ROSATI AND FROBENIUS

DAVID T.-B. G. LILIENFELDT

Abstract. These are the notes of two talks I gave at the Honda–Tate seminar at the Hebrew University of Jerusalem on April 30, 2023 and May 7, 2023. Let q be a power of a prime number. Given an abelian variety over a finite field with q elements, we define the geometric Frobenius endomorphism and show that its characteristic polynomial is a q-Weil polynomial. This relies crucially on the positivity of the Rosati involution, a result whose proof we also give. These expository notes are entirely based on the book [1] and contain no novel mathematical contributions on my part, except for the mistakes I may have introduced. I thank Shaul Zemel for spotting some of those mistakes in a previous version.

1. Introduction: the Honda-Tate theorem

We begin by recalling necessary notations, conventions, facts, and definitions about abelian varieties:

- k: arbitrary field with fixed algebraic closure $\bar{k}$
- Variety$/k$: separated k-scheme of finite type that is geometrically integral
- Curve$/k$: 1-dimensional variety$/k$
- Abelian variety$/k$: complete group variety$/k$
- Elliptic curve$/k$: 1-dimensional abelian variety$/k$
- Dual of abelian variety X/k: $X^t := \mathrm{Pic}^0_{X/k}$ connected component of the identity of the Picard scheme
- Poincaré bundle: universal line bundle P_X on $X \times \mathrm{Pic}_{X/k}$ (trivialized along the zero section $0 \times \mathrm{Pic}_{X/k}$) restricted to $X \times X^t$
- Isogeny of abelian varieties$/k$: homomorphism $f\colon X \longrightarrow Y$ such that $\dim(X) = \dim(Y)$ and $\ker(f)$ is a finite group scheme
- Polarization of abelian variety X/k: symmetric isogeny $\lambda\colon X \longrightarrow X^t$ such that $(\mathrm{id}, \lambda)^* P_X$ is an ample line bundle on X
- $q = p^m$: power of a prime number
- q-Weil number: algebraic integer π such that $|\iota(\pi)| = \sqrt{q}$ for all complex embeddings $\iota\colon \mathbb{Q}[\pi] \hookrightarrow \mathbb{C}$
- Conjugacy: two q-Weil numbers are conjugate if their minimal polynomials over $\mathbb{Q}$ are equal.

The goal of the seminar is to prove the following result:

Date: May 8, 2023.

Theorem 1.1 (Honda–Tate)**.** *The map that assigns to a simple abelian variety X over $\mathbb{F}_q$ its geometric Frobenius endomorphism π_X gives a bijection of sets*

$$\{\textit{isogeny classes of simple abelian varieties}/\mathbb{F}_q\} \xrightarrow{\sim} \{\textit{conjugacy classes of } q-\textit{Weil numbers}\}.$$

The injectivity of the map in Theorem 1.1 is a consequence of Tate's theorem [1, §16.3], while the surjectivity is due to Honda [1, §16.5]. The proof will be covered in the next lectures. The goal of today is to define the geometric Frobenius endomorphism of an abelian variety over $\mathbb{F}_q$ and explain in what sense this endomorphism is a q-Weil number. We follow [1, §16.1].

2. Rosati

A crucial ingredient in the proof that "the geometric Frobenius is a q-Weil number" is the positivity of the Rosati involution for polarized abelian varieties. We therefore begin by proving this result over an arbitrary field k.

2.1. **The endomorphism algebra.** Let X be an abelian variety of dimension g over k. Let $\mathrm{End}(X)$ denote the ring of endomorphism of X (defined over k) and let $\mathrm{End}^0(X) := \mathrm{End}(X) \otimes \mathbb{Q}$ denote the associated endomorphism algebra.

2.1.1. *Poincaré splitting.* The abelian variety X is isogenous over k to a product of powers of simple abelian varieties

$$X \sim_k Y_1^{m_1} \times \ldots \times Y_n^{m_n}, \tag{2.1}$$

such that $Y_i \not\sim_k Y_j$ for $i \neq j$ [1, Corollary 12.5]. A homomorphism between two simple abelian varieties is either trivial or an isogeny. In particular, $D_i := \mathrm{End}^0(Y_i)$ is a division algebra for each i, and we have

$$\mathrm{End}^0(X) = M_{m_1}(D_1) \times \ldots \times M_{m_n}(D_n). \tag{2.2}$$

