# LATTICES IN TATE MODULES

BJORN POONEN AND SERGEY RYBAKOV

Abstract. 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 $A \in \mathrm{M}_{2g}(\mathbb{Z})$ such that each Tate module $T_\ell X$ has a $\mathbb{Z}_\ell$-basis on which the action of $u$ is given by $A$.

## 1. Introduction

Let $X$ be an abelian variety of dimension $g$ over a field $k$ of characteristic $p \geq 0$. Let $\operatorname{End} X$ be its endomorphism ring. Let $\operatorname{End}^\circ X := (\operatorname{End} X) \otimes \mathbb{Q}$. Define Tate modules

$$T_\ell = T_\ell X := \varprojlim_n X[\ell^n](\overline{k}) \qquad V_\ell = V_\ell X := T_\ell X \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \qquad \text{for each } \ell \neq p$$

$$\mathbb{T} = \mathbb{T}X := \prod_{\ell \neq p} T_\ell X \qquad \mathbb{V} = \mathbb{V}X := \mathbb{T}X \otimes_{\mathbb{Z}} \mathbb{Q} = {\prod_{\ell \neq p}}' (V_\ell X, T_\ell X);$$

these are free rank $2g$ modules over $\mathbb{Z}_\ell$, $\mathbb{Q}_\ell$, $\hat{\mathbb{Z}}^{(p)} := \prod_{\ell \neq p} \mathbb{Z}_\ell$, and $\mathbb{A}^{(p)} := \hat{\mathbb{Z}}^{(p)} \otimes_{\mathbb{Z}} \mathbb{Q} := \prod'_{\ell \neq p}(\mathbb{Q}_\ell, \mathbb{Z}_\ell)$, respectively (all products and restricted products are over the finite primes $\ell$, excluding $p$ if $p > 0$).

**Definition 1.1.** Given rings $R \subseteq R'$ and corresponding modules $M \subseteq M'$, say that $M$ is an $R$-lattice in $M'$ if $M$ has an $R$-basis that is an $R'$-basis for $M'$.

Zarhin [Zar20, Theorem 1.1] proved that given $u \in \operatorname{End}^\circ X$, there exists a matrix $A \in \mathrm{M}_{2g}(\mathbb{Q})$ such that for every $\ell \neq p$, there is a $\mathbb{Q}_\ell$-basis of $V_\ell$ on which the action of $u$ is given by $A$; equivalently, there exists a $u$-stable $\mathbb{Q}$-lattice in the $(\prod_{\ell \neq p} \mathbb{Q}_\ell)$-module $\prod_{\ell \neq p} V_\ell$. Our main theorem refines this as follows:

**Theorem 1.2.**
(a) *For each $u \in \operatorname{End}^\circ X$, there exists a $u$-stable $\mathbb{Q}$-lattice $V \subset \mathbb{V}$.*
(b) *For each $u \in \operatorname{End} X$, there exists a $u$-stable $\mathbb{Z}$-lattice $T \subset \mathbb{T}$.*

The following restatement of (b) answers a question implicit in [Zar20, Remark 1.2]:

**Corollary 1.3.** *Let $u \in \operatorname{End} X$. Then there exists a matrix $A \in \mathrm{M}_{2g}(\mathbb{Z})$ such that for every $\ell \neq p$, there is a $\mathbb{Z}_\ell$-basis of $T_\ell X$ on which the action of $u$ is given by $A$.*

*Date*: July 13, 2021.
2020 *Mathematics Subject Classification.* Primary 14K02; Secondary 14K05.
*Key words and phrases.* Abelian variety, Tate module, endomorphism.
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 National Science Foundation grant DMS-1601946 and Simons Foundation grants #402472 and #550033.

## 2. Proof

**Lemma 2.1.** *Let $E$ be a number field contained in* $\operatorname{End}^\circ X$*. Let* $\mathcal{O} = E \cap \operatorname{End} X$*. Let* $h = 2(\dim X)/[E : \mathbb{Q}]$*. Then*

(i) *The* $(E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell)$*-module* $V_\ell$ *is free of rank* $h$*.*
(ii) *For each* $\ell \nmid p \operatorname{disc} \mathcal{O}$*, the* $(\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell)$*-module* $T_\ell$ *is free of rank* $h$*.*
(iii) *The* $(E \otimes_{\mathbb{Q}} \mathbb{A}^{(p)})$*-module* $\mathbb{V}$ *is free of rank* $h$*.*

*Proof.*

(i) This is [Rib76, Theorem 2.1.1].
(ii) Fix $\ell \nmid p \operatorname{disc} \mathcal{O}$, where $\operatorname{disc} \mathcal{O}$ is the discriminant of $\mathcal{O}$. For each prime $\lambda$ of $\mathcal{O}$ dividing $\ell$, let $\mathcal{O}_\lambda \subset E_\lambda$ be the completions of $\mathcal{O} \subset E$ at $\lambda$. Since $\ell \nmid \operatorname{disc} \mathcal{O}$, the ring $\mathcal{O}_\lambda$ is a discrete valuation ring with fraction field $E_\lambda$, and

$$E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \simeq \prod_{\lambda | \ell} E_\lambda \quad \text{and} \quad \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \simeq \prod_{\lambda | \ell} \mathcal{O}_\lambda.$$

