_3(S)$, $f_{1,*}(f_2 \circ f_1)^{-1}(P_3) = f_2^{-1}(P_3)$.*

And if $P_2 \in G_2(S)$, and $i : \mathrm{Ker} f_1 \to \mathrm{Ker} f_2 \circ f_1$ is the inclusion, then $i_* f_1^{-1}(P_2) = (f_2 \circ f_1)^{-1}(f_2(P_2))$.

Proof. For the first statement, apply Lemma 3.19 to the natural morphism $(f_2 \circ f_1)^{-1}(P_2) \to f_2^{-1}(P)$ induced by f_1 and above $f_1 : \mathrm{Ker}(f_2 \circ f_1) \to \mathrm{Ker} f_2$.

For the second statement, we have an inclusion in $G_1, f_1^{-1}(P_2) \to (f_2 \circ f_1)^{-1}(f_2(P_2))$ over i and we also conclude by Lemma 3.19. □

3.4. **The group structure on torsors.** By the abstract theory of cohomology, the maps in Equation (2) are group morphisms. For Section 4, we need to describe the group structure on cohomology in order to define the bilinearity of the Tate pairing. We explain the form this group structure takes on torsors.

Definition 3.23 (Group structure)**.** The canonical map $q : G \times G \to G$ induces a group structure on $H^1(S, G)$ via $H^1(S, G) \times H^1(S, G) \to H^1(S, G \times G) \to H^1(S, G)$, $(X_1, X_2) \mapsto X_1 \star X_2$.

By Definition 3.12 and Lemma 3.13, the group structure is explicitly given as follow: if X_1/S and X_2/S are two G-torsors, then $X_1 \times X_2$ is a $G \times G$-torsor, and $X_1 \star X_2$ is given by $q_*(X_1 \times X_2)$. In summary: $(X_1 \star X_2)/S$ is given by $(X_1 \times X_2 \times G)/(G \times G)$ where the action is given on T-points by $(g_1, g_2).(x_1, x_2, g) = (g_1.x_1, g_2.x_2, g g_1^{-1} g_2^{-1})$.

The neutral point is the trivial torsor, and the inverse of X is the torsor $\mathrm{Hom}(X, G)$.

Remark 3.24. It is elementary to check that G is the neutral point for the group structure on $H^1(S,G)$. It is also easy to check that $\mathrm{Hom}(X,G)$ is a G-torsor, and the evaluation map $X \times \mathrm{Hom}(X,G) \to G$ shows that $X \star \mathrm{Hom}(X,G) \simeq G$ by Lemma 3.27.

Note however that this is an isomorphism, not an equality. Likewise, associativity only holds up to isomorphism. There is probably something clever to say about ∞-categories here to keep track of the coherence conditions, but by lack of familiarity on this subject we will contend ourselves to work up to isomorphisms. Still, we will try to be careful to keep track of our isomorphisms, this will be useful for formulas in Section 5.

This group structure behaves as expected:

Lemma 3.25. *Let $\alpha : G \to H$ be a group morphism, then $\alpha_* : H^1(S,G) \to H^1(S,H)$ is a group morphism. Namely, given X_1, X_2 two G-torsors, $\alpha_*(X_1 \star X_2) = (\alpha_* X_1) \star (\alpha_* X_2)$.*

Proof. Both are equal to the pushforward of $X_1 \times X_2$ through $G \times G \to H$, which can be written as $G \times G \to H \times H \to H$ or as $G \times G \to G \to H$. □

Lemma 3.26. *Let $\alpha : G \to H$ be a group morphism, $f_1 : X_1 \to Y_1$ and $f_2 : X_2 \to Y_2$ two morphisms above α. Then we have a morphism $f_1 \star f_2 : X_1 \star X_2 \to Y_1 \star Y_2$ above α.*

Proof. Apply Lemma 3.21 to the diagram

$$\begin{array}{ccc} G \times G & \longrightarrow & H \times H \\ \downarrow & & \downarrow \\ G & \longrightarrow & H \end{array}$$

□

Lemma 3.27. *Let X_1, X_2, X be G-torsors and $f : X_1 \times X_2 \to X$ a morphism above $G \times G \to G$. Then f induces an isomorphism $X_1 \star X_2 \to X$.*

Proof. This is a special case of Lemma 3.19. □

Lemma 3.28. *Let $\alpha : G \to H$ be a group morphism with kernel K, $P_1, P_2 \in H(S)$. Then $\alpha^{-1}(P_1 + P_2) \simeq \alpha^{-1}(P_1) \star \alpha^{-1}(P_2)$.*

Proof. Addition gives a morphism $\alpha^{-1}P_1 \times \alpha^{-1}P_2 \to \alpha^{-1}(P_1 + P_2)$ above $\mathrm{Ker}\,\alpha \times \mathrm{Ker}\,\alpha \to \ker \alpha$, so we can apply Lemma 3.27. □

Lemma 3.29. *Let $\alpha_1, \alpha_2 : G \to H$ be two group morphisms, and $\alpha = \alpha_1 + \alpha_2$. Let X/S be a G-torsor. Then $\alpha_* X = \alpha_{1,*} X \star \alpha_{2,*} X$.*

Proof. The map α factorizes through $G \to G \times G \to H \times H \to H$ where the first map is the diagonal, the second map is given by (α_1, α_2), and the last map is the canonical map given by the group structure. So the pushforward of X by α along this decomposition is as follow by Lemma 3.20: first we get $X \times X$ as a $G \times G$ torsor, then $\alpha_{1,*} X \times \alpha_{2,*} X$ as a $H \times H$ torsor, then $\alpha_{1,*} X \star \alpha_{2,*} X$ as a H-tosor. □

Lemma 3.30. *If X/G is a G-torsor, and $X^{\star,d}$ is the torsor induced by the multiplication by d via the group structure on $H^1(S,G)$, and $[d] : G \to G$ is the morphism of multiplication by d on G, then $X^{\star,d} = [d]_* X$.*

If $0 \to K \to G \xrightarrow{\alpha} H \to 0$ is an exact sequence and $P \in H(S)$, then $[d]_* \alpha^{-1}(P) = \alpha^{-1}(dP)$.

Proof. The first statement is a consequence of Lemma 3.29, and the second of Lemma 3.28. We can also apply Lemma 3.19 to the multiplication by $[d]$ map on G which induces a map $\alpha^{-1}(P) \to \alpha^{-1}(dP)$ over $\operatorname{Ker}\alpha \xrightarrow{[d]} \operatorname{Ker}\alpha$. □

3.5. **μ_n-torsors.** We conclude this section by the description of μ_n-torsors over S. From now on, we assume that n is invertible on S, and τ will be the étale topology. This is merely for convenience, because in this case μ_n will be étale over S rather than just fppf, hence we can work with étale torsors.

Lemma 3.31. *$H^1(S, \mu_n)$ is in bijection with the isomorphism classes of the pairs (L, α) where $L \in \operatorname{Pic}(S)$ is an invertible bundle and $\alpha : L^n \to O_S$ an isomorphism, i.e., a trivialisation of L^n.*

Proof. The Kummer sequence $1 \to \mu_n \to \mathbb{G}_m \to \mathbb{G}_m \to 1$ induced by $x \mapsto x^n$ is exact in the étale topology. (This is also why we need n invertible. In general this sequence is always exact in the fppf topology.) It induces the sequence

$$1 \to H^0(S, \mu_n) \to H^0(S, \mathbb{G}_m) \to H^0(S, \mathbb{G}_m) \to H^1(S, \mu_n) \to H^1(S, \mathbb{G}_m) \to H^1(S, \mathbb{G}_m)$$

thus we get a map $H^0(S, \mathbb{G}_m) \to H^1(S, \mu_n) \to \operatorname{Pic}(S)[n]$ by Example 3.9. From this map we obtain the bijection stated in the Lemma by unraveling the definitions, see [Stacks, Tag 040Q]. □

Example 3.32 (μ_n-torsors over a field)**.** If $S = \operatorname{Spec} k$ is a field (of characteristic prime to n), then $\operatorname{Pic}(S)$ is trivial, and we obtain that $H^1(k, \mu_n) \simeq H^1(\operatorname{Gal}(\bar{k}/k), \mu_n) \simeq k^*/k^{*,n}$: any μ_n-torsor over k is isomorphic to the torsor $x^n = \xi$ for a ξ in k^*. The link with Lemma 3.31 is as follows: to an isomorphism (of k-vector spaces) $\alpha : k \to k$ corresponds the torsor $x^n = \xi := \alpha(1)$.

So given a μ_n-torsor X/k we have two representatives. The element $\xi \in k^*/k^{*,n}$ given by the second isomorphism gives an explicit equation (i.e., an isomorphism) with the torsor $x^n = \xi$. And the cocycle $\Xi \in H^1(G, \mu_n)$ given by the first isomorphism (see Remark 3.10) gives the Galois action of $G = \operatorname{Gal}(\bar{k}/k)$ on X (e.g., by twisting the natural Galois action of G on μ_n by Ξ). If two torsors X_1, X_2 are represented by $\xi_1, \xi_2 \in k^*/k^{*,n}$, then $X_1 \star X_2$ is represented by $\xi_1\xi_2$, indeed $(x_1^n = \xi_1) \times (x_2^n = \xi_2) \to (x^n = \xi_1\xi_2)$, $(x_1, x_2) \mapsto x_1x_2$ is a morphism above the product $\mu_n \times \mu_n \to \mu_n$ so we may apply Lemma 3.19.

In particular, X corresponds to a twisted Galois structure on μ_n, hence by Galois theory to a field extension k'/k. We recover Kummer theory (in the more general case where we don't assume $\mu_n \subset k^*$).

Example 3.33 (μ_n-torsors over an elliptic curve)**.** Let E/k be an elliptic curve (as always we assume n invertible on k). By Lemma 3.31, a μ_n-torsor X is given by an element $\mathcal{L}$ of n-torsion in the Picard group of E, and an isomorphism $O_E \to \mathcal{L}^n$. Via the canonical identification $R \mapsto (R) - (0_E)$ of E with $\operatorname{Pic}^0(E)$ (the torsion elements of $\operatorname{Pic}(E)$ are of degree 0), the line bundle $\mathcal{L}$ corresponds to a point $P \in E[n](k)$ of n-torsion. To fix an isomorphism of O_E with $\mathcal{L}^n$ then corresponds to a choice of rational function $f_{n,P}$ with divisor $n(P) - n(0_E)$. The μ_n torsor X may informally be interpreted as $f_{n,P}^{1/n}$.

The map $[n] : E \to E$ is a finite étale cover, and $f_{n,P} \circ [n]$ has for divisor $n \sum_{T \in E[n]} ((P_1 + T) - (T))$ for any P_1 such that $P = nP_1$. The divisor $\sum_{T \in E[n]} ((P_1 + T) - (T))$ is principal and rational, we let $g_{n,P}$ be a rational function representing it. Since $g_{n,P}^n$ and $f_{n,P} \circ [n]$ have the same divisors, they differ by a constant c . Let $k' = k(c^{1/n})$, this is an étale extension of k. It follows that $c^{1/n} g_{n,P}$ gives a trivialisation of our μ_n-torsor over the étale cover $[n] : E_{k'} \to E$.

This example explains why the functions $f_{n,P}$ and $g_{n,P}$ naturally appear in the algorithmic computation of the Tate pairing, see Section 4.4.

4. The Tate pairing over a scheme

Following the seminal work [FR94; FMR99] introducing the Tate pairing in cryptography in the context of Jacobians of curves over a finite field for the isogeny of multiplication by $[n]$, most texts restrict to this context.

An exception is [Bru11] which proves the general case of non degeneracy of the Tate-Cartier pairing associated to a separable isogeny of abelian varieties over a finite field. However, Bruin only gives formulas for the Tate pairing for Jacobians over a finite field. In [LR15], we gave formulas for the Tate pairing for general abelian varieties over a finite field in the theta model.

In this section, we give a general definition of the Tate pairing related to an isogeny over a base scheme. Then we specialize to a field and show that the usual formulas still work for abelian varieties when appropriately adjusted, see Equation (13). Finally we recover the usual standard results when specializing further to finite fields.

4.1. The Weil pairing.

Let A/S be a principally polarised abelian scheme.

We first need the Weil-Cartier pairing (see [EGM12, Chapter XI]):

Theorem 4.1. *If $f : A \to B$ is an isogeny, the Cartier-Weil pairing $e_{W,f}$ is a non-degenerate pairing* $\mathrm{Ker} f \times \mathrm{Ker} \hat{f} \to \mathbb{G}_m$.

Proof. Recall that as an fppf sheaf, $\widehat{A}$ is isomorphic to $\mathrm{Ext}^1(A, \mathbb{G}_m)$. For instance an explicit isomorphism is given by $\mathcal{L} \in \mathrm{Pic}^0(A) \mapsto G(\mathcal{L})$ where $G(\mathcal{L})$ is the theta group; it is an extension of A by $\mathbb{G}_m$ when $\mathcal{L}$ is algebraically trivial because its associated polarisation is 0.

Then the exact sequence $0 \to \mathrm{Ker} f \to A \to B \to 0$ induces $0 \to \mathrm{Hom}(B, \mathbb{G}_m) \to \mathrm{Hom}(A, \mathbb{G}_m) \to \mathrm{Hom}(f, \mathbb{G}_m) \to \mathrm{Ext}^1(B, \mathbb{G}_m) \to \mathrm{Ext}^1(A, \mathbb{G}_m) \to \mathrm{Ext}^1(\mathrm{Ker} f, \mathbb{G}_m)$. Now $\mathrm{Hom}(A, \mathbb{G}_m) = 0$ since $\mathbb{G}_m$ is affine and A is proper, we have seen that we can identify $\mathrm{Ext}^1(A, \mathbb{G}_m)$ with $\widehat{A}$, and $\mathrm{Ext}^1(\mathrm{Ker} f, \mathbb{G}_m) = 0$ because $\mathrm{Ker} f$ is finite. So we get $0 \to \mathrm{Hom}(K, \mathbb{G}_m) \to \hat{B} \to \widehat{A} \to 0$ and it is an exercise to check that the map $\hat{B} \to \widehat{A}$ corresponds to $\hat{f}$. So $\mathrm{Ker} \hat{f} \simeq \mathrm{Hom}(K, \mathbb{G}_m)$, and the Weil pairing corresponds to Cartier duality. See also [EGM12, § 7.2] for a sleek direct proof. □

If $\mathrm{Ker} f$ is of exponent n (in particular if f is an n-isogeny), the Weil-Cartier pairing lends in μ_n. We will assume from now that all our isogenies have kernel of exponent dividing n, and recall that we also assume that n is invertible on S.

There are many different variants and interpretations of the Weil pairing, see [Rob21b, § 4.1.1] for an overview. The Weil pairing is invariant by base change and commutes with the Galois action (i.e., the action of the étale fundamental group). The compatibility of the Weil pairing with isogenies is given by [EGM12, Proposition 11.21]:

$$e_{W,h\circ g\circ f}(P, Q) = e_{W,g}(f(P), \hat{h}(Q)) \tag{3}$$

for any $P \in f^{-1} \mathrm{Ker}\, g$ and $Q \in \hat{h}^{-1} \mathrm{Ker}\, \hat{g}$. And by biduality [EGM12, Proposition 11.17],

$$e_{W,f}(P, Q) = e_{W,\hat{f}}(Q, P)^{-1}. \tag{4}$$

4.2. **The Tate pairing.** We let $f : A \to B$ be an isogeny as in Section 4.1, and let $K = \mathrm{Ker} f$. From the exact sequence $0 \to K \to A \to B \to 0$ we get a long exact sequence as in Equation (2):

$$0 \to H^0(S,K) \to H^0(S,A) \to H^0(S,B) \to H^1(S,K) \to H^1(S,A) \to H^1(S,B).$$

In particular we obtain a map $H^0(S,B) \to H^1(S,K)$. This map is described as follows (see Section 3): to an S-point $P : S \to B$ we associate the K-torsor $f^{-1}(P)$. Now if we are also given a S-point $Q : S \to \mathrm{Ker}\hat{f}$ of order $m \mid n$, the Weil pairing applied to Q gives a map $\phi_Q : \mathrm{Ker} f \to \mu_m$. We can pushforward our torsor $f^{-1}(P)$ through this map.

Definition 4.2. Let $f : A \to B$ be an isogeny of exponent n, $P \in B(S)$ and $Q \in \mathrm{Ker}\hat{f}(S)$ a point of order $m \mid n$. The Tate pairing $e_{T,f}(P,Q)$ is the μ_m-torsor over S given by $\phi_{Q,*}(f^{-1}(P))$ where $\phi_Q : \mathrm{Ker} f \to \mu_m \subset \mu_n = e_{W,f}(\cdot, Q)$.

Remark 4.3 (Order)**.** Of course, since Q is also of order n, we also get a version of $e_{T,f}(P,Q)$ as a μ_n-torsor. It is simply given by the image of $e_{T,f}(P,Q)$ via $i_* : H^1(S,\mu_m) \to H^1(S,\mu_n)$ where $i : \mu_m \to \mu_n$ is the inclusion.

Note however that although i is injective, this is not the case in general for the pushforward map $i_* : H^1(S,\mu_m) \to H^1(S,\mu_n)$. So seeing all our pairings in $H^1(S,\mu_n)$ lose information! This is why we were careful to define our pairing in the correct cohomology group. We will see this situation again when we study bilinearity (see Remark 4.5) and non degeneracy over a finite field (see Theorem 4.22).

If $S = \mathrm{Spec}\,\mathbb{F}_q$ is a finite field, then $H^1(S,\mu_m) \to H^1(S,\mu_n)$ is injective whenever $\mu_n \subset \mathbb{F}_q$. But in this paper we want to investigate the general case of the Tate pairing when only a subgroup of μ_n is rational. In this situation, our refined definition will be useful.

Proposition 4.4. *The Tate pairing is bilinear.*

Proof. Let $P \in B(S)$, $Q_1, Q_2 \in \mathrm{Ker}\hat{f}(S)$, with Q_1, Q_2 of n-torsion. Then by bilinearity of the Weil pairing, $e_{W,f}(\cdot, Q) : \mathrm{Ker} f \to \mu_n = e_{W,f}(\cdot, Q_1) e_{W,f}(\cdot, Q_2)$, so by Lemma 3.29, $e_{T,f}(P,Q) = e_{T,f}(P,Q_1) \star e_{T,f}(P,Q_2)$.

