Endomorphism Rings and Tate modules

Vivian Yu

February 13, 2024

In this talk, we will study the properties of endomorphism rings and introduce Tate modules for abelian varieties following mainly §5 of Dembélé's notes.

1 Endomorphism ring of an abelian variety

Let A, B be abelian varieties over a field k and consider the set of homomorphisms of abelian varieties $\mathrm{Hom}(A, B)$. If $f, g \in \mathrm{Hom}(A, B)$, then we have a homomorphism $f + g$ by pointwise addition. This gives $\mathrm{Hom}(A, B)$ the stucture of an abelian group with the trivial morphism as the identity element. With $A = B$, we see that $\mathrm{End}(A)$ has a natural ring stucture with composition as multiplication.

Lemma 1.1. Let A, B be abelian varieties over a field k. Then the group $\mathrm{Hom}(A, B)$ is torsion-free, i.e. for $f \in \mathrm{Hom}(A, B)$ and $0 \neq n \in \mathbb{Z}$, $n \cdot f = 0$ implies that $f = 0$.

Proof. We know that $n \cdot f = f \circ [n]_A$. For $n \neq 0$, we know that $[n]_A$ is an isogeny, which is in particular surjective. Thus, if $n \cdot f = 0$, then $f = 0$. □

2 The isogeny category

Define a category **Isog** as follows. The objects are abelian varieties. For two abelian varieties A and B, we put

$$\mathrm{Hom}_{\mathbf{Isog}}(A, B) = \mathrm{Hom}(A, B) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

We also write

$$\mathrm{Hom}^0(A, B) := \mathrm{Hom}_{\mathbf{Isog}}(A, B), \quad \mathrm{End}^0(A) := \mathrm{End}_{\mathbf{Isog}}(A).$$

If $f : A \to B$ is an isogeny, then there exists an isogeny $g : B \to A$ such that $gf = [n]$, for some n explain. It follows that $\frac{1}{n}g$ is the inverse to f in **Isog**. In other words, isogenies are isomorphisms in **Isog**. In fact, **Isog** is an abelian category [1].

Theorem 2.1 (Poincaré reducibility)**.** *Let A be an abelian variety, and let B be an abelian subvariety. Then there exists an abelian subvariety C such that $B \cap C$ is finite and $B \times C \to A$ is an isogeny.*

[1]A category $\mathcal{A}$ is abelian if it is additive, if all kernels and cokernels exist, and if the natural map $Coim(f) \to Im(f)$ is an isomorphism for all morphisms f of $\mathcal{A}$. "the category that snake lemma works".

Proof. proof details Let $i : B \hookrightarrow A$ be the inclusion and $i^\vee : A^\vee \to B^\vee$ its dual. Let $\lambda : A \to A^\vee$ be a polarization on A. Then, let

$$X = \ker(i^\vee \circ \lambda),$$

let C be the reduced subscheme of the zero component of X. Then C is an abelian variety[2]. From the theorem of dimension of fibres of morphisms, we know that

$$\dim C \geq \dim A - \dim B.$$

The restriction of $i^\vee \circ \lambda$ to B is $\lambda|_B$, whose kernel is finite since λ is an isogeny. Thus, $B \cap C$ is finite and $B \times C \to A$ is an isogeny. □

Definition 2.1. Let A be a non-zero abelian variety X over a field k. We say that A is simple if the only subvarieties of A are 0 and A.

Note that an abelian variety that is simple over the ground field k need not be simple over an extension of k. Therefore, we will always specify by saying k-simple.

If we consider the simple abelian varieties to be the simple objects of the category **Isog**, Poincaré's theorem shows that **Isog** is semi-simple as an abelian category.

From the formalism of abelian categories, we know that:

1. The decomposition (up to isogeny) into a product of simple abelian varieties is unique (up to isogeny).

2. If A is a simple abelian variety then $\mathrm{End}^0(A)$ is a division algebra over $\mathbb{Q}$.

In particular,

Proposition 2.1. *Let A be a non-zero abelian variety over k. Then A is isogenous to a product of k-simple abelian varieties. More precisely, there exists k-simple abelian varieties $B_1, \ldots, B_r$, which are pairwise non k-isogenous, and positive integers $n_1, \ldots, n_r$ such that A is k-isogenous to $B_1^{n_1} \times \cdots \times B_r^{n_r}$, which we denote by*

$$A \sim_k B_1^{n_1} \times \cdots \times B_r^{n_r}.$$

Up to permutation, the B_i's are unique up to k-isogenies, and the corresponding multiplicities n_i are uniquely determined.

