A FRAMEWORK FOR TATE MODULES OF ABELIAN VARIETIES UNDER ISOGENY

SARAH FREI, KATRINA HONIGS, AND JOHN VOIGHT

Abstract. We explain the linear algebraic framework provided by Tate modules of isogenous abelian varieties in a category-theoretic way.

1. Introduction

1.1. **Setup.** Let K be a number field with algebraic closure K^{al}. Let A be an abelian variety over K of dimension $g := \dim A \geq 1$. For example, we may take $A = E$ an elliptic curve over K, the case $g = 1$. Many important arithmetic features of A are reflected in its torsion subgroups $A[n](K^{\mathrm{al}}) \simeq (\mathbb{Z}/n\mathbb{Z})^{2g}$ for $n \geq 1$. The equations that define the n-torsion subgroup define a variety $A[n]$ of dimension zero over K; and the finite set of points $A[n](K^{\mathrm{al}})$ is defined over its splitting field, a minimal finite Galois extension of K denoted $K(A[n])$. The Galois group $\mathrm{Gal}(K(A[n]) \,|\, K)$ acts on $A[n]$ preserving the group law, so each element acts via an element of $\mathrm{Aut}(A[n](K^{\mathrm{al}}))$, giving an injective homomorphism

$$\mathrm{Gal}(K(A[n]) \,|\, K) \hookrightarrow \mathrm{Aut}(A[n](K^{\mathrm{al}})) \simeq \mathrm{GL}_{2g}(\mathbb{Z}/n\mathbb{Z}).$$

It is convenient to lift this to the absolute Galois group $\mathrm{Gal}_K := \mathrm{Gal}(K^{\mathrm{al}} \,|\, K)$ to obtain a linear representation

$$\overline{\rho}_{A,n} \colon \mathrm{Gal}_K \to \mathrm{Aut}(A[n](K^{\mathrm{al}})) \simeq \mathrm{GL}_{2g}(\mathbb{Z}/n\mathbb{Z}) \tag{1.1.1}$$

with $\ker \overline{\rho}_{A,n} = \mathrm{Gal}(K^{\mathrm{al}} \,|\, K(A[n]))$. Studying the Galois representation $\overline{\rho}_{A,n}$—for example, using techniques in number theory, group theory, and linear algebra—remains an essential technique for understanding A and is itself an interesting pursuit.

Rather than working with one n at a time, it is convenient to package all of them together by forming the adelic Tate module

$$\widehat{T}A := \varprojlim_{n} A[n](K^{\mathrm{al}}) \simeq \widehat{\mathbb{Z}}^{2g} \tag{1.1.2}$$

where $\widehat{\mathbb{Z}} := \varprojlim_n \mathbb{Z}/n\mathbb{Z} \simeq \prod_p \mathbb{Z}_p$, and the associated Galois representation

$$\rho_A \colon \mathrm{Gal}_K \to \mathrm{Aut}(\widehat{T}A) \simeq \mathrm{GL}_{2g}(\widehat{\mathbb{Z}}). \tag{1.1.3}$$

One obtains the representations $\overline{\rho}_{A,n}$ by composing ρ_A with reduction modulo n. Allowing denominators, we obtain the adelic Tate representation $\widehat{V}A := \widehat{T}A \otimes \mathbb{Q} \simeq \widehat{\mathbb{Q}}^{2g}$.

In this article, we unpack how the adelic Tate module (with its Galois action) changes under isogeny. This is a well-known, fundamental tool that is used frequently in arithmetic geometry. For example, in his work on local-global principles for torsion, Katz [K81,

Date: March 16, 2025.

2020 *Mathematics Subject Classification.* Primary: 11G10, 11F80. Secondary: 14K15, 11G05.

Key words and phrases. Abelian varieties, Tate modules, Galois representations.

p. 482] calls this the “dictionary between A''s which are l-power-isogenous to A over K and $\mathrm{Gal}(\overline{K}/K)$-stable *lattices* in $T_l(A) \otimes \mathbb{Q}$”. This dictionary as a bijection is also stated by Lan [Lan13, §1.3.5], again without proof. Here, we formulate this dictionary within a category-theoretic framework, so that future matrix calculations with Tate modules can be understood via commutative diagrams.

1.2. **Results.** Let A_0 be a (fixed) abelian variety over K. Let $\varphi\colon A_0 \to A$ be an isogeny over K^{al}. Then φ induces an natural inclusion $\widehat{T}\varphi\colon \widehat{T}A_0 \hookrightarrow \widehat{T}A$ of adelic Tate modules, which becomes an isomorphism $\widehat{V}\varphi\colon \widehat{V}A_0 \xrightarrow{\sim} \widehat{V}A$. Composing the natural inclusion $\widehat{T}A \hookrightarrow \widehat{V}A$ with $(\widehat{V}\varphi)^{-1}$, we obtain an inclusion $\widehat{T}A \hookrightarrow \widehat{V}A_0$ whose image is a sublattice denoted $\Lambda\varphi \subseteq \widehat{V}A_0$.

Our first main result is as follows (proven in more generality in Theorem 3.2.12). Recall that a functor is essentially bijective if it induces a bijection on the sets of isomorphism classes of objects.

Theorem 1.2.1. *The association $\varphi \mapsto \Lambda\varphi$ determines a functor Λ from*

$$\text{the category of isogenies } \varphi\colon A_0 \to A \text{ over } K^{\mathrm{al}}$$

to

$$\text{the category of sublattices of } \widehat{V}A_0.$$

The functor Λ has the following properties.

(a) *Λ is faithful and essentially bijective.*

(b) *The functor is equivariant with respect to the action of Gal_K, restricting to an equivalence between the category of abelian varieties that are isogenous (over K) to A_0 and the category of Gal_K-stable sublattices of $\widehat{V}A_0$.*

(c) *For an isogeny $\varphi\colon A_0 \to A$, there is a natural isomorphism $\ker\varphi \simeq \Lambda\varphi/\Lambda(\mathrm{id}_{A_0}) = \operatorname{coker}\widehat{T}\varphi$ that is Gal_K-equivariant.*

The morphisms in the two categories in Theorem 1.2.1 are described in section 3.2.

Remark 1.2.2. The whole setup generalizes to work with abelian schemes over an arbitrary scheme S, taking isogenies whose degree is a nonzerodivisor on the base and with the Galois group replaced by the étale fundamental group of S.

With this conceptual framework in mind, we then turn to some computations, explaining how to extract explicit change of basis matrices that explain how isogenous abelian varieties have conjugate Galois representations; we similarly track how polarizations change. We provide an extended example that came up in recent work [FHV23], giving an example of abelian surfaces A such that the ℓ-torsion of A and its dual $A^\vee$ are not isomorphic as Galois representations, i.e., $\rho_{A,\ell} \not\simeq \rho_{A^\vee,\ell}$.

1.3. **Contents.** We begin by providing background on abelian varieties and relevant structures such as polarizations and duality in section 2. In section 3 we explain (in a categorical context) how Galois actions on Tate modules change under isogenies, along with an illustrating example. We define the functor that satisfies Theorem 1.2.1 in section 3.2. We concretely work with this framework by providing change of basis matrices in section 4. In section 5, we work through a detailed example elaborating on the main result of [FHV23].

We hope that this will serve as a useful framework for others interested in studying Galois images of torsion subgroups and Tate modules of abelian varieties.

Acknowledgements. The authors would like to thank Asher Auel, Nils Bruin, and Bjorn Poonen for helpful comments. Frei was supported by an AMS-Simons Travel grant and by NSF grant DMS-2401601. Honigs was supported by an NSERC Discovery grant. Voight was supported by grants from the Simons Foundation: (550029, JV) and (SFI-MPS-Infrastructure-00008650, JV).

2. Background on abelian varieties

In this section, we set notation and give background on isogenies and Tate modules (section 2.1), dual abelian varieties (section 2.2), the Weil pairing (section 2.3), and polarizations (section 2.4). For further reading, a standard reference for abelian varieties is the book of Mumford [Mum70]; we also recommend Hindry–Silverman [HS00, Part A], the work of Milne [Mil86a, Mil08], and Birkenhake–Lange [BL04] for complex abelian varieties. To just get started with introduction via the perspective of elliptic curves, we suggest Silverman [Sil09]. We endeavour in this section to give a motivated version suitable for study in our formalism.

A key result is Proposition 2.1.4; here, we provide a simple proof.

2.1. Isogenies and Tate modules.

Let k be a field and let $p := \operatorname{char} k$, allowing $p = 0$. Let $k^{\mathrm{s}} \subseteq k^{\mathrm{al}}$ be a separable closure of k and an algebraic closure of k, respectively. Let A and A' be abelian varieties over k with common dimension $g := \dim A = \dim A'$. To avoid trivialities, we suppose that $g \geq 1$.

An *isogeny* $\varphi \colon A \to A'$ is a surjective homomorphism, or equivalently a homomorphism with finite kernel $\#(\ker \varphi)(k^{\mathrm{al}}) < \infty$. (Some authors take the zero map to be an isogeny; we do not.) An isogeny is *separable* if the corresponding finite extension $k(A) \supseteq k(A')$ of function fields is separable, or equivalently $(\ker\varphi)(k^{\mathrm{al}}) = (\ker\varphi)(k^{\mathrm{s}})$ and $[k(A) : k(A')] = \#(\ker\varphi)(k^{\mathrm{s}})$—analogous to the usual condition for a finite extension of fields to be Galois. (The reader may wish to focus on the case $k = \mathbb{Q}$ where all isogenies are separable; but the setup permits an arbitrary field.)

We pause to give a bit of motivation before proceeding further. Over the complex numbers $k = \mathbb{C}$, abelian varieties are complex tori, and isogenies can be understood using linear algebra. Indeed, we have an isomorphism $A(\mathbb{C}) \simeq V/\Lambda$ where $V \simeq \mathbb{C}^g$ is a complex vector space of dimension g and $\Lambda \subseteq V$ is a lattice of rank $2g$. (More precisely, we take $V = \operatorname{Hom}(\Omega^1(A), \mathbb{C})$ dual to the space $\Omega^1(A)$ of holomorphic 1-forms and $\Lambda = H_1(A, \mathbb{Z})$.) Then every isogeny of complex abelian varieties $V/\Lambda \to V'/\Lambda'$ is defined by a $\mathbb{C}$-linear isomorphism $V \to V'$ such that $\varphi(\Lambda) \subseteq \Lambda'$, and

$$\ker\varphi = \varphi^{-1}(\Lambda')/\Lambda \cong \Lambda'/\varphi(\Lambda) = \operatorname{coker}(\phi\colon \Lambda \hookrightarrow \Lambda'). \tag{2.1.1}$$

This is such a convenient description! We seek to replicate it over an arbitrary field k, and Tate modules allow us to consider (separable) isogenies in an analogous way.

We can begin linearizing, as in the introduction, by working with a torsion subgroup $A[n]$—but instead of working with just one, to complete the analogy we package them together, as follows.

Let $\ell \neq p = \operatorname{char} k$ be prime. The ℓ-*adic Tate module* of A is the projective limit

$$T_\ell A := \varprojlim_j A[\ell^j](k^{\mathrm{s}}) \simeq \mathbb{Z}_\ell^{2g}. \tag{2.1.2}$$

Concretely, an element of $T_\ell A$ is a sequence $P = (P_1, P_2, \dots)$ where $P_j \in A[\ell^j](k^{\mathrm{s}})$ and $\ell P_j = P_{j-1}$ for all $j \geq 2$.