Let $P_1, P_2 \in B(S)$, $Q \in \mathrm{Ker}\hat{f}(S)$, with Q of n-torsion, $\phi_Q = e_{W,f}(\cdot, Q)$. Then $e_{T,f}(P_1 + P_2, Q) = \phi_{Q,*}(f^{-1}(P_1 + P_2)) = \phi_{Q,*}(f^{-1}(P_1) \star f^{-1}(P_2)) = \phi_{Q,*}(f^{-1}(P_1)) \star \phi_{Q,*}(f^{-1}(P_2)) = e_{T,f}(P_1) \star e_{T,f}(P_2)$ by Lemmas 3.25 and 3.28. □

Remark 4.5 (Bilinearity)**.** Let Q_1 be a point of order n_1 and $Q_2 = dQ_1$ where $n_1 = dn_2$. We have a map $\mu_{n_1} \to \mu_{n_2}$ given by $\zeta \mapsto \zeta^d$. By bilinearity of the Weil pairing, the map $\phi_{Q_2} : \mathrm{Ker} f \to \mu_{n_2}$ is exactly given by the composition of $\phi_{Q_1} : \mathrm{Ker} f \to \mu_{n_1}$ with this map. From the definition and the functoriality of the pushforward, we get that $e_{T,f}(P,Q_2) \in H^1(\mathbb{F}_q, \mu_{n_2})$ is the pushforward of $e_{T,f}(P,Q_1) \in H^1(\mathbb{F}_q, \mu_{n_1})$ along this projection $\mu_{n_1} \to \mu_{n_2}$.

This gives a refined version of Proposition 4.4. Indeed, we can also consider the map $\zeta \mapsto \zeta^d$ as an application $\mu_{n_1} \to \mu_{n_1}$, this is the composition of the exponentiation $\mu_{n_1} \to \mu_{n_2}$ above with the canonical inclusion $\mu_{n_2} \subset \mu_{n_1}$. As above, we obtain that $e_{T,f}(P,Q_2) \in H^1(\mathbb{F}_q, \mu_{n_1})$ is the pushforward by this "multiplication by d" of $e_{T,f}(P,Q_1)$. This is the standard version of bilinearity (on the right) of the Tate pairing, as recovered by applying Proposition 4.4. But by Remark 4.3 this second version loose information! (Note also that although the projection map $\mu_{n_1} \to \mu_{n_2}$ is surjective, it need not stay surjective on $H^1(S,\mu_{n_1}) \to H^1(S,\mu_{n_2})$. This will be the case however if S is of cohomological dimension ≤ 1, e.g., $S = \mathrm{Spec}\,\mathbb{F}_q$.)

One should be careful that this refined version does not work for bilinearity on the left. Let $n_1 = dn_2$ and Q a point of order n_1. Let $P_2 = dP_1$. Then a priori $e_{T,f}(P_2, Q)$ lives in $H^1(S, \mu_{n_1})$. Of course, by bilinearity, this is also $e_{T,f}(P_1, dQ)$, which we have seen has a natural interpretation in $H^1(S, \mu_{n_2})$. Explicitly, multiplication by d induces an isomorphism $f^{-1}(P_2) = [d]_* f^{-1}(P_1)$ by Lemma 3.30. By bilinearity of the Weil pairing, this induces our isomorphism $e_{T,f}(P_2, Q) = e_{T,f}(P_1, dQ) \in H^1(S, \mu_{n_1})$. However, $e_{T,f}(P_2, Q)$ has no natural interpretation in $H^1(S, \mu_{n_2})$.

The compatibility of the Tate pairing with isogenies is given by:

Proposition 4.6. *Let $f : A \to B, g : B \to C, h : C \to D$ be isogenies over S, $P \in C(S)$ and $Q \in \operatorname{Ker} \widehat{h \circ g}(S)$ of order n. Then*

$$e_{T,h\circ g\circ f}(h(P), Q) = e_{T,g}(P, \hat{h}(Q)) \in H^1(S, \mu_n).$$

Proof. This is a nice exercise using Equation (3) and the definitions. We can treat h and f separately.

The isogeny f induces a morphism $\operatorname{Ker} g \circ f \to \operatorname{Ker} g$, and by Equation (3) the map $e_{W,g\circ f}(\cdot, Q) = e_{W,g}(f(\cdot), Q) : \operatorname{Ker} g \circ f \to \mu_n$ factors through this map. And $f_*(g \circ f)^{-1}(P) \simeq g^{-1}(P)$ by Lemma 3.22. So $e_{T,g\circ f}(P, Q) = e_{T,g}(P, Q)$.

We also have the inclusion $i : \operatorname{Ker} g \to \operatorname{Ker} h \circ g$. By Equation (3), the map $e_{W,g}(\cdot, \hat{h}Q) = e_{W,h\circ g}(\cdot, Q) : \operatorname{Ker} g \to \mu_n$ factor through this inclusion. Since $i_* g^{-1}(P) \simeq (h \circ g)^{-1}(h(P))$ by Lemma 3.22, we get that $e_{T,h\circ g}(h(P), Q) = e_{T,g}(P, \hat{h}(Q))$. □

We remark that the same proof works if we do not assume our isogenies to be separable, we just need that Q should be of order n with n invertible. (Or work with fppf torsors rather than étale torsors, see Remark 4.10.)

Corollary 4.7. *Let $\alpha : A \to B$ be a a-isogeny between principally polarised abelian varieties. For $P \in A(S)$ and $Q \in B[n](S)$,*

$$e_{T,n}(\alpha(P), Q) = e_{T,n}(P, \tilde{\alpha}(Q))$$

so in particular, for $P \in A(S)$ and $Q \in A[n](S)$,

$$e_{T,n}(\alpha(P), \alpha(Q)) = e_{T,n}(P, Q)^a.$$

Proof. Since α commutes with n, we have $e_{T,n}(\alpha(P), Q) = e_{T,n\circ\alpha}(\alpha(P), Q) = e_{T,n}(P, \tilde{\alpha}Q)$ by Proposition 4.6 and the second equation follows by bilinearity. □

Remark 4.8 (Base change)**.** The Tate pairing commutes with base change and the Galois action. More precisely, if $S' \to S$ is a map of scheme, and f' the base change of f, P', Q' the base change of P, Q, then $e_{T,f'}(P', Q') = f^* e_{T,f}(P, Q)$ is the base change of $e_{T,f}(P, Q) \in H^1(S, \mu_n)$ via the pullback map $H^1(S, \mu_n) \to H^1(S', \mu_n)$.

As a torsor, this is simply the corresponding torsor over S base changed to S'. As a cocycle (via the isomorphism $H^1(S, \mu_n) \simeq H^1(\pi^1_{\text{etale}}(S, \bar{s}), \mu_n)$), it is simply the cocycle in $H^1(\pi^1_{\text{etale}}(S', \bar{s}'), \mu_n)$ given by composition of the cocycle above and the map $\pi^1_{\text{etale}}(S', \bar{s}') \to \pi^1_{\text{etale}}(S, \bar{s})$ induced by functoriality of étale fundamental groups.

In particular, if $\operatorname{Ker} f$ admits a section over S', then the Tate pairing becomes trivial over S'. This is a fundamental difference between the Weil and Tate pairing, the Weil pairing takes value in μ_n, but the Tate pairing takes value in μ_n-torsors, and two torsors non isomorphic over S may become isomorphic after base change.

Remark 4.9 (Weil's restriction of scalar and trace)**.** If $\pi : S' \to S$ is a map, then we have a pushforward map π_* on étale sheaves [Stacks, Tag 03PV]: if F'/S' is an étale sheaf, $\pi_* F'(V) = F'(V \times_S S')$. For instance, if X'/S' is a scheme seen as an étale sheave, then the pushforward is Weil's restriction of scalar $R_{S'/S}(X')$. It will be represented by an algebraic space if f is proper flat of finite presentation [Ols+06, Theorem 1.5], and by a scheme if $S' \to S$ is finite locally free and X' is AF-finite (e.g., quasi-projective) by [BLR12, Theorem 7.6.4].

If π is a finite morphism, then π_* is exact [Stacks, Tag 03QN], so $H^i(S', F') \simeq H^i(S, F)$. In particular, G'-torsors X'/S' correspond bijectively to $\pi_* G'$-torsors X/S, in fact $X = \pi_* X'$ [DA70, XIV, Proposition 8.4 et Remarques 8.5].

Still for π finite, in the context of a Tate pairing $e_{T,f'}(P', Q')/S'$ associated to an isogeny $f' : A' \to B'$ over S', this means that in particular we can consider its pushforward/Weil restriction to S, to get a $\pi_* \mu_n$-torsor over S. By the isomorphisms above, we get that the Weil restriction commutes with the long exact cohomology sequence, so the end result is the same if we take the Weil restriction of ${f'}^{-1}(P')$ first then map it through the Weil restriction of the morphism $e_{W,f'}(\cdot, Q')$. And the Weil restriction of ${f'}^{-1}(P')$ is also isomorphic to taking the Weil restriction of P' (seen as a morphism $S' \to A'$) and then applying the fiber functor $(\pi_* f')^{-1}$.

Let us now assume that π is finite étale. Then since π is proper, $\pi_* = \pi_!$, and π_* is both a left and right adjoint of π^{-1}. In particular, $\pi_* \pi^{-1}$ is a comonad, hence for any étale sheaf F we have a natural counit $\pi_* \pi^{-1} F \to F$: this is the trace map Tr, see [Stacks, Tag 03SH].

Coming back to the Tate pairing, since μ_n is defined over S, then we can pushforward the $\pi^{-1}\mu_n$-torsor $e_{T,f'}(P', Q')/S'$ through π_* followed by the trace map $\pi_* \pi^{-1} \mu_n \to \mu_n$ to get a μ_n torsor $\mathrm{Tr}_* e_{T,f'}(P', Q')$ over S.

If $f' : A' \to B'$ is the pullback of an isogeny $f : A \to B$ over S, then we can also apply the trace map to transform the $\ker f'$-torsor $(f')^{-1}(P')$ to a $\ker f$-torsor, and by linearity of f we have that $\mathrm{Tr}_* (f')^{-1}(P') = f^{-1}(\mathrm{Tr}\, P')$. If Q' is the pullback of $Q : S \to \ker \hat{f}$, then by bilinearity of the Tate pairing, $\mathrm{Tr}\, e_{T,f'}(P', Q') = e_{T,f}(\mathrm{Tr}\, P', Q)$ as a μ_n-torsor over S. Likewise, if $P' : S' \to A'$ is the pullback of $P : S \to A$, then by bilinearity we have $\mathrm{Tr}\, e_{T,f'}(P', Q') = e_{T,f}(P, \mathrm{Tr}\, Q')$.

Remark 4.10 (The case $n = p$)**.** If $S = \operatorname{Spec} k$ is a field of characteristic p and in the general case when n is not assumed to be prime to p, the Weil pairing still gives an identification between $\ker \hat{f}$ and $(\ker f)^\vee$. So we could still define the Tate pairings as elements of $H^1_{\mathrm{fppf}}(S, \mu_n)$ as in Definition 4.2, i.e., as fppf μ_n-torsors. However, if $S = \operatorname{Spec} k$ is a perfect field, infinitesimal group schemes over k have no non-trivial torsors [Čes15, Lemma 5.7]. So $H^1_{\mathrm{fppf}}(k, \mu_{p^m}) = 1$ and the Tate pairing does not bring any information at the level $p^{v_p(n)}$ part of μ_n.

4.3. **The Weil pairing over a field.** If $S = \operatorname{Spec} k$ is a field, an explicit definition of the Weil pairing is as follows: let $Q \in \ker \hat{f}$, Q corresponds to a divisor D_Q on $\hat{B}$. The pullback of D_Q by f is trivial since Q is in the kernel of the dual isogeny, so $f^* D_Q = \mathrm{Div}(g_{f,Q})$ for some function $g_{f,Q} \in k(A)$. Then if $P \in \ker f$, $\tau_P^* f^* D_Q = f^* D_Q$, so the function $\tau_P^* g_{f,Q}$ has the same divisor as $g_{f,Q}$. They need not be the same but they differ by an invertible constant: this is $e_f(P, Q)$:

$$e_f(P, Q) = g_{f,Q}(x + P)/g_{f,Q}(x). \tag{5}$$

If $\mathcal{L}$ and $\mathcal{M}$ are principal polarisations on A and B and $f : (A, \mathcal{L}) \to (B, \mathcal{M})$ an n-isogeny, then composing the Weil pairing with the polarisation $\Phi_{\mathcal{M}}$ gives the Weil pairing associated

to $\Phi_M \circ f$: $\mathrm{Ker} f \times \mathrm{Ker}\tilde{f} \to \mu_n$. If Θ_A, Θ_B are divisors associated to the polarisations, then to a (0-dimensional) cycle $Z = \sum n_i(P_i)$ on A we can associate the divisor $D_Z = \sum n_i \tau_{P_i}^* \Theta_A$. By the theorem of the square and the definition of the polarisation, the divisor D_Z is principal if $\deg Z = 0$ and $S(Z) := \sum n_i P_i \in \mathrm{Ker}\, \Phi_{\mathcal{L}} = 0$. In this case we let $g_Z = g_{D_Z}$ be an associated function. Given $Q \in \mathrm{Ker}\tilde{f}$ and $P \in \mathrm{Ker} f$, we let Z_Q, Z_P be any cycle equivalent to $(Q) - (0_B)$ and $(P) - (0_A)$ respectively. Then D_{Z_Q} is a divisor representing the point $\Phi_M(Q)$, the divisor $f^* D_{Z_Q}$ is principal and we let g_{f,Z_Q} be a function associated to it. Then Equation (5) becomes

$$e_f(P,Q) = g_{f,Z_Q}(x+P)/g_{f,Z_Q}(x). \tag{6}$$

Now if $f = [n]$ is the multiplication, in the context of elliptic curves and Jacobians it is possible to use Weil's reciprocity to give an alternative definition of the Weil pairing. One can use an extension due to Lang [Lan58] to prove a similar formula for abelian varieties (see also [LR15; Rob21b, § 4.1.2]): if Z_1, Z_2 are principal cycles, then $g_{Z_1}(Z_2) = g_{Z_2}(Z_1)$ provided these values are well defined.

Using Lang's reciprocity, one can show that for $P, Q \in A[n]$, f_{n,Z_Q} a function associated to the cycle nZ_Q and likewise for f_{n,Z_P}, then (up to a sign) [Lan58, Theorem 6]:

$$e_{W,n}(P,Q) = f_{n,Z_Q}(Z_P)/f_{n,Z_P}(Z_Q). \tag{7}$$

Remark 4.11 (Elliptic curves and Jacobians)**.** We recover the usual formula for the Weil pairing on an elliptic curve by taking $Z_P = (P) - (0)$, $Z_Q = (Q) - (0)$. In this case the cycles are already divisors. Let $P, Q \in E[n]$, Q_0 such that $nQ_0 = Q$. Let $g_{n,Q}$ be a function with divisor $\sum_{T \in E[n]} (Q_0 + T) - (T) = [n]^*((Q) - (0_E))$. Let $f_{n,Q}$ be a function with divisor $n(Q) - n(0_E)$. Then the formula above become:

$$e_{W,n}(P,Q) = g_{n,Q}(P+x)/g_{n,Q}(P) = f_{n,Q}((P) - (0_E))/f_{n,P}((Q) - (0_E)). \tag{8}$$

The last definition is used for computations because it is well suited for Miller's double and add algorithm [Mil04]. Notice that $f_{n,Q}$ has a pole at 0_E so cannot be directly evaluated there, but there is a way to make the formula $f_{n,Q}((P) - (0_E))$ make sense (see [Rob21a, Lemma 3.5.3]) and equal to $f_{n,Q}(P)$ if $f_{n,Q}$ is appropriately normalised at infinity.

For Jacobians $J = \mathrm{Jac}(C)$, a function on C induce a function on J. The functions involved in the Weil pairing all come from functions on C, so it is possible to compute the Weil pairing on $P, Q \in J$ by seeing them as divisors on C and evaluating similar functions as in Equation (8) on them. This allows to work entirely on the curve.

At least over Jacobians, it is thus possible to make sense of Equation (7) by using Weil's extended reciprocity theorem, even if the support of Z_P is not disjoint form the support of D_{Z_Q} (and conversely), see [Rob17, § 3.4].

Formula for the Weil pairing on abelian varieties in the theta model are given in [LR10; LR15].

Remark 4.12 (Restricting the Weil pairing to subgroups)**.** Let $A/\mathbb{F}_q$ be a principally polarised abelian variety over a finite field, the Weil pairing $e_{W,n} : A[n] \times A[n] \to \mu_n$ is non degenerate. Assume for simplicity that n is prime. Let P be the characteristic polynomial of π_q on $A[n]$, P_1 an irreducible factor, and $A[n]_{P_1}$ the characteristic subspace associated to P_1. Since π_q is q-symplectic with respect to $e_{W,n}$, if $P_2 = X^{\deg P_1} P_1(q/X)$ is the q-reciprocal polynomial of P_1, then P_2 also divides P and we have another characteristic subspace $A[n]_{P_2}$. (Note that we can have $P_1 = P_2$.)

Let $A'[n] = A[n]_{P_1} + A[n]_{P_2}$. Then the Weil pairing $e_{W,n}$ is non degenerate when restricted to $A[n]_{P_1} \times A[n]_{P_2}$.

Indeed, let us first assume that $P_1 \neq P_2$. Write $P(X) = P_1(X)^e P_2(X)^e R(X)$, with R prime to P_1 and P_2 and q-reciprocal. The subgroup $A[n]_{P_2}$ is the image by $P_1^e(\pi_q)R(\pi_q)$ on $A[n]$. Let $x \in A[n]_{P_1}$, we want to find $y \in A[n]$ such that $e_{W,n}(x, P_1^e(\pi_q)R(\pi_q)(y)) \neq 1$. But $e_{W,n}(x, P_1^e(\pi_q)R(\pi_q)(y)) = e_{W,n}(P_1^e(\widetilde{\pi}_q)R(\widetilde{\pi}_q)(x), y) = e_{W,n}(P_2^e(\pi_q)R(\pi_q)(\pi_q^{-\deg P}x), y)$ where $\widetilde{\pi}_q = q/\pi_q$ and we have used that R is q-reciprocal, and P_2 is the q-reciprocal of P_1. So y exists by non degeneracy of the Weil pairing, since $(P_2^e(\pi_q)R(\pi_q))(\pi_q^{-\deg P_1}x) \neq 0$ as $x \in \operatorname{Ker} P_1^e(\pi_q)$ and P_1 is prime to $P_2^e R$. The same reasoning holds for non degeneracy on the right. A similar proof holds when $P_1 = P_2$.