2.1.2. *Endomorphism algebras of Tate modules.* For any prime $\ell \neq \mathrm{char}(k)$, we have the Tate module $T_\ell(X) := \varprojlim X[\ell^n](\bar{k}) \simeq \mathbb{Z}_\ell^{2g}$ and the associated $\mathbb{Q}_\ell$-vector space $V_\ell(X) := T_\ell(X) \otimes \mathbb{Q}_\ell \simeq \mathbb{Q}_\ell^{2g}$. Any endomorphism $f \in \mathrm{End}(X)$ preserves torsion points and thus induces endomorphisms $T_\ell(f) \in \mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(X))$ and $V_\ell(f) \in \mathrm{End}_{\mathbb{Q}_\ell}(V_\ell(X))$. The resulting map

$$\mathrm{End}(X) \otimes \mathbb{Z}_\ell \longrightarrow \mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(X))$$

is injective with torsion-free cokernel [1, Theorem 12.10]. As a consequence, $\mathrm{End}(X)$ is a free $\mathbb{Z}$-module of rank $\leq 4g^2$.

2.1.3. *Characteristic polynomial.* Associated to an endomorphism $f \in \mathrm{End}(X)$ there is a unique monic polynomial $P_f(t) \in \mathbb{Q}[t]$ of degree $2g$ satisfying the property

$$P_f(n) := \deg([n]_X - f), \text{ for all } n \in \mathbb{Z}. \tag{2.3}$$

See [1, Proposition 12.15] for a justification of the existence of such a polynomial. The uniqueness is clear since polynomials only have finitely many zeros. The polynomial P_f is called the *characteristic polynomial* of f.

If $f \in \mathrm{End}^0(X)$, then we choose $n \in \mathbb{Z}$ such that $nf \in \mathrm{End}(X)$ and define

$$\deg(f) := n^{-2g}\deg(nf) \qquad \text{and} \qquad P_f(t) := n^{-2g}P_{nf}(nt).$$

Then $P_f(t) \in \mathbb{Q}[t]$ is a monic polynomial of degree $2g$ satisfying

$$P_f(r) := \deg(r - f), \text{ for all } r \in \mathbb{Q}, \tag{2.4}$$

where $r - f$ is interpreted as an element of $\mathrm{End}^0(X)$.

Definition 2.1. Following [1, Definition 12.16], we define the trace of $f \in \mathrm{End}^0(X)$ to be

$$\mathrm{trace}(f) = -(2g-1)\text{th coefficient of } P_f.$$

For all $\ell \neq \mathrm{char}(k)$, $P_f(t)$ is equal to the characteristic polynomial $P_{\ell,f} \in \mathbb{Q}_\ell[t]$ of $V_\ell(f)$ acting on the $2g$-dimensional $\mathbb{Q}_\ell$-vector space $V_\ell(X)$ [1, Theorem 12.18], i.e.,

$$P_f(t) = P_{\ell,f}(t) = \det(t \cdot \mathrm{id} - V_\ell(f)). \tag{2.5}$$

As a consequence, we have

(a) $P_f(f) = 0$ [1, Corollary 12.19]

(b) $P_f \in \mathbb{Z}[t]$ for all $f \in \mathrm{End}(X)$ [1, Corollary 12.20]

(c) $\mathrm{trace}(fg) = \mathrm{trace}(gf)$, for all $f, g \in \mathrm{End}^0(X)$ [1, Corollary 12.21].

2.2. **The Rosati involution.** Let X be an abelian variety over k and let $\lambda \colon X \longrightarrow X^t$ be a polarization. The Rosati involution is an involution of the endomorphism algebra

$$\dagger \colon \mathrm{End}^0(X) \longrightarrow \mathrm{End}^0(X),$$

which depends on the polarization λ. If $f \in \mathrm{End}^0(X)$, then

$$f^\dagger := \lambda^{-1} \circ f^t \circ \lambda,$$

where $f^t \colon X^t \longrightarrow X^t$ is the dual homomorphism and λ^{-1} makes sense after tensoring with $\mathbb{Q}$, i.e. in $\mathrm{Hom}(X^t, X) \otimes \mathbb{Q}$, since λ is an isogeny. Note that $\dagger$ is an involution by symmetry of λ.