A homomorphism $\varphi \colon A \to A'$ induces a homomorphism $T_\ell(\varphi) \colon T_\ell A \to T_\ell A'$, and when φ is an isogeny, the finiteness of the kernel implies that $T_\ell(\varphi)$ is injective.

For complex abelian varieties (when $k = \mathbb{C}$), we recover in this way the ℓ-adic part of the description above. We have

$$A[\ell^j](\mathbb{C}) = (\ell^{-j}\Lambda)/\Lambda \cong \Lambda/\ell^j\Lambda$$

for all j, so $T_\ell A \cong \Lambda \otimes \mathbb{Z}_\ell$ is the ℓ-adic completion of Λ. An isogeny $\varphi \colon V/\Lambda \to V'/\Lambda'$ induces a map of ℓ-adic Tate modules $T_\ell(\varphi) \colon \Lambda \otimes \mathbb{Z}_\ell \to \Lambda' \otimes \mathbb{Z}_\ell$ (applying the isogeny in each component, checking compatibility); and taking the ℓ-primary subgroups in (2.1.1) we see that

$$(\ker \varphi)(\mathbb{C})_\ell \cong (\Lambda' \otimes \mathbb{Z}_\ell)/(\varphi(\Lambda) \otimes \mathbb{Z}_\ell) \cong \operatorname{coker} T_\ell(\varphi). \tag{2.1.3}$$

The following proposition shows that (2.1.3) extends in general.

Proposition 2.1.4. *Let $\varphi \colon A \to A'$ be an isogeny of abelian varieties with kernel H. Let $H[\ell^\infty]$ be the ℓ-primary (or ℓ-Sylow) subgroup of H. Then $H[\ell^\infty]$ is naturally isomorphic to the cokernel of $T_\ell(\varphi) \colon T_\ell A \to T_\ell A'$.*

Proof. We will show, via the snake lemma, that this map is induced by a connecting homomorphism.

Abbreviate $A_j := A[\ell^j](K^{\mathrm{al}})$. For $n, r \geq 1$, the sequence

$$0 \to A_n \to A_{n+r} \xrightarrow{\cdot \ell^n} A_r \to 0$$

is exact. The maps are compatible, so for all $r \geq 1$ and taking the limit over n, we claim that the sequence

$$0 \to T_\ell A \to \varprojlim_n A_{n+r} \to A_r \to 0$$

is exact. The left map is just interpreting the same sequence in two different ways, which is visibly injective. Indeed, projective limits are always left exact so it suffices to show that the map to A_r is surjective. This map takes $(P_n)_n$ with $P_n \in A_{n+r}$ and maps to the common element $\ell P_1 = \ell^n P_n$ for all n. Hence, for any $Q = P_0 \in A_r$, a lift $(P_n)_n \in \varprojlim_n A_{n+r}$ is obtained by inductively choosing $P_n \in A_{n+r}$ satisfying $\ell P_n = P_{n-1}$ for $n \geq 1$.

Repeating the abbreviation with A' and H, we put the exact sequences together to get:

$$\begin{tikzcd}
0 \arrow[r] & T_\ell A \arrow[r] \arrow[d, "\varphi"] & \varprojlim_n A_{n+r} \arrow[r, "\cdot \ell^n"] \arrow[d, "\varphi"] & A_r \arrow[r] \arrow[d, "\varphi"] & 0 \\
0 \arrow[r] & T_\ell A' \arrow[r] & \varprojlim_n A'_{n+r} \arrow[r, "\cdot \ell^n"] & A'_r \arrow[r] & 0
\end{tikzcd} \tag{2.1.5}$$

We now apply the snake lemma. The kernel of the middle vertical map is 0 since $\ker\varphi$ is finite, so we obtain the exact sequence

$$0 \to H_r \xrightarrow{\delta} T_\ell A'/\varphi(T_\ell A) \to \varprojlim_n A'_{n+r}/\varprojlim_n \varphi(A_{n+r}). \tag{2.1.6}$$

To be explicit, the connecting map δ is defined as follows: for $P \in H_r$, lift to $(P_n)_n \in \varprojlim_n A_{n+r}$ (as in the end of the previous paragraph) and map

$$\delta(P) = \varphi((P_n)_n) = (\varphi(P_1), \varphi(P_2), \dots) \in T_\ell A'. \tag{2.1.7}$$

(We do not need to, but can check that $\ell^n\varphi(P_n) = \varphi(\ell^n P_n) = \varphi(P) = O$ so $\varphi(P_n) \in A'[\ell^n]$.)

Now we take $r \geq 1$ to be such that $\ell^r = \#H_\infty$; then $H_r = H_\infty$. To finish, we need to check that the final map in (2.1.6) is the zero map. Indeed, the class of $(Q_n)_n \in T_\ell A' \leq \prod_n A'_n$ maps to the class of $(Q_n)_n \in \prod_n A'_{n+r}$, so we want to show for all $n \geq 1$ and all $Q_n \in A'_n$ that $Q_n = \varphi(P'_n)$ for some $P'_n \in A_{n+r}$. But $\deg\varphi = \ell^r$ so there exists an isogeny $\psi\colon A' \to A$ such that $\ell^r = \varphi\psi$; therefore, if $P_n \in A_{n+r}$ is such that $\ell^r P_n = Q_n$ then $P'_n := \psi(P_n)$ has $\varphi(P'_n) = \ell^r P_n = Q_n$ and since $\ell^{n+r}P_n = \ell^n Q_n = O$ we have $\ell^{n+r}P'_n = \psi(\ell^{n+r}P_n) = O$ and so $P'_n \in A_{n+r}$ as desired.

Finally, the connecting isomorphism δ is natural, because the snake is natural. □

Example 2.1.8. Consider the case $g = 1$, so $A = E$ is an elliptic curve. Choose a basis $P_1 = (P_{1,n})_n$, $P_2 = (P_{2,n})_n$ for $T_\ell E$. Consider the isogeny $\varphi\colon E \to E'$ with kernel $H = H_\ell = \langle P_{1,1}\rangle$. That is, E' is the quotient $E/\langle P_{1,1}\rangle$. Then it is straightforward to verify that $P'_1 := (\varphi(P_{1,n+1}))_n$ and $P'_2 := (\varphi(P_{2,n}))_n$ is a basis for $T_\ell E'$.

As in the proof of Proposition 2.1.4, we compute the isomorphism $\delta\colon H \xrightarrow{\sim} \operatorname{coker}(T_\ell(\varphi))$, both groups isomorphic to $\mathbb{Z}/\ell\mathbb{Z}$. We lift $P_{1,1}$ to $(P_{1,2}, P_{1,3}\dots) \in T_\ell E$; so $\delta(P_{1,1})$ is the class of $(\varphi(P_{1,n+1}))_n = P'_1 \in T_\ell E'$ in $\operatorname{coker}(T_\ell\varphi)$.

As in the introduction, we simultaneously keep track of all ℓ-adic Tate modules (where $\ell \neq p$) as follows. Let

$$\widehat{\mathbb{Z}}' := \prod_{\ell\neq p} \mathbb{Z}_\ell \tag{2.1.9}$$

be the prime-to-p profinite completion of $\mathbb{Z}$. We define the *(prime-to-p) adelic Tate module* of A by

$$\widehat{T}A := \varprojlim_{\substack{n\\ p\nmid n}} A[n](k^{\mathrm{s}}) \simeq \prod_{\ell\neq p} T_\ell A. \tag{2.1.10}$$

(We write $\widehat{T}A$ instead of $\widehat{T}'A$ to ease notation.) Then $\widehat{T}A$ is a free $\widehat{\mathbb{Z}}'$-module of rank $2g$. The previous constructions extend to $\widehat{T}$ in each component, in particular from an isogeny $\varphi\colon A \to A'$ we obtain a homomorphism $\widehat{T}(\varphi)\colon \widehat{T}A \to \widehat{T}A'$. Let $\widehat{V}A := \widehat{T}A \otimes_{\mathbb{Z}} \mathbb{Q}$ be the *(prime-to-p) adelic Tate representation* of A.

Remark 2.1.11. In the adelic Tate module, if $p \neq 0$ we can also include the case $\ell = p$; but in this case, the p-adic Tate module in characteristic p behaves quite differently—it is quite meager in comparison, due to inseparability. One can use the Dieudonné module instead: see for example Fontaine [Fon77, Chapitre III].

We then obtain the following more general statement.

Proposition 2.1.12. *Let $\varphi\colon A \to A'$ be a separable isogeny of abelian varieties with kernel H. Then H is naturally isomorphic to the cokernel of $\widehat{T}(\varphi)\colon \widehat{T}A \to \widehat{T}A'$.*

Proof. The statement follows from Proposition 2.1.4 by comparing ℓ-primary parts. □

2.2. **Duals.** Associated naturally to A is the *dual abelian variety* $A^\vee := \mathbf{Pic}^0_A$. More precisely, the *relative Picard functor* $\underline{\mathrm{Pic}}_A$, which associates to a k-scheme S the group $\mathrm{Pic}(A \times_k S)$, is represented by a group scheme $\mathbf{Pic}_A$ over k, and $\mathbf{Pic}^0_A$ is the connected component containing the identity (the structure sheaf $\mathscr{O}_A$) [Kle14, section 3]. The group $\mathrm{Pic}^0(A) = \mathbf{Pic}^0_A(k)$ consists of those line bundles $\mathscr{L}$ on A such that $t_P^*\mathscr{L}_{k^{\mathrm{al}}} \simeq \mathscr{L}_{k^{\mathrm{al}}}$ for all $P \in A(k^{\mathrm{al}})$.

Over the complex numbers $k = \mathbb{C}$, the dual admits a concrete description. For $A(\mathbb{C}) \simeq V/\Lambda$ where $V \simeq \mathbb{C}^g$, let

$$V^* := \mathrm{Hom}_{\overline{\mathbb{C}}}(V, \mathbb{C}) \tag{2.2.1}$$

be the $\mathbb{C}$-vector space of $\mathbb{C}$-*antilinear* functionals: that is, $f \in V^*$ means $f\colon V \to \mathbb{C}$ is an $\mathbb{R}$-linear map such that $f(ax) = \overline{a}x$ for all $x \in V$ and $a \in \mathbb{C}$. (Antilinear functionals come naturally out of Hermitian forms, where one component is $\mathbb{C}$-linear but the other is $\mathbb{C}$-antilinear.) The imaginary part of the evaluation map

$$\begin{aligned} V^* \times V &\to \mathbb{C} \\ (f, x) &\mapsto \operatorname{Im} f(x) \end{aligned} \tag{2.2.2}$$

defines a canonical, nondegenerate, $\mathbb{R}$-bilinear form. The dual of Λ under this pairing, namely

$$\Lambda^* := \{f \in V^* : \operatorname{Im} f(x) \subseteq \mathbb{Z}\} \subseteq V^* \tag{2.2.3}$$

is a lattice and

$$A^\vee(\mathbb{C}) \simeq V^*/\Lambda^*. \tag{2.2.4}$$

So in simple linear algebraic terms, the dual abelian variety is obtained from the dual lattice (with respect to (2.2.2)).

Example 2.2.5. Suppose $E = V/\Lambda$ with $V = \mathbb{C}$ and $\Lambda = \mathbb{Z}\tau + \mathbb{Z}$, so $\omega_1 = \tau$, $\omega_2 = 1$ is a $\mathbb{Z}$-basis for Λ. Then $V^* = \mathbb{C}e$ where $e(x) = \overline{x}$, and it is straightforward to compute that a $\mathbb{Z}$-basis for Λ^* is $\omega_1^* = e/\operatorname{Im}(\overline{\tau})$, $\omega_2^* = -\tau e/\operatorname{Im}(\overline{\tau}) = \tau e/\operatorname{Im}(\tau)$.