Proof. Repetitively apply Poincare reducibility proves the existence of a decomposition. The uniqueness of decomposition follows from the fact that a homomorphism between two simle abelian varieties is either zero or an isogeny □

Corollary 2.1.1. Let A be an abelian variety defined over k.

1. If A is a simple abelian variety then $\mathrm{End}_k^0(A)$ is a division algebra.

2. If $A \sim_k B_1^{n_1} \times \cdots \times B_r^{n_r}$, we have

$$\mathrm{End}_k^0(A) = M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r),$$

where $D_i = \mathrm{End}_k^0(B_i)$.

[2]definition used:

Proof. (i) Since $\mathrm{End}_k^0(A)$ consists only of isogenies, which are invertible. Thus, $\mathrm{End}_k^0(A)$ is a division algebra. □

In fact, we can say more about $\mathrm{End}_k^0(A)$ when A is k-simple using the Albert classification.

Let A be a k-simple abelian variety of dimension g. Let $D = \mathrm{End}_k^0(A)$ and let F be the center of D. Let

$$\iota : D \to D,\ x \mapsto x^\dagger$$

be the Rosati involution[3] on A. Let $F^\dagger = \{x \in D \mid x^\dagger = x\}$ be the fixed elements of the involution. If fact, $F^\dagger$ is a totally real subfield of F. Let $e = [F : \mathbb{Q}]$ and $e^\dagger = [F^\dagger : \mathbb{Q}]$. Let $d \geq 1$ be such that $[D : F] = d^2$.

Theorem 2.2 (Albert classification)**.** *Let A and D be as above. Then D is isomorphic to an algebra of one of the following four types:*

1. *$D = F = F^\dagger$, and the Rosati involution is the identity map. In this case, $e \mid g$.*
2. *$F = F^\dagger$, and D is a totally indefinite quaternion division algebra over F. i.e., for any embedding $\sigma : F \to \mathbb{R}$, one has that $D \otimes_\sigma \mathbb{R} \cong M_2(\mathbb{R})$. In this case $2e \mid g$.*
3. *$F = F^\dagger$, and D is a totally definite quaternion division algebra over F. i.e., for any embedding $\sigma : F \to \mathbb{R}$, one has that $D \otimes_\sigma \mathbb{R} \cong \mathbb{H}$, where $\mathbb{H}$ is the Hamiltonian quaternion algebra. In this case $e^2 \mid g$.*
4. *F is a CM extension of $F^\dagger$ and D is a division algebra with center F. In this case $e^\dagger d^2 \mid g$ if $char(k) = 0$ and $e^\dagger d \mid g$ if $char(k) > 0$.*

3 The Tate module of an abelian variety

Let A/k be an abelian variety of dimension g and let n be an integer such that $(char(k), n) = 1$. We have an isomorphism of abelian groups corollary 1.18:

$$A[n](\bar{k}) = (\mathbb{Z}/n\mathbb{Z})^{2g}.$$

Let $\ell \neq char(k)$ be a prime. The ℓ-adic Tate module of A:

$$T_\ell(A) := \varprojlim A[\ell^n]$$

is defined by the inverse limit of the groups $A[\ell^n](\bar{k})$, where the transition maps are multiplication by ℓ. Thus, we have an isomorphism

$$T_\ell(A) \cong \mathbb{Z}_\ell^{2g}.$$

The Tate module comes equipped with a Galois action by the absolute Galois group $G_k = \mathrm{Gal}(\bar{k}/k)$ which is compatible with the inverse limit. Upon picking a basis, this action can be thought of as a homomorphism

$$\rho : G_k \to GL_{2g}(\mathbb{Z}_\ell).$$

If $f : A \to B$ is a homomorphism of abelian varieties, then f induces a $\mathbb{Z}_\ell$-linear G_k-equivariant map

$$T_\ell f : T_\ell(A) \to T_\ell(B).$$

[3]for $x \in D$, the Rosati involution associated to a polarization is $x^\dagger = \phi^{-1} \circ x^\vee \circ \phi$

Lemma 3.1. Let A and B be abelian varieties over a field k, and $f \in \mathrm{Hom}(A, B)$. Let ℓ be as above. If $T_\ell(f)$ is divisible by ℓ^m in $\mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell(A), T_\ell(B))$ then f is divisible by ℓ^m in $\mathrm{Hom}(A, B)$.