2.2.1. *Characteristic polynomial.* We clearly have $\deg(f) = \deg(f^\dagger)$. Moreover, if $n \in \mathbb{Z}$, then

$$[n]_X^\dagger = \lambda^{-1} \circ [n]_X^t \circ \lambda = \lambda^{-1} \circ [n]_{X^t} \circ \lambda = \lambda^{-1} \circ \lambda \circ [n]_X = [n]_X.$$

As a consequence, for all $n \in \mathbb{Z}$, we have

$$P_f(n) = \deg([n]_X - f) = \deg(([n]_X - f)^\dagger) = \deg([n]_X^\dagger - f^\dagger) = \deg([n]_X - f^\dagger) = P_{f^\dagger}(n).$$

It follows that

$$P_f = P_{f^\dagger} \qquad \text{and} \qquad \mathrm{trace}(f) = \mathrm{trace}(f^\dagger). \tag{2.6}$$

2.2.2. *Polarizations and line bundles.* Let L be a line bundle on X. Consider the associated Mumford bundle

$$\Lambda(L) := m^*L \otimes \mathrm{pr}_1^* L^{-1} \otimes \mathrm{pr}_2^* L^{-1}$$

on $X \times X$, where $m \colon X \times X \longrightarrow X$ is the group operation map (i.e., $m(x,y) = x + y$). Viewing $\Lambda(L)$ as a family of line bundles on the first copy of X parametrized by the second copy of X gives rise to a map

$$\varphi_L \colon X \longrightarrow X^t, \qquad x \mapsto [t_x^* L \otimes L^{-1}].$$

This is a homomorphism by the Theorem of the Cube [1, Theorem 2.7]. Moreover, it is symmetric (i.e., $\lambda^t = \lambda$) by symmetry of the construction. If L is ample (i.e., there exists $n, N \in \mathbb{N}$ and a closed immersion $\pi \colon X \longrightarrow \mathbb{P}^N$ such that $L^n = \pi^* \mathcal{O}(1)$), then φ_L is a polarization on X. Conversely, a homomorphism $\lambda \colon X \longrightarrow X^t$ is a polarization if and only if there exists a finite separable extension $k \subset K$ and an ample line bundle L on X_K such that $\varphi_L = \lambda_K$ [1, Corollary 11.5].

In the proof of the next result we will use the fact that any line bundle L is isomorphic to $\mathcal{O}_X(D)$ for some Weil divisor D (determined up to linear equivalence). Here, $\mathcal{O}_X(D)$ is the line bundle whose space of global sections is given by

$$H^0(X, \mathcal{O}_X(D)) = \{f \in k(X)^\times \mid \mathrm{div}(f) + D \geq 0\}.$$

Concretely, D is obtained by taking any global section of L and taking its vanishing locus. The map $L \mapsto c_1(L) := [D]$ establishes the well-known isomorphism

$$c_1 \colon \mathrm{Pic}(X) \simeq \mathrm{CH}^1(X)$$

between isomorphism classes of line bundles on X and the codimension 1 Chow group of Weil divisors modulo ratonal (i.e., linear) equivalence. The element $c_1(L)$ is the first Chern class, which explains the notation. We recall that a line bundle L is ample if and only if L is non-degenerate (i.e., φ_L is an isogeny) and effective (i.e., $L \simeq \mathcal{O}_X(D)$ for some effective divisor D) [1, Proposition 2.22].

The Chow ring $\mathrm{CH}(X) = \bigoplus_{i=0}^g \mathrm{CH}^i(X)$ of algebraic cycles modulo rational equivalence is graded by codimension with product given by the intersection product

$$\mathrm{CH}^i(X) \times \mathrm{CH}^j(X) \longrightarrow \mathrm{CH}^{i+j}(X), \qquad ([Z_1], [Z_2]) \mapsto [Z_1 \cdot Z_2],$$

for representatives Z_1 and Z_2 that intersect transversally. If D is a Weil divisor, so that $[D] \in \mathrm{CH}^1(X)$, then we abusively write D^g for $\deg([D]^g) \in \mathbb{Z}$, the degree of the g-fold self-intersection $[D]^g \in \mathrm{CH}^g(X)$. Similarly, if D' is another Weil divisor, we write $D^{g-1} \cdot D'$ for $\deg([D]^{g-1} \cdot [D'])$. In this notation, if $L \simeq \mathcal{O}_X(D)$, then the Riemann–Roch theorem for abelian varieties [1, Theorem 9.11] can be stated as the equality

$$\deg(\varphi_L) = \left(\frac{c_1(L)^g}{g!}\right)^2 = \left(\frac{D^g}{g!}\right)^2. \tag{2.7}$$