Put a bit more abstractly, $A^\vee(\mathbb{C}) = \mathbf{Pic}^0_A(\mathbb{C})$ is the kernel of the map

$$\mathrm{Pic}(A) \simeq H^1(A, \mathscr{O}_A^\times) \to H^2(A, \mathbb{Z}), \tag{2.2.6}$$

the boundary map in the long exact sequence in cohomology induced by the exponential sequence

$$0 \to \mathbb{Z} \to \mathscr{O}_A \to \mathscr{O}_A^\times \to 1$$

(where $\mathbb{Z}$ is the constant sheaf) arising from $s \mapsto \exp(2\pi i s)$ for a section s of $\mathscr{O}_A$. For further details, see Mumford [Mum70, section II.9] or Swinnerton-Dyer [SD74, §8].

The universal line bundle $\mathscr{P}$ on $A \times A^\vee$ of the functor represented by $\mathbf{Pic}^0_A$ is called the *Poincaré bundle*: a point $Q \in A^\vee$ by definition gives a line bundle $\mathscr{L}_Q$ up to isomorphism, and $\mathscr{P}|_{A\times\{Q\}} \simeq \mathscr{L}_Q$. The bundle $\mathscr{P}$ furthermore gives rise to a natural isomorphism [Mum70, Corollary, p. 132]

$$\begin{aligned} i_A\colon A &\xrightarrow{\sim} (A^\vee)^\vee \\ P &\mapsto \mathscr{P}|_{\{P\}\times A^\vee}. \end{aligned} \tag{2.2.7}$$

A homomorphism $\varphi\colon A \to A'$ of abelian varieties induces a dual homomorphism

$$\varphi^\vee\colon (A')^\vee \to A^\vee$$

by pullback of line bundles, i.e. $\varphi^\vee := \varphi^*\colon \mathbf{Pic}^0_{A'} \to \mathbf{Pic}^0_A$. If φ is an isogeny, then so is $\varphi^\vee$. For an isogeny of complex abelian varieties $\varphi\colon V/\Lambda \to V'/\Lambda'$ so $\varphi(\Lambda) \subseteq \Lambda'$, the pullback

$$\begin{aligned} \varphi^\vee\colon (V')^*/(\Lambda')^* &\to V^*/\Lambda^* \\ f &\mapsto \varphi^*(f) = f \circ \varphi \end{aligned} \tag{2.2.8}$$

indeed gives $\varphi^\vee((\Lambda')^*) \subseteq \Lambda^*$, and we now have $\ker \varphi^\vee = \Lambda^*/\varphi^\vee((\Lambda')^*)$.

Example 2.2.9. For $\varphi\colon E \to E'$ an isogeny of elliptic curves, we recover the dual isogeny $\varphi^\vee\colon \mathbf{Pic}^0(E') \to \mathbf{Pic}^0(E)$ by restricting the pullback map $Q \mapsto \sum_{P \in \varphi^{-1}(Q)} P$ [Sil09, §III.6] (taking classes), then applying the canonical isomorphism $E \cong \mathbf{Pic}^0(E)$ and the same with E'.

2.3. **Weil pairing.** Recall that a finite-dimensional vector space and its dual admit a tautological perfect pairing. There is an analogous pairing as follows.

Theorem 2.3.1 (Tautological Weil pairing). *Let $n \in \mathbb{Z}_{>0}$ be coprime to the characteristic of k. Then there is a canonical perfect, bilinear pairing*

$$\langle \cdot, \cdot \rangle_n\colon A[n] \times A^\vee[n] \to \mu_n, \tag{2.3.2}$$

compatible with the action of Gal_k.

We call (2.3.2) the *tautological Weil pairing*. This pairing is an expression of *Cartier duality* (for torsion in abelian varieties), and it is equivalently expressed by a canonical isomorphism

$$\beta_n\colon A^\vee[n] \xrightarrow{\sim} \mathrm{Hom}(A[n], \mu_n), \tag{2.3.3}$$

Proof of Theorem 2.3.1. For a detailed proof and properties of the pairing, see Oda [Oda69, Theorem 1.1]. See also Antieau–Auel [AA21, §2.2].

A definition of the pairing (2.3.2) follows along similar lines as in the case of elliptic curves [Sil09, §III.8]: see Mumford [Mum70, p. 184–185] or Hindry–Silverman [HS00, Exercise A.7.8]. Given $Q \in A^\vee[n](k^{\mathrm{al}})$ corresponding to $\mathscr{L} = \mathscr{L}_Q \simeq \mathscr{O}(D)$, we will construct a map $A[n](k^{\mathrm{al}}) \to \mu_n(k^{\mathrm{al}})$ as follows. By assumption, both $\mathscr{L}^{\otimes n}$ and $[n]^*\mathscr{L}$ are trivial, and therefore $nD = \mathrm{div}(f)$ and $[n]^*D = \mathrm{div}(g)$ for some $f = f_Q, g = g_Q \in k^{\mathrm{al}}(A)^\times$. Since

$$\mathrm{div}(f \circ [n]) = [n]^*(nD) = n([n]^*D) = n\,\mathrm{div}(g) = \mathrm{div}(g^n),$$

the functions $f \circ [n]$ and g^n differ by a scalar constant. Now for all $X \in A(k^{\mathrm{al}})$ and $P \in A[n](k^{\mathrm{al}})$, we have $(f \circ [n])(X + P) = (f \circ [n])(X)$, and therefore $g^n(X+P)/g^n(X) = 1$ and $g(X+P)/g(X)$ is constant, independent of X (but may depend on Q). Thus, we obtain a map

$$\begin{aligned} \beta_n\colon A[n](k^{\mathrm{al}}) &\to \mu_n \\ P &\mapsto \frac{g(X+P)}{g(X)} \end{aligned} \tag{2.3.4}$$

(for any choice of $X \in A(k^{\mathrm{al}})$ such that $g(X)$ and $g(X+P)$ are defined and nonzero), and

$$\langle P, Q \rangle_n = g_Q(P)/g_Q(X+P)$$

completing the definition of the pairing. □

For $\ell \neq \operatorname{char} k$, the pairing with $n = \ell^j$ is compatible with the multiplication-by-ℓ map, so together they yield a perfect bilinear pairing on ℓ-adic Tate modules:

$$\langle \cdot, \cdot \rangle \colon T_\ell A \times T_\ell(A^\vee) \to \mu_{\ell^\infty}(k^{\mathrm{s}}) \simeq \mathbb{Z}_\ell. \tag{2.3.5}$$

We can also adelically put these together

$$\langle \cdot, \cdot \rangle \colon \widehat{T} A \times \widehat{T}(A^\vee) \to \mu'_\infty(k^{\mathrm{s}}) \simeq \widehat{\mathbb{Z}}'. \tag{2.3.6}$$

Given a separable isogeny $\varphi \colon A \to A'$ with $\ker \varphi \subseteq A[n]$, comparing the left- and right-kernels of the tautological Weil pairing yields a canonical perfect pairing

$$\ker \varphi \times \ker \varphi^\vee \to \mu_n. \tag{2.3.7}$$

Finally, the Weil pairing is equivariant with respect to the action of $\mathrm{Gal}_k := \mathrm{Gal}(k^{\mathrm{s}} \,|\, k)$, where Gal_k acts on μ_n by the mod n cyclotomic character ε_n [Sil09, section III.8] (see also Lemma 5.1.3). The points of $\mu_n(k^{\mathrm{al}}) = \langle \zeta_n \rangle$ are the nth roots of unity and the cyclotomic character

$$\varepsilon_n \colon \mathrm{Gal}_k \to \mathrm{Aut}(\mu_n(k^{\mathrm{al}})) \simeq (\mathbb{Z}/n\mathbb{Z})^\times, \tag{2.3.8}$$

is uniquely defined by $\sigma(\zeta_n) = \zeta_n^{\varepsilon_n(\sigma)}$ for all $\sigma \in \mathrm{Gal}_k$. Then, for all $\sigma \in \mathrm{Gal}_k$ and all $P \in A(k^{\mathrm{al}})$ and $Q \in A^\vee(k^{\mathrm{al}})$, we have

$$\langle \sigma(P), \sigma(Q) \rangle = \langle P, Q \rangle^\sigma = \varepsilon_n(\sigma) \cdot \langle P, Q \rangle. \tag{2.3.9}$$

2.4. **Polarizations.** If $\mathscr{L}$ is an ample line bundle on A, then the morphism

$$\begin{aligned} \varphi_{\mathscr{L}} \colon A &\to A^\vee \\ P &\mapsto \tau_P^* \mathscr{L} \otimes \mathscr{L}^{-1} \end{aligned} \tag{2.4.1}$$

is an isogeny, where $\tau_P \colon A \to A$ is the translation by P map, defined by $Q \mapsto Q + P$. (By contrast, note that if $\mathscr{L} \in \mathrm{Pic}^0(A)$, then (2.4.1) is the zero map.) This observation motivates the following definition.

Definition 2.4.2. An isogeny $\lambda \colon A \to A^\vee$ is a *polarization* if there is a finite separable field extension $K \supset k$ and an ample line bundle $\mathscr{L}$ on A_K so that $\lambda_K = \varphi_{\mathscr{L}}$.

A polarization λ is *principal* if it is an isomorphism, in which case we say that A is *principally polarized* by λ.

Polarizations can also be identified among isogenies over the ground field k: they are the isogenies $\lambda \colon A \to A^\vee$ where the line bundle $(\mathrm{id}, \lambda)^* \mathscr{P}$ on A is ample and λ is *symmetric*, meaning that $\lambda^\vee \circ i_A = \lambda$. Given such an isogeny $\lambda \colon A \to A^\vee$, the line bundle $\mathscr{L}$ as in Definition 2.4.2 can be constructed, after a possible finite separable extension, as a bundle satisfying the relation $[2]^* \mathscr{L} \simeq ((\mathrm{id}, \lambda)^* \mathscr{P})^2$ [Mum70, Theorem 2, p. 188].

Over the complex numbers, the existence of a polarization distinguishes abelian varieties among complex tori. Indeed, an ample line bundle on $A(\mathbb{C}) = V/\Lambda$ is specified by a positive definite Hermitian form $H \colon V \times V \to \mathbb{C}$ such that $E := \operatorname{Im} H$ has $E(\Lambda, \Lambda) \subseteq \mathbb{Z}$ (more generally, see the Appell–Humbert theorem for a linear-algebraic description of line bundles on A). The restriction $E|_\Lambda \colon \Lambda \times \Lambda \to \mathbb{Z}$ is alternating, and so there exists a $\mathbb{Z}$-basis of Λ in which the Gram matrix is

$$[E] = \begin{pmatrix} 0 & D \\ -D & 0 \end{pmatrix} \tag{2.4.3}$$

where $D = \operatorname{diag}(d_1, \dots, d_g)$ is diagonal with $d_i \geq 1$. Then $\ker \lambda \simeq (\mathbb{Z}/d_1\mathbb{Z})^2 \oplus \cdots \oplus (\mathbb{Z}/d_g\mathbb{Z})^2$, and so λ is principal if and only if $d_1 = \cdots = d_g = 1$.