These induce decompositions

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

By (i), $\dim_{E_\lambda} V_\lambda = h$. Since $T_\lambda$ is a torsion-free finitely generated $\mathcal{O}_\lambda$-module that spans $V_\lambda$, it is free of rank $h$ over $\mathcal{O}_\lambda$. Thus $T_\ell = \prod_{\lambda|\ell} T_\lambda$ is free of rank $h$ over $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \simeq \prod_{\lambda|\ell} \mathcal{O}_\lambda$.
(iii) We have $E \otimes_{\mathbb{Q}} \mathbb{A}^{(p)} = \prod' (E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell, \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell)$, so (iii) follows from (i) and (ii). □

*Proof of Theorem 1.2.*

(a) We work in the category of abelian varieties over $k$ up to isogeny. By [Zar20, Theorem 2.4], $u$ is contained in a subring of $\operatorname{End}^\circ X$ isomorphic to $\prod_i \mathrm{M}_{r_i}(E_i)$ for some number fields $E_i$. Then $X$ is isogenous to $\prod Y_i^{r_i}$ for some abelian varieties $Y_i$ with $E_i \subseteq \operatorname{End}^\circ Y_i$. If we can find an $E_i$-stable $\mathbb{Q}$-lattice $V_i \subset \mathbb{V} Y_i$ for each $i$, then we may take $V = \prod V_i^{r_i}$. In other words, we have reduced to the case that $u \in E \subseteq \operatorname{End}^\circ X$ for some number field $E$. By Lemma 2.1(iii),

$$\mathbb{V} = W \otimes_{\mathbb{Q}} (E \otimes_{\mathbb{Q}} \mathbb{A}^{(p)})$$

for some $\mathbb{Q}$-vector space $W$. Then $V := W \otimes_{\mathbb{Q}} E$ is a $u$-stable $\mathbb{Q}$-lattice in $\mathbb{V}$.
(b) Given $u \in \operatorname{End} X$, choose $V$ as in (a). We have

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

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

## 3. Generalizations and counterexamples

In Theorem 1.2, suppose that instead of fixing one endomorphism $u$, we consider a $\mathbb{Q}$-subalgebra $R \subset \operatorname{End}^\circ X$ (or subring $R \subset \operatorname{End} X$) and ask for an $R$-stable $\mathbb{Q}$-lattice (respectively, $\mathbb{Z}$-lattice), i.e., one that is $r$-stable for every $r \in R$.

1. If $R$ is contained in a subring of $\operatorname{End}^\circ X$ isomorphic to $\prod_i \mathrm{M}_{r_i}(E_i)$ 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 $\operatorname{End}^\circ X$ is a quaternion algebra, then for $R = \operatorname{End}^\circ X$, there is no $R$-stable $\mathbb{Q}$-lattice in any $V_\ell$, since $R$ cannot act on a 2-dimensional $\mathbb{Q}$-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 $\operatorname{End}^\circ Y$ is a quaternion algebra $B$, and $X = Y^2$, and

$$R = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} : a \in \mathbb{Q} \text{ and } b \in B \right\} \subset \mathrm{M}_2(B) = \operatorname{End}^\circ X.$$

The ideal $\left(\begin{smallmatrix} 0 & B \\ 0 & 0 \end{smallmatrix}\right)$ has square zero, so $R$ is commutative. For each nonzero $b \in B$, we have

$$\left(\begin{smallmatrix} 0 & b \\ 0 & 0 \end{smallmatrix}\right) X = 0 \times Y, \qquad \text{so} \qquad \left(\begin{smallmatrix} 0 & b \\ 0 & 0 \end{smallmatrix}\right) \mathbb{V}X = 0 \times \mathbb{V}Y,$$

which is of rank 2.

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

$$\left(\begin{smallmatrix} 0 & B \\ 0 & 0 \end{smallmatrix}\right) \hookrightarrow \operatorname{Hom}(V/W, W) \subset \operatorname{End} V.$$

It is an isomorphism since

$$\dim \left(\begin{smallmatrix} 0 & B \\ 0 & 0 \end{smallmatrix}\right) = 4 = \dim \operatorname{Hom}(V/W, W).$$

Since $\dim_{\mathbb{Q}} \left(\begin{smallmatrix} 0 & b \\ 0 & 0 \end{smallmatrix}\right) V = 2$ for each nonzero $b \in B$, we have $\dim_{\mathbb{Q}} f(V) = 2$ for each nonzero

$$f \in \operatorname{Hom}(V/W, W) \subset \operatorname{End} V,$$

which is absurd. Thus there is no $R$-stable $\mathbb{Q}$-lattice in $\mathbb{V}X$.

## References


[Rib76] Kenneth A. Ribet, *Galois action on division points of Abelian varieties with real multiplications*, Amer. J. Math. **98** (1976), no. 3, 751–804, DOI 10.2307/2373815. MR457455 ↑2

[Zar20] Yuri G. Zarhin, *On matrices of endomorphisms of abelian varieties*, Mathematics Research Reports **1** (2020), 55–68. ↑1, 2



Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139-4307, USA

*Email address*: poonen@math.mit.edu

*URL*: http://math.mit.edu/~poonen/

Institute for information transmission problems of the Russian Academy of Sciences

Interdisciplinary Scientific Center J.-V. Poncelet (ISCP)

*Email address*: rybakov.sergey@gmail.com