2.2.3. *Positivity of the Rosati involution.*

Theorem 2.2 (Theorem 12.26 of [1])**.** *Let X be an abelian variety of dimension g over k with a polarization $\lambda \colon X \longrightarrow X^t$ and associated Rosati involution $\dagger$.*

i) *If $\lambda = \varphi_L$ for some ample line bundle $L = \mathcal{O}_X(D)$ and $f \in \mathrm{End}(X)$, then*

$$\mathrm{trace}(ff^\dagger) = 2g\frac{D^{g-1} \cdot f^*D}{D^g}.$$

ii) *The bilinear pairing*

$$\mathrm{End}^0(X) \times \mathrm{End}^0(X) \longrightarrow \mathbb{Q}, \qquad (f, g) \mapsto \mathrm{trace}(fg^\dagger)$$

is symmetric and positive-definite.

Remark 2.3. The above formula *i)* makes sense for L ample, since $D^g \neq 0$ in this case. This follows from Riemann–Roch (2.7) and the fact that L is non-degenerate, i.e., φ_L is an isogeny, which implies that $\deg(\varphi_L) \neq 0$.

Proof. By property (*c*) of the trace discussed in §2.1.3, we have $\mathrm{trace}(ff^\dagger) = \mathrm{trace}(f^\dagger f)$. In particular, $\mathrm{trace}(ff^\dagger)$ is the $(2g-1)$th coefficient of the characteristic polynomial $P_{f^\dagger f}(t) \in \mathbb{Q}[t]$ by Definition 2.1. By (2.4), for all $n \in \mathbb{Z}$ we have

$$\begin{aligned}
\deg(\varphi_L) P_{f^\dagger f}(n) &= \deg(\varphi_L) \deg([n]_X - \lambda^{-1} f^t \lambda f) \\
&= \deg(n\varphi_L - f^t \varphi_L f) \\
&= \deg(\varphi_{L^n} - \varphi_{f^*L}) \\
&= \deg(\varphi_{L^n \otimes f^* L^{-1}}).
\end{aligned}$$

Applying Riemann–Roch (2.7) to both sides of this equality yields

$$(c_1(L)^g)^2 P_{f^\dagger f}(n) = (c_1(L^n \otimes f^*L^{-1})^g)^2 = ((nc_1(L) - c_1(f^*L))^g)^2.$$

Consider the polynomial $Q(t) = \sum_{j=0}^{g} b_j t^j \in \mathbb{Q}[t]$ of degree g with coefficients defined by

$$b_j := \binom{g}{j}(-1)^{g-j}(c_1(L)^j \cdot c_1(f^*L)^{g-j}).$$

Then, for all $n \in \mathbb{Z}$, we have

$$Q(n) = (nc_1(L) - c_1(f^*L))^g.$$

We deduce the equality of polynomials

$$(c_1(L)^g)^2 P_{f^\dagger f}(t) = Q(t)^2.$$

Comparing the $(2g-1)$th coefficients yields

$$(c_1(L)^g)^2 \mathrm{trace}(f^\dagger f) = 2g c_1(L)^g (c_1(L)^{g-1} \cdot c_1(f^*L)),$$

and $i)$ follows since $c_1(f^*L) = f^*c_1(L) = f^*D$.

The pairing in $ii)$ is symmetric by (2.6). To see that it is positive-definite, it is enough to base-change to $\bar{k}$. Then there exists an ample line bundle $L \simeq \mathcal{O}_X(D)$ such that $\lambda = \varphi_L$. We need to prove that for $0 \neq f \in \mathrm{End}^0(X)$, $\mathrm{trace}(ff^\dagger) > 0$. Because the trace is homogeneous of degree 2, it is enough to prove this for $f \in \mathrm{End}(X)$. We may then apply $i)$. According to [3, §21 Proof of Theorem 1], for any effective divisor S and any ample divisor T, we have $T^{g-1} \cdot S > 0$. In particular, $D^g > 0$, so by $i)$ it suffices to prove that f^*D is effective because then $D^{g-1} \cdot f^*D > 0$. For a proof that f^*D is effective, we refer to [1, End of proof of Lemma 12.9]. □

We end this section with a useful result.