4.4. **The Tate pairing over a field.** We now unravel Definition 4.2 when $S = \operatorname{Spec} k$ is a field. We have an isogeny $f : A/k \to B/k$ (of exponent n), a point $P \in B(k)$ and a point $Q \in \operatorname{Ker}\hat{f}(k)$. To P we associate the $\operatorname{Ker} f$-torsor $f^{-1}(P)$. Using the Weil pairing with Q, we have a map $\phi_Q = e_{W,n}(\cdot, Q) : \operatorname{Ker} f \to \mu_n$; the Tate pairing $e_{T,f}(P, Q)$ is then the pushforward of $f^{-1}(P)$ by ϕ_Q.

The Tate pairing takes value in $H^1(k, \mu_n)$. By Example 3.32, $H^1(k, \mu_n) \simeq k^*/k^{*,n}$, and by Remark 3.10, $H^1(k, \mu_n) \simeq H^1(G, \mu_n)$ where $G = \operatorname{Gal}(k)$ is the Galois group of k. We explain how to switch between these isomorphisms. If X/k is a μ_n-torsor, it is trivialised over $\overline{k}$ (it has a geometric point!), so $X_{\overline{k}} \simeq \mu_n$. Thus X is the descent of $X_{\overline{k}}$ through $\operatorname{Spec}\overline{k} \to \operatorname{Spec} k$, and this descent is encoded by gluing data on $\operatorname{Spec}\overline{k} \times_{\operatorname{Spec} k} \operatorname{Spec}\overline{k}$. Since $\overline{k} \otimes_k \overline{k} = \sum_{\sigma \in G} \overline{k}^{\sigma}$ where $\overline{k}^{\sigma}$ is the $\overline{k}$-vector space $\overline{k}$ with action twisted by σ, this gluing data is given by a cocycle $\Xi : G \to \mu_n$. This is the cocycle representing X/k. Concretely it is given as follows: let P_0 be any point in $X(\overline{k})$. Then the cocycle representing X is given by

$$\Xi : \sigma \in G \mapsto \zeta_\sigma \in \mu_n \text{ where } \sigma(P_0) = \zeta_\sigma \cdot P_0. \tag{9}$$

In the particular case where X is the μ_n-torsor $X : x^n = \xi$ associated to some $\xi \in k^*$, if $\xi_0^n = \xi$, then this cocycle is $\sigma \mapsto \sigma(\xi_0)/\xi_0 \in \mu_n$.

Conversely, given a cocycle in $H^1(G, \mu_n)$, then by Galois descent it encodes a scheme X/k which will be a μ_n-torsor. It is not obvious how to find a $\xi \in k^*/k^{*,n}$ representing X/k however. But if one can find a ξ_0 such that the cocycle is given (up to a coboundary) by $\sigma \mapsto \sigma(\xi_0)/\xi_0 \in \mu_n$, then a representative of X is $\xi = \xi_0^n$.

Going back to the Tate pairing associated to an isogeny f, if B is principally polarised by $\mathcal{M}$, the Tate pairing associated to f composed with $\Phi_{\mathcal{M}}$, or equivalently the Tate pairing associated to $\Phi_{\mathcal{M}} \circ f$ gives a pairing $e_{T,f} : B(k)/f(A(k)) \times \operatorname{Ker}\tilde{f}(k) \to H^1(k, \mu_n)$. Let $P \in B(k), Q \in \operatorname{Ker}\tilde{f}(k), P_0 \in A(\overline{k})$ any point such that $P = f(P_0)$. By Definition 4.2 and our recipe above, the associated cocycle representing $e_{T,f}(P, Q)$ in $H^1(G, \mu_n)$ is given by

$$e_{T,f}(P, Q) : \sigma \in G \mapsto e_{W,f}(\sigma(P_0) - P_0, Q) \in \mu_n. \tag{10}$$

Plugging Equation (6), we get

$$e_{T,f}(P, Q) : \sigma \in G \mapsto \sigma(g_{f,Z_Q}((P_0) - (0)))/g_{f,Z_Q}((P_0) - (0)) \in \mu_n, \tag{11}$$

using that g_{f,Z_Q} is rational hence commute with σ.

In this situation there is also an explicit formula for identifying this μ_n-torsor as represented by some $\xi \in k^*/k^{*,n}$. Indeed, by our recipe above and Equation (11), we have that $\xi = g_{f,Z_Q}((P_0) - (0)))^n$. Now with the functions we have defined in Section 4.3,

$f_{n,Z_Q} \circ f = g^n_{f,Z_Q}$ (if appropriately normalized; indeed they have the same divisors). So $f_{n,Z_Q}((P)-(0)) = g^n_{f,Z_Q}((P_0)-(0))$, and we obtain:

$$e_{T,f}(P,Q) = f_{n,Z_Q}((P)-(0)) \in k^*/k^{*,n}. \tag{12}$$

(It is also possible to recover Equation (12) from Equation (7) but this uses Weil's or Lang's reciprocity theorem, it is not as direct as using Equation (6).) In particular, we recover that $e_{T,f}(P,Q) = e_{T,n}(P,Q)$, this is a particular case of Proposition 4.6.

Note that if (for instance) $A = E$ is an elliptic curve, and we take $Z_Q = (Q)-(0)$, then if we let $f_{n,Q} = f_{n,Z_Q}$ and we normalize it appropriately at infinity, then $f_{n,Z_Q}((P)-(0)) = f_{n,Q}(P)$. Also, if $A = \mathrm{Jac}(C)$ is a Jacobian, we can work directly over C as in Remark 4.11.

More generally on an abelian variety A, if Z_P is any cycle equivalent to $(P)-(0)$, then

$$e_{T,n}(P,Q) = f_{n,Z_Q}(Z_P), \tag{13}$$

indeed by Lang's reciprocity this differ from Equation (12) by an n-th power.

Lemma 4.13. *Let $f : A \to B$ be an n-isogeny, $P \in B(k)/f(A(k))$, $Q \in \mathrm{Ker}\tilde{f}$, $P_0 \in f^{-1}(P)$. With the notations above, a representative of $e_{T,f}(P,Q)$ is given by $f_{n,Z_Q}((P)-(0))$, and a map $f^{-1}(P) \to e_{T,f}(P,Q)$ above the map $\phi_Q = e_f(\cdot,Q) : \mathrm{Ker}f \to \mu_n$ is given by $\Phi : P_0 \mapsto g_{f,Z_Q}((P_0)-(0))$, if f_{n,Z_Q} and g_{f,Z_Q} are appropriately normalised so that $f_{n,Z_Q} \circ f = g^n_{f,Z_Q}$.*

Proof. The representative comes from the discussion above: $f_{n,Z_Q} \circ f$ has the same divisor as g^n_{f,Z_Q}, so they are equal up to renormalisation. So if $P_0 \in f^{-1}(P)$, we have $g_{f,Z_Q}((P_0)-(0))^n = f_{n,Z_Q}((P)-(0))$ so the map lends in the torsor $x^n = e_{T,f}(P,Q)$. Now translating P_0 by $T \in \mathrm{Ker}f$, changes $\Phi(P_0)$ by $\Phi(P_0+T) = e_{W,f}(T,Q)\Phi(P_0)$ by Equation (6). Hence Φ commutes with the action of $\mathrm{Ker}f$ on the domain and μ_n on the codomain. □

4.5. **The Tate pairing over $\mathbb{F}_q$.** Let $G/\mathbb{F}_q$ be a finite abelian Galois module. Then a standard calculation [Ser68], using the inflation-restriction spectral sequence, Tate's cohomology groups and the Herbrand quotient shows:

Proposition 4.14. *$H^0(\mathbb{F}_q,G) = G(\mathbb{F}_q) = G[\pi_q - 1]$, $H^1(\mathbb{F}_q,G) = G(\mathbb{F}_q)/(\pi_q-1)$, $\#H^0(\mathbb{F}_q,G) = \#H^1(\mathbb{F}_q,G)$, and $H^i(\mathbb{F}_q,G) = 0$ for $i > 1$.*

In fact, one can also see that $\mathbb{F}_q$ is of cohomological dimension 1 because by the Chevalley-Warning theorem it is a C_1-field and a C_1-field is of cohomological dimension 1 (see e.g., [Stacks, Tag 0A2M]).

Remark 4.15 (Representation of μ_n-torsors)**.** As a corollary, we get a third interpretation (compared to Section 4.4) of $H^1(\mathbb{F}_q,\mu_n)$: $H^1(\mathbb{F}_q,\mu_n) \simeq \mu_n/(\pi_q-1)$. Let $G = \mathrm{Gal}(\mathbb{F}_q)$, it is procyclic generated by π_q. Given a cocyle $\Xi : G \to \mu_n$ in $H^1(G,\mu_n)$ representing a μ_n-torsor X, the element of $\mu_n/(\pi_q-1)$ associated to X is $\Xi(\pi_q)$. If Ξ' is another cocycle representing X, it will differ from Ξ by a coboundary $\pi^n \mapsto \pi^n(\zeta_0)/\zeta_0$, then $\Xi'(\pi_q) = \Xi(\pi_q)\zeta_0^{q-1}$, hence lies in the same equivalence class of μ_n modulo $\pi_q - 1$. Conversely, if $[\zeta] \in \mu_n/(\pi_q-1)$, and we take any representative ζ, then a cocycle corresponding to Ξ (up to coboundary) is given by $\Xi(\pi_q) = \zeta$, i.e., $\Xi(\pi_q^m) = \zeta\pi_q(\zeta)\dots\pi_q^{m-1}(\zeta)$.

In particular, recall that if $\xi \in \mathbb{F}_q^*/\mathbb{F}_q^{*,n}$, the μ_n-torsor associated to $x^n = \xi$ has for cocycle $\sigma \mapsto \sigma(\xi_0)/\xi_0$ for a ξ_0 such that $\xi = \xi_0^n$. So taking $\sigma = \pi_q$, we obtain the element

$\xi_0^{q-1} = \xi^{(q-1)/n}$. Here, when $n \nmid q-1$, $\xi^{(q-1)/n}$ is an abuse of notation for the element ξ_0^{q-1}, it lies in $\mu_n/(\pi_q - 1)$ and not in μ_n.

In summary (see also Example 3.32), given a μ_n-torsor X, the first isomorphism $H^1(\mathbb{F}_q, \mu_n) \simeq \mathbb{F}_q^*/\mathbb{F}_q^{*,n}$ gives explicit equations (i.e., an isomorphism) for X: $x^n = \xi$, if ξ represents X. The second and third isomorphism, $H^1(\mathbb{F}_q, \mu_n) \simeq H^1(\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q), \mu_n) \simeq \mu_n/(\pi_q - 1)$ gives the Galois structure of X. Notably, if X is represented by ζ_X, then as a Galois module, X is isomorphic to μ_n with the twisted Galois action $\star$ given by $\pi_q^m \star \zeta = (\pi_q^m \cdot \zeta) \times \zeta_X^{\frac{q^m-1}{q-1}}$.

Let μ_m be the image of $\pi_q - 1$ on μ_n. Then there are m other distinct representatives for X: $\zeta_X\zeta'$ for $\zeta' \in \mu_m$. In the twisted Galois action above, μ_n decomposes into a disjoint union $\mu_n = \bigsqcup \mu_{n,\zeta'}$ where $\mu_{n,\zeta'} = \{\zeta \in \mu_n \mid \zeta^{q-1} = \zeta'\}$ is of order $d = n/m$, and for $\zeta \in \mu_{n,\zeta'}$ the twisted action of π_q on this ζ is given by $\pi_q \star \zeta = (\zeta_X\zeta')\zeta$.

Example 4.16 (Change of order)**.** Let $n = md$ and $i : \mu_m \to \mu_n$ denote the inclusion. We can describe the pushforward map $i_* : H^1(\mathbb{F}_q, \mu_m) \to H^1(\mathbb{F}_q, \mu_n)$ on torsor in terms of our different representatives above as follows. If X is a μ_m-torsor represented by a cocycle Ξ with value in μ_m, then i_*X is the μ_n-torsor represented by $i \circ \Xi$. Taking the image of π_q by Ξ, we get that $i_* : \mu_m/(\pi_q - 1) \to \mu_n/(\pi_q - 1)$ is the natural map $[\zeta] \mapsto [\zeta]$. On the other hand, if X is represented by $x^m = \xi$, then the cocycle associated comes from any ξ_0 such that $\xi_0^m = \xi$. The same ξ_0 gives the cocycle associated to i_*X, hence it is represented by $\xi_0^n = \xi^d$, i.e., the map $i_* : \mathbb{F}_q^*/\mathbb{F}_q^{*,m} \to \mathbb{F}_q^*/\mathbb{F}_q^{*,n}$ is given by $\xi \mapsto \xi^d$.

We also have the projection map $p : \mu_n \to \mu_d, \zeta \mapsto \zeta^m$. If X is represented by the cocycle Ξ, p_*X is represented by $p \circ \Xi$, and $p \circ \Xi(\pi_q) = \Xi(\pi_q)^m$, hence $p_* : \mu_n/(\pi_q - 1) \to \mu_m/(\pi_q - 1)$ is also the natural map $[\zeta] \mapsto [\zeta^m]$ induced by p. On the other hand, if X is represented by $x^n = \xi$, then $x \mapsto x^m$ is a morphism between $x^n = \xi$ and $x^d = \xi$ above p, hence p_*X is represented by $x^d = \xi$ by Lemma 3.19. So $\mathbb{F}_q^*/\mathbb{F}_q^{*,n} \to \mathbb{F}_q^*/\mathbb{F}_q^{*,d}$ is given by $\xi \mapsto \xi$.

The exact sequence $1 \to \mu_m \to \mu_n \to \mu_d \to 1$ induces a long exact sequence of cohomology:

$$1 \to \mu_m(\mathbb{F}_q) \to \mu_n(\mathbb{F}_q) \to \mu_d(\mathbb{F}_q) \to H^1(\mathbb{F}_q, \mu_m) \to H^1(\mathbb{F}_q, \mu_n) \to H^1(\mathbb{F}_q, \mu_d) \to 0,$$

using that $\mathbb{F}_q$ is of cohomological dimension 1. If $\mu_n(\mathbb{F}_q) = \mu_d(\overline{\mathbb{F}}_q)$ (i.e., the subgroup of rational roots of unity is μ_d), then by Proposition 4.14, $\#H^1(\mathbb{F}_q, \mu_n) = d$, and since $H^1(\mathbb{F}_q, \mu_n) \simeq \mu_n/(\pi_q - 1)$, it follows that $(\pi_q - 1)\mu_n = \mu_m$. In this case, the maps induced by exponentiation $H^1(\mathbb{F}_q, \mu_n) = \mu_n/(\pi_q - 1) \to H^1(\mathbb{F}_q, \mu_d) = \mu_d$ is an isomorphism. And μ_m is the largest subgroup μ' of μ_n such that the image of $H^1(\mathbb{F}_q, \mu') \to H^1(\mathbb{F}_q, \mu_n)$ is trivial.

Example 4.17 (Iterating n-th roots)**.** Assume that $\xi \in \mathbb{F}_q^{*,n}$, i.e., the torsor $x^n = \xi$ is trivial. Among all the rational roots of $x^n = \xi$, is there one such that the associated torsor $y^n = x$ is still trivial? If x is a rational root, the other ones are given by $x\zeta$, where $\zeta \in \mu_n(\mathbb{F}_q)$. The element x induces the element $x^{(q-1)/n}$ in $H^1(\mathbb{F}_q, \mu_n) = \mu_n/(\pi_q - 1)$. So if $\zeta \in \mu_n(\mathbb{F}_q) \mapsto \zeta^{(q-1)/n} \in \mu_n/(\pi_q - 1)$ is surjective, we can always correct our x to get a trivial torsor. Furthermore, since both set have the same cardinal by Proposition 4.14, the map above is then an isomorphism: there is a unique x with $x^n = \xi$ such that $y^n = x$ is a trivial torsor. We might call this x the canonical n-th root of ξ, and we can then iterate it.

For instance, if $\mu_n(\mathbb{F}_q) = \mu_d$, then $(\pi_q - 1)(\mu_n) = \mu_m$ with $n = dm$. If furthermore m is prime to d, then m is prime to $q-1$ because $d = n \wedge (q-1)$. Hence $x \mapsto x^m$ is an isomorphism on $\mathbb{F}_q^*$: every element has a unique rational m-th root. Via the isomorphism $\mu_n/(\pi_q - 1) \to \mu_d, \zeta \mapsto \zeta^m$, the map above has the same image as the map $\mu_n(\mathbb{F}_q) = \mu_d \to \mu_d, \zeta \mapsto \zeta^{(q-1)/d}$. Hence if (and only if) $(q-1)/d$ is prime to d (if d is prime, an equivalent condition is that $\mathbb{F}_q^*$ has no points of primitive order d^2), each trivial torsor $x^n = \xi$ has a unique element x such that $y^n = x$ is trivial. A well known example concern square roots on $\mathbb{F}_q^*$ when $q = 3 \mod 4$.

Definition 4.18. Given a principally polarised abelian variety $A/\mathbb{F}_q$, $P \in A(\mathbb{F}_q)$ and $Q \in A[n](\mathbb{F}_q)$, we call the reduced Tate pairing the Tate pairing $e_{T,n}(P,Q) \in H^1(\mathbb{F}_q, \mu_n)$ seen in $\mu_n/(\pi_q - 1)$ via Proposition 4.14. By Equations (10) to (13), the reduced Tate pairing is given by

$$(14)\quad \begin{aligned} e_{T,n}(P,Q) = e_{W,n}(\pi_q P_0 - P_0, Q) &= g_{\ell, Z_Q}((P_0) - (0))^{q-1} \\ &= f_{n,Z_Q}((P) - (0))^{(q-1)/n} = f_{n,Z_Q}(Z_P)^{(q-1)/n} \in \mu_n/(\pi_q - 1) \end{aligned}$$

where $nP_0 = P$.

