Lattices in Tate modules

Bjorn Poonen*1, and Sergey Rybakovb,c,1

*Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139-4307; bLaboratory 13, Institute for Information Transmission Problems of the Russian Academy of Sciences, Moscow 127051, Russia; and cInterdisciplinary Scientific Center J.-V. Poncelet, Moscow 119002, Russia

Edited by Kenneth Ribet, Department of Mathematics, University of California, Berkeley, CA; received July 18, 2021; accepted October 15, 2021

Refining a theorem of Zarhin, we prove that, given a g-dimensional abelian variety X and an endomorphism u of X, there exists a matrix A ∈ M_{2g}(Z) such that each Tate module T_{ℓ}X has a Z_{ℓ}-basis on which the action of u is given by A, and similarly for the covariant Dieudonné module if over a perfect field of characteristic p.

abelian variety | Tate module | endomorphism | Dieudonné module

Introduction

Let X be an abelian variety of dimension g over a field k of characteristic p ≥ 0. Let End X be its endomorphism ring. Let End^0 X := (End X) ⊗ Q. Define Tate modules

\[ T_{ℓ} = T_{ℓ}X := \lim_{\to \ell \to X} [\ell^g]\mathbb{Q}(\mathbb{F}) \]

for each prime ℓ ≠ p

\[ V_{ℓ} = V_{ℓ}X := T_{ℓ}X \otimes_{\mathbb{Z}} \mathbb{Q}_{ℓ} \]

for each prime ℓ ≠ p

\[ T = T X := \bigoplus_{ℓ \neq p} T_{ℓ}X \]

\[ V = VX := TX \otimes_{\mathbb{Z}} Q \simeq \bigoplus_{ℓ \neq p} (V_{ℓ}X, T_{ℓ}X) \]

these are free rank 2g modules over Z_{ℓ}, Q_{ℓ}, \hat{Z}^{(p)} := \bigoplus_{ℓ \neq p} Z_{ℓ}, and

\[ A^{(p)} := \hat{Z}^{(p)} \otimes_{\mathbb{Z}} Q \simeq \bigoplus_{ℓ \neq p} (Q_{ℓ}, Z_{ℓ}) \]

respectively. If p > 0 and k is perfect, we have also a p-adic analog of T_{ℓ}X, namely, the covariant Dieudonné module M_{ℓ}(X), and we define

\[ M := M_{ℓ}(X) \]

M_{Q} := M \otimes_{\mathbb{Z}} Q = M[1/p] \]

\[ T_{W} := T \times M \]

\[ V_{W} := T_{W} \otimes_{\mathbb{Q}} V = V \times M_{Q} \]

these are free rank 2g modules over the ring of Witt vectors W := W(k), its fraction field

\[ K := W \otimes_{\mathbb{Q}} Q = W[1/p] \]

the product \( \hat{Z}^{(p)} \times W \), and

\[ A_{W} := (\hat{Z}^{(p)} \times W) \otimes_{\mathbb{Z}} Q = A \times Q \]

respectively.

Definition 1.1: Given rings R ⊆ R’ and corresponding modules L ⊆ L’, say that L is an R-lattice in L’ if L has an R-basis that is an R’-basis for L’.

Zarhin (ref. (1), Theorem 1.1) proved that, given u ∈ End^0 X, there exists a matrix A ∈ M_{2g}(Z) such that, for every ℓ ≠ p, there is a Q_{ℓ}-basis of V_{ℓ} on which the action of u is given by A; equivalently, there exists a u-stable Q-lattice in the (\bigoplus_{ℓ \neq p} Q_{ℓ})-module \( \prod_{ℓ \neq p} V_{ℓ} \). Our main theorem refines this, as follows.

Theorem 1.2. Let u ∈ End^0 X.

(a) There exists a u-stable Q-lattice V ⊂ V.

(b) There exists a u-stable Z-lattice T ⊂ T.

(c) If p > 0 and k is perfect, then there exists a u-stable Q-lattice V ⊂ V_{W}.

(d) If p > 0 and k is perfect, then there exists a u-stable Z-lattice T ⊂ T_{W}.

The following restatement of (b) answers a question implicit in ref. (1), Remark 1.2.