Proposition 2.4 (Proposition 14.4 i) of [2]). *Let X be an abelian variety over k with a polarization $\lambda\colon X \longrightarrow X^t$. Then $|\mathrm{Aut}(X, \lambda)| < \infty$.*

Proof. Let α be an automorphism of X that respects the polarization λ. This means that $\alpha^t \circ \lambda \circ \alpha = \lambda$, or in other words $\alpha^\dagger \alpha = \mathrm{id}_X$. In particular, $\mathrm{trace}(\alpha^\dagger \alpha) = 2g$. This shows that

$$\mathrm{Aut}(X, \lambda) \subset \mathrm{End}(X) \cap \{\alpha \in \mathrm{End}(X) \otimes \mathbb{R} \mid \mathrm{trace}(\alpha^\dagger \alpha) = 2g\}.$$

But $\mathrm{End}(X)$ is a free $\mathbb{Z}$-module and thus a discrete subset of the compact $\mathrm{End}(X) \otimes \mathbb{R}$ (a product of spaces of matrices with coefficients in real division algebras (2.2)). The condition $\mathrm{trace}(\alpha^\dagger \alpha) = 2g$ being a closed condition, we conclude that $\mathrm{Aut}(X, \lambda)$ is finite. □

3. Frobenius

Let $m \in \mathbb{N}$ and let p be a prime. In this section we specialize to the case $k = \mathbb{F}_q$ for $q = p^m$. We fix an algebraic closure $\bar{\mathbb{F}}_q \supset \mathbb{F}_q$.

3.1. **Frobenius morphisms.**

3.1.1. *The absolute Frobenius.* Let X be an $\mathbb{F}_p$-scheme. The absolute Frobenius is the morphism of $\mathbb{F}_p$-schemes
$$\mathrm{Frob}_X\colon X \longrightarrow X$$
given by the identity on topological spaces and by raising to the p-th power on sections. More precisely, the map on sheaves $\mathrm{Frob}_X^{\#}\colon \mathcal{O}_X \longrightarrow \mathcal{O}_X$ takes a section s to s^p. If $f\colon X \longrightarrow Y$ is a morphism of $\mathbb{F}_p$-schemes, then
$$\mathrm{Frob}_Y \circ f = f \circ \mathrm{Frob}_X \tag{3.1}$$
because $f^{\#}(s^p) = f^{\#}(s)^p$ for any section s of $\mathcal{O}_Y$.

3.1.2. *The relative Frobenius.* Let S be an $\mathbb{F}_p$-scheme and let X be an S-scheme with structure morphism $\pi\colon X \longrightarrow S$. Define $X^{(p)} := X \times_{\mathrm{Frob}_S} S$ with projection map $W\colon X^{(p)} \longrightarrow X$. Using (3.1) and the universal property of fiber products, there is a unique morphism of S-schemes $F_{X/S}\colon X \longrightarrow X^{(p)}$ such that $W \circ F_{X/S} = \mathrm{Frob}_X$. This morphism is called the relative Frobenius.

To fix ideas, consider $S = \mathrm{Spec}(R)$ for some $\mathbb{F}_p$-algebra R and let $X = \mathrm{Spec}(R[t_1, \ldots, t_m]/I)$ for some ideal $I = (f_1, \ldots, f_n) \subset R[t_1, \ldots, t_m]$. Note that $\mathrm{Frob}_S\colon \mathrm{Spec}(R) \longrightarrow \mathrm{Spec}(R)$ is the morphism induced by the map of $\mathbb{F}_p$-algebras $\varphi\colon R \longrightarrow R$, $r \mapsto r^p$. Let $f_i^{(p)}$ denote the polynomial f_i but with coefficients raised to the p-th power and let $I^{(p)} := (f_1^{(p)}, \ldots, f_n^{(p)})$. Then
$$X^{(p)} = X \times_{\mathrm{Frob}_S} S = \mathrm{Spec}(R[t_1, \ldots, t_m]/I \otimes_\varphi R) = \mathrm{Spec}(R[t_1, \ldots, t_m]/I^{(p)})$$
and the relative Frobenius is induced by the map of R-algebras
$$R[t_1, \ldots, t_m]/I^{(p)} \longrightarrow R[t_1, \ldots, t_m]/I, \qquad r \mapsto r, \quad t_i \mapsto t_i^p.$$
On the other hand, the absolute Frobenius Frob_X is induced by the map of $\mathbb{F}_p$-algebras
$$R[t_1, \ldots, t_m]/I \longrightarrow R[t_1, \ldots, t_m]/I, \qquad r \mapsto r^p, \quad t_i \mapsto t_i^p.$$
FInally, the morphism $W\colon X^{(p)} \longrightarrow X$ is induced by the map
$$R[t_1, \ldots, t_m]/I \longrightarrow R[t_1, \ldots, t_m]/I^{(p)}, \qquad r \longrightarrow r^p, \quad t_i \mapsto t_i.$$

