Université Grenoble Alpes

ANNALES DE L'INSTITUT FOURIER

Yuri G. Zarhin

Tate classes on self-products of Abelian varieties over finite fields

Tome 72, nº 6 (2022), p. 2339-2383.

https://doi.org/10.5802/aif.3483

Les *Annales de l'Institut Fourier* sont membres du Centre Mersenne pour l'édition scientifique ouverte
www.centre-mersenne.org e-ISSN : 1777-5310

Ann. Inst. Fourier, Grenoble
72, 6 (2022) 2339-2383

TATE CLASSES ON SELF-PRODUCTS OF ABELIAN VARIETIES OVER FINITE FIELDS

by Yuri G. ZARHIN (*)

Abstract. — We deal with g-dimensional abelian varieties X over finite fields. We prove that there is a universal constant (positive integer) $N = N(g)$ that depends only on g that enjoys the following property. If a certain self-product of X carries an *exotic* Tate class then the self-product X^{2N} of X also carries an exotic Tate class. This gives a positive answer to a question of Kiran Kedlaya.

Résumé. — Nous étudions des variétés abéliennes X de dimension g sur des corps finis. Nous prouvons l'existence d'une constante universelle (entière positive) $N = N(g)$, qui ne dépend que de g et a la propriété suivante: si une certaine puissance de X admet une classe de Tate exotique, la puissance X^{2N} de X admet une classe de Tate exotique aussi. Cela donne une réponse positive à une question de Kiran Kedlaya.

1. Introduction

Let X be an abelian variety of positive dimension g over a finite field $k = \mathbb{F}_q$ of characteristic p (where q is a power of p), Fr_X the Frobenius endomorphism of X, and $\mathcal{P}_X[t] \in \mathbb{Z}[t]$ the characteristic polynomial of Fr_X, which is a degree $2g$ monic polynomial with integer coefficients. [8, 15]. Let $L = L_X$ be the splitting field of $\mathcal{P}_X[t]$ over the field $\mathbb{Q}$ of rational numbers and therefore is a number field. Since $\deg(\mathcal{P}_X) = 2g$, the degree $[L_X : \mathbb{Q}]$ divides $(2g)!$. (In fact, one may prove that $[L_X : \mathbb{Q}]$ divides $2^g g!$, see below). We write R_X for the set of eigenvalues of Fr_X; clearly, R_X coincides with the set of roots of $\mathcal{P}_X[t] \in \mathbb{Z}[t]$ and is viewed as a certain finite subset of L_X^*. Clearly, R_X consists of algebraic integers and $\#(R_X) \leqslant 2g$. (The equality holds if and only if $\mathcal{P}_X[t]$ has no repeated roots.) By a classical theorem

Keywords: Abelian varieties, Tate classes, Finite fields.
2020 *Mathematics Subject Classification:* 11G10, 11G25, 14G15.
(*) The author was partially supported by Simons Foundation Collaboration grant # 585711.

of A.Weil [8], all algebraic numbers $\alpha \in R_X$ have the same archimedean value $\sqrt{q}$. In addition, $\alpha \mapsto q/\alpha$ is a *permutation* of R_X. If α is a root of $\mathcal{P}_X[t]$ (i.e., $\alpha \in R_X$) then we write $\mathrm{mult}_X(\alpha)$ for its multiplicity. It is well known that if $\alpha \in R_X$ then

$$\mathrm{mult}_X(\alpha) = \mathrm{mult}_X(q/\alpha); \text{ if } \quad \alpha = q/\alpha \text{ then } \mathrm{mult}_X(\alpha) \text{ is even.} \tag{1.1}$$

In particular, the constant term $\prod_{\alpha \in R_X} \alpha^{\mathrm{mult}_X(\alpha)}$ of $\mathcal{P}_X[t]$ is q^g.

The Galois group $\mathrm{Gal}(L_X/\mathbb{Q})$ of $L_X/\mathbb{Q}$ permutes elements of R_X and

$$\mathrm{mult}_X(\sigma(\alpha)) = \mathrm{mult}_X(\alpha) \ \ \forall\, \sigma \in \mathrm{Gal}\,(L_X/\mathbb{Q})\,, \alpha \in R_X. \tag{1.2}$$

In this paper we continue our study of multiplicative relations between elements of R_X that was started in [6, 20, 21, 22]. (In [6, 20] we concentrated on abelian varieties with rather special type of Newton polygons; in [21, 22] we studied abelian varieties of small dimension). In order to state results of the present paper, we need the following definitions.