When $n \mid q-1$, we recover the usual process of the final exponentiation in the Tate pairing, which gives the reduced Tate pairing. In general, we let $d = n \wedge (q-1)$, then $\mu_n(\mathbb{F}_q) \simeq \mu_d$ and $\mu_n/(\pi_q - 1) \to \mu_d, \zeta \mapsto \zeta^{n/d}$ is an isomorphism, and via this isomorphism the reduced Tate pairing is given by $e_{T,n}(P,Q) = f_{n,Z_Q}(Z_P)^{(q-1)/d} \in \mu_d$.

Remark 4.19 (Change of order in the Tate pairing)**.** If $d = n \wedge (q-1)$, $n = dm$, $P \in A(k)$, $Q \in A[n]$, and $e_{T,n}(P,Q)$ is interpreted as being in μ_d by the isomorphism $H^1(\mathbb{F}_q, \mu_n) \simeq \mu_d$ from Example 4.16, then by the refined version of bilinearity of Remark 4.5, $e_{T,n}(P,Q) = e_{T,d}(P, mQ) \in \mu_d$.

Remark 4.20 (Base change over $\mathbb{F}_q$)**.** We can refine Remark 4.8 over a finite field. The Tate pairing $e_{T,f}(P,Q)$ seen as a torsor $x^n = \xi$ over $\mathbb{F}_q$ is still represented by the same torsor $x^n = \xi$ when seen over $\mathbb{F}_{q^d}$ where $\xi \in \mathbb{F}_q^* \subset \mathbb{F}_{q^d}^*$. However the isomorphism class of this torsor can change: the pullback map $H^1(\mathbb{F}_q, \mu_n) \to H^1(\mathbb{F}_{q^d}, \mu_n)$ corresponds via the isomorphisms $H^1(\mathbb{F}_q, \mu_n) = \mu_n/(\pi_q - 1), H^1(\mathbb{F}_{q^d}, \mu_n) = \mu_n/(\pi_q^d - 1)$ to the exponentiation $\mu_n/(\pi_q - 1) \to \mu_n/(\pi_q^d - 1), \zeta \mapsto \zeta^{(q^d-1)/(q-1)}$. Indeed, remember by Remark 4.15 that the isomorphism $H^1(\mathbb{F}_q, \mu_n) \simeq \mu_n/(\pi_q - 1)$ correspond to taking the cocycle representing the torsor and to evaluate it at π_q. If $\xi_0^n = \xi$, then the element representing $e_{T,f}(P,Q)$ over $\mathbb{F}_q$ in $\mu_n/(\pi_q - 1)$ is then $\pi_q(\xi_0)/\xi_0$, while the element representing $e_{T,f}(P,Q)$ over $\mathbb{F}_{q^d}$ in $\mu_n/(\pi_{q^d} - 1)$ is $\pi_{q^d}(\xi_0)/\xi_0$.

Since $(q^d - 1)/(q-1) = 1 + q + q^2 + \cdots + q^{d-1}$, and $\zeta^q \equiv \zeta$ in $\mu_n/(\pi_q - 1)$, then, if $(\pi_q^d - 1)(\mu_n) = (\pi_q - 1)(\mu_n)$, i.e., if $\mu_n(\mathbb{F}_q) = \mu_n(\mathbb{F}_{q^d})$ (this is of course the case if $\pi_q = 1$ on μ_n, i.e., $n \mid q-1$), this exponentiation map corresponds to $\zeta \mapsto \zeta^d$.

Remark 4.21 (Trace map over finite fields)**.** We can refine the form Weil's scalar restriction from Remark 4.9 takes from torsors over $\mathbb{F}_{q^d}$ to torsors over $\mathbb{F}_q$ (note that $\mathbb{F}_{q^d}/\mathbb{F}_q$ is finite étale). Recall that if $G/\mathbb{F}_q$ is a finite étale group, and $X'/\mathbb{F}_{q^d}$ is a G'-torsor over $\mathbb{F}_{q^d}$ (where G' is the base change of G to $\mathbb{F}_{q^d}$), then we can build a G-torsor over $\mathbb{F}_q$ by first taking the Weil restriction of X' to get a $R_{\mathbb{F}_{q^d}/\mathbb{F}_q} G'$ torsor, then mapping it through the natural counit

morphism $R_{\mathbb{F}_{q^d}/\mathbb{F}_q}G' \to G$. Via Proposition 4.14, the corresponding map on cohomology is the natural projection $H^1(\mathbb{F}_{q^d}, G') \simeq G/(\pi_q^d - 1) \to H^1(\mathbb{F}_q, G) \simeq G/(\pi_q - 1)$.

In the special case where $G = \mu_n$, so we can also represent a μ_n-torsors by $\xi \in k^*/k^{*,n}$, then the morphism corresponds to $\xi \in \mathbb{F}_{q^d}^*/\mathbb{F}_{q^d}^{*,n} \mapsto \xi\pi_q(\xi)\cdots\pi_q^{d-1}(\xi) \in \mathbb{F}_q^*/\mathbb{F}_q^{*,n}$, i.e., in this case the trace map Tr is the norm of $\mathbb{F}_{q^d}/\mathbb{F}_q$.

As mentioned in Remark 4.9, by bilinearity of the Weil pairing, if $P' \in B(\mathbb{F}_{q^d})$ and Q is rational, and we let $P = \operatorname{Tr} P' = P' + \pi_q(P') + \cdots \pi_q^{d-1}(P')$, then looking at the non reduced Tate pairings in $\mathbb{F}_{q^d}^*$ and $\mathbb{F}_q^*$ respectively, $\operatorname{Tr} e_{T,f}(P', Q) := e_{T,f}(P', Q)^{1+q+\cdots+q^{d-1}} = e_{T,f}(P, Q) \in \mathbb{F}_q^*/\mathbb{F}_q^{*,n}$. Taking this equality to the power $(q-1)/n$, and remarking that $(q^d - 1)/n = (1 + q + \cdots + q^{d-1})(q-1)/n$, then the *reduced* Tate pairings satisfies $\operatorname{Tr} e_{T,f}(P', Q) = e_{T,f}(P, Q) \in \mu_n/(\pi_q - 1)$ where as explained above, for the reduced Tate pairing the trace is simply the projection $\mu_n/(\pi_q^d - 1) \to \mu_n/(\pi_q - 1)$.

We have similar formulas if P is rational but Q' is defined above $\mathbb{F}_{q^d}$ with $Q = \operatorname{Tr} Q'$: for the non reduced Tate pairings, $\operatorname{Tr} e_{T,f}(P, Q') := e_{T,f}(P, Q')^{1+q+\cdots+q^{d-1}} = e_{T,f}(P, Q) \in \mathbb{F}_q^*/\mathbb{F}_q^{*,n}$, and for the reduced Tate pairing: $\operatorname{Tr} e_{T,f}(P, Q') = e_{T,f}(P, Q) \in \mu_n/(\pi_q - 1)$.

We now prove non degeneracy of the Tate pairing; this is a special feature of finite fields.

Theorem 4.22. *Let $f : A \to B$, $P \in B(\mathbb{F}_q)$, $Q \in \operatorname{Ker}\hat{f}$ of exact order $d \mid n$. Then $e_{T,f}(\cdot, Q) : B(\mathbb{F}_q)/f(A(\mathbb{F}_q)) \to H^1(\mathbb{F}_q, \mu_d)$ is surjective.*

Hence if $Q \in \operatorname{Ker}\hat{f}$ is of order dividing n, $H^1(\mathbb{F}_q, \mu_n)$ is not trivial and $e_{T,f}(P, Q) \in H^1(\mathbb{F}_q, \mu_n)$ is trivial for all $P \in B(\mathbb{F}_q)/A(\mathbb{F}_q)$, then Q is of order d a strict divisor of n.

Proof. First by Lang's theorem on triviality of torsors of a smooth connected algebraic group $G/\mathbb{F}_q$ [Lan56], $H^1(\mathbb{F}_q, A) = 0$: all A-torsors have a rational points hence are trivial. So $B(\mathbb{F}_q) \to H^1(\mathbb{F}_q, \operatorname{Ker} f)$ is surjective: all $\operatorname{Ker} f$-torsors comes from the preimage by f of a point $P \in B(\mathbb{F}_q)$. Secondly, given a point $Q \in \operatorname{Ker}\hat{f}(\mathbb{F}_q)$ of exact order $d \mid n$, since the application $\phi_Q = e_{W,n}(\cdot, Q) : \operatorname{Ker} f \to \mu_d$ is surjective by non degeneracy of the Weil pairing, and $\mathbb{F}_q$ is of cohomological dimension 1 (in particular all gerbes are trivial), then $\phi_{Q,*} : H^1(\mathbb{F}_q, \operatorname{Ker} f) \to H^1(\mathbb{F}_q, \mu_d)$ is surjective. Combining these two surjections, we get that $e_{T,f}(\cdot, Q) : B(\mathbb{F}_q) \to H^1(\mathbb{F}_q, \mu_d)$ is surjective. □

Remark 4.23 (Non degeneracy)**.** By the proof above, $H^1(\mathbb{F}_q, \operatorname{Ker} f) \simeq B(\mathbb{F}_q)/A(\mathbb{F}_q)$. Furthermore, $H^1(\mathbb{F}_q, \operatorname{Ker} f)$ has the same cardinal as $H^0(\mathbb{F}_q, \operatorname{Ker} f) = \operatorname{Ker} f(\mathbb{F}_q)$ by Proposition 4.14. Now suppose that $\operatorname{Ker} f$ is of exact exponent n and that $\mu_n \subset \mathbb{F}_q$ so that $H^1(\mathbb{F}_q, \mu_n) = \mu_n$. Then the Tate pairing $B(\mathbb{F}_q)/A(\mathbb{F}_q) \times \operatorname{Ker} f(\mathbb{F}_q) \to \mu_n$ is non-degenerate on the right by Theorem 4.22, and since both groups on the left have same cardinal and are of exponent n, they are dual to each other. Hence the Tate pairing is also non-degenerate on the left.

More generally, if μ_d is the subgroup of μ_n generated by $\mu_n(\mathbb{F}_q)$, then $H^1(\mathbb{F}_q, \mu_n) \simeq \mu_d$ by Example 4.16. And if $e_{T,n}(P, Q)$ is trivial for all $P \in B(\mathbb{F}_q)/A(\mathbb{F}_q)$, then Q is of order dividing $m = n/d$ by Theorem 4.22. Of course this can be recovered from the refined version of bilinearity, as explained in Remark 4.19, $e_{T,n}(P, Q)$ seen in μ_d is naturally equal to $e_{T,d}(P, mQ)$, and since $d \mid q - 1$, we can apply the usual non degeneracy of the Tate pairing over a finite field.

Let us give a direct proof that the Tate pairing over $\mathbb{F}_q$ is non-degenerate on the left when $\mu_n \subset \mathbb{F}_q$. This is instructive to see why the argument does not work over a more general field k. Let $K' \subset \mathrm{Ker} f$ be the orthogonal of $\mathrm{Ker}\hat{f}(\mathbb{F}_q)$ under the Weil pairing $e_{W,f}$. We have an exact sequence $0 \to K' \to \mathrm{Ker} f \to H \to 0$ where $H = \mathrm{Ker} f/K' \simeq (\mathrm{Ker}\hat{f}(\mathbb{F}_q))^\vee$ by non degeneracy of the Weil pairing. The isogeny $f : A \to B$ decomposes as $f = f_2 \circ f_1 : A \to C \to B$ where $\mathrm{Ker} f_1 = K'$ and $\mathrm{Ker} f_2 \simeq \mathrm{Ker} f/K' \simeq H$. If $P \in B(\mathbb{F}_q)$, $f_{1,*}f^{-1}(P) = f_2^{-1}(P)$ by Lemma 3.22. Taking a basis $(Q_1, \dots, Q_r)$ of $\mathrm{Ker}\hat{f}(\mathbb{F}_q)$ (we assume that $\mathrm{Ker}\hat{f}(\mathbb{F}_q) \simeq (\mathbb{Z}/n\mathbb{Z})^r$ for simplicity, the general case can be treated similarly, see Remark 5.5 below), the map $\Phi : \mathrm{Ker} f \to \mu_n^r, P \mapsto e_{W,r}(P, Q_i)$ induces an isomorphism between $H = \ker f/K'$ and μ_n^r. Since Φ factorizes though f_1, and by definition of the Tate pairing, $\Phi_* f^{-1}(P) = \Phi_* f_2^{-1}(P)$ is the μ_n^r-torsor represented by the $(e_{T,f}(P, Q_i)$ (this is the same argument as in Proposition 5.1 below). Since Φ is an isomorphism from H to μ_n^r, we see that Φ_* is an isomorphism above Φ of $f_2^{-1}(P)$ with the μ_n^r-torsor given by the $(e_{T,f}(P, Q_i))$. In conclusion: $e_{T,f}(P, Q)$ is trivial for all $Q \in \mathrm{Ker}\hat{f}(\mathbb{F}_q)$ is equivalent to $f_2^{-1}(P)$ is trivial. It remains to show that in this case, $f^{-1}(P)$ is trivial too. We thus need to prove that $f_{1,*} : H^1(\mathbb{F}_q, \mathrm{Ker} f) \to H^1(\mathbb{F}_q, H)$ is injective. Up to now, the whole argument did not need that $\mu_n \subset \mathbb{F}_q$ or even that k is a finite field, this is where we will need these hypothesises.

By the long exact sequence in cohomology, to prove that $f_{1,*}$ is injective is the same as requiring that $H(\mathbb{F}_q) \to H^1(\mathbb{F}_q, K') = K'(\mathbb{F}_q)/(\pi_q - 1)$ is surjective. If $h \in H(\mathbb{F}_q)$, and $g \in f_2^{-1}(h)$, the image of h in $K'(\mathbb{F}_q)/(\pi_q - 1)$ is represented by $\pi_q(g) - g \in K'$. Since $\mu_n \subset \mathbb{F}_q$, $\mu_n = (\mathbb{Z}/n\mathbb{Z})^\vee \simeq (\mathbb{Z}/n\mathbb{Z})$, hence $H \simeq \mathrm{Ker}\hat{f}(\mathbb{F}_q)$ as a Galois module, and $H(\overline{\mathbb{F}}_q) = H(\mathbb{F}_q)$. In particular, $f_2^{-1}H(\mathbb{F}_q) = \mathrm{Ker} f(\overline{\mathbb{F}}_q)$, so we just need to show that the image of $\pi_q - 1 : \mathrm{Ker} f \to K'$ is surjective. But $\#K'\#H = \#\mathrm{Ker} f = \#(\pi_q - 1)(\mathrm{Ker} f)\#\mathrm{Ker} f(\mathbb{F}_q)$. Since $\#H = \#\mathrm{Ker}\hat{f}(\mathbb{F}_q) = \#\mathrm{Ker} f(\mathbb{F}_q)$ (because $\mathrm{Ker} f$ and $\mathrm{Ker}\hat{f}$ are Galois dual and $q = 1 \mod n$), we get that $\#K' = \#(\pi_q - 1)(\mathrm{Ker} f)$ as we wanted.

Remark 4.24 (Restriction to subgroups)**.** All proofs I know [FMR99; Heß04; Sch05; Bru11] of non degeneracy of the Tate pairing suppose that $\mu_n \subset \mathbb{F}_q$. Indeed, for non degeneracy, by Remark 4.23 it is harmless to only deal with this case.

Furthermore, when $\mu_n \not\subset \mathbb{F}_q$, n is prime and d is the embedding degree, they have a refined version of the n-Tate pairing restricted to subgroups of $A[n](\mathbb{F}_{q^d})$. Indeed, they define the subgroups $\mathbb{G}_1$, $\mathbb{G}_2$ to be the subgroups of $A(\mathbb{F}_{q^d})$ where π_q has eigenvalue 1 and q respectively, and show that the n-Tate pairing $A(\mathbb{F}_{q^d})/nA(\mathbb{F}_{q^d}) \times A[n](\mathbb{F}_{q^d}) \to \mu_n$ over $\mathbb{F}_{q^d}$ is still non-degenerate (under certain conditions) when restricted to $\mathbb{G}_1 \times \mathbb{G}_2$ or $\mathbb{G}_2 \times \mathbb{G}_1$ (provided that they are not empty).