Proof. If $T_\ell(f)$ is divisible by ℓ^m, we know that f vanishes on $A[\ell^m](\bar{k})$. Since $(n, char(k)) = 1$, we know that $A[\ell^m]$ is an etale group scheme. Thus, f is zero on $A[\ell^m]$ and $\ker[\ell^m]_A = A[\ell^m] \subset \ker(f)$. Therefore, f factors through $[\ell^m]_A$. □

The Tate module construction can be applied to $\mathbf{G}_m$. In this case, if $(n, char(k)) = 1$, then the $\bar{k}$-points of $\mathbf{G}_m[n]$ are just the group n-th roots of unity, which is isomorphic to $\mathbb{Z}/n\mathbb{Z}$. Thus, we have a group isomorphism

$$T_\ell(\mathbf{G}_m) \cong \mathbb{Z}_\ell.$$

The Galois action of G_k gives a representation

$$\varepsilon : G_k \to GL_1(\mathbb{Z}_\ell) = \mathbb{Z}_\ell^\times,$$

which is just the cyclotomic character we are familiar with. One often writes $\mathbb{Z}_\ell(1)$ for $T_\ell(\mathbf{G}_m)$.

4 The Weil pairings

Proposition 4.1. *Let A/k be an abelian variety and $n > 0$ an integer such that $(n, char(k)) = 1$. Then there exists a pairing*

$$e_n : A[n] \times A^\vee[n] \to \mu_n$$

that is

1. *Bilinear*
2. *Non-degnerate*
3. *Galois equivariant: $e_n(\sigma x, \sigma y) = \sigma e_n(x, y)$ for $\sigma \in G_k$.*
4. *Compatibility: if $x \in A[nm]$ and $y \in A^\vee[n]$, then $e_{nm}(x, y) = e_n(mx, y)$.*

Let $\lambda : A \to A^\vee$ be a polarization on A[4]. Then, we obtain the pairing

$$\begin{aligned} e_n^\lambda : A[n] \times A[n] &\to \mu_n \\ (x, y) &\mapsto e_n(x, \lambda(y)). \end{aligned}$$

We call e_n and e_n^λ *Weil pairings.* Note that e_n^λ satisfies the same properties as e_n. Moreover, we have an additional property does it come from property of dual:

$$e_n^\lambda(x, x) = 1 \implies e_n^\lambda(x, y) = e_n^\lambda(y, x)^{-1},$$

which we call *alternating*.

The Weil pairing also behaves well under isogenies. In particular,

[4] A polarization is an isogeny $\phi : A \to A^\vee$ associated with an ample line bundle

Proposition 4.2. *Let $f : A \to B$ be an isogeny of polarized varieties, where λ_A and λ_B are the respective polarizations. Then we have*

$$e_n^{\lambda_B}(f(x), y) = e_n^{\lambda_A}(x, f^\vee(y)), \quad \textit{for all } x \in A[n],\ y \in B[n].$$

The compatibility condition allows us to take inverse limit of the $e_{\ell^n}^{\lambda}$'s to obtain a pairing on the Tate module:

$$e^\lambda : T_\ell(A) \times T_\ell(A) \to \mathbb{Z}_\ell(1).$$

This pairing satisfies the same properties as e_n.

The following propositions show how the Tate module is relevant in the study of morphisms.

Proposition 4.3. *Let A/k be an abelian variety. The degree map*

$$\begin{aligned} \mathrm{End}^0(A) &\to \mathbb{Q} \\ c \otimes \phi &\mapsto c \deg(\phi) \end{aligned}$$

is a homogeneous polynomial function[5] *of degree $2g$ on $\mathrm{End}^0(A)$. i.e.*

$$\deg(n\phi) = n^{2g} \deg(\phi).$$

Corollary 4.0.1. Let the notations be as in the proposition above. There is a polynomial $P_\phi(X) \in \mathbb{Q}[X]$ of degree $2g$ such that for all $n \in \mathbb{Q}$,

$$P_\phi(n) = \deg(\phi - [n]_A).$$

We see that P_ϕ is monic and it has integer coefficients when $\phi \in \mathrm{End}(A)$. We call P_ϕ the characteristic polynomial of ϕ and we define the trace of ϕ by the equation

$$P_\phi(X) = X^{2g} - \mathrm{Tr}(\phi)X^{2g-1} + \cdots + \deg(\phi).$$

Proposition 4.4. *Let A be as above and let $\phi \in \mathrm{End}(A)$. For ℓ as before, $P_\phi(X)$ is the characteristic polynomial of ϕ acting on $V_\ell(A) = T_\ell(A) \otimes \mathbb{Q}_\ell$. Hence, the trace and degree of ϕ are the trace and determinant of ϕ acting on $V_\ell(A)$.*

[5] Note that this definition is only well defined for End instead of for End^0 due to the "homogeneous polynomial" behavior.