Example 2.4.4. Elliptic curves are always principally polarized. We follow (2.4.1). For $\mathscr{L} = \mathscr{O}(D)$,

$$\tau_P^*\mathscr{L} \otimes \mathscr{L}^{-1} \simeq \mathscr{O}(\tau_{-P}(D)) \otimes \mathscr{O}(-D) \simeq \mathscr{O}(\tau_{-P}(D) - D). \tag{2.4.5}$$

Now let $D = [O]$ be the origin (divisor of degree 1); then

$$\tau_{-P}([O]) - [O] = [-P] - [O] \sim [O] - [P],$$

since $[P] + [-P] \sim 2[O]$. Plugging back in,

$$\tau_P^*\mathscr{L} \otimes \mathscr{L}^{-1} \simeq \mathscr{O}([O] - [P]). \tag{2.4.6}$$

Unfortunately, this is the *negative* of the natural isomorphism $\kappa \colon E \xrightarrow{\sim} E^\vee$ given by $P \mapsto [P] - [O]$ [Sil09, §III.6], and thus κ does not define a polarization—the sign is caused by moving between line bundles and divisors.

Example 2.4.7. If C is a nice (i.e., smooth, projective, geometrically integral) curve of genus g over k with $C(k) \neq \emptyset$, then its Jacobian $J := \mathbf{Pic}^0(C)$ is principally polarized by the theta divisor $\Theta \subset J$, the translate under the isomorphism $J \cong \mathbf{Pic}_C^{g-1}$ of the image of the natural morphism $\operatorname{Sym}^{g-1} C \to \mathbf{Pic}_C^{g-1}$. More generally, see Milne [Mil86b, section 1].

There is a second natural morphism $J \to J^\vee$, which is the inverse of the pullback morphism $j^* \colon J^\vee \to J$ induced by the inclusion $j \colon C \hookrightarrow J$. Again, there is a negative sign relating the two: $\varphi_{\mathscr{O}(\Theta)} = -(j^*)^{-1}$ [Mil86b, Lemma 6.9].

Now let $\lambda \colon A \to A^\vee$ be a polarization. Then we can plug it into the tautological Weil pairing, giving a (possibly degenerate) bilinear pairing on $A[n]$:

$$\begin{aligned} \langle \cdot, \cdot \rangle_{n,\lambda} \colon A[n] \times A[n] &\to \mu_n \\ (P, Q) &\mapsto \langle P, \lambda(Q) \rangle_n \end{aligned} \tag{2.4.8}$$

Taking λ to be the principal polarization in Example 2.4.4, we recover the usual formula for the Weil pairing [Sil09, section III.8] (noting how the sign is compensated for).

Lemma 2.4.9. *The (left or right) kernel of the Weil pairing for* λ *is exactly* $\ker \lambda$.

Proof. If $Q \in A[n]$ has

$$\langle P, Q \rangle_{n,\lambda} = \langle P, \lambda(Q) \rangle_n = 1$$

for all $P \in A[n]$, then $\lambda(Q) = O$ so $Q \in \ker \lambda_0$. The other containment is immediate. □

Given a polarization $\lambda_0 \colon A_0 \to A_0^\vee$ associated with an ample line bundle $\mathscr{L}$ (cf. Definition 2.4.2), we may construct other polarizations.

Definition 2.4.10. Let $f \colon A \to A_0$ be an isogeny. The *pullback* of λ_0 by f is the composition $f^*\lambda_0 := f^\vee \circ \lambda_0 \circ f$:

$$\begin{tikzcd} A \arrow[r, "f^*\lambda_0"] \arrow[d, "f"'] & A^\vee \\ A_0 \arrow[r, "\lambda_0"] & A_0^\vee \arrow[u, "f^\vee"'] \end{tikzcd}$$

The pullback $f^*\lambda_0$ is the polarization associated with the line bundle $f^*\mathscr{L}$.

Definition 2.4.11. Let $\varphi\colon A_0 \to A$ be an isogeny such that $\ker(\varphi)$ is isotropic under the pairing given by λ_0, and let d be the minimum value so that $\ker(\varphi) \subseteq \ker(d\lambda_0)$. The *pushforward* of λ_0 by φ is the map $\varphi_*\lambda_0$ filling in the following diagram.

(2.4.12)
$$\begin{tikzcd}
A_0 \arrow[r, "d\lambda_0"] \arrow[d, "g"'] & A_0^\vee \\
A \arrow[r, "g_*\lambda_0"] & A^\vee \arrow[u, "g^\vee"']
\end{tikzcd}$$

The diagram (2.4.12) can be filled in and $\varphi_*\lambda_0$ is a polarization by Mumford [Mum70, Corollary, p. 231]. The value of d in the definition of the pushforward of a polarization divides the exponent e_φ of φ since $A_0[e_\varphi] \subseteq \ker(e_\varphi\lambda_0)$.

3. Functorial aspects of Tate modules

Here we introduce the functor from abelian varieties that are isogenous quotients of a fixed abelian variety A_0 to sublattices of an associated adelic lattice, and we prove Theorem 1.2.1. In the next section, we will address common computational cases.

In section 3.1, we begin by showing a motivating example of how to conjugate the Galois action of an elliptic curve to find the action on the torsion of an isogenous curve. In section 3.2 we develop a formal categorical framework for our methods and prove our main result.

Throughout, let k be a field with characteristic $p \geq 0$.

3.1. A guiding example.

We begin with a simple example computing the Galois action on the ℓ-torsion of an elliptic curve that is isogenous to a curve whose Galois structure is known.

Let E be an elliptic curve over k and let $\ell \neq p$ be a prime number. Let $\varphi\colon E \to E'$ be a cyclic isogeny with the choice of basis $P_1, P_2 \in T_\ell E$ as in Example 2.1.8. We suppose that the point $P_{1,1} \in E[\ell](k)$ generating the kernel is a k-rational point, so the isogeny φ is defined over k as well. Let $\sigma \in \mathrm{Gal}_k$. Then $\sigma P_{1,1} = P_{1,1}$ and $\sigma P_{2,1} = b_1 P_{1,1} + d_1 P_{2,1}$ for some $b_1, d_1 \in \mathbb{F}_\ell$ with $d_1 \neq 0$, so the action of σ on $E[\ell]$ in this basis is given by

$$\begin{pmatrix} 1 & b_1 \\ 0 & d_1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_\ell).$$

(We are taking the column convention; the row convention is also used [RSZB+22, Remark 2.1].)

We now compute the action of σ on a basis for $E'[\ell]$ consisting of images of points under φ. In Example 2.1.8 we use the basis $P_1' := \{\varphi(P_{1,n+1})\}_n$, $P_2' := \{\varphi(P_{2,n})\}$ for $T_\ell E'$, so we may take our basis for $E'[\ell]$ to be $P_{1,1}' = \varphi(P_{1,2})$ and $P_{2,1}' = \varphi(P_{2,1})$. Note that it is not possible to choose points in $E[\ell]$ whose images under φ are a basis for $E'[\ell]$; we must choose at least one of the points in E to be ℓ^2-torsion. To determine the action of σ on $P_{1,1}'$, we need to know the action of σ on $P_{1,2}$. The action of σ on $E[\ell^2]$ is given by $\begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/\ell^2\mathbb{Z})$, where

$$\begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} \equiv \begin{pmatrix} 1 & b_1 \\ 0 & d_1 \end{pmatrix} \pmod{\ell}.$$

If we write $P'_{2,2} := \varphi(P_{2,2})$, then we have

$$\begin{aligned} \sigma P'_{1,1} &= \varphi(\sigma P_{1,2}) = \varphi(a_2 P_{1,2} + c_2 P_{2,2}) = 1P'_{1,1} + c_2 P'_{2,2}, \\ \sigma P'_{2,1} &= \varphi(\sigma P_{2,1}) = \varphi(b_1 P_{1,1} + d_1 P_{2,1}) = d_1 P'_{2,1}. \end{aligned} \tag{3.1.1}$$

We know that $c_2 = \ell c'$ for some $c' \in \mathbb{F}_\ell$, and $c_2 P'_{2,2} = c' P'_{2,1}$. The action of σ on $E'[\ell]$ is thus given by

$$\begin{pmatrix} 1 & 0 \\ c' & d_1 \end{pmatrix}.$$

It is interesting to see how the matrix giving the action of σ on $E'[\ell]$ differs from the one giving the action on $E[\ell]$: it is lower rather than upper triangular. Both b_1 and b_2 do not appear, but c_2 does have an effect. Although it is possible to find a point of $E'[\ell]$ fixed by σ, the point one might solve for has dependence on c' and d_1, which will vary as σ does, meaning that $E'[\ell]$ need not have any nontrivial k-points.

Now that we see how that goes, we will reinterpret the above by thinking of it as obtained from a *change of basis* on the ℓ-adic modules: see Example 4.2.3.

3.2. **From isogenies to Tate modules.** Let A_0 be a (fixed) abelian variety over k of dimension g; it will function like a basepoint. Let $\varphi\colon A_0 \to A$ be an isogeny. Given the action of the Galois group on $T_\ell A_0$, we may determine the action on $T_\ell A$ by identifying it with a sublattice of $V_\ell A_0 := T_\ell A_0 \otimes \mathbb{Q}_\ell$. This approach also facilitates comparing the Galois actions on more than one quotient of A_0.

In this section, we describe this as a functor from isogenies to sublattices. In order to introduce the category that keeps track of isogenies $\varphi\colon A_0 \to A$, we will use the following general categorical construction. Given a category and a particular choice of object, we may form a new category where we restrict our attention to morphisms into (resp. out of) that object, called a *slice* (resp. *coslice*) category.

Example 3.2.1. Let CRing be the category of commutative rings under ring homomorphisms, and let R be an object of CRing, i.e., a commutative ring. Then the objects and morphisms of the coslice category of CRing under R, denoted CRing^R, are R-algebras and R-algebra homomorphisms.

A natural way to form the category we are interested in is to first consider a category whose objects are abelian varieties and whose morphisms are isogenies, and then take the coslice category for A_0.

Let $\mathcal{I}_{k^{\mathrm{s}}} = \mathsf{AbVar}'_{k^{\mathrm{s}}}$ be the category whose objects are abelian varieties over k^{s} and whose morphisms are isogenies with degree prime to p. Then Gal_k acts on $\mathcal{I}_{k^{\mathrm{s}}}$ (i.e., its elements act as functors compatible with the usual axioms for a group), with fixed subcategory $\mathcal{I}_k$, the subcategory with objects and morphisms defined over k.

The objects of the coslice category of $\mathcal{I}_{k^{\mathrm{s}}}$ under A_0, denoted $\mathcal{I}_{k^{\mathrm{s}}}^{A_0}$, are isogenies whose domain is A_0; the morphisms of this coslice category are commuting triangles of isogenies:

$$\begin{tikzcd} & A_0 \arrow[dl, "\varphi"'] \arrow[dr, "\varphi'"] & \\ A \arrow[rr, "\psi"'] & & A'. \end{tikzcd} \tag{3.2.2}$$

Remark 3.2.3. In a coslice category, the identity morphism on the fixed object is an initial object of the coslice category.

Next we define the category of sublattices, where we will compute Galois actions.

Let $\mathcal{T}_{A_0}$ be the category whose objects are $\widehat{\mathbb{Z}}'$-lattices $T \subset \widehat{V}A_0$ containing $\widehat{T}A_0$ and whose morphisms are injective maps of lattices in $\widehat{V}A_0$

$$\begin{tikzcd} T \arrow[rr, hook] \arrow[dr, hook] & & T' \arrow[dl, hook'] \\ & \widehat{V}A_0 & \end{tikzcd} \tag{3.2.4}$$

or equivalently containments $T \hookrightarrow T'$. In particular, for an object T the quotient $T/\widehat{T}A_0$ is finite. We consider only injections of lattices in $\mathcal{T}_{A_0}$ since, as discussed in section 2.1, isogenies induce injective maps between Tate modules.