We can recover this result as follows. Let A be principally polarised, assume that n is prime and $A[n](\mathbb{F}_q)$ is non empty. So $\mathbb{G}_1$ is non empty, and $\mathbb{G}_2$ its Galois dual (thanks to the Weil pairing) is non empty too over $\mathbb{F}_{q^d}$. Let $\phi : B \to A$ be the dual isogeny of the quotient $A \to \hat{B} := A/\mathbb{G}_2$ (here we identify A with $\widehat{A}$ via the principal polarisation). Then we get a non-degenerate pairing $A(\mathbb{F}_{q^d})/\phi(B)(\mathbb{F}_{q^d}) \times \mathbb{G}_2(\mathbb{F}_{q^d}) \to \mu_n$ by Theorem 4.22. But $\mathrm{Ker}\,\phi$ is the Galois dual of $\mathbb{G}_2$ hence is isomorphic to $\mathbb{G}_1$, so $A(\mathbb{F}_{q^d})/\phi(B)(\mathbb{F}_{q^d}) \simeq H^1(\mathbb{F}_{q^d}, \mathbb{G}_1) \simeq H^1(\mathbb{F}_q, \mathbb{G}_1) \simeq A(\mathbb{F}_q)/\phi(B)(\mathbb{F}_q)$, hence we have a non-degenerate pairing $A(\mathbb{F}_q)/\phi(B)(\mathbb{F}_q) \times \mathbb{G}_2(\mathbb{F}_{q^d}) \to \mu_n$. Since n is prime, then if $A(\mathbb{F}_q)$ does not have points of n^2-torsion, the inclusion $\mathbb{G}_1(\mathbb{F}_q) \to A(\mathbb{F}_q)$ induces an isomorphism $\mathbb{G}_1(\mathbb{F}_q) \simeq$

$A(\mathbb{F}_q)/nA(\mathbb{F}_q) \simeq A(\mathbb{F}_q)/\phi(B)(\mathbb{F}_q)$, so we get a non-degenerate pairing

$$\mathbb{G}_1(\mathbb{F}_q) \times \mathbb{G}_2(\mathbb{F}_{q^d}) \to \mu_n.$$

More generally, if n is prime and $d > 1$, then q is a primitive d-th root of unity modulo n by the definition of the embedding degree. Since $\pi_q^d = 1$ on $A[n](\mathbb{F}_{q^d})$ and d is prime to n, π_q splits $A[n](\mathbb{F}_{q^d})$ into eigenspaces with eigenvalues $1, q, \dots, q^{d-1}$, that we denote by $\mathbb{G}_1, \mathbb{G}_2, \dots, \mathbb{G}_d$. The Galois dual of $\mathbb{G}_i$ is $\mathbb{G}_{3-i}$ (because π_q acts by q^{i-1} on $\mathbb{G}_i$ and q/q^{i-1} on $\mathbb{G}_i^\vee$), with the convention that $\mathbb{G}_0 = \mathbb{G}_d, \mathbb{G}_{-1} = \mathbb{G}_{d-1}, \dots$ Incidentally, the Weil pairing $e_{W,n}$ is non degenerate on $\mathbb{G}_i \times \mathbb{G}_{3-i}$ by Remark 4.12. We can look at the Tate-Cartier pairing given by the dual isogeny ϕ_2 of $A \to \widehat{C} = A/\mathbb{G}_{3-i}$, to obtain a non-degenerate pairing $A(\mathbb{F}_{q^d})/\phi_2(C)(\mathbb{F}_{q^d}) \times \mathbb{G}_{3-i}(\mathbb{F}_{q^d}) \to \mu_n$ by Theorem 4.22. Assume that $A(\mathbb{F}_{q^d})$ does not have points of n^2-torsion. Then $A[n](\mathbb{F}_{q^d}) \simeq A(\mathbb{F}_{q^d})/nA(\mathbb{F}_{q^d})$, because the map is injective by assumption and they have the same cardinal over $\mathbb{F}_q$. Now $\operatorname{Ker}\phi_2 \simeq \mathbb{G}_{3-i}^\vee \simeq \mathbb{G}_i$ as a Galois module. Furthermore, since $A(\mathbb{F}_{q^d})/\phi_2(C)(\mathbb{F}_{q^d})$ is isomorphic as a Galois module to $H^1(\mathbb{F}_{q^d}, \operatorname{Ker}\phi_2) \simeq H^1(\mathbb{F}_{q^d}, \mathbb{G}_i) \simeq \mathbb{G}_i$, we get that the projection $A[n] \to A(\mathbb{F}_{q^d})/\phi_2(C)(\mathbb{F}_{q^d})$ kills all the $\mathbb{G}_j$ with $j \neq i$. Hence the injection $\mathbb{G}_i \to A(\mathbb{F}_{q^d})/\phi_2(C)(\mathbb{F}_{q^d})$ is a bijection, and we obtain a non-degenerate pairing $\mathbb{G}_i \times \mathbb{G}_{3-i} \to \mu_n$. As a special case, in this situation, the Tate pairing restricted to $\mathbb{G}_2 \times \mathbb{G}_1 \to \mu_n$ is non-degenerate.

Similarly, let $\mathbb{F}_{q^e}$ be the smallest extension such that $A[n] \subset A[n](\mathbb{F}_{q^e})$. Let G' be one of the characteristic subspace of $A[n]$ and G'' its Galois dual (i.e., the characteristic space associated to the q-reciprocal of the irreducible polynomial associated to G'). Then if $A(\mathbb{F}_{q^e})$ does not contain a point of n^2-torsion, by the same reasoning as above, the Tate pairing restricted to $G' \times G''$ is non-degenerate.

Example 4.25. Let $E/\mathbb{F}_q$ be an elliptic curve whose ℓ-Sylow $E(\mathbb{F}_q)[\ell^\infty]$ of $E(\mathbb{F}_q)$ is generated by (P, Q) where P is of order ℓ^2 and Q of order ℓ.

Assume first that $\mu_{\ell^2} \subset \mathbb{F}_q$. Then $e_{T,\ell^2}(Q, P)$ is of order ℓ by bilinearity, hence $e_{T,\ell^2}(P, P)$ has to be of primitive order ℓ^2 by non degeneracy, so (the reduced Tate pairings) $e_{T,\ell^2}(Q, \ell P) = 1, e_{T,\ell^2}(Q, \ell P) \neq 1$. And $e_{T,\ell^2}(Q, Q) = e_{T,\ell}(Q, Q), e_{T,\ell^2}(P, Q) = e_{T,\ell}(P, Q)$, they are of order at most ℓ by bilinearity and one of them is non-trivial by non degeneracy.

Now if $\mu_\ell \subset \mathbb{F}_q$ but $\mathbb{F}_q$ does not contains all of μ_{ℓ^2}, the situation is very different. If ζ is a primitive ℓ^2 root of unity, $\pi_q(\zeta) = \zeta^{\ell m}$ for some m invertible modulo ℓ, and $H^1(\mathbb{F}_q, \mu_{\ell^2}) \simeq \mu_{\ell^2}/(\pi - 1) \simeq \mu_\ell$ (where the last isomorphism is given by exponentiation by ℓ). Both $e_{T,\ell^2}(Q, P)$ and $e_{T,\ell^2}(P, P)$ are of order at most ℓ in $H^1(\mathbb{F}_q, \mu_{\ell^2})$, hence $e_{T,\ell^2}(Q, \ell P) = e_{T,\ell^2}(P, \ell P) = 1 \in H^1(\mathbb{F}_q, \mu_{\ell^2})$. However, when seen in $H^1(\mathbb{F}_q, \mu_\ell)$ (see Remark 4.5), $e_{T,\ell^2}(Q, \ell P) = e_{T,\ell}(Q, \ell P)$ need not be trivial, and likewise for $e_{T,\ell^2}(P, \ell P) = e_{T,\ell}(P, \ell P)$.

5. Application to fibers and radical isogenies

In this section we will use the Tate pairings to study fibers of an isogeny. As an application, we will prove the multiradical conjecture. We will work over a base scheme S, but since everything in sight is flat over S, it is essentially harmless to work fibrally over S, i.e., to assume that S is a field.

5.1. **The Galois structure of fibers of isogenies.** The basic idea is as follows. Let $f : A \to B$ be an isogeny (of exponent n as usual) over S. Assume we have a primitive n-root of unity ζ

over S, i.e., a section $\zeta : S \to \mu_n$ that is fibrally primitive. Given ζ and a basis $(Q_1, \dots, Q_r)$ of $\mathrm{Ker}\, \hat{f}$ (i.e., given sections of $\mathrm{Ker}\, \hat{f}/S$ which form a basis fibrally), the Weil pairing gives a canonical dual basis on $\mathrm{Ker}\, f$, and can be used to express a point $P \in \mathrm{Ker}\, f$ in terms of this dual basis.

When $P \in B(S)$, the Tate pairing gives a similar description on the $\mathrm{Ker}\, f$-torsor $f^{-1}(P)$:

Proposition 5.1. *Given a basis $(Q_1, \dots, Q_r) \in \hat{B}(S)$ of $\mathrm{Ker}\, \hat{f}$, the torsor $f^{-1}(P)$ splits (canonically[8]) as a μ_n^r-torsor whose isomorphism classes are given by $(e_{T,f}(P, Q_1), \dots, e_{T,f}(P, Q_r)) = (e_{T,n}(P, Q_1), \dots, e_{T,n}(P, Q_r))$.*

Proof. The basis $(Q_1, \dots, Q_r)$ gives a canonical splitting

$$\Phi : \mathrm{Ker}\, f \to \mu_n^r, P \mapsto (e_{W,f}(P, Q_1), \dots, e_{W,f}(P, Q_r)).$$

Transporting the torsor $f^{-1}(P)$ under Φ gives a canonical splitting as a μ_n^r torsor, and its individual components are given by the $e_{T,f}(P, Q_i)$ by the definition of the Tate pairing. The last equality comes from Proposition 4.6. □

Corollary 5.2. *If the Tate pairings $e_{T,f}(P, Q_1), \dots, e_{T,f}(P, Q_r)$ are all trivial, then $P \in f(A(S))$.*

Proof. The torsor $f^{-1}(P)$ is then isomorphic to the trivial μ_n^r-torsor by Proposition 5.1, hence has a section over S. □

Remark 5.3 (Partial fiber information)**.** In the case where our sections $Q_1, \dots, Q_r$ do not span the full $\mathrm{Ker}\, \tilde{f}$, we only have partial information on the fiber $f^{-1}(P)$. This is similar to what happens with the Weil pairing. Let $H \subset \mathrm{Ker}\, \tilde{f}$ be the subgroup spanned by the Q_i and $K' \subset \mathrm{Ker}\, f$ be its orthogonal under the Weil pairing. Since the Q_i are rational, H is isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^r$. Hence $\mathrm{Ker}\, f/K' \simeq H^\vee$ is isomorphic, via the map $\Phi : P \in \mathrm{Ker}\, f \mapsto e_{W,f}(P, Q_i)$ induced by the Weil pairing, to μ_ℓ^r.

Now we can decompose f as $f = f_2 \circ f_1$ with $\mathrm{Ker}\, f_1 = K'$. Then as in Proposition 5.1, $f^{-1}(P)/K' \simeq \Phi_* f^{-1}(P) \simeq f_2^{-1}(P)$ (see also Remarks 3.14 and 4.23). So the r Tate pairings above give the $\mathrm{Ker}\, f/K' \simeq H^\vee \simeq \mu_\ell^r$ torsor isomorphic to (i.e., parametrizing) $f^{-1}(P)/K' \simeq f_2^{-1}(P)$. The larger H is, the smaller K' will be, and the more information we will have on $f^{-1}(P)$.

One should be careful that the situation is different than with the Weil pairing above. Over a field k, for the Weil pairing, $\Phi(P) \in \mu_\ell^r$ describes a point in $P \in \mathrm{Ker}\, f/K'$ given by the r *coordinates* $e_{W,f}(P, Q_i)$ in $\mu_\ell(\bar{k})$. By contrast, for $P \in B(k)$, $f^{-1}(P)/K' \simeq \Phi_* f^{-1} P$ is a μ_n^r-torsor, whose isomorphism class is given by the r Tate pairings $e_{T,n}(P, Q_i)$. These pairings should really be seen individually as representing μ_n*-torsors*, they are not coordinates! When given by an element $\xi \in k^*/k^{*,n}$ the Tate pairing represents the n-points in $\overline{k}^*$ such that $x^n = \xi$, and when $k = \mathbb{F}_q$ and the (reduced) Tate pairing is given by an element $[\zeta] \in \mu_n/(\pi_q - 1)$, it represents the torsor whose associated cocycle Ξ evaluated at π_q is ζ (see Remarks 3.10 and 4.15).

Example 5.4. Let $f : E_1 \to E_2$ be an n-isogeny of elliptic curves defined over a field k. Assume that $\mathrm{Ker}\, \tilde{f} \subset E_2[N]$ is generated by $P \in E_2(k)$, and let $R \in E_2(k)$. Then by Proposition 5.1, $f^{-1}(R)$ is isomorphic to the μ_n-torsor $e_{T,n}(R, P)$, above the isomorphism $e_{W,n}(\cdot, P) : \mathrm{Ker}\, f \to \mu_n$. We will come back to this in Example 5.14.

[8] Once we have fixed the basis $(Q_1, \dots, Q_r)$.

Let Q be another generator of $\operatorname{Ker}\tilde{f}$. Then the same $\operatorname{Ker} f$-torsor $f^{-1}(R)$ is also isomorphic to the μ_n-torsor $e_{T,n}(R,Q)$, above the isomorphism $e_{W,n}(\cdot,Q) : \operatorname{Ker} f \to \mu_n$.

Notice that $e_{T,n}(R,P)$ and $e_{T,n}(R,Q)$ need not be isomorphic as μ_n-torsors (in fact, if $\mu_n \subset k$, they won't be isomorphic unless $P = Q$). Recall that if X is a G-torsor, then isomorphisms of X are given on points by $x \mapsto g \cdot x$ for a $g \in G$. These are isomorphisms of X where the action of G is fixed. On the other hand, if $\alpha \in \operatorname{Aut}(G)$, there is also an isomorphism $X \to \alpha_* X$ above α, which changes the action of G through α, hence is not an isomorphism of G-torsors.

Remark 5.5 (Basis)**.** In the statement of Proposition 5.1, we have implicitly assumed that all our Q_i are of exact order n, this is the case for instance if n is prime. In general, if $\operatorname{Ker} f$ has all its points rational, we can find a basis $(Q_1, \dots, Q_r)$ of order $(n_1, \dots, n_r)$ with $n_i \mid n_{i+1}$. (By the equivalence of category between finite étale covers $T \to S$ and finite sets with an action by $\pi^1_{\text{etale}}(S,\bar{s})$, a finite étale abelian group $T \to S$ corresponds to a finite $\mathbb{Z}$-module G with an action by $\pi^1_{\text{etale}}(S,\bar{s})$, and the points are rational when this action is trivial. There is certainly a basis as above for G seen as a $\mathbb{Z}$-module, which we translate back via our equivalence of category.) Then the isomorphism of Proposition 5.1 should be amended to take $\Phi(P) = (e_{T,n_i}(P,Q_i))$ and it lends in $\mu_{n_1} \otimes \dots \otimes \mu_{n_r}$. We'll stick to our simplifying assumption above for the rest of this section, the general case is easy to adapt.

Remark 5.6 (The Galois structure of the fiber)**.** By Example 3.32, the interpretation of Proposition 5.1 over a field k is as follows. The map Φ from the proof gives an isomorphism of $\operatorname{Ker} f$ with μ_n^r, and to give a point $T \in \operatorname{Ker} f$ is the same as to give $\Phi(T) = (e_{W,f}(T,Q_i))$.

Now if $P \in B(k)$ and the torsor $f^{-1}(P)$ is described by the Tate pairings $e_{T,f}(P,Q_i)$, then if these pairings are given by elements $\xi_i \in k^*/k^{*,n}$, $f^{-1}(P)$ is canonically isomorphic (via Φ_* and our choice of basis) to the scheme $\{x_i^n = \xi_i\}$. (Warning: this scheme describes $f^{-1}(P)$ as an abstract étale scheme over k, not as embedded inside A!) To give a point of $f^{-1}(P)$ over some étale extension k'/k is then the same thing as to give a tuple (ξ_i') in k' such that $\xi_i'^n = \xi_i$.

Conversely, if the pairings are represented by cocycles in $H^1(\operatorname{Gal}(\bar{k}/k), \mu_n)$, then these cocycles give the Galois structure of $f^{-1}(P)$. In particular, if $k = \mathbb{F}_q$, then by Remark 4.15, if the reduced Tate pairings are given by classes $[\zeta_i] \in \mu_n/(\pi_q - 1)$, then the Galois module structure of $f^{-1}(P)$ is isomorphic to μ_n^r together with the twisted action of π_q given by: $\pi_q \star (s_1, \dots, s_r) = (\pi_q(s_1)\zeta_1, \dots, \pi_q(s_r)\zeta_r)$.

Example 5.7 (The Galois structure of the fiber of an isogeny between elliptic curves over a finite field)**.** Let $E/\mathbb{F}_q$ be an elliptic curve, with a rational point of exact order n, $P \in E[n](\mathbb{F}_q)$. Let $f : E \to E' = E/\langle P \rangle$ be the corresponding isogeny, and $Q \in E(\mathbb{F}_q)$. Then by Proposition 5.1, from $e_{T,\tilde{f}}(Q,P) = e_{T,n}(Q,P)$, we can recover the Galois structure on $f^{-1}(Q)$ as follows.

Fix ζ_0 a primitive n-th root of unity in $\overline{\mathbb{F}}_q$, this fixes (via the Weil pairing) an isomorphism $\operatorname{Ker}\tilde{f} \simeq \mu_n$, and in particular a generator P' of $\operatorname{Ker}\tilde{f}$ determined by $e_{W,f}(P,P') = 1$. Fix a representative $\zeta \in \mu_n$ of the reduced Tate pairing $e_{T,n} = [\zeta] \in \mu_n/(\pi_q - 1)$.

Via the isomorphism $\operatorname{Ker}\tilde{f} \simeq \mu_n$ above, this ζ corresponds to the point $T' = uP' \in \operatorname{Ker}\tilde{f}$, where u is such that $\zeta = \zeta_0^u$. Then there is a point $Q' \in \tilde{f}^{-1}(Q)$ such that $\pi_q(Q') = Q' + T'$. If Q'' is another point in the fiber, then $Q'' = Q' + T$ for some $T \in \operatorname{Ker}\tilde{f}$. Then $\pi_q(Q'') = Q'' + T' + \pi_q(T) - T$. Let μ_m be the image of $\pi_q - 1$ on μ_n, so the image of $\pi_q - 1$ on $\operatorname{Ker}\tilde{f}$

is $\mathrm{Ker}\tilde{f}[m]$. Then as in Remark 4.15, $\tilde{f}^{-1}(Q)$ is a disjoint union of m set of points $\tilde{f}^{-1}(Q)_T$ for $T \in \mathrm{Ker}\tilde{f}[m]$, where π_q acts on $Q' \in \tilde{f}^{-1}(P)_T$ by $\pi_q(Q') = Q' + T' + T$.

Remark 5.8 (Explicit formula)**.** Over a field k, we can use Lemma 4.13 to give an explicit isomorphism between $f^{-1}(P)$ and the torsor $\{x_i^n = e_{T,n}(P, Q_i)\}$: with the notations of this Lemma, $\Psi : P_0 \in f^{-1}(P) \mapsto (g_{f,Z_{Q_i}}((P_0) - (0)))$ is an isomorphism between $f^{-1}(P)$ and $\{x_i^n = e_{T,n}(P, Q_i) = f_{n,Z_{Q_i}}((P) - (0))\}$. Here we assume that the $f_{n,Z_{Q_i}}$ and $g_{f,Z_{Q_i}}$ are appropriately normalised thus that $g^n_{f,Z_{Q_i}} = f_{n,Z_{Q_i}} \circ f$ so that $g_{f,Z_{Q_i}}((P_0) - (0))^n = f_{n,Z_{Q_i}}((P) - (0))$ and Ψ lends in the correct torsor.