Corollary 1.3. Let u ∈ End X. Then there exists a matrix A ∈ M_{2g}(Z) such that, for every ℓ ≠ p, there is a Z_{ℓ}-basis of T_{ℓ}X on which the action of u is given by A, and such that, if p > 0 and k is perfect, there is a W-basis of M_{ℓ}(X) on which the action of u is given by A.

The characteristic 0 case of Theorem 1.2 can be proved by reducing to the case k = C and taking rational or integral homology (ref. (1), Remark 1.2). But pairs (X, u) in characteristic p > 0 cannot always be lifted to characteristic 0 (ref. (2), Example 14.5), so the general case does not seem to follow easily from this.

Proof

Lemma 2.1. Suppose that p > 0 and k is perfect. Let L be a finite extension of Q_{p}. Let N be an (L ⊗_{Q_{p}} K)-module with an automorphism \( F \) that is L-linear and K-semilinear with respect to the Frobenius automorphism \( \phi \) of K. Then N is free over L ⊗_{Q_{p}} K.

Proof: The residue field \( \ell \) of \( \ell \) is finite, so it has a largest subextension \( \ell’ \) embeddable in \( k \). Let \( L’ ⊆ L \) be the corresponding unramified extension of \( Q_{p} \). Then

\[ L’ ⊗_{Q_{p}} K \simeq \bigoplus_{ι ∈ I} K \]

Applying \( L ⊗_{L’} \) yields

\[ L ⊗_{Q_{p}} K \simeq \bigoplus_{ι ∈ I} L_{ι} \]

where each \( L_{ι} \) is a field since \( K \) is absolutely unramified and any tensor product \( ℓ ⊗_{p} k \) is a field. Now \( N = \bigoplus_{ι ∈ I} N_{ι} \), where each \( N_{ι} \) is a \( L_{ι} \)-vector space.

The action of \( \phi \) on \( K \) induces a permutation \( π \) of \( ℓ \) that is transitive since \( ℓ’/Q_{p} \) is Galois with group generated by the Frobenius automorphism. If \( i ∈ I \) and \( j = π(i) \), then the compatible actions of \( \phi \) of \( K \) and \( F \) on \( N \) induce compatible isomorphisms \( L_{ι} \cong L_{j} \) and \( N_{ι} \cong N_{j} \) for each \( i \), so \( \dim_{L_{ι}} N_{ι} = \dim_{L_{j}} N_{j} \). It follows, by transitivity of \( π \), that \( \dim_{L_{ι}} N_{ι} \) is independent of \( i \). Thus the module \( N = \bigoplus_{ι ∈ I} N_{ι} \) is free over \( L ⊗_{Q_{p}} K \simeq \bigoplus_{ι ∈ I} L_{ι} \).

Lemma 2.2. Let E be a number field contained in End^0 X. Let \( O = E ∩ End X \). Let \( h = (dim X)/|E : Q| \). Then

(i) The \( (E ⊗_{Q} Q_{ι}) \)-module \( V_{ι} \) is free of rank \( h \).

(ii) If p > 0 and k is perfect, then the \( (E ⊗_{Q} K) \)-module \( M_{Q} \) is free of rank \( h \).

Author contributions: B.P. and S.R. performed research and wrote the paper.

The authors declare no competing interest.

This open access article is distributed under the Creative Commons Attribution License 4.0 (CC BY).

To whom correspondence may be addressed. Email: poonen@math.mit.edu or rybakovsergey@gmail.com.

Published November 30, 2021.
(iii) For each $\ell \nmid p$ disc $O$, the $(O \otimes_{Z} Z_{\ell})$-module $T_{\ell}$ is free of rank $h$.

(iv) The $(E \otimes_{Q} A_{E}^{(p)})$-module $V$ is free of rank $h$.

(v) If $p > 0$ and $k$ is perfect, then the $(E \otimes_{Q} A_{W})$-module $V_{W}$ is free of rank $h$.

Proof:

(i) This is ref. (3), Theorem 2.1.1.