We now define a functor

$$\Lambda\colon \mathcal{I}_{k^{\mathrm{s}}}^{A_0} \to \mathcal{T}_{A_0}, \tag{3.2.5}$$

which shows how Tate modules of isogenous quotients of A_0 are identified with sublattices of $\widehat{V}A_0$.

For any $(\varphi\colon A_0 \to A) \in \operatorname{Ob}\mathcal{I}^{A_0}$, we have the injective $\widehat{\mathbb{Z}}'$-linear map $\widehat{T}\varphi\colon \widehat{T}A_0 \hookrightarrow \widehat{T}A$ and the isomorphism $\widehat{V}\varphi\colon \widehat{V}A_0 \xrightarrow{\sim} \widehat{V}A$.

Definition 3.2.6. We define the sublattice of $\widehat{V}A_0$ associated with $\widehat{T}A$ via φ to be

$$\Lambda\varphi := (\widehat{V}\varphi)^{-1}(\widehat{T}A),$$

which is the image of $\widehat{T}A$ in $\widehat{V}A_0$ under the dotted arrow in the following commutative diagram:

$$\begin{tikzcd} \widehat{T}A_0 \arrow[r, "\widehat{T}\varphi"] \arrow[d, "\otimes\mathbb{Q}"'] & \widehat{T}A \arrow[d, "\otimes\mathbb{Q}"] \arrow[dl, dashed] \\ \widehat{V}A_0 \arrow[r, "\sim", "\widehat{V}\varphi"'] & \widehat{V}A. \end{tikzcd} \tag{3.2.7}$$

We write the ℓ-adic part of $\Lambda\varphi$ as $\Lambda_\ell\varphi$.

For a morphism ψ in $\mathcal{I}_{k^{\mathrm{s}}}^{A_0}$ as in (3.2.2), we define

$$\Lambda\psi := (\widehat{V}\varphi)^{-1} \circ \widehat{T}\psi \circ \widehat{V}\varphi \tag{3.2.8}$$

giving a map $\Lambda\psi\colon \Lambda\varphi \to \Lambda\varphi'$.

The map $\Lambda\psi$ comes from the commutative diagram (3.2.9). The longer diagonal dotted arrow factors through the shorter diagonal arrow via $\widehat{T}\psi$. The map $\Lambda\psi$ is the image of $\widehat{T}\psi$

in $\widehat{V}A_0$ via the dotted arrows:

$$\begin{tikzcd}
\widehat{T}A_0 \arrow[r, "\widehat{T}\varphi"] \arrow[rr, bend left, "\widehat{T}\varphi'"] \arrow[d] & \widehat{T}A \arrow[r, "\widehat{T}\psi"] \arrow[d] \arrow[dl, dashed] & \widehat{T}A' \arrow[d] \arrow[dll, dashed] \\
\widehat{V}A_0 \arrow[r, "\sim", "\widehat{V}\varphi"'] \arrow[rr, bend right, "\widehat{V}\varphi'"'] & \widehat{V}A \arrow[r, "\sim", "\widehat{V}\psi"'] & \widehat{V}A'
\end{tikzcd} \tag{3.2.9}$$

In particular, $\Lambda\psi$ is injective and defines a morphism in the category $\mathcal{T}_{A_0}$.

Lemma 3.2.10. *The association $\varphi \mapsto \Lambda\varphi$ in Definition 3.2.6 defines a covariant functor $\Lambda \colon \mathcal{I}_{k^{\mathrm{s}}}^{A_0} \to \mathcal{T}_{A_0}$.*

Proof. We indeed get from applying Λ an object in the category $\mathcal{T}_{A_0}$, since an isogeny $A_0 \to A$ induces an inclusion $\widehat{T}A_0 \hookrightarrow \widehat{T}A$ giving an inclusion $\widehat{T}A_0 = \Lambda(\mathrm{id}_{A_0}) \subseteq \Lambda\varphi$.

Next we check functoriality: it follows from functoriality of the Tate module, since given given

$$\begin{tikzcd}
 & A_0 \arrow[dl, "\varphi"'] \arrow[d, "\varphi'"] \arrow[dr, "\varphi''"] & \\
A \arrow[r, "\psi"'] & A' \arrow[r, "\psi'"'] & A''
\end{tikzcd}$$

we have

$$\Lambda(\psi' \circ \psi) = \iota^{-1}(\widehat{T}(\psi' \circ \psi))\iota = \iota^{-1}(\widehat{T}(\psi') \circ \widehat{T}(\psi))\iota = \Lambda\psi' \circ \Lambda\psi$$

where $\iota = \widehat{V}\varphi$. (We could also see this by stacking commutative diagrams like (3.2.9).) Clearly Λ also preserves the identity. □

We are almost ready to prove our main result. We first prove a useful statement, recalling Proposition 2.1.4.

Proposition 3.2.11. *The association*

$$H \mapsto \Lambda(\varphi_H \colon A_0 \to A_0/H)$$

defines an inclusion-preserving bijection between

$$\textit{the set of subgroups } H \leq A_0[m](k^{\mathrm{s}})$$

and

$$\textit{the set of lattices } L \subseteq (1/m)(\widehat{T}A_0).$$

Proof. Write $L_0 := \Lambda(\mathrm{id}_{A_0}) = \widehat{T}A_0$. The multiplication by m map $A_0 \to A_0$ corresponds to the inclusion $L_0 \hookrightarrow (1/m)L_0$, and Proposition 2.1.12 gives a natural isomorphism $A_0[m](k^{\mathrm{s}}) \xrightarrow{\sim} (1/m)L_0/L_0$.

Let $H \leq H' \leq A_0(k^{\mathrm{s}})[m]$ be subgroups. Then we have a composition $A_0 \to A_0/H \to A_0/H' \to A_0$ with the outer map given by multiplication by m. By functoriality, this gives the containments of lattices

$$L_0 \subseteq L \subseteq L' \subseteq (1/m)L_0$$

where $L = \Lambda\varphi_H$ and $L' = \Lambda\varphi_{H'}$. This shows the map is inclusion-preserving and injective. To show it is surjective, let $L \subseteq (1/m)L_0$. Then $L/L_0 \leq ((1/m)L_0)/L_0 \simeq A_0[m](k^{\mathrm{s}})$ maps to a subgroup $H \leq A_0[m](k^{\mathrm{s}})$, and the map $\varphi_H \colon A_0 \to A_0/H$ also has kernel H, so $\Lambda\varphi_H = L$. (This map defines an inverse.) □

We now prove our main result, stated in the current level of generality.

Theorem 3.2.12. *The functor $\varphi \mapsto \Lambda\varphi$ has the following properties.*

(a) *Λ is faithful and essentially bijective.*

(b) *Λ is equivariant with respect to the action of Gal_k, so it restricts to a functor Λ_k between the category of abelian varieties that are isogenous (over k) to A_0 and the category of Gal_k-stable sublattices of $\widehat{V}A_0$. If k is a finite field or a number field, then in fact Λ_k is an equivalence of categories.*

(c) *Given an isogeny $\varphi \colon A \to A_0$, there is a natural isomorphism $\ker\varphi \simeq \Lambda\varphi/\Lambda\,\mathrm{id}_{A_0} = \operatorname{coker}\widehat{T}\varphi$ equivariant for Gal_k.*

Theorem 1.2.1 is the special case where the base field k is a number field.

Proof. We skip ahead and prove part (c): it is a restatement of Proposition 2.1.12 that for any isogeny $\varphi \colon A_0 \to A$, $\ker\varphi$ is isomorphic to $\operatorname{coker}\Lambda\varphi$.

Next, we prove part (a). Since $\widehat{T}$ is a faithful functor, so is Λ. To see that Λ is essentially surjective, let $L \supseteq L_0 := \Lambda(\mathrm{id}_{A_0})$ be a $\widehat{\mathbb{Z}}'$-lattice. Then the quotient L/L_0 is finite of exponent say m, so that $L \subseteq (1/m)L_0$. We then apply Proposition 3.2.11 to get a subgroup $H \leq A[m](k^{\mathrm{s}})$ such that $\varphi_H \colon A \to A/H$ has $\Lambda\varphi_H = L$.

To show that Λ is essentially injective, suppose that for two isogenies φ, φ' we have an isomorphism $\Lambda\varphi \simeq \Lambda\varphi'$ in $\mathcal{T}_{A_0}$. Therefore we have containments $\Lambda\varphi \subseteq \Lambda\varphi' \subseteq \Lambda\varphi$ so equality holds throughout. Therefore from (c) we have $\ker\varphi = \ker\varphi'$. In particular, the map φ' factors through φ

(3.2.13)

$$\begin{tikzcd}
& A_0 \arrow[dl, "\varphi"'] \arrow[dr, "\varphi'"] & \\
A \arrow[rr, dashed, "\psi"] & & A'
\end{tikzcd}$$

to give an isomorphism $\psi \colon A \to A'$ which yields an isomorphism from φ to φ' in $\mathcal{I}_{k^{\mathrm{s}}}^{A_0}$.

In general, it is open problem to decide if Λ is full: this says that every map of Tate modules (with source $\widehat{T}A_0$) arises from an isogeny with source A_0. This is the statement of the Tate isogeny conjecture for A_0.

For part (b), the functoriality of the Tate module implies equivariance under Gal_k and objects and isogeny fixed by Gal_k descend to k. We retain faithfulness, and the argument for essentially surjectivity in (a) extends as the quotient is Gal_k-stable so the subgroup H is also Gal_k-stable, hence φ_H is defined over k. Finally, we secure fullness since the Tate isogeny conjecture is known over finite fields by Tate and over number fields by Faltings. □

Remark 3.2.14. There is a functor from $\mathcal{I}_{k^s}^{A_0}$ to the category of Gal_k-representations that sends an object A to the Galois representation $\mathrm{Gal}_k \to \mathrm{Aut}(\widehat{T}A)$ and sends isogenies to equivariant maps. Then Theorem 3.2.12(b) shows that this functor factors through Λ. In the next section we furthermore choose change of basis matrices for these equivariant maps, using the lattice maps defined by Λ.

4. Change of basis

In this section, we explain how to compute with the Galois representation attached to the Tate module of an isogenous abelian variety in matrix terms. After the main definitions in section 4.1, we show how this works for isogenies defined by their kernel in section 4.2. We conclude in section 4.3 by addressing polarizations and dual isogenies.

4.1. **Bases.** With A_0 as a reference object, we choose a $\widehat{\mathbb{Z}}'$-basis β_0 for $L_0 := \Lambda\,\mathrm{id}_{A_0} = \widehat{T}A_0$. This gives us a $\widehat{\mathbb{Q}}'$-basis for the ambient space $\widehat{V}A_0$. Abbreviate $n := 2g$ throughout.

For any isogeny $\varphi\colon A_0 \to A$, we may then choose a basis β for $L := \Lambda\varphi$ and write this in terms of the basis β_0. We write these in the columns of a matrix $M = M_\varphi \in \mathrm{M}_n(\widehat{\mathbb{Q}}')$; in more standard linear algebra terms, $M = [\mathrm{id}]_\beta^{\beta_0}$ is the change of basis matrix for $\widehat{V}A_0$ from β to β_0. A different choice of basis β corresponds to column operations on M and is therefore given by multiplying M on the right by an element of $\mathrm{GL}_n(\widehat{\mathbb{Z}}')$, so we obtain a unique class in $\mathrm{M}_n(\widehat{\mathbb{Q}}')/\,\mathrm{GL}_n(\widehat{\mathbb{Z}}')$.