3.1.3. *The geometric Frobenius.* Let $S = \mathrm{Spec}(\mathbb{F}_q)$ with $q = p^m$. The geometric Frobenius is the morphism of S-schemes $\pi_X := \mathrm{Frob}_X^m$ given by the m-th iterated power of the absolute Frobenius. It is a morphism of S-schemes because $\mathrm{Frob}_S^m = \mathrm{id}_S$. It can also be described by iterating the absolute Frobenius m times
$$\pi_X = F^m_{X/\mathbb{F}_q} = F_{X^{(p^{m-1})}/\mathbb{F}_q} \circ F_{X^{(p^{m-2})}/\mathbb{F}_q} \circ \ldots \circ F_{X^{(p)}/\mathbb{F}_q} \circ F_{X/\mathbb{F}_q}. \tag{3.2}$$

3.2. **The roots of geometric Frobenius.**

Let X be an abelian variety of dimension g over $\mathbb{F}_q$. If $\mathbb{F}_q \subset K$ is a field extension, then π_X acts on $X(K)$ by taking $(x\colon \mathrm{Spec}(K) \longrightarrow X)$ to $\pi_X \circ x = x \circ \pi_{\mathrm{Spec}(K)}$. If we consider a closed immersion $X \longrightarrow \mathbb{P}^N$ for some $N \in \mathbb{N}$, then in projective coordinates we have
$$\pi_X([x_0\colon \ldots : x_N]) = [x_0^q\colon \ldots : x_N^q].$$
Let $n \in \mathbb{N}$ and consider the extension $\mathbb{F}_q \subset \mathbb{F}_{q^n} \subset \bar{\mathbb{F}}_q$ of degree n. We then have
$$X(\mathbb{F}_{q^n}) = \{x \in X(\bar{\mathbb{F}}_q) \mid \pi_X^n(x) = x\}.$$
Because $0 \in X(\mathbb{F}_q)$, we have $\pi_X(0) = 0$ and π_X is a endomorphism. It commutes with all other endomorphisms by (3.1), so it lies in the center of $\mathrm{End}^0(X)$. Define the Verschiebung map
$$V_{X/\mathbb{F}_q} := F^t_{X^t/\mathbb{F}_q}\colon X^{(p)} \longrightarrow X. \tag{3.3}$$

We then have

$$V_{X/\mathbb{F}_q} \circ F_{X/\mathbb{F}_q} = [p]_X \qquad \text{and} \qquad F_{X/\mathbb{F}_q} \circ V_{X/\mathbb{F}_q} = [p]_{X^{(p)}} \tag{3.4}$$

(see the proof of [1, Proposition 7.34]). In particular, $F_{X/\mathbb{F}_q}$ is an isogeny of degree p^g. It follows from (3.2) that π_X is an isogeny of degree q^g. We let f_X denote its characteristic polynomial as defined in §2.1.3. We recall that it is a monic polynomial $f_X(t) \in \mathbb{Z}[t]$ (by property (*b*) of §2.1.3) of degree $2g$ satisfying $f_X(n) = \deg([n]_X - \pi_X)$ for all $n \in \mathbb{Z}$.

Lemma 3.1. *Suppose that X is elementary (i.e., a power of a simple abelian variety). Then $\mathbb{Q}[\pi_X] \subset \mathrm{End}^0(X)$ is a number field and f_X is a power of the minimal polynomial* $\min(\pi_X;\mathbb{Q})$ *of π_X over $\mathbb{Q}$.*

Proof. Suppose that $X = Y^m$ with Y a simple abelian variety. Then $D = \mathrm{End}^0(Y)$ is a division algebra and $\mathrm{End}^0(X) = M_m(D)$. Observe that $\mathbb{Q}[\pi_X]$ lies in the center $\{\mathrm{diag}(z) \in M_m(D) \mid z \in Z(D)\}$ of $\mathrm{End}^0(X) = M_m(D)$, which is a field. Since $f_X \in \mathbb{Z}[t]$ is monic of degree $2g$ with $f_X(\pi_X) = 0$, we see that $\pi_X^{-1} \in \mathbb{Q}[\pi_X]$ and we deduce that $\mathbb{Q}[\pi_X]$ is a field with $[\mathbb{Q}[\pi_X] \colon \mathbb{Q}] \leq 2g$.