(ii) The following proof is essentially a combination of the proofs of ref. (4), Proposition 1.4.3 of (1) and ref. (3), Theorem 2.1.1. Write $E \otimes_{Q} Q_{p} \simeq \prod E_{i}$ for some finite extensions $E_{i}$ of $Q_{p}$. Correspondingly, $M_{Q} \simeq \bigoplus M_{j}$. The Frobenius automorphism of the Dieudonné module $M$ induces an $E_{i}$-linear and $K$-semilinear automorphism of $M$. By Lemma 2.1, the $(E \otimes_{Q} K)$-module $M$ is free.

On the other hand, by ref. (5) (p. 96), Corollary, for any $x \in E$, the characteristic polynomials of the actions of $x$ on $M_{Q}$ and $V_{i}$ are the same. Now repeat the proof of ref. (3), Theorem 2.1.1.

(iii) Fix $\ell \mid p$ disc $O$, where disc $O$ is the discriminant of $O$. For each prime $\lambda$ of $O$ dividing $\ell$, let $\lambda \subset E_{\ell}$ be the completion of $O$ at $\lambda$. Since $\ell \mid p$ disc $O$, the ring $O_{\lambda}$ is a discrete valuation ring with fraction field $E_{\lambda}$, and

$$E \otimes_{Q} Q_{p} \simeq \prod_{\lambda | \ell} E_{\lambda} \text{ and } O \otimes_{Z} Z_{\ell} \simeq \prod_{\lambda | \ell} O_{\lambda}.$$ 

These induce decompositions

$$V_{\ell} = \prod_{\lambda | \ell} V_{\lambda} \text{ and } T_{\ell} = \prod_{\lambda | \ell} T_{\lambda}.$$

By (i), $\dim_{E_{\ell}} V_{\ell} = h$. Since $T_{\ell}$ is a torsion-free finitely generated $O_{\ell}$-module that spans $V_{\ell}$, it is free of rank $h$ over $O_{\ell}$. Thus $T_{\ell} = \prod_{\lambda | \ell} T_{\lambda}$ is free of rank $h$ over $O \otimes_{Z} Z_{\ell} \simeq \prod_{\lambda | \ell} O_{\lambda}$.

(iv) We have $E \otimes_{Q} A_{E}^{(p)} = \prod (E \otimes_{Q} Q_{p}, O \otimes_{Z} Z_{p})$, so (iv) follows from (i) and (iii).

(v) Similarly, this follows from (i), (ii), and (iii).

Proof of Theorem 1.2:

(a) We work in the category of abelian varieties over $k$ up to isogeny. By ref. (1), Theorem 2.4, $u$ is contained in a subring of $E^{\infty}$ isomorphic to $\prod M_{r}(E_{i})$ for some number fields $E_{i}$. Then $X$ is isogenous to $\prod Y_{i}$ for some abelian varieties $Y_{i}$ with $E_{i} \subseteq E^{\infty}$. If we can find an $E_{i}$-stable $Q$-lattice $V_{i} \subseteq \prod Y_{i}$, then we may take $V = \prod V_{i}$. In other words, we have reduced to the case that $u \in E \subseteq E^{\infty}$ for some number field $E$. By Lemma 2.2 (iv),

$$V = P \otimes_{Q} (E \otimes_{Q} A_{E}^{(p)})$$

for some $Q$-vector space $P$. Then $V := P \otimes_{Q} E$ is a $u$-stable $Q$-lattice in $V$.

(b) Given $u \in E^{\infty}$, choose $V$ as in (a). We have

$$Q \cap \hat{Z}^{(p)} = Z[1/p],$$

which we interpret as $Z$ if $p = 0$. Then $V \cap T$ is a $Z[1/p]$-lattice in $T$. Since $Z[u] \subset \text{End } X$ is a finite $Z$-module, the $Z[u]$-submodule generated by any $Z[1/p]$-basis of $V \cap T$ is a $u$-stable $Z$-lattice.

(c) As in the proof of (a), we reduce to the case in which $u \in E \subseteq E^{\infty}$ for some number field $E$. By Lemma 2.2 (v),

$$\forall W = P \otimes_{Q} (E \otimes_{Q} A_{W})$$

for some $Q$-vector space $P$. Then $V := P \otimes_{Q} E$ is a $u$-stable $Q$-lattice in $V$.