The inverse $M^{-1} = [\mathrm{id}]_{\beta_0}^{\beta}$ is the matrix which describes the inclusion $\widehat{T}A_0 \hookrightarrow \Lambda(\varphi)$, and in particular it has entries in $\widehat{\mathbb{Z}}'$. Now, if $\sigma \in \mathrm{Aut}(\widehat{T}A_0)$, we obtain a matrix $[\sigma]_{\beta_0} \in \mathrm{GL}_n(\widehat{\mathbb{Z}}')$ which describes its action on the basis β; we then have

(4.1.1)
$$\begin{tikzcd}
\widehat{T}A_0 \arrow[r, "\sigma"] \arrow[d] & \widehat{T}A_0 \arrow[d] \\
\Lambda\varphi \arrow[r, "\sigma"] & \Lambda\varphi
\end{tikzcd}$$

and thus

(4.1.2)
$$[\sigma]_\beta = [\mathrm{id}]_{\beta_0}^{\beta}[\sigma]_{\beta_0}[\mathrm{id}]_{\beta}^{\beta_0} = M^{-1}[\sigma]_{\beta_0}M.$$

The *Hermite normal form* (an integral echelon form) gives a unique choice for the matrix M. For convenience, we rescale M minimally by a positive integer writing $mM = M'$ with now $M' \in \mathrm{M}_n(\widehat{\mathbb{Z}}')$—we then divide back through by m at the end. By column operations, we may suppose that M' is lower triangular. We may further multiply by a unique element in $\widehat{\mathbb{Z}}'^{\times}$ so that the diagonal entries a_i are in $\mathbb{Z}_{>0}$ (rescaling the basis elements), and further that the entries in row i below the diagonal are in $\{0, \dots, a_i - 1\}$ (taking the elementary matrix which subtracts an appropriate multiple of the ith column). The matrix M' and hence M is then unique with these choices. However, this may not be the best for any individual calculation; and care must be taken so that this normalization is compatible with composition. In particular, we will not always write our change of basis matrices in this form.

This change of basis also gives us a way to work with compositions, as usual. For example, given another isogeny $\psi\colon A \to A'$, the change of basis matrix to a basis β' of $\widehat{T}A'$ for the composition $\psi\varphi\colon A_0 \to A'$ is obtained by multiplying the change of basis matrices:

(4.1.3)
$$[\mathrm{id}]_{\beta'}^{\beta_0} = [\mathrm{id}]_{\beta}^{\beta_0}[\mathrm{id}]_{\beta'}^{\beta}.$$

Example 4.1.4. Suppose $A = A_0$, i.e., φ is an endomorphism of A_0 (with finite kernel, so still an isogeny). In this case, we may choose $\beta = \beta_0$ and $M \in \mathrm{M}_n(\widehat{\mathbb{Z}}')$ is the matrix of $\widehat{T}\varphi$ in the basis β_0.

In particular, the multiplication by $m \geq 1$ map on A_0 has matrix $\operatorname{diag}(m, \ldots, m)$.

4.2. **Isogenies given in terms of kernels.** We now show how to exhibit a change of basis for an isogeny in terms of its kernel. This amounts to writing out a suitably explicit version of the connecting homomorphism δ in Proposition 2.1.4.

We start with the fixed basis β_0 for $\widehat{T}A_0$. Let $\varphi\colon A_0 \to A$ be an isogeny. Let $m \in \mathbb{Z}_{\geq 1}$ be such that $\ker \varphi \leq A_0[m](k^{\mathrm{s}})$. Let $x_1, \ldots, x_r \in \widehat{T}A_0$ be elements whose reduction modulo m generate $\ker \varphi$.

Lemma 4.2.1. *A generating set for $L = \Lambda\varphi$ is*

$$\beta_0 \cup \{x_1/m, \ldots, x_r/m\}.$$

Proof. This is just another way of writing out Proposition 3.2.11. □

To get a matrix, we proceed as follows. Let

$$[x_1]_{\beta_0}, \ldots, [x_r]_{\beta_0} \in (\widehat{\mathbb{Z}}')^n$$

be the coordinate vectors of the generators of $\ker \varphi$ in the basis β_0. Then by Lemma 4.2.1, a generating set is given by the columns of the identity matrix horizontally joined to the matrix with columns $(x_1/m, \ldots, x_r/m)$.

To get a basis, we then perform column echelonization of this matrix. Concretely, we choose a minimal set of generators for $\ker \varphi$ that is lower triangular when written as a matrix—this is again possible by column operations. It may have some zero entries along the diagonal, so we transport in the corresponding column from the identity matrix whenever a pivot is missing; we see that the remaining columns of the identity matrix are already in the span. This matrix gives a change of basis matrix M from the previous section.

Said in an algorithmic (recursive) way, a change of basis matrix $M = (a_{ij})_{i,j}$ is determined from right to left as follows. Dropping subscripts, let $P_1, \ldots, P_n$ be the image of the basis β_0 in $A_0[m](k^{\mathrm{s}})$. Let $b_{n,n} \in \mathbb{Z}_{\geq 1}$ be the smallest positive integer such that $b_{n,n}P_n \in \ker \varphi$, and let $a_{n,n} = b_{n,n}/m$. Let $b_{n-1,n-1} \in \mathbb{Z}_{\geq 1}$ be minimal such that $b_{n-1,n-1}P_{n-1} \in \ker \varphi + \langle P_n \rangle$, and then find minimal $b_{n,n-1} \in \mathbb{Z}/m\mathbb{Z}$ such that

$$b_{n-1,n-1}P_{n-1} + b_{n,n-1}P_n \in \ker \varphi. \tag{4.2.2}$$

We then continue this inductively and define $M = (b_{i,j}/m)_{i,j}$. Note that the matrix M produced in this way has entries in $(1/m)\mathbb{Z}$.

Example 4.2.3. Let $\varphi\colon E \to E'$ be the isogeny of elliptic curves given by Example 2.1.8 where P_1, P_2 is a basis for $T_\ell E$ and $\ker \varphi = \langle P_{1,1} \rangle$. We take $m = \ell$.

We have minimally $\ell P_{2,1} \in \ker \varphi$ so $b_{2,2} = \ell$. And $P_{1,1} \in \ker \varphi$ so $b_{1,1} = 1$ and $b_{2,1} = 0$. This gives the change of basis matrix

$$M = \begin{pmatrix} 1/\ell & 0 \\ 0 & 1 \end{pmatrix}.$$

In other words, $(1/\ell)P_1, P_2$ is a basis for $\Lambda\varphi$.

We can now describe the Galois action on $T_\ell E'$ by conjugating the action on $T_\ell E$:

$$\begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1/\ell & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & \ell b \\ c/\ell & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ c' & d_1 \end{pmatrix} \pmod{\ell}. \tag{4.2.4}$$

Despite the presence of the fraction $1/\ell$ in the action we computed, this outcome is still an element of $\mathrm{GL}_2(\mathbb{Z}_\ell)$, since $c \equiv 0 \pmod{\ell}$. As promised, this matrix conjugation recovers the action calculated by hand in section 3.1.

4.3. **Polarizations and duals.** In this section, we look at a special case where isogenies define polarizations or are dual to isogenies where we have already chosen how the functor acts.

Let $\lambda_0 \colon A_0 \to A_0^\vee$ be a polarization. Then by the matrix Frobenius form, as in (2.4.3) we may choose a basis for $\widehat{T}A_0$ such that the induced Tate pairing $\widehat{T}A_0 \times \widehat{T}A_0 \to \widehat{\mathbb{Z}}'$ is of the form

$$\begin{pmatrix} 0 & D \\ -D & 0 \end{pmatrix} \tag{4.3.1}$$

where $D = \mathrm{diag}(d_1, \ldots, d_g)$ and $d_1 \mid \cdots \mid d_g$ with $d_i \in \mathbb{Z}_{\geq 1}$.

Lemma 4.3.2. *The matrix (4.3.1) defines a change of basis matrix M^{-1} for $\Lambda\lambda_0$.*

Proof. We compute that the inverse to the Gram matrix is

$$\begin{pmatrix} 0 & -D^{-1} \\ D^{-1} & 0 \end{pmatrix}$$

(where $D^{-1} = \mathrm{diag}(1/d_1, \ldots, 1/d_g)$). To prove the lemma, we need to show that

$$-(1/d_1)P_{g+1}, \ldots, -(1/d_g)P_{2g}, (1/d_1)P_1, \ldots, (1/d_g)P_g$$

is a basis for $\Lambda\lambda_0$.

Let $m = d_g$, so that $\ker \lambda_0 \leq A_0[m]$ (since $d_1 \mid \cdots \mid d_g$). By Proposition 3.2.11, as elaborated upon in the previous section, it is equivalent to show that

$$-(m/d_1)P_{g+1,m}, \ldots, -(m/d_g)P_{2g,m}, (m/d_1)P_{1,m}, \ldots, (m/d_g)P_{g,m}$$

is a minimal generating set for $\ker \lambda_0$. These elements generate a subgroup of size $(d_1 \cdots d_g)^2 = \# \ker \lambda_0$, so it suffices to show that they belong to the kernel.

Recall from Lemma 2.4.9 that the kernel of the Weil pairing for λ_0 is $\ker \lambda_0$. With this, the verification is straightforward: e.g., for $i \leq g$,

$$\langle P_j, (m/d_i)P_i \rangle_{m,\lambda_0} \equiv 0 \pmod{m}$$

for all j: if $j \neq i + g$ then we get zero, otherwise we get $-d_i(m/d_i) \equiv 0 \pmod{m}$. □

Example 4.3.3. Let $\lambda_0 \colon A_0 \to A_0^\vee$ be a polarization with type $(d_1, \ldots, d_g)$ and let $\ell \neq p$ a prime. Let $D_\ell := \mathrm{diag}(\ell^{n_1}, \ldots, \ell^{n_g})$, where ℓ^{n_i} is the highest power of ℓ dividing d_i. Choosing a basis for $T_\ell A_0$ as explained above, the change of basis matrix for the ℓ-adic part of λ_0 is

$$M_{\lambda_0,\ell} = \begin{pmatrix} 0 & -D_\ell^{-1} \\ D_\ell^{-1} & 0 \end{pmatrix}.$$

If λ_0 is a principal polarization on an elliptic curve, then for any $\ell \neq p$, we get

$$M_{\lambda_0,\ell} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

If λ_0 is a $(1,3)$-polarization on an abelian surface (we will see $(1,\ell)$-polarizations in section 5), the Gram matrix for the Tate pairing, and hence $M_{\lambda_0,\ell}^{-1}$, is

$$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 3 \\ -1 & 0 & 0 & 0 \\ 0 & -3 & 0 & 0 \end{pmatrix}.$$

Next, let $\varphi\colon A \to B$ and suppose we have a change of basis matrix M_φ associated to φ. We may identify $\widehat{V}A^\vee, \widehat{V}B^\vee$ with the dual vector spaces of $\widehat{V}A, \widehat{V}B$; the dual of a basis for $\widehat{T}A \subset \widehat{V}A$ gives a basis for $\widehat{T}A^\vee$. With these choices, the change of basis matrix $M_{\varphi^\vee}$ for $\varphi^\vee\colon B^\vee \to A^\vee$ is the transpose of M_φ.

In the following example, we compute the pullback and pushforward of a principal polarization on an elliptic curve.