Using this formula, the proof of Proposition 5.1 can be reformulated as follows:

(1) Fix any $P_0 \in f^{-1}(P)$. Then $\mathrm{Ker}f \to f^{-1}(P), T \mapsto P_0 + T$ is a bijection ($f^{-1}(P)$ is a $\mathrm{Ker}f$-torsor). Similarly, for the μ_n^r-torsor $\{x_i^n = e_{T,n}(P, Q_i)\}$, given a point (ξ_i') in it, the action of μ_n^r on this point gives a bijection of μ_n^r with this torsor.
(2) The map $\Phi : \mathrm{Ker}f \to \mu_n^r$ from Proposition 5.1 is an isomorphism.
(3) The map Ψ commutes (above Φ) with the action of $\mathrm{Ker}f$ on the left and of μ_n^r on the right, namely we check that if $\Psi(P_0) = (x_1, \dots, x_r)$, then $\Psi(P_0 + T) = (x_1 e_{W,f}(T, Q_1), \dots, x_r e_{W,f}(T, Q_r)$. This is immediate from Equation (6).

From these facts, it follows that Ψ is a bijection, and we can use Ψ^{-1} to parametrizes the points in $f^{-1}(P)$.

The same formula works in the situation of Remark 5.3: Ψ gives then a morphism $f^{-1}(P) \to f^{-1}(P)/K'$ above $\Phi : \mathrm{Ker}f \to \mathrm{Ker}f/K' \simeq \mu_n^r$.

Remark 5.9 (The rational points in the fiber)**.** When $S = \mathrm{Spec}\,k$ is a field and the fiber $f^{-1}(P)$ is trivial, i.e., has a rational point, it would be interesting to refine Proposition 5.1 to parametrize all rational points $f^{-1}(P)(k)$ in the fiber.

We can give such a description if we assume furthermore that the Weil pairing $e_{W,f}$ stays non-degenerate when restricted to $\mathrm{Ker}f(k) \times \mathrm{Ker}\hat{f}(k)$. Let $K' = \mathrm{Ker}\hat{f}(k)^{\perp}$ as in Remark 4.23. Then $K' \cap \mathrm{Ker}f(k) = 0$ by our hypothesis, so $\mathrm{Ker}f(k)$ splits the exact sequence $0 \to K' \to \mathrm{Ker}f \to H \to 0$ of Remark 4.23, i.e., $\mathrm{Ker}f = \mathrm{Ker}f(k) \oplus K'$. It follows that the $\mathrm{Ker}f$-torsor $f^{-1}(P)$ splits canonically as $f^{-1}(P) = X_1 \oplus X_2$ where X_1 is a $\mathrm{Ker}f(k)$-torsor and X_2 a K'-torsor.

Factorising $f = f_2 \circ f_1$ as in Remarks 4.23 and 5.3 with $\mathrm{Ker}f_1 = K'$, we get that $f_{1,*}f^{-1}(P) = f_2^{-1}(P) \simeq f_{1,*}X_1$ since $f_{1,*}X_2$ is a $f_1(K') = 0$-torsor. Since f_1 restricts to an isomorphism $\mathrm{Ker}f(k) \to f(\mathrm{Ker}f(k)), X_1 \mapsto f_{1,*}X_1$ is an isomorphism above f_1.

If we fix a basis (Q_i) of $\mathrm{Ker}\hat{f}(k)$ and we let $\Phi : \mathrm{Ker}f \to \mu_n^r, P \mapsto e_{W,f}(P, Q_i)$, then by our hypothesis, Φ induces an isomorphism of $\mathrm{Ker}f(k)$ with μ_n^r. So $\Phi_* f^{-1}(P) \simeq \Phi_* X_1$ is described as a torsor by the Tate pairings $e_{T,f}(P, Q_i)$ as in Proposition 5.1. We can even give an explicit isomorphism Ψ exactly as in Remark 5.8. Thus if $f^{-1}(P)$ is trivial, then X_1 corresponds to the $\mathrm{Ker}f(k)$-torsor given by $f^{-1}(P)(k)$. We can thus use the isomorphism Ψ^{-1} to parametrizes the rational points $f^{-1}(P)(k)$.

Remark 5.10 (The case of a finite field)**.** When $k = \mathrm{Spec}\,\mathbb{F}_q$ is a finite field, we have a refinement of Proposition 5.1, Corollary 5.2, and Remark 5.9 if $\mu_n \subset \mathbb{F}_q$. First, by the non degeneracy of the Tate pairing over a finite field (Theorem 4.22 and Remark 4.23), to test if $f^{-1}(P)$ is trivial we just need to test if $e_{T,f}(P, Q)$ is trivial for all $Q \in \mathrm{Ker}\hat{f}(\mathbb{F}_q)$. We do not need that all the points of $\mathrm{Ker}\hat{f}$ have to be rational as in the hypothesis of Proposition 5.1.

Now assume that $e_{W,f}$ is non-degenerate on $\mathrm{Ker} f(\mathbb{F}_q) \times \mathrm{Ker}\hat{f}(\mathbb{F}_q)$, so we are in the situation of Remark 5.9, and $f^{-1}(P)$ splits canonically as $f^{-1}(P) = X_1 \oplus X_2$ with X_1 a $\mathrm{Ker} f(\mathbb{F}_q)$-torsor. We will give another argument, in this special case, for non degeneracy on the left than the one given in Remark 4.23.

Write $f = g_2 \circ g_1 : A \to C' \to B$ with $\mathrm{Ker}\, g_1 = \mathrm{Ker} f(\mathbb{F}_q)$, then $g_{1,*}f^{-1}(P) \simeq g_2^{-1}(P) \simeq g_{1,*}X_2$, and $X_2 \to g_{1,*}X_2$ is an isomorphism above g_1. But $\mathrm{Ker}\, g_2 \simeq K'$ has no rational point. Hence $g_2 : C'(\mathbb{F}_q) \to B(\mathbb{F}_q)$ is injective, and it is bijective because C' and B are isogenous hence have the same cardinal. In particular, X_2 is always trivial, so $f^{-1}(P)$ is trivial if and only if X_1 is trivial, if and only if the $e_{T,f}(P,Q)$ are trivial for $Q \in \mathrm{Ker} f(\mathbb{F}_q)$.

We now give some examples of applications of Proposition 5.1 and Remark 5.3 before proving the multiradical isogeny conjecture.

5.2. **Divisibility.**

Example 5.11 (Divisibility on an abelian variety)**.** Let us explain how to recover some well known results on divisibility on an abelian variety. Let A/k be a principally polarised abelian variety, and $P \in A(k)$. A natural question is whether P is n-divisible in k (n prime to the characteristic).

(1) If $A[n] \subset A(k)$ and has a basis $Q_1, \dots, Q_{2g}$, then by Proposition 5.1, P is n-divisible if and only if $e_{T,n}(P,Q_1), \dots, e_{T,n}(P,Q_{2g})$ are trivial. In that case, one may then invert the map Ψ from Remark 5.8 to express all the preimages P_0 such that $nP_0 = P$.

For instance take $n = 2$ and $A = E$ an elliptic curve, assume that $E : y^2 = h(x)$ is given by a short Weierstrass equation and that the three Weierstrass points Q_1, Q_2, Q_3 are rational. With the notations of Section 4.4, we have $f_{2,Q_i} = (x - x(Q_i))$. So we recover the well known result that P is divisible by two if and only if the three (non reduced) Tate pairings $e_{T,2}(P,Q_i) = (x(P) - x(Q_i))$ are squares in k. If P itself is a Weierstrass point, then $f_{2,P}((P) - (0))$ is of course not equal to $f_{2,P}(P) = 0$, we need to change the normalisation of $f_{2,P}$ in this case. This is done by using the uniformiser y which is of valuation 1 at P (any other uniformiser would work too). We have $e_{T,2}(P,P) = \frac{x-x(P)}{y^2}(P) = \frac{x-x(P)}{h(x)}(P) = \frac{1}{h'(x(P))}$. We also recover the well known criteria that a point of 2-torsion P is halvable if and only if $h'(x(P))$ is a square in k and the $x(P) - x(Q_i)$ are also squares.

(2) If $A[n]$ has no rational point in k, then multiplication by n is injective, hence bijective on $A_{\mathrm{tors}}(k)$.

(3) If $k = \mathbb{F}_q$ is a finite field, it is of course well known that we can use non degeneracy to treat the general case of n-divisibility on an abelian variety $A/\mathbb{F}_q$ even if $A[n] \not\subset A(\mathbb{F}_q)$ provided that $\mu_n \subset \mathbb{F}_q$ (this is a special case of Remark 5.10). Indeed, the Tate pairing on $A(\mathbb{F}_q)/nA(\mathbb{F}_q) \times A[n](\mathbb{F}_q) \to \mu_n$ is non-degenerate (see Section 4.5), so $P \in A(\mathbb{F}_q)$ is divisible by n if and only if the $e_{T,n}(P,Q)$ for $Q \in A[n](\mathbb{F}_q)$ are not all trivial.

Even if we don't have such a strong result for a general field k, the examples given above shows that the Tate pairing is still useful in the case of a generate field to test for divisibility. And the same argument as in Remark 5.10 shows that we cannot hope to have such a stronger result for a general field: if $A[n](k) = 0$, $[n]$ is injective on $A(k)$ but will not be surjective if $A(k)$ is infinite.

If P is n-divisible, and the Weil pairing $e_{W,n}$ restricted to $A[n](k) \times A[n](k)$ is non-degenerate (see also Remark 4.12), then we can use the Tate pairings to parametrize $[n]^{-1}(P)(k)$ by Remark 5.9. Indeed, the rational points in the fiber form

a torsor under $A[n](k)$, and the map ψ from Remark 5.9 gives an explicit bijection between this torsor and the μ_n^r-torsor $\{x_i^n = e_{T,n}(P, Q_i)\}$ where $(Q_1, \dots, Q_r)$ is a basis of $A[n](k)$.

Example 5.12 (Montgomery curves)**.** Let $E/k : y^2 = h(x)$ be an elliptic curve with a point of 2-torsion $P \in E[2](k)$. Then by the computation in Example 5.11, $e_{T,2}(P, P)$ is trivial if and only if $h'(x(P))$ is a square. But the cocycle description of the Tate pairing is given by $e_{T,2}(P, P) : \sigma \in \mathrm{Gal}(k) \mapsto e_{W,2}(\sigma P_0 - P_0, P)$ by Equation (10), where P_0 is any point in $E(\bar{k})$ such that $P = 2P_0$. So $e_{T,2}(P, P)$ is trivial if and only if $\sigma(P_0) = P_0$ or $\sigma(P_0) = P_0 + P = -P_0$ for all $\sigma \in \mathrm{Gal}(k)$, if and only if $x(P_0)$ is rational (i.e., P_0 projects to a rational point on the Kummer line), if and only if the subgroup $\langle P_0 \rangle$ is rational. In other words: $e_{T,2}(P, P)$ is trivial if and only if P lies in a rational cyclic subgroup of order 4. Note that conversely, if K is a rational cyclic subgroup of order 4, then the unique point of 2-torsion P in K has to be rational.

Note also that since $\mu_2 \subset k^*$, $H^1(k, \mu_2) = \mathrm{Hom}(\mathrm{Gal}(k), \mu_2)$, so a quadratic twist of E is given by a morphism $\mathrm{Gal}(k) \to \mu_2$, and if we take the morphism which sends σ to 1 if $\sigma(P_0) = P_0$, and to -1 if $\sigma(P_0) = -P_0$, then for the corresponding twist E', we have $P_0 \in E'(k)$.

By Proposition 5.1, if $f : E \to E_2 = E/\langle P \rangle$ is the isogeny with kernel $\langle P \rangle$, and $\tilde{f}$ the dual (contragredient) isogeny, then $e_{T,2}(P, P) = 1$ if and only if the fiber $\tilde{f}^{-1}(P)$ is a trivial μ_2-torsor, i.e., has a rational point. The isogeneous curve E_2 always has a rational point of 2-torsion Q_1 spanning $f(E[2])$. The remaining two points of 2-torsion Q_2, Q_3 are given precisely by the fiber $\tilde{f}^{-1}(P)$, so E_2 has full rational 2-torsion precisely exactly when $\tilde{f}^{-1}(P)$ is trivial. So an equivalent condition of $e_{T,2}(P, P) = 1$ is that E_2 has its 2-torsion rational. This can also be seen directly from our previous equivalent condition: if K is rational cyclic of order 4 containing P, then $f(K)$ is a rational subgroup of order 2 spanned either by Q_2 or Q_3 (and it is easy to check that there is always another cyclic rational subgroup K' containing P such that $f(K')$ is spanned by the other point). Conversely, if Q_2 is rational (equivalently if Q_3 is), then $f^{-1}(Q_2)$ is rational cyclic of order 4. We see that the Tate pairing gives information on the Galois action of the isogenous curve, we will expand on this in Section 5.3.

We recover the well known criterion for when an elliptic curve with a rational point of 2-torsion P can be put in Montgomery form with P sent to $(0, 0)$ [OKSoo]. Indeed if we send P to $(0, 0)$ the elliptic curve has equation $y^2 = x(x^2 + Ax + \gamma)$, and $\gamma = h'(0)$ and $e_{T,2}(P, P)$ are in the same class in $k^*/k^{*,2}$ by the above computation. So there is a change of variable such that $\gamma = 1$ if and only if $e_{T,2}(P, P)$ is trivial. In particular, we also recover that an elliptic curve has a Montgomery (with P sent to $(0, 0)$) form if and only if it has a cyclic rational subgroup of order four (containing P), if and only if $E/\langle P \rangle$ has a Legendre model.

Now if $k = \mathbb{F}_q$ is a finite field and P is the unique point of 2-torsion, then $e_{T,2}(P, P) = 1$ implies that there is already a rational point of 4-torsion above P by non degeneracy of the Tate pairing. This can be seen directly: if Q is another point of 2-torsion, then $\pi_q(Q) = Q + P$ because $\pi_q(Q) \neq Q$ by assumption. Since $e_{T,2}(P, P) = 1$, if we let P_0 any point such that $P = 2P_0$, then either $\pi_q(P_0) = P_0$ already, or $\pi_q(P_0) = P_0 + P$. In the latter case $\pi_q(P_0 + Q) = P_0 + Q + 2P = P_0 + Q$ so $P_0 + Q$ is a rational point of 4-torsion above P.

However, in the situation where all points of 2-torsion are rational, $e_{T,2}(P, P) = 1$ is not sufficient to have a rational point of 4-torsion above P, we also need $e_{T,2}(P, Q) = 1$ where Q is one of the other 2-torsion point. So we also recover the well known fact that either a

Montgomery curve over a finite field either has its full 2-torsion rational, or it has a rational point of 4-torsion.

Usually these facts are proved using the explicit doubling formula on an elliptic curve. The advantage of our more conceptual approach is that it can be easily generalised to other torsion orders or to abelian varieties. For instance, if $\mu_n \subset k$ and T is a point of exact order n in an elliptic curve E/k, and $n = n_1 n_2$ then the same reasoning as above shows that T is inside a rational cyclic subgroup K of order $n_1 n$ if and only if $e_{T,n}(n_2 T, T)$ is trivial. Indeed, if T' is a point such that $n_1 T' = T$, so that $nT' = n_2 T$, then $e_{T,n}(n_2 T, T)$ is trivial if and only if for each $\sigma \in \mathrm{Gal}(k)$, $\sigma(T') - T' \in \langle T \rangle$.

Example 5.13 (Iterating divisions)**.** If $A/\mathbb{F}_q$ is a principally polarised abelian variety, and $\mu_n \subset \mathbb{F}_q$, then we can try to iterate divisions by n as in Example 4.17. We know that $e_{T,n} : A(\mathbb{F}_q)/nA(\mathbb{F}_q) \times A[n](\mathbb{F}_q) \to \mu_n$ is non-degenerate. If $A[n](\mathbb{F}_q) \cap nA(\mathbb{F}_q) = 0$ (if n is prime this is the same as requiring that $A(\mathbb{F}_q)$ has no points of primitive n^2-torsion), then $A[n](\mathbb{F}_q) \simeq A(\mathbb{F}_q)/nA(\mathbb{F}_q)$ (we have injection by hypothesis, and they have the same cardinality), so $e_{T,n} : A[n](\mathbb{F}_q) \times A[n](\mathbb{F}_q) \to \mu_n$ is non-degenerate (see also Remark 4.23). Given a basis $(Q_1, \dots, Q_r)$ of $A[n](\mathbb{F}_q)$ (we assume that all Q_i have exact order n for simplicity, see Remark 5.5), then $T \in A[n](\mathbb{F}_q) \mapsto e_{T,n}(T, Q_i) \in \mu_n^r$ is surjective, since it is injective from our hypothesis and so bijective since both sets have the same cardinal.

Given a point $P \in nA(\mathbb{F}_q)$, $P_0 \in A(\mathbb{F}_q)$ such that $P = nP_0$, all other rational preimages are given by the $P_0 + T, T \in A[n](\mathbb{F}_q)$. We let $\Phi = (e_{W,n}(\cdot, Q_i))$. The torsor $\Phi_*[n]^{-1}(P_0 + T)$ differs from the torsor $\Phi_*[n]^{-1}(P_0)$ by the element $(e_{T,n}(T, Q_i)) \in \mu_n^r$. Hence, by the bijection above, there is exactly one $P_0 \in A(\mathbb{F}_q)$ such that $\Phi_*[n]^{-1}(P_0) = (e_{T,n}(P_0, Q_i))$ is trivial. By non degeneracy of the Tate pairing over finite fields, this implies that there is exactly one such P_0 such that $nP_0 = P$ and $[n]^{-1}P_0$ is trivial, i.e., $P_0 \in nA(\mathbb{F}_q)$.