Let $\alpha \in \bar{\mathbb{Q}}$ be a root of f_X. Let $\ell \neq p$ be a prime and recall that $P_{\ell,\pi_X}(t) = \det(t \cdot \mathrm{id} - V_\ell(\pi_X)) = f_X$ (2.5). Thus α is an eigenvalue of $V_\ell(\pi_X)$. Let $g := \min(\pi_X;\mathbb{Q})$. Then $g(\alpha)$ is an eigenvalue of $g(V_\ell(\pi_X))$. But $g(V_\ell(\pi_X)) = V_\ell(g(\pi_X)) = 0$ so $g(\alpha) = 0$. Hence, all roots of f_X are roots of g. This implies that f_X divides a power of g. By irreducibility of g, this forces f_X to equal a power of g. □

Theorem 3.2. *Let X be an abelian variety of dimension g over $\mathbb{F}_q$. Then*

i) *Every complex root α of f_X has absolute value $|\alpha| = \sqrt{q}$.*

ii) *If α is a complex root of f_X, then so it $\bar{\alpha} = q/\alpha$ and they occur with the same multiplicity. If $\alpha = \sqrt{q}$ or $\alpha = -\sqrt{q}$ occurs as a root, then it occurs with even multiplicity.*

Proof. i) It suffices to treat the case where X is simple. Indeed, by (2.1), X is isogenous over k to a product $X_1 \times \ldots \times X_m$ of simple abelian varieties. If $\ell \neq p$, then at the level of Tate modules this isogeny gives an isomorphism of $V_\ell(X)$ with the direct sum of the $V_\ell(X_i)$. This isomorphism respects the various geometric Frobenii. Thus, in terms of characteristic polynomials we get a decomposition

$$P_{\ell,\pi_X} = P_{\ell,\pi_{X_1}} \ldots P_{\ell,\pi_{X_m}},$$

and consequently a decomposition $f_X = f_{X_1} \ldots f_{X_m}$.

Suppose now that X is a simple abelian variety over $\mathbb{F}_q$ and let $\lambda \colon X \longrightarrow X^t$ be a polarization with Rosati involution †. We claim that $\pi_X \circ \pi_X^\dagger = [q]_X$. Indeed, we have

$$\pi_X \circ \lambda^{-1} \circ \pi_X^t \circ \lambda = \lambda^{-1} \circ \pi_{X^t} \circ \pi_X^t \circ \lambda$$

by (3.1). It thus suffices to show that $\pi_{X^t} \circ \pi_X^t = [q]_{X^t}$. Recall from (3.3) that $F^t_{X/\mathbb{F}_q} = V_{X^t/\mathbb{F}_q}$ and thus, by using (3.4) and (3.2), we obtain

$$\pi_{X^t} \circ \pi_X^t = F^m_{X^t/\mathbb{F}_q} \circ V^m_{X^t/\mathbb{F}_q} = [p^m]_{X^t} = [q]_{X^t}.$$

By Lemma 3.1 and the simplicity of X, $\mathbb{Q}[\pi_X]$ is a number field and $f_X = \min(\pi_X;\mathbb{Q})^m$ for some $m \in \mathbb{N}$. It follows that the complex roots of f_X are the $\iota(\pi_X)$ for all complex embeddings $\iota \colon \mathbb{Q}[\pi_X] \hookrightarrow \mathbb{C}$. Since $\pi_X^\dagger = q/\pi_X$, the Rosati involution preserves $\mathbb{Q}[\pi_X]$. Since $f_X = \min(\pi_X;\mathbb{Q})^m$, we have $\mathrm{trace}(x) = m\mathrm{Tr}_{\mathbb{Q}[\pi_X]/\mathbb{Q}}(x)$ for all $x \in \mathbb{Q}[\pi_X]$. It follows from Theorem 2.2 that $\mathbb{Q}[\pi_X]$ is a number field with an involution † such that the quadratic form $\mathbb{Q}[\pi_X] \longrightarrow \mathbb{Q}, x \mapsto \mathrm{Tr}_{\mathbb{Q}[\pi_X]/\mathbb{Q}}(xx^\dagger)$ is positive-definite. This places strong restrictions on $\mathbb{Q}[\pi_X]$: in fact, $\mathbb{Q}[\pi_X]$ is either

(a) totally real with $\dagger = \mathrm{id}$,

(b) a CM-field with $\iota(x^\dagger) = \overline{\iota(x)}$ for all $x \in \mathbb{Q}[\pi_X]$ and all complex embeddings $\iota\colon \mathbb{Q}[\pi_X] \hookrightarrow \mathbb{C}$.