Example 4.3.4. Let $\varphi\colon E \to E'$ be the cyclic isogeny introduced in Example 2.1.8; we computed M_φ in Example 4.2.3. Choose a basis for $T_\ell E'$ so that, given the principal polarization $\lambda_0\colon E' \to E'^\vee$, the change of basis matrix is $M_{\lambda_0} = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, as shown in Example 4.3.3.

To compute the pullback of λ_0 by φ, we use the equality $\varphi^*\lambda_0 = \varphi^\vee \circ \lambda_0 \circ \varphi$ from Definition 2.4.10 along with (4.1.3), and so the change of basis matrix $M_{\varphi^*\lambda_0}$ is given by the following matrix:

$$M_\varphi M_{\lambda_0} M_{\varphi^\vee} = \begin{pmatrix} 1/\ell & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1/\ell & 0 \\ 0 & 1 \end{pmatrix}^T = \begin{pmatrix} 0 & -1/\ell \\ 1/\ell & 0 \end{pmatrix}.$$

This means that the pullback $\varphi^*\lambda_0$ is ℓ times the principal polarization on E (recalling that the Gram matrix for the polarization is given by $M_{\varphi^*\lambda_0}^{-1}$).

Next, suppose $\lambda_0\colon E \to E^\vee$ is the principal polarization on E. We may compute the pushforward of λ_0 by φ since the kernel of φ is isotropic under the pairing given by λ_0. As ℓ is the smallest value so that $\ker(\varphi) \subseteq \ker(\ell\lambda_0)$, we have the following equality from Definition 2.4.11: $\ell\lambda_0 = \varphi^\vee \circ \varphi_*\lambda_0 \circ \varphi$. This means $M_{\varphi_*\lambda_0}$ is given by the following matrix:

$$M_\varphi^{-1} M_{\ell\lambda_0} M_{\varphi^\vee}^{-1} = \begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1/\ell \\ 1/\ell & 0 \end{pmatrix} \begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Thus, the pushforward $\varphi_*\lambda_0$ is a principal polarization on the elliptic curve E'.

5. An extended example

In this section, we give an extended example demonstrating how to use the technical tools developed in sections 3-4 to compute the Galois action on abelian surfaces which are isogenous to a fixed abelian surface. We start with the construction of an abelian surface A, and then we will compute the Galois action on both $A[\ell]$ and on $A^\vee[\ell]$ by comparing $T_\ell A$ and $T_\ell A^\vee$ inside $V_\ell A_0$ for A_0 a product of elliptic curves isogenous to both A and $A^\vee$.

Fix a prime ℓ, and let E_1 and E_2 be elliptic curves over $\mathbb{Q}$ with $P \in E_1[\ell](\mathbb{Q})$ and $Q \in E_2[\ell](\mathbb{Q})$ $\mathbb{Q}$-rational ℓ-torsion points. Let

$$G := \langle (P,Q) \rangle \leqslant E_1 \times E_2 \quad \text{and} \quad A := (E_1 \times E_2)/G,$$

with the quotient map $q\colon E_1 \times E_2 \to A$. We will consider A with the polarization λ which is the pushforward under q (cf. Definition 2.4.11) of the principal product polarization λ_0 on $E_1 \times E_2$. In [FHV23, Lemma 2.1.2], we show that λ is a $(1,\ell)$-polarization, although we will not need that fact here.

This construction is considered in [FHV23, Construction 2.1.1], although that is not the first appearance of such a surface in the literature; it is described on MathOverflow [CP10], implicitly suggested as an exercise [Gor02, Exercise 6.35], and recently exhibited [BS23, Theorem 2.5].

5.1. **Computing the Galois action on A.** To understand the action of the Galois group on $A[\ell]$, we use the image of the Galois action on $T_\ell(E_1 \times E_2)$, along with a change of basis matrix for $\Lambda q \subset V_\ell(E_1 \times E_2)$, as explained in section 4.

In our example of interest (both here and in section 5.2), the isogenies all have degrees which are powers of ℓ, so we need only consider the ℓ-adic portion of the Tate modules in question. In particular, we will be interested in the mod ℓ representation, which we obtain by reducing modulo ℓ the Tate module.

For any elliptic curve E with a rational point $P \in E[\ell](\mathbb{Q})$, let P_1, P_2 be a basis for $T_\ell(E)$ such that $P_1 \bmod \ell = P$. Then the image of the ℓ-adic Galois representation

$$\rho_{E,\ell}\colon \operatorname{Gal}_{\mathbb{Q}} \to \operatorname{Aut}(T_\ell(E)(\mathbb{Q}^{\mathrm{al}})) \simeq \operatorname{GL}_2(\mathbb{Z}_\ell)$$

is contained in

$$\left\{ \begin{pmatrix} a & b \\ \ell c & d \end{pmatrix} \in \mathrm{M}_2(\mathbb{Z}_\ell) : a, d \in \mathbb{Z}_\ell^\times, a \equiv 1 \bmod \ell \right\} \leqslant \operatorname{GL}_2(\mathbb{Z}_\ell). \tag{5.1.1}$$

Moreover, reducing modulo ℓ, the representation

$$\bar{\rho}_{E,\ell}\colon \operatorname{Gal}_{\mathbb{Q}} \to \operatorname{Aut}(E[\ell](\mathbb{Q}^{\mathrm{al}})) \simeq \operatorname{GL}_2(\mathbb{F}_\ell)$$

has image contained in

$$\left\{ \begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix} \in \mathrm{M}_2(\mathbb{F}_\ell) : d \in \mathbb{F}_\ell^\times \right\} \leqslant \operatorname{GL}_2(\mathbb{F}_\ell).$$

With this observation in mind, we choose a basis $\{P_1, P_2, Q_1, Q_2\}$ for $T_\ell(E_1 \times E_2) \simeq \mathbb{Z}_\ell^4$ that satisfies the following:

- $P_1 \bmod \ell = P \in E_1[\ell](\mathbb{Q})$,
- $Q_1 \bmod \ell = Q \in E_2[\ell](\mathbb{Q})$,
- $\{P_1, P_2\}$ is a symplectic basis for $T_\ell E_1$, and
- $\{Q_1, Q_2\}$ is a symplectic basis for $T_\ell E_2$.

Then the Galois action on $(E_1 \times E_2)[\ell](\mathbb{Q}^{\mathrm{al}})$ has image contained in the subgroup

$$\left\{ \begin{pmatrix} 1 & b_1 & 0 & 0 \\ 0 & d_1 & 0 & 0 \\ 0 & 0 & 1 & b_2 \\ 0 & 0 & 0 & d_2 \end{pmatrix} \in \mathrm{M}_4(\mathbb{F}_\ell) : a_1, d_1, a_2, d_2 \in \mathbb{F}_\ell^\times \right\} \leqslant \operatorname{GL}_4(\mathbb{F}_\ell). \tag{5.1.2}$$

In fact, there is a further condition on elements in the image of $\bar{\rho}_{E_1 \times E_2, \ell}$, determined by the Galois equivariance of the Weil pairing. We summarize this in the following lemma.

Lemma 5.1.3. *For any elliptic curve E over $\mathbb{Q}$ and points $P, Q \in E[\ell](\mathbb{Q}^{\mathrm{al}})$, the cyclotomic character $\varepsilon_\ell \colon \mathrm{Gal}_{\mathbb{Q}} \to \mathbb{Z}_\ell^\times$ satisfies $\langle \bar\rho_{E,\ell}(\sigma)P, \bar\rho_{E,\ell}(\sigma)Q\rangle = \varepsilon_\ell(\sigma) \cdot \langle P, Q\rangle$, for all $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$, where $\langle \cdot, \cdot \rangle$ is the Weil pairing. Moreover, this implies that if $\bar\rho_{E,\ell}(\sigma) = M \in \mathrm{GL}_2(\mathbb{F}_\ell)$, then $\varepsilon_\ell(\sigma) = \det M$.*

Proof. The first claim follows directly from the Galois equivariance of the Weil pairing [Sil09, section III.8]. For the second statement, let $\{P_1, P_2\}$ be a symplectic basis for $E[\ell](\mathbb{Q}^{\mathrm{al}})$, so that, as in Example 4.3.3, the Gram matrix for the Weil pairing is

$$B := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Then for points $P = a_1P_1 + a_2P_2$ and $Q = b_1P_2 + b_2P_2$ in $E[\ell](\mathbb{Q}^{\mathrm{al}})$, we have

$$\langle \bar\rho_{E,\ell}(\sigma)P, \bar\rho_{E,\ell}(\sigma)Q\rangle = \begin{pmatrix} a_1 & a_2 \end{pmatrix} M^T B M \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = \det M \cdot \begin{pmatrix} a_1 & a_2 \end{pmatrix} B \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = \det M \cdot \langle P, Q \rangle.$$

Thus, $\varepsilon_\ell(\sigma) = \det M$. □

Consequently, for our elliptic curves E_1 and E_2, $\det \bar\rho_{E_1,\ell}(\sigma) = \det \bar\rho_{E_2,\ell}(\sigma)$ for all $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$, so $d_1 = d_2$. Lemma 5.1.3 also holds for any ℓ^n-torsion points (or more generally on $T_\ell(E)$), and this implies that $\rho_{E_1\times E_2,\ell}(\mathrm{Gal}_{\mathbb{Q}})$ is contained in

$$G_\ell := \left\{ \begin{pmatrix} a_1 & b_1 & 0 & 0 \\ \ell c_1 & d_1 & 0 & 0 \\ 0 & 0 & a_2 & b_2 \\ 0 & 0 & \ell c_2 & d_2 \end{pmatrix} \in \mathrm{M}_4(\mathbb{Z}_\ell) : \begin{array}{c} a_1, d_1, a_2, d_2 \in \mathbb{Z}_\ell^\times, \\ a_1 \equiv a_2 \equiv 1 \bmod \ell, \text{ and} \\ a_1d_1 - \ell b_1c_1 = a_2d_2 - \ell b_2c_2 \end{array} \right\} \leqslant \mathrm{GL}_4(\mathbb{Z}_\ell). \tag{5.1.4}$$

For convenience, we rewrite the elements in G_ℓ as

$$\begin{pmatrix} 1+x_1\ell & b_1+y_1\ell & 0 & 0 \\ w_1\ell & d+z_1\ell & 0 & 0 \\ 0 & 0 & 1+x_2\ell & b_2+y_2\ell \\ 0 & 0 & w_2\ell & d+z_2\ell \end{pmatrix} = \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix} \tag{5.1.5}$$

where:

- $d \in \{1, \ldots, \ell-1\}$,
- $b_1, b_2 \in \{0, \ldots, \ell-1\}$, and
- $w_i, x_i, y_i, z_i \in \mathbb{Z}_\ell$

still subject to the condition (Lemma 5.1.3) that

$$\det A_1 = \det A_2. \tag{5.1.6}$$

Now, we follow the discussion in section 4 to write down the change of basis matrix for $\Lambda_\ell q \subseteq V_\ell(E_1 \times E_2)$. Recall that $A = (E_1 \times E_2)/\langle (P, Q)\rangle$, so we can take $\{P_1, P_2, \frac{1}{\ell}(P_1 + Q_1), Q_2\}$ as a basis for $\Lambda_\ell q$. Then the change of basis matrix M_q is given by

$$M_q = \begin{pmatrix} 1 & 0 & 1/\ell & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1/\ell & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{5.1.7}$$

This choice does not follow the algorithmic approach given after Lemma 4.2.1 for finding the change of basis matrix, but it is a straightforward exercise to see how this choice differs from that by column operations. As in (4.1.2), to understand the Galois action on $A[\ell](\mathbb{Q}^{\mathrm{al}})$, we conjugate the elements (5.1.5) above by M_q, which gives

$$\begin{pmatrix} 1+x_1\ell & b_1+y_1\ell & x_1-x_2 & -b_2-y_2\ell \\ w_1\ell & d+z_1\ell & w_1 & 0 \\ 0 & 0 & 1+x_2\ell & b_2\ell+y_2\ell^2 \\ 0 & 0 & w_2 & d+z_2\ell \end{pmatrix}, \tag{5.1.8}$$

with the same conditions on the variables. To get the image of $\bar{\rho}_{A,\ell}\colon \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{GL}_4(\mathbb{F}_\ell)$, we reduce this subgroup modulo ℓ. That is, the image of $\bar{\rho}_{A,\ell}$ is contained in the subgroup

$$\left\{ \begin{pmatrix} 1 & b_1 & x_1-x_2 & -b_2 \\ 0 & d & w_1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & w_2 & d \end{pmatrix} \in \mathrm{M}_4(\mathbb{F}_\ell) : \begin{matrix} d \in \mathbb{F}_\ell^\times \\ b_i, w_i, x_i \in \mathbb{F}_\ell \end{matrix} \right\} \leqslant \mathrm{GL}_4(\mathbb{F}_\ell).$$

5.2. **Computing the Galois action on $A^\vee$.** Next, we compute the Galois action on $A^\vee[\ell](\mathbb{Q}^{\mathrm{al}})$, again using the framework developed in sections 3-4. To do this, we will use the isogeny between A and $A^\vee$ given by the $(1,\ell)$-polarization λ on A to relate their Galois representations.