If we now also assume that the Weil pairing $e_{W,n}$ restricted to $A[n](\mathbb{F}_q) \times A[n](\mathbb{F}_q)$ is non-degenerate, then by the discussion at the end of Example 5.11, $\Phi_*[n]^{-1}(P)$ is isomorphic to $[n]^{-1}(P)(\mathbb{F}_q)$ when $P \in nA(\mathbb{F}_q)$. Now we represent the torsor $[n]^{-1}(P)(\mathbb{F}_q)$ by the r representatives $\xi_i \in \mathbb{F}_q^*$ given by $\Phi_*[n]^{-1}(P)$. Since this torsor is trivial by assumption, all the ξ_i are n-powers in $\mathbb{F}_q^*$. In the case where $\mu_n \cap \mathbb{F}_q^{*,n} = 1$ also (i.e., n prime to $(q-1)/n$), then by Example 4.17, each ξ_i has a unique n-th root ξ_i' which is still an n-power. So there is a canonical choice of ξ_i', which corresponds by the isomorphism Ψ of Example 5.11 to a point $P_1 \in [n]^{-1}(P)(\mathbb{F}_q)$. On the other hand by the discussion above there is also a unique point $P_0 \in [n]^{-1}(P)(\mathbb{F}_q)$ such that P_0 is still in $nA(\mathbb{F}_q)$.

It is thus natural to ask about the relationship between P_0 and P_1. We leave that as an open question. Note that we cannot expect P_0 to be equal to P_1 in all cases because we could change our representative of the Tate pairing, this can change P_1 but will not change P_0. What we could hope to do is to find some explicit relationship for some explicit representatives. This would allow being able to find the iterated division by working entirely on the μ_n-side. Note that [CDHV22] have a conjectural a formula in the very close setting of iterated radical isogenies.

5.3. The Galois structure of the isogeneous abelian variety.

Example 5.14 (Probing the Galois action on the n-torsion of an isogenous elliptic curve)**.** Let $E/\mathbb{F}_q$ be an elliptic curve, with a rational point of exact order n, $P \in E[n](\mathbb{F}_q)$. Let $f : E \to E' = E/\langle P \rangle$ be the corresponding isogeny. Then using Proposition 5.1 and Example 5.7, from

$e_{T,n}(P,P)$, we can recover the Galois structure on $E'[n]$ as follows. Since $\tilde{f}(E'[n]) = \mathrm{Ker} f$ and $\mathrm{Ker}\tilde{f} = f(E[n]) \subset E'[n]$ we have that $E'[n] = \bigcup_{i\in\mathbb{Z}/n\mathbb{Z}} \tilde{f}^{-1}(iP)$. Since P is rational, π stabilizes each fiber $\tilde{f}^{-1}(iP)$. These fibers are μ_n-torsors, and their Galois structures are determined by the Tate pairings $e_{T,\tilde{f}}(iP,P) = e_{T,n}(iP,P)$ by Proposition 5.1. By bilinearity, the Tate pairing $e_{T,n}(P,P)$ is sufficient to recover the Galois action on each fiber.

More concretely, we have that $\mathrm{Ker}\tilde{f} = \tilde{f}^{-1}(0_E)$ is the Galois dual of $\mathrm{Ker} f \simeq \mathbb{Z}/n\mathbb{Z}$, so $\mathrm{Ker}\tilde{f} \simeq \mu_n$. Next, fix a basis $(Q_1,Q_2) \in E'[n](\overline{\mathbb{F}}_q)$. Without loss of generality we can assume that $Q_1 \in \mathrm{Ker}\tilde{f}$ and that $\tilde{f}(Q_2) = P$. We have $\pi_q(Q_1) = qQ_1$ by the isomorphism above. Let $\zeta_0 = e_{W,f}(P,Q_1)$, and fix a representative $\zeta \in \mu_n$ of the reduced Tate pairing $e_{T,n} = [\zeta] \in \mu_n/(\pi_q - 1)$. If $\zeta = \zeta_0^u$, then by Example 5.7, there is a point $Q_2' \in \tilde{f}^{-1}(P)$ such that $\pi_q Q_2' = Q_2' + uQ_1$.

Thus, up to changing Q_2 by Q_2', we have that on the basis (Q_1,Q_2) of $E'[n]$, π_q is given by $\begin{pmatrix} 0 & u \\ q & 1 \end{pmatrix}$. Hence we know the conjugacy class of π_q acting on $E'[n]$.

If (P_1,P_2) is a basis of $E(\mathbb{F}_q)$, then the same method allows to compute the Galois structure of $\tilde{f}^{-1}(E(\mathbb{F}_q))$ from the Tate pairings $e_{T,\tilde{f}}(P_i,P) = e_{T,n}(P_i,P)$, and in particular to recover the group structure of $E'(\mathbb{F}_q) \subset \tilde{f}^{-1}(E(\mathbb{F}_q))$.

Example 5.15 (Pairing the volcano)**.** As a special case of Example 5.14, assume that $n = \ell^e$ and that $\mu_{\ell^e} \subset \mathbb{F}_q$. Let $P \in E[\ell^e](\mathbb{F}_q)$, $E' = E/\langle P\rangle$ and let (Q_1,Q_2) be the basis of $E'[\ell^e]$ described above in Example 5.14. Then $\mu_{\ell^e} \simeq \mathbb{Z}/\ell^e\mathbb{Z}$ and $\pi(Q_1) = Q_1$. So by the description of the action of π_q on Q_2 above, if the reduced Tate pairing $e_{T,\ell^e}(P,P)$ is of exact order $\ell^{e'}$, then $E'[\ell^e](\mathbb{F}_q) \simeq \mathbb{Z}/\ell^e \times \mathbb{Z}/\ell^{e-e'}$.

More generally, if $\mu_{\ell^e}(\mathbb{F}_q) = \mu_{\ell^d}$, then the reduced Tate pairing $e_{T,\ell^e}(P,P)$ can be seen as living in μ_{ℓ^d} by Remark 4.19, and $e_{T,\ell^e}(P,P) = e_{T,\ell^d}(P,\ell^{e-d}P) \in \mu_{\ell^d}$. Then still by Example 5.14, if $e_{T,\ell^e}(P,P) \in \mu_{\ell^d}$ is of exact order $\ell^{e'}$, then $E'[\ell^d](\mathbb{F}_q) \simeq \mathbb{Z}/\ell^d\mathbb{Z} \times \mathbb{Z}/\ell^{d-e'}\mathbb{Z}$.

In particular, if E is ordinary, we can use the structure theorem of the torsion on ℓ-volcanoes of ordinary curves to probe the level of E' [MMSTV06; IJ13, §2]. We recall that if $E(\mathbb{F}_q)$ has a point of order ℓ, then the group structure of the rational ℓ^∞-torsion of the elliptic curves in the ℓ-volcano is the same at each volcano level. If E_0 is at the bottom level, $E_0[\ell^\infty(\mathbb{F}_q)] \simeq \mathbb{Z}/\ell^f\mathbb{Z}$ is cyclic. If E_1 is at level 1, $E_1[\ell^\infty(\mathbb{F}_q)] \simeq \mathbb{Z}/\ell^{f-1}\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$. At level 2, $E_2[\ell^\infty(\mathbb{F}_q)] \simeq \mathbb{Z}/\ell^{f-2}\mathbb{Z} \times \mathbb{Z}/\ell^2\mathbb{Z}$ and so on. And either the number of level is less then $f/2$, or f is even and at each level e above $f/2$, $E_e[\ell^\infty(\mathbb{F}_q)] \simeq \mathbb{Z}/\ell^{f/2}\mathbb{Z} \times \mathbb{Z}/\ell^{f/2}\mathbb{Z}$. In this case the level $f/2$ is then called the first level of stability, and then the level f, if it exists, is the second level of stability.

We see in particular that our curve E' above is at the level $d - e'$ if $e' > 0$, or at level $\geq d$ is $e' = 0$, i.e., the Tate pairing is trivial. This allows to probe strictly descending isogenies in the volcano (hence also find the horizontal or ascending ℓ-isogenies). Note also that once an isogeny starts descending in the volcano, all the remaining steps must be descending, so if we know the level of E and E' and the height of the volcano, we can recover the level of each of the intermediate curves when decomposing the ℓ^e-isogeny as e ℓ-isogenies.

Let us give some examples:

- If we are above the first stability level, $E[\ell^\infty](\mathbb{F}_q) \simeq \mathbb{Z}/\ell^{f/2}\mathbb{Z} \times \mathbb{Z}/\ell^{f/2}\mathbb{Z}$. Then certainly $\mu_{\ell^{f/2}} \subset \mathbb{F}_q$ by non degeneracy of the Weil pairing. We can probe isogenies

of degree $\ell^{f/2}$: if $P \in E[\ell^{f/2}]$, and $e_{T,\ell^{f/2}}(P,P)$ is of exact order $\ell^{e'}$, then $E' = E/\langle P\rangle$ has for rational $\ell^{f/2}$-torsion $E'[\ell^{f/2}](\mathbb{F}_q) = \mathbb{Z}/\ell^{f/2}\mathbb{Z} \times \mathbb{Z}/\ell^{f/2-e'}\mathbb{Z}$.

If E is at level $\geq f$, i.e., above the second stability level, all isogeneous curves E' have full rational $\ell^{f/2}$-torsion, so all self pairings $e_{T,\ell^{f/2}(P,P)}$ are trivial. We do not have enough torsion to probe deeper, a solution is to take a field extension of degree ℓ^v to get more torsion as in [IJ13, § 4].

If E is at level e with $f/2 \leq e < f$, then the strictly descending $\ell^{f/2}$-isogenies reach level $e - f/2$, so their kernel is generated by P with $e_{T,\ell^{f/2}}(P,P)$ of exact order $\ell^{e'}$ with $e' = f - e$. This is the maximal order a self Tate pairing can have: all other isogenies reach a level $\geq e - f/2$ so their corresponding self pairings have smaller order. In particular, if $e_{T,\ell^{f/2}}(P,P)$ is of order strictly smaller than ℓ^{f-e} for $P \in E[\ell^{f/2}]$, then $\ell^{f/2-1}P$ generates an ascending or horizontal isogeny (and conversely).

By bilinearity, this maximal order of the self pairings can be computed from the Tate pairings (and DLPs) $e_{T,\ell^{f/2}}(P_1,P_1), e_{T,\ell^{f/2}}(P_2,P_2), e_{T,\ell^{f/2}}(P_1,P_2), e_{T,\ell^{f/2}}(P_2,P_1)$, where (P_1,P_2) is a basis of $E[\ell^{f/2}]$ [IJ13, § 3].

- If we are at level $e < f/2$, below the first stability level, then $E[\ell^\infty](\mathbb{F}_q) = \mathbb{Z}/\ell^{f-e}\mathbb{Z} \times \mathbb{Z}/\ell^e\mathbb{Z}$. We have $\mu_{\ell^e} \subset \mathbb{F}_q$. The strictly descending ℓ^e-isogenies reach level 0, hence they are exactly those generated by $P \in E[\ell^e]$ with $e_{T,\ell^e}(P,P)$ of exact order ℓ^e. If the self pairing $e_{T,\ell^e}(P,P)$ is of order strictly less than ℓ^e for $P \in E[\ell^e]$, then $\ell^{e-1}P$ generates an ascending or horizontal isogeny (and conversely).

  We can also describe the level of $E/\langle P\rangle$ when P has order ℓ^u, $u > e$:
  - If $\mu_{\ell^{e+1}} \not\subset \mathbb{F}_q$ then we are at the top of the volcano (if we could climb up we would have the full ℓ^{e+1}-rational torsion on the isogeneous curve, which would imply $\mu_{\ell^{e+1}} \subset \mathbb{F}_q$). If $P \in E[\ell^\infty](\mathbb{F}_q)$ is of order ℓ^u, and $e_{T,\ell^u}(P,P)$ is of order $\ell^{e'}$ in $H^1(\mathbb{F}_q, \mu_{\ell^u}) \simeq \mu_{\ell^e}$, then the isogeneous curve is at level $e - e'$, so the first $(u - e')$ ℓ-steps in the ℓ^u-isogeny generated by P have to be horizontal, and the e' remaining ones are descending.
  - If $\mu_{\ell^{e+1}} \subset \mathbb{F}_q$, we let $f - e \geq d > e$ such that $\mu_{\ell^{f-e}}(\mathbb{F}_q) = \mu_{\ell^d}$. If (P_1,P_2) is a basis of $E[\ell^\infty](\mathbb{F}_q)$ with P_1 of order ℓ^{f-e} and P_2 of order ℓ^e, then by non degeneracy of the Tate pairing, since $e_{T,\ell^{f-e}}(P_2,P_1)$ is of order at most ℓ^e, then $e_{T,\ell^{f-e}}(P_1,P_1) = e_{T,\ell^d}(P_1, \ell^{f-e-d}P_1)$ has to be of exact order ℓ^d in $H^1(\mathbb{F}_q, \mu_{\ell^{f-e}}) \simeq \mu_{\ell^d}$. It follows that if $E' = E/\langle P_1\rangle$, $E'[\ell^d](\mathbb{F}_q) \simeq \mathbb{Z}/\ell^d\mathbb{Z}$, so E' is at level 0.

    Let d' be the height of the volcano (which means it has $d'+1$ levels). If $d' \leq f/2$ (this is the case if $d \leq f/2$ because then $d' \leq d \leq f/2$), the isogeny with kernel generated by P_1 has to climb the first $d' - e$ steps, stay horizontal for $f - 2d'$ steps, and then go down for the last d' steps. Otherwise, f is even and the volcano has height at least $f/2$. The isogeny with kernel generated by P_1 has to climb the first $f/2 - e$ steps, and then go down the remaining $f/2$ steps.

Anyway, this result is both simpler (once we have Proposition 5.1!) and refines most of the very interesting results of [IJ10; IJ13]. (One motivation of this paper, beside the application to multi-radical isogenies, was to get a better understanding of the underlying reason why Tate pairings are related to the volcano structure, as was proven in [IJ13]. Note also how [IJ13, Lemma 4.6.a, Lemma 4.7 and Lemma 4.6.b-c] are direct applications of Proposition 4.6 and

Remark 4.21 respectively. This is one advantage in having a more conceptual approach: the proofs are often simpler, and more general, than by directly using the explicit formulas.)

Example 5.16 (Probing the rational structure of an isogeneous abelian variety)**.** We can extend Example 5.14 to abelian varieties. Given a principally polarized abelian variety $A/\mathbb{F}_q$ and an n-isogeny $f : A \to B$ spanned by rational points $\mathrm{Ker} f = \langle P_1, \dots, P_g \rangle$, $P_i \in A(\mathbb{F}_q)$, then by Proposition 5.1 the Tate pairings $e_{T,n}(P, P_i)$ encode the Galois structure of the fiber $\tilde{f}^{-1}(P)$. In particular, given a basis $T_1, \dots, T_m$ of $A(\mathbb{F}_q)$, we can recover the global Galois structure of $\tilde{f}^{-1}(A(\mathbb{F}_q))$ from the Tate pairings $e_{T,n}(T_j, P_i)$. From this we can then extract the group structure of $B(\mathbb{F}_q)$ (via DLP and linear algebra), since $B(\mathbb{F}_q) \subset \tilde{f}^{-1}(A(\mathbb{F}_q))$. Note how we can probe $B(\mathbb{F}_q)$ from $A(\mathbb{F}_q)$ and $\mathrm{Ker} f$ without ever having to actually compute B.

The computation does not require $\mu_n \subset \mathbb{F}_q$ but it requires $\mathrm{Ker} f = \mathrm{Ker} f(\mathbb{F}_q)$. If that is not the case, we can work with an extension $\mathbb{F}_{q^d}$ where all the points of the kernel are defined. The Tate pairings over $\mathbb{F}_{q^d}$ then gives the $\mathbb{F}_{q^d}$-Galois structure of the fibers $\tilde{f}^{-1}(P)$, i.e., as a $\mathbb{Z}[\pi_q^d]$-module. This may not be enough to recover the $\mathbb{F}_q$-Galois structure of $\tilde{f}^{-1}(P)$. It depends on whether the base change map $H^1(\mathbb{F}_q, \mathrm{Ker}\tilde{f}) \to H^1(\mathbb{F}_{q^d}, \mathrm{Ker}\tilde{f})$ is injective. If it is, then $\tilde{f}^{-1}(P)$ seen as a $\mathrm{Ker}\tilde{f}$ torsor over $\mathbb{F}_{q^d}$ has a unique way to descend as a $\mathrm{Ker}\tilde{f}$ torsor over $\mathbb{F}_q$ (i.e., it has no non-trivial twists that become isomorphic over $\mathbb{F}_{q^d}$). Via Proposition 4.14, this map can be rewritten as $\mathrm{Ker}\tilde{f}/(\pi_q - 1) \to \mathrm{Ker}\tilde{f}/(\pi_{q^d} - 1)$, $\Xi(\pi_q) \mapsto \Xi(\pi_{q^d})$ where Ξ is a cocycle representing the torsor we are pulling back. By the cocycle property, this maps $[P] \in \mathrm{Ker}\tilde{f}/(\pi_q - 1)$ to $[P + \pi P + \cdots + \pi^{d-1}P] \in \mathrm{Ker}\tilde{f}/(\pi_{q^d} - 1)$. Given the Galois action on $\mathrm{Ker} f$, one can recover the Galois action on $\mathrm{Ker}\tilde{f}$ by duality, so injectivity of the base change map can be checked by linear algebra.

5.4. **Multi-radical isogenies.** We now prove the multi-radical isogeny conjecture. As a warm-up, we first obtain:

Corollary 5.17. *Under the notations of Section 2, the locus* $\{(P'_1, \dots, P'_g) \mid \tilde{f}(P'_i) = P_i\}$ *splits canonically as a* $\mu_n^{g^2}$*-torsor whose components have isomorphism classes given by the* $e_{T,n}(P_i, P_j)$.

Proof. We apply Proposition 5.1 to each of the g-torsors $\tilde{f}^{-1}(P_i)$; they are described by the $e_{T,\tilde{f}}(P_i, P_j)$ where we identify $\widehat{A}$ with A via the principal polarisation. But $e_{T,\tilde{f}}(P_i, P_j) = e_{T,n}(P_i, P_j)$ by Proposition 4.6. □

We now only need to take into account that we require our (P'_i) are required to also be isotropic to define a non backtracking isogeny.

Theorem 5.18. *The locus* $\mathcal{L}_f$ *of Lemma 2.2 splits canonically as a* $\mu_n^{g(g+1)/2}$*-torsor whose components are given by the* $e_{T,n}(P_i, P_j)$, $i \le j$.