(d) Let $V$ be as in (c). We have $Q \cap (\hat{Z}^{(p)} \times W) = Z$. Then $V \cap T_{W}$ is a $u$-invariant $Z$-lattice in $T_{W}$.

Generalizations and Counterexamples

In Theorem 1.2, suppose that, instead of fixing one endomorphism $u$, we consider a $Q$-subalgebra $R \subseteq E^{\infty}$ (or subring $R \subseteq E$) and ask for an $R$-stable $Q$-lattice (respectively, $Z$-lattice), that is, one that is $r$ stable for every $r \in R$.

1. If $R$ is contained in a subring of $E^{\infty}$ isomorphic to $\prod M_{r}(E_{i})$ for some number fields $E_{i}$, then the proof of Theorem 1.2 shows that an $R$-stable lattice exists.

2. Serre observed that if $X$ is an elliptic curve such that $E^{0} X$ is a quaternion algebra, then for $R = E^{\infty}$, there is no $R$-stable $Q$-lattice in any $V_{i}$, since $R$ cannot act on a two-dimensional $Q$-vector space.

3. If $R$ is assumed to be commutative, then the conclusions of Theorem 1.2 can still fail. For example, suppose that $Y$ is an elliptic curve such that $E^{0} Y$ is a quaternion algebra $B$, and $X = Y^{2}$, and

$$R = \left\{ \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} : a \in Q \text{ and } b \in B \right\} \subseteq M_{2}(B) = E^{0} Y.$$

The ideal $(0 0 0 0)$ has square zero, so $R$ is commutative. For each nonzero $b \in B$, we have

$$(0 \ b \ 0 \ 0) X = 0 \times Y, \text{ so } (0 \ b \ 0 \ 0) \forall X = 0 \times \forall Y,$$

which is of rank 2.

Suppose that there is an $R$-stable $Q$-lattice $V$ in $\forall X$. Let $U := V \cap (0 \times \forall Y)$, which is a $Q$-vector space of dimension at most 2. Then, for every nonzero $b \in B$, the image $(0 0 0 0)$ $V$ is a 2-dimensional $Q$-lattice in $0 \times \forall Y$, contained in $U$, and hence equal to $U$. Thus we obtain a $Q$-linear injection

$$(0 0 0 0) \hookrightarrow \text{Hom}(V/U, U) \subseteq \text{End } V.$$

It is an isomorphism since

$$\dim (0 0 0 0) = 4 = \dim \text{Hom}(V/U, U).$$

Since $\dim Q(0 0 0) V = 2$ for each nonzero $b \in B$, we have $\dim Q f(V) = 2$ for each nonzero $f$ in $\text{Hom}(V/U, U) \subseteq \text{End } V$, which is absurd. Thus there is no $R$-stable $Q$-lattice in $\forall X$.

Data Availability. There are no data underlying this work.

ACKNOWLEDGMENTS. This article arose out of a discussion initiated at the virtual conference "Arithmetic, Geometry, Cryptography and Coding Theory" hosted by the Centre International de Rencontres Mathématiques in Luminy in 2021. B.P. was supported, in part, by NSF Grants DMS-1601946 and DMS-2101040 and Simons Foundation Grants 402472 and 550033. We are grateful to a reviewer for suggesting that we prove Theorem 1.2 (c) and (d).
1. Y. G. Zarhin, On matrices of endomorphisms of abelian varieties. *Math. Res. Reports* 1, 55–68 (2020).

2. F. Oort, “Lifting algebraic curves, abelian varieties, and their endomorphisms to characteristic zero” in *Algebraic Geometry, Bowdoin, 1985: Proceedings of Symposia in Pure Mathematics*, S. J. Bloch, Ed. (American Mathematical Society, Providence, RI, 1987), vol. 46, pp. 165–195.

3. K. A. Ribet, Galois action on division points of abelian varieties with real multiplications. *Am. J. Math.* 98, 751–804 (1976).

4. C. L. Chai, B. Conrad, F. Oort, *Complex Multiplication and Lifting Problems* (Mathematical Surveys and Monographs, American Mathematical Society, Providence, RI, 2014), vol. 195.

5. M. Demazure, *Lectures on p-Divisible Groups* (Lecture Notes in Mathematics, Springer, 1972), vol. 302.