First, as mentioned in section 5.1, the polarization λ on A is the pushforward of the principal polarization λ_0 on $E_1 \times E_2$ by the quotient isogeny q (cf. Definition 2.4.11), as shown in the following commutative diagram:

$$\begin{tikzcd} E_1 \times E_2 \arrow[r, "\ell\lambda_0"] \arrow[d, "q"] & (E_1 \times E_2)^\vee \\ A \arrow[r, "\lambda"] & A^\vee. \arrow[u, "q^\vee"'] \end{tikzcd} \tag{5.2.1}$$

This commutative diagram allows us to directly compare the actions of the Galois group on $T_\ell A$ and $T_\ell A^\vee$ as sublattices of $V_\ell(E_1 \times E_2)$. If M_λ is the change of basis matrix from a basis of $T_\ell A^\vee$ in $V_\ell A$, we must conjugate the elements (5.1.8), which describe the Galois action on $T_\ell A$, by M_λ. Alternatively (and equivalently), the change of basis matrix associated to the composition λq is given by $M_q M_\lambda$, as in (4.1.3), so we could conjugate the elements (5.1.5), which describe the Galois action on $T_\ell(E_1 \times E_2)$, by this product.

To find a change of basis matrix for λ which is compatible with the bases already chosen for $T_\ell(E_1 \times E_2)$ and $T_\ell A$, we use the equality $\ell\lambda_0 = q^\vee \circ \lambda \circ q$ from (5.2.1), which means $M_\lambda = M_q^{-1} M_{\ell\lambda_0} (M_q^T)^{-1}$. Following the discussion about change of basis matrices for polarizations in section 4.3 (cf. Example 4.3.4), we find

$$M_{\ell\lambda_0} = \begin{pmatrix} 0 & -1/\ell & 0 & 0 \\ 1/\ell & 0 & 0 & 0 \\ 0 & 0 & 0 & -1/\ell \\ 0 & 0 & 1/\ell & 0 \end{pmatrix}.$$

Thus,

$$M_\lambda = \begin{pmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \ell & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -\frac{1}{\ell} & 0 & 0 \\ \frac{1}{\ell} & 0 & 0 & 0 \\ 0 & 0 & 0 & -\frac{1}{\ell} \\ 0 & 0 & \frac{1}{\ell} & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \ell & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}^T = \begin{pmatrix} 0 & -\frac{1}{\ell} & 0 & \frac{1}{\ell} \\ \frac{1}{\ell} & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 \\ -\frac{1}{\ell} & 0 & 1 & 0 \end{pmatrix}.$$

One can check that the cokernel of M_λ^{-1}, which we recall from Proposition 2.1.4 is isomorphic to the kernel of λ, has ℓ^2 elements, confirming that the polarization type of λ is $(1, \ell)$. Finally, conjugating the Galois action on $T_\ell A$ by M_λ gives the subgroup

$$\left\{ M_\lambda^{-1} \begin{pmatrix} 1 + x_1\ell & b_1 + y_1\ell & x_1 - x_2 & -b_2 - y_2\ell \\ w_1\ell & d + z_1\ell & w_1 & 0 \\ 0 & 0 & 1 + x_2\ell & b_2\ell + y_2\ell^2 \\ 0 & 0 & w_2 & d + z_2\ell \end{pmatrix} M_\lambda \in \mathrm{M}_4(\mathbb{Z}_\ell) : \begin{array}{c} d \in \mathbb{F}_\ell^\times, \\ b_i \in \mathbb{F}_\ell, \\ w_i, x_i, y_i, z_i \in \mathbb{Z}_\ell \end{array} \right\}$$

$$= \left\{ \begin{pmatrix} d + z_1\ell & -w_1\ell & 0 & 0 \\ -b_1 - y_1\ell & 1 + x_1\ell & 0 & 0 \\ z_1 - z_2 & -w_1 & d + z_2\ell & -w_2 \\ b_2 + y_2\ell & 0 & -b_2\ell - y_2\ell^2 & 1 + x_2\ell \end{pmatrix} \in \mathrm{M}_4(\mathbb{Z}_\ell) : \begin{array}{c} d \in \mathbb{F}_\ell^\times, \\ b_i \in \mathbb{F}_\ell, \\ w_i, x_i, y_i, z_i \in \mathbb{Z}_\ell \end{array} \right\}$$

in $\mathrm{GL}_4(\mathbb{Z}_\ell)$. This subgroup reduces mod ℓ to the subgroup

$$\left\{ \begin{pmatrix} d & 0 & 0 & 0 \\ -b_1 & 1 & 0 & 0 \\ z_1 - z_2 & -w_1 & d & -w_2 \\ b_2 & 0 & 0 & 1 \end{pmatrix} \in \mathrm{M}_4(\mathbb{F}_\ell) : \begin{array}{c} d \in \mathbb{F}_\ell^\times \\ b_i, w_i, z_i \in \mathbb{F}_\ell \end{array} \right\} \leqslant \mathrm{GL}_4(\mathbb{F}_\ell).$$

Thus, the image of the mod ℓ representation $\bar{\rho}_{A^\vee,\ell} \colon \mathrm{Gal}_\mathbb{Q} \to \mathrm{Aut}(A^\vee[\ell](\mathbb{Q}^{\mathrm{al}})) \simeq \mathrm{GL}_4(\mathbb{F}_\ell)$ is contained in this subgroup.

Remark 5.2.2. The Galois action on $A^\vee$ can also be computed using the fact that $\rho_{A^\vee,\ell}$ is the contragredient representation to $\rho_{A,\ell}$ twisted by the cyclotomic character [FHV23, Lemma 2.4.1]. That result, given in [FHV23, Proposition 2.4.2], precisely matches this computation. The following determinantal condition (5.1.6) from the cyclotomic character is necessary to compare the two:

$$z_1 - z_2 = b_1w_1 - b_2w_2 - dx_1 + dx_2 \in \mathbb{F}_\ell.$$

References

[AA21] Benjamin Antieau and Asher Auel, *Explicit descent on elliptic curves and splitting Brauer classes*, preprint, 2021, `arXiv:2106.04291`. 2.3

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

[BS23] Pawel Borówka and Anatoli Shatsila, *Hyperelliptic genus 3 curves with involutions and a Prym map*, 2023, preprint, `arXiv:2308.07038`. 5

[CP10] Brian Conrad and Bjorn Poonen, *Non-principally polarized complex abelian varieties*, 2010, `https://mathoverflow.net/q/17014`. 5

[Fon77] Jean-Marc Fontaine, *Groupes p-divisibles sur les corps locaux*, Astérisque, no. 47-48, Société Mathématique de France, Paris, 1977. 2.1.11

[FHV23] Sarah Frei, Katrina Honigs, and John Voight, *On abelian varieties whose torsion is not self-dual*, 2023. 1.2, 1.3, 5, 5.2.2

[Gor02] Eyal Z. Goren, *Lectures on Hilbert modular varieties and modular forms*, CRM Monograph Ser., vol. 14, Amer. Math. Soc., Providence, RI, 2002. 5

[HS00] Marc Hindry and Joseph S. Silverman, *Diophantine geometry: an introduction*, Grad. Texts in Math., vol. 201, Springer, New York, 2000. 2, 2.3

[K81] Nicholas M. Katz, *Galois properties of torsion points on abelian varieties*, Inv. Math. **62** (1981), 481–502. 1.1

[Kle14] Steven L. Kleiman, *The Picard scheme*, Alexandre Grothendieck: a mathematical portrait, 35–74. Int. Press, Somerville, MA, 2014. 2.2

[Lan13] Kai-Wen Lan, *Arithmetic compactifications of PEL-type Shimura varieties*, London Math. Soc. Monogr. Ser., vol. 36, Princeton University Press, Princeton, 2013. 1.1

[Mil86a] J.S. Milne, *Abelian varieties,* Arithmetic geometry (Storrs, Conn., 1984), Springer-Verlag, New York, 1986, 103–150. 2

[Mil86b] J.S. Milne, *Jacobian varieties,* Arithmetic geometry (Storrs, Conn., 1984), Springer-Verlag, New York, 1986, 167–212. 2.4.7

[Mil08] James S. Milne, *Abelian varieties (v2.00)*, 2008, available at `http://www.jmilne.org/math/`. 2

[Mum70] David Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, vol. 5, reprint of 2nd ed., Hindustan Book Agency, New Delhi, 2008. 2, 2.2, 2.3, 2.4, 2.4

[Oda69] Tadao Oda, *The first de Rham cohomology group and Dieudonné modules*, Ann. Sci. École Norm. Sup. (4)2(1969), 63–135. 2.3

[RSZB+22] Jeremy Rouse, Andrew V. Sutherland, and David Zureick-Brown, *ℓ-adic images of Galois for elliptic curves over* $\mathbb{Q}$, appendix with John Voight, Forum Math., Sigma **10** (2022), e62. 3.1

[Sil09] Joseph H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Grad. Texts in Math., vol. 106, Springer, Dordrecht, 2009. 2, 2.2.9, 2.3, 2.3, 2.4.4, 2.4, 5.1

[SD74] H. P. F. Swinnerton-Dyer, *Analytic theory of abelian varieties*, London Mathematical Society Lecture Note Series, no. 14, Cambridge Univ. Press, London-New York, 1974. 2.2

Department of Mathematics, Dartmouth College, Kemeny Hall, Hanover, NH 03755, USA
Email address: `sarah.frei@dartmouth.edu`

Department of Mathematics, Simon Fraser University, 8888 University Drive, Burnaby, British Columbia V5A 1S6, Canada
Email address: `khonigs@sfu.ca`

Department of Mathematics, Dartmouth College, Kemeny Hall, Hanover, NH 03755, USA; Carslaw Building (F07), Department of Mathematics and Statistics, University of Sydney, NSW 2006, Australia
Email address: `jvoight@gmail.com`