Proof. Fix a trivialisation $(P'_1, \dots, P'_g)$ of $\mathcal{L}_f$ over an étale extension S' of S. Then given $T \to S'$, the other elements of $\mathcal{L}_f(T)$ are given by $(P'_1 + T_1, \dots, P'_g + T_g)$ where $T_i \in \mathrm{Ker}\tilde{f}(T)$ and the $P'_i + T_i$ are still isotropic. Since the P'_i are isotropic, and $\mathrm{Ker}\tilde{f}$ also, this condition amounts to $e_{W,n}(P'_i, T_j)e_{W,n}(T_i, P'_j) = 1$. By Equation (3) and biduality (Equation (4)), this is the same as requiring

$$\frac{e_{W,f}(P_i, T_j)}{e_{W,f}(P_j, T_i)} = 1. \tag{15}$$

These antisymmetry conditions defines a subgroup H of $\mathrm{Ker}\,\tilde{f}^g$ under which $\mathcal{L}_f$ is a torsor. We will show that H is isomorphic to $\mu_n^{g(g+1)/2}$.

Indeed, by Equation (15), the matrix of pairings $M = e_{W,f}(P_i, T_j)$ is antisymmetric, $M_{ij} = M_{ji}^{-1}$. So M is completely determined by the $M_{ij}, i \leq j$, and it is not hard to check that H is of degree $n^{g(g+1)/2}$.

Let $\Phi : H \subset \mathrm{Ker}\,\tilde{f}^g \to \mu_n^{g(g+1)/2}$ given on points by

$$(T_1, \dots, T_g) \mapsto (e_{W,\hat{f}}(T_j, P_i))_{j \leq i}.$$

We claim that this maps splits H, i.e., is an isomorphism. Indeed, it is injective: by biduality, $e_{W,f}(P_i, T_j) = e_{W,\hat{f}}(T_j, P_i)^{-1}$. If $T = (T_1, \dots, T_g) \in \mathrm{Ker}\,\Phi(T)$, then all $e_{W,f}(P_i, T_1) = 1$ so T_1 is trivial (since X/S is separated, two sections which coincide fibrally coincide on S). All $e_{W,f}(P_i, T_2)$ for $i \geq 2$ are trivial, but also $e_{W,f}(P_1, T_2) = 1$ by the antisymmetry condition, so T_2 is trivial, and so on. By considering the degree, Φ is surjective, hence bijective.

Let $p_j : H \to \mathrm{Ker}\,\hat{f}, (T_1, \dots, T_g) \mapsto T_j$ denote the j-th projection. If $j \leq i$, the component $e_{W,\hat{f}}(p_j(\cdot), P_i)$ of the map Φ factorizes through p_j. We also have a j-th projection map $\mathcal{L}_f \to \tilde{f}^{-1}(P_j)$ above p_j, hence an isomorphism $p_{j,*}\mathcal{L}_f \simeq \tilde{f}^{-1}(P_j)$ by Lemma 3.19. It follows by functoriality that $e_{W,\hat{f}}(p_j(\cdot), P_i)_*\mathcal{L}_f = e_{W,\hat{f}}(\cdot, P_i)_*\tilde{f}^{-1}(P_j) = e_{T,\hat{f}}(P_j, P_i)$. By Proposition 4.6, $e_{T,\hat{f}}(P_j, P_i) = e_{T,n}(P_j, P_i)$. Taking all the components $e_{W,\hat{f}}(p_j(\cdot), P_i)$ of Φ, we obtain that $\Phi_*\mathcal{L}_f$ is a $\mu_n^{g(g+1)/2}$-torsor whose components are given by the $e_{T,n}(P_j, P_i)$, $j \leq i$. □

Remark 5.19 (Formula)**.** It follows from Theorem 5.18, Lemma 3.31, and Example 3.32 that the locus $\mathcal{L}_f$ giving the non backtracking isogenies is described by n-radicals of the Tate pairings. When $S = \mathrm{Spec}\,k$ is a field, by Example 3.32, the $g(g+1)/2$ Tate pairings correspond to torsors given by $x_{ij}^n = \xi_{ij}, \xi_{ij} \in k^*$. If S is a scheme, then from Lemma 3.31 we know that a μ_n-torsor corresponds to a pair (L, α) where α is an isomorphism of $L^n \to O_S$. The radical interpretation is that we take n-radicands of the section $\alpha^{-1}(1) \in L^n$, the only difference is that these radicands will live in L rather than in O_S.

Over a field, we can use Lemma 4.13 and Remark 5.8 to give an explicit isomorphism between $\mathcal{L}_f$ and the torsors induced by the $e_{T,n}(P_i, P_j) = e_{T,\hat{f}}(P_i, P_j), i \leq j$, namely: $\Psi : (P'_1, \dots, P'_g) \in \mathcal{L}_f \mapsto g_{\tilde{f}, Z_{P_j}}((P'_i) - (0))$.

(It may be more convenient to use the torsors given by the $e_{T,n}(P_i, -P_j)$, in order to be able to evaluate the functions above without trouble. If X is a μ_n-torsor represented by $x^n = e_{T,n}(P_i, P_j)$, then $x \mapsto 1/x$ induces an isomorphism with μ_n-torsor represented by $x^n = e_{T,n}(P_i, -P_j)$ above the map $\mu_n \to \mu_n, \zeta \mapsto \zeta^{-1}$.)

Like in Remark 5.8, we can use Ψ to reformulate the proof of Theorem 5.18 as follows:

(1) Fix any $(P'_1, \dots, P'_g) \in \mathcal{L}_f$, namely $\tilde{f}(P'_i) = P_i$ and the P'_i are isotropic. Let H be the subgroup of $\mathrm{Ker}\,\tilde{f}^g$ satisfying by the antisymmetry conditions of Equation (15). Then all other points of $\mathcal{L}_f$ are given by $(P'_i + T_i)$, $(T_i) \in H$.

(2) The map $\Phi : H \to \mu_n^{g(g+1)/2}$ from Theorem 5.18 is an isomorphism.

(3) The map Ψ commutes (above Φ) with the action of H on the left and of $\mu_n^{g(g+1)/2}$ on the right, namely we check that if $\Psi((P'_1, \dots, P'_g)) = (x_{ij})$, then $\Psi(P'_i + T_i) = (x_{ij} e_{W,\hat{f}}(P_i, T_j))$. This is immediate from Equation (6).

However, for applications to cryptography, we really want the inverse isomorphism Ψ^{-1}. Explicit formula will depend on the model chosen of course. In an upcoming work we will use [FLR11; LR22] to give explicit formulas for multi-radical isogenies of abelian varieties in the theta model.

Example 5.20 (Families)**.** Let $X_1(n)/\mathbb{Q}(\zeta_n)$ be the modular curve associated to the level subgroup $\Gamma_1(n)$. We will assume that n is large enough so that the corresponding modular stack has no inertia, so the universal elliptic curve with a point of order n does exists over the scheme $X_1(n)$. (In fact $n \geq 3$ is enough if we remove the curves with j-invariant 0 or 1728.)

Let $(\mathcal{E}, P)/X_1(n)$ be the universal elliptic curve and f the isogeny of kernel $\langle P \rangle$. Then by Theorem 5.18 there are universal radical formula ψ_1 parametrizing the fiber $\tilde{f}^{-1}(P)$ via the μ_n-torsor $e_{T,n}(P,P) \in H^1(X_1(n), \mu_n)$.

Assume we have computed a radical formula $\psi_{2,\eta}$ over the generic point η of $X_1(n)$. Since we can act on ψ_1 by the automorphism group μ_n, we can assume that $\psi_{1,\eta} = \psi_{2,\eta}$. Now assume that there is an open U over which we can extend $\psi_{2,\eta}$ to a morphism ψ_2 (i.e., points in U are points of "good reduction" of our formula). Then the locus $\psi_1 = \psi_2$ is a closed subscheme of U by separateness, it contains the generic point, so since $X_1(n)$ is reduced (because it is smooth over $\mathbb{Z}[1/n]$), $\psi_1 = \psi_2$ on U. So ψ_2 gives correct radical formula over U.

Note also that since we know that ψ_1 is defined everywhere, it is always possible to tweak our explicit formula for $\psi_{2,\eta}$ so that they have good reduction on any point x (i.e., on a small affine neighborhood V of x) of $X_1(n)$.

Finally working over a familly S also allows for an evaluation/interpolation approach to compute radical isogeny formulas. Namely, we can evaluate Ψ on some fibers of S via Remark 5.19, and then invert it. This gives radical formulas on these fibers, that may not glue together because the automorphism group is μ_n. However, if we choose a rigidification over S, and we compute the radical formulas over fibers corresponding to this rigidification, then we can glue the formula together by interpolation.

Of course, the same reasoning holds in higher dimension.

References

[AGV72] M. Artin, A. Grothendieck, and J. Verdier. *Théorie des topos et cohomologie étale des schémas. (SGA4)*. 1972 (cit. on pp. 2, 6, 7).

[Art69] M. Artin. "Algebraization of formal moduli. I". In: *Global analysis (papers in honor of K. Kodaira)* (1969), pp. 21–71 (cit. on p. 4).

[BLR12] S. Bosch, W. Lütkebohmert, and M. Raynaud. *Néron models*. Vol. 21. Springer Science & Business Media, 2012 (cit. on p. 15).

[Bru11] P. Bruin. "The Tate pairing for abelian varieties over finite fields". In: *J. de theorie des nombres de Bordeaux* 23.2 (2011), pp. 323–328 (cit. on pp. 12, 22).

[CD21] W. Castryck and T. Decru. "Multiradical isogenies". In: *Cryptology ePrint Archive* (2021) (cit. on pp. 1, 3).

[CDHV22] W. Castryck, T. Decru, M. Houben, and F. Vercauteren. "Horizontal racewalking using radical isogenies". In: *Cryptology ePrint Archive* (2022) (cit. on pp. 3, 29).

[CDV20] W. Castryck, T. Decru, and F. Vercauteren. "Radical isogenies". In: *International Conference on the Theory and Application of Cryptology and Information Security*. Springer. 2020, pp. 493–519 (cit. on p. 3).

[Čes15] K. Česnavičius. "Topology on cohomology of local fields". In: *Forum of Mathematics, Sigma*. Vol. 3. Cambridge University Press. 2015, e16 (cit. on p. 15).

[DA70] M. Demazure and M. Artin. *Schémas en groupes (SGA3)*. Springer Berlin, Heidelberg, New York, 1970 (cit. on pp. 5, 15).

[EGM12] B. Edixhoven, G. van der Geer, and B. Moonen. *Abelian varieties*. Book project, 2012. URL: http://van-der-geer.nl/~gerard/AV.pdf (cit. on pp. 5, 6, 12).

[FLR11] J.-C. Faugère, D. Lubicz, and D. Robert. "Computing modular correspondences for abelian varieties". In: *Journal of Algebra* 343.1 (Oct. 2011), pp. 248–277. DOI: 10.1016/j.jalgebra.2011.06.031. arXiv: 0910.4668 [cs.SC]. URL: http://www.normalesup.org/~robert/pro/publications/articles/modular.pdf. HAL: hal-00426338. (Cit. on p. 34).

[FMR99] G. Frey, M. Muller, and H.-G. Ruck. "The Tate pairing and the discrete logarithm applied to elliptic curve cryptosystems". In: *Information Theory, IEEE Transactions on* 45.5 (1999), pp. 1717–1719 (cit. on pp. 12, 22).

[FR94] G. Frey and H.-G. Rück. "A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves". In: *Mathematics of computation* 62.206 (1994), pp. 865–874 (cit. on pp. 1, 12).

[Fu11] L. Fu. *Etale cohomology theory*. Vol. 13. World Scientific, 2011 (cit. on pp. 6, 7).

[Gir71] J. Giraud. *Cohomologie non abélienne*. Vol. 179. Springer Nature, 1971 (cit. on p. 4).

[GD64] A. Grothendieck and J. Dieudonné. "Eléments de géométrie algébrique". In: *Publ. math. IHES* 20.24 (1964), p. 1965 (cit. on pp. 4, 5, 7).

[Gro71] A. Grothendieck. "Revêtement étales et groupe fondamental (SGA1)". In: *Lecture Note in Math.* 224 (1971) (cit. on pp. 4, 6, 7).

[Heß04] F. Heß. "A note on the Tate pairing of curves over finite fields". In: *Archiv der Mathematik* 82.1 (2004), pp. 28–32 (cit. on p. 22).

[IJ10] S. Ionica and A. Joux. "Pairing the volcano". In: *Algorithmic number theory*. Springer, 2010, pp. 201–218 (cit. on p. 31).

[IJ13] S. Ionica and A. Joux. "Pairing the volcano". In: *Mathematics of Computation* 82.281 (2013), pp. 581–603 (cit. on pp. 30, 31).

[Lan58] S. Lang. "Reciprocity and Correspondences". In: *American Journal of Mathematics* 80.2 (1958), pp. 431–440 (cit. on p. 16).

[Lan56] S. Lang. "Algebraic groups over finite fields". In: *American Journal of Mathematics* 78.3 (1956), pp. 555–563 (cit. on p. 21).

[LR10] D. Lubicz and D. Robert. "Efficient pairing computation with theta functions". In: ed. by G. Hanrot, F. Morain, and E. Thomé. Vol. 6197. Lecture Notes in Comput. Sci. 9th International Symposium, Nancy, France, ANTS-IX, July 19-23, 2010, Proceedings. Springer–Verlag, July 2010. DOI: 10.1007/978-3-642-14518-6_21. URL: http://www.normalesup.org/~robert/pro/publications/articles/pairings.pdf. Slides: 2010-07-ANTS-Nancy.pdf (30min, International Algorithmic Number Theory Symposium (ANTS-IX), July 2010, Nancy), HAL: hal-00528944. (Cit. on p. 16).

[LR15] D. Lubicz and D. Robert. "A generalisation of Miller's algorithm and applications to pairing computations on abelian varieties". In: *Journal of Symbolic Computation* 67 (Mar. 2015), pp. 68–92. DOI: 10.1016/j.jsc.2014.08.

001. URL: http://www.normalesup.org/~robert/pro/publications/articles/optimal.pdf. HAL: hal-00806923, eprint: 2013/192. (Cit. on pp. 12, 16).

[LR22] D. Lubicz and D. Robert. "Fast change of level and applications to isogenies". In: *Research in Number Theory (ANTS XV Conference)* 9.1 (Dec. 2022). DOI: 10.1007/s40993-022-00407-9. URL: http://www.normalesup.org/~robert/pro/publications/articles/change_level.pdf. HAL: hal-03738315. (Cit. on p. 34).

[Mil04] V. S. Miller. "The Weil Pairing, and Its Efficient Calculation". In: *J. Cryptology* 17.4 (2004), pp. 235–261. DOI: 10.1007/s00145-004-0315-8 (cit. on p. 16).

[Mil06] J. S. Milne. *Arithmetic duality theorems*. Vol. 20. Citeseer, 2006 (cit. on p. 1).

[Mil16] J. S. Milne. "Étale Cohomology (PMS-33), Volume 33". In: *Étale Cohomology (PMS-33), Volume 33*. Princeton university press, 2016 (cit. on pp. 4, 7).

[MMSTV06] J. Miret, R. Moreno, D. Sadornil, J. Tena, and M. Valls. "An algorithm to compute volcanoes of 2-isogenies of elliptic curves over finite fields". In: *Applied Mathematics and Computation* 176.2 (2006), pp. 739–750 (cit. on p. 30).

[OKS00] K. Okeya, H. Kurumatani, and K. Sakurai. "Elliptic curves with the Montgomery-form and their cryptographic applications". In: *Public Key Cryptography*. Vol. 1751. Springer. 2000, pp. 238–257 (cit. on p. 28).

[Ols+06] M. C. Olsson et al. "Hom-stacks and restriction of scalars". In: *Duke Mathematical Journal* 134.1 (2006), pp. 139–164 (cit. on p. 15).

[Ray70] M. Raynaud. *Faisceaux amples sur les schémas en groupes et les espaces homogenes*. Vol. 119. Springer, 1970 (cit. on p. 4).

[Rob17] D. Robert. *Guide to Pairing-Based Cryptography*. 2017. URL: https://www.worldcat.org/title/guide-to-pairing-based-cryptography/oclc/971264380. Chapter 3 on « Pairings » with Sorina Ionica, and Chapter 10 on « Choosing Parameters » with Sylvain Duquesne, Nadia El Mrabet, Safia Haloui and Franck Rondepierre (cit. on p. 16).

[Rob21a] D. Robert. "Efficient algorithms for abelian varieties and their moduli spaces". HDR thesis. Université Bordeaux, June 2021. URL: http://www.normalesup.org/~robert/pro/publications/academic/hdr.pdf. Slides: 2021-06-HDR-Bordeaux.pdf (1h, Bordeaux). (Cit. on p. 16).

[Rob21b] D. Robert. *General theory of abelian varieties and their moduli spaces*. Mar. 2021. URL: http://www.normalesup.org/~robert/pro/publications/books/avtheory.pdf. Draft version. (Cit. on pp. 12, 16).

[Ryd13] D. Rydh. "Existence and properties of geometric quotients". In: *Journal of Algebraic Geometry* 22.4 (May 13, 2013), pp. 629–669. ISSN: 1056-3911, 1534-7486. DOI: 10.1090/S1056-3911-2013-00615-3. arXiv: 0708.3333 (cit. on p. 5).

[Sch05] E. F. Schaefer. "A new proof for the non-degeneracy of the Frey-Rück pairing and a connection to isogenies over the base field". In: *Computational aspects of algebraic curves* 13 (2005), pp. 1–12 (cit. on p. 22).

[Ser68] J. Serre. *Corps locaux*. Hermann Paris, 1968 (cit. on p. 18).

[Stacks] T. Stacks Project Authors. *Stacks Project*. https://stacks.math.columbia.edu. 2018 (cit. on pp. 4–7, 11, 15, 18).

INRIA Bordeaux–Sud-Ouest, 200 avenue de la Vieille Tour, 33405 Talence Cedex FRANCE
Email address: damien.robert@inria.fr
URL: http://www.normalesup.org/~robert/

Institut de Mathématiques de Bordeaux, 351 cours de la liberation, 33405 Talence cedex FRANCE