In any case, we obtain $|\iota(\pi_X)|^2 = \iota(\pi_X \pi_X^\dagger) = q$.

We now justify the above classification (we refer to [3, p. 193-194] for more details). Let F be the subfield of $\mathbb{Q}[\pi_X]$ fixed by $\dagger$. Suppose first that $\mathbb{Q}[\pi_X] = F$. Then $\dagger = \mathrm{id}$ and $\mathrm{Tr}_{\mathbb{Q}[\pi_X]/\mathbb{Q}}(x^2) > 0$ for all $0 \neq x \in \mathbb{Q}[\pi_X]$, i.e., $\mathbb{Q}[\pi_X]$ is a number field with positive-definite trace form. Let v be an infinite place and consider the completion $\mathbb{Q}[\pi_X]_v$. Then $\mathrm{Tr}_{\mathbb{Q}[\pi_X]_v/\mathbb{R}}(x_v^2) > 0$ for all $0 \neq x_v \in \mathbb{Q}[\pi_X]_v$ excludes $\mathbb{Q}[\pi_X]_v = \mathbb{C}$. Thus, all infinite places are real and we are in case (a). Suppose next that $\mathbb{Q}[\pi_X] \neq F$. Then $\mathbb{Q}[\pi_X] = F(\sqrt{\alpha})$ for some $\alpha \in F$ and $(\sqrt{\alpha})^\dagger = -\sqrt{\alpha}$. By the same argument as in the previous case, the subfield F is totally real. For all $x \in \mathbb{Q}[\pi_X]$, $\mathrm{Tr}_{\mathbb{Q}[\pi_X]/\mathbb{Q}}(x)$ coincides with the trace $\mathrm{Tr}(x)$ of left multiplication by x on $\mathbb{Q}[\pi_X]$. Now, $\mathbb{Q}[\pi_X]$ is a 2-dimensional F-algebra with a positive involution in the sense that $\mathrm{Tr}(xx^\dagger) > 0$ for all $0 \neq x \in \mathbb{Q}[\pi_X]$. It follows that the extension of $\dagger$ to $\mathbb{Q}[\pi_X] \otimes_F \mathbb{R}$ is a positive involution. Let v be an archimedean place of F (necessarily real). Then $\mathbb{Q}[\pi_X] \otimes_v \mathbb{R}$ is a 2-dimensional $\mathbb{R}$-algebra with a positive involution. Note that $\mathbb{Q}[\pi_X] \otimes_v \mathbb{R}$ is either $\mathbb{R}^2$ or $\mathbb{C}$. However, the standard involution on $\mathbb{R}^2$ is not positive since for $\alpha = (x, y) \in \mathbb{R}^2$, $\mathrm{Tr}(\alpha\bar{\alpha}) = 2xy$. This excludes $\mathbb{Q}[\pi_X] \otimes_v \mathbb{R} = \mathbb{R}^2$ and we are in case (b).

ii) If $\sqrt{q}$ or $-\sqrt{q}$ occurs as a root, then we are in case (a) above, i.e., $\mathbb{Q}[\pi_X]$ is totally real and $\sqrt{q}$ and $-\sqrt{q}$ are the only possible roots. Hence $f_X(t) = (t - \sqrt{q})^n (t + \sqrt{q})^{2g-n}$ and $f_X(0) = (-1)^n q^g$. But $f_X(0) = \deg(f_X) = q^g$ by definition of the characteristic polynomial, hence n is even. $\square$

References

[1] Bas Edixhoven, Ben Moonen, Gerard van der Geer, *Abelian varieties*, `http://van-der-geer.nl/~gerard/AV.pdf`

[2] James S. Milne, *Abelian varieties*, `https://www.jmilne.org/math/CourseNotes/AV.pdf`

[3] David Mumford, *Abelian varieties*, `https://wstein.org/edu/Fall2003/252/references/mumford-abvar/Mumford-Abelian_Varieties.pdf`

Einstein Institute of Mathematics, Hebrew University of Jerusalem, Israel

E-mail address: `davidterborchgram.lilienfeldt@mail.huji.ac.il`