Definition 1.1. — *An integer-valued function $e\colon R_X \to \mathbb{Z}$ is called*

(i) **admissible** *if there exists an integer d such that*

$$\prod_{\alpha \in R_X} \alpha^{e(\alpha)} = q^d; \tag{1.3}$$

Such a d is called the **degree** *of e and is denoted* $\deg(e)$.

The nonnegative integer $\sum_{\alpha \in R_X} |e(\alpha)|$ is called the **weight** *of e and denoted* $\mathbf{wt}(e)$.

(ii) **trivial** *if*

$$e(\alpha) = e(q/\alpha) \ \ \forall\, \alpha \in R_X; \ e(\beta) \in 2\mathbb{Z} \ \ \forall\, \beta \in R_X \ \textit{ with } \ \beta^2 = q. \tag{1.4}$$

Definition 1.2. — *An* admissible *integer-valued function $e\colon R_X \to \mathbb{Z}$ is called* **reduced** *if it enjoys the following properties:*

(i) $\deg(e) \geqslant 1$ *and all* $e(\alpha) \geqslant 0$.
(ii) *If $\alpha \in R_X$ and $\alpha \neq q/\alpha$ then either $e(\alpha) = 0$ or $e(q/\alpha) = 0$.*
(iii) *$e(\beta) = 0$ or 1 $\forall\, \beta \in R_X$ with $\beta^2 = q$.*

Remarks 1.3.

(i) It follows from (1.1) that $\alpha \mapsto \mathrm{mult}_X(\alpha)$ is a trivial admissible function of degree g and weight $2g$.
(ii) Every trivial function is admissible.
(iii) If $e\colon R_X \to \mathbb{Z}$ is admissible then it follows from Weil's theorem that

$$2\deg(e) = \sum_{\alpha \in R_X} e(\alpha). \tag{1.5}$$

(iv) If $e\colon R_X \to \mathbb{Z}$ is reduced admissible then it follows from (1.5) that

$$\mathbf{wt}(e) = 2\deg(e). \tag{1.6}$$

Our first main result is the following assertion.

Theorem 1.4. — *Let g be a positive integer. There exists a positive integer $N = N(g)$ that depends only on g and enjoys the following property.*

Let X be a g-dimensional abelian variety over a finite field k such that there exists a nontrivial admissible function $R_X \to \mathbb{Z}$. Then there exists a reduced admissible function of degree $\leqslant N(g)$.

Our main tool in the proof of Theorem 1.4 is the multiplicative (sub)-group $\Gamma(X,k) \subset L_X^*$ generated by R_X, which was first introduced in [17, 18] (see also [6, 20, 21, 22]).

Definition 1.5.

(i) *We say that $k = \mathbb{F}_q$ is* small *with respect to X if there exist* distinct $\alpha_1, \alpha_2 \in R_X$ *such that α_1/α_2 is a* root of unity.

(ii) *We say that k is* sufficiently large *with respect to X if $\Gamma(X,k)$ does* not *contain roots of unity except 1 (see [21, 22]).*

Remarks 1.6.

(i) If k is *not* small with respect to X then there is at most one $\beta \in R_X$ with $\beta^2 = q$.

(ii) If k is sufficiently large with respect to X then it is *not* small.

The role of $\Gamma(X,k)$ is explained by the following statement.

Lemma 1.7. — *Suppose that k is not small with respect to X. Then the following three conditions are equivalent.*

(i) *There exists a nontrivial admissible function $R_X \to \mathbb{Z}$.*

(ii) *There exists a reduced admissible function $R_X \to \mathbb{Z}$.*

(iii) *The rank of $\Gamma(X,k)$ does not exceed $\lfloor \#(R_X)/2 \rfloor$.*

Our second main result deals with Tate classes on abelian varieties (see [13, 14, 15, 19, 21] and Section 7.4 below for the definition of these classes and their basic properties). Recall that a Tate class is called *exotic* if it *cannot* be presented as a linear combination of products of divisor classes.

Theorem 1.8. — *Let g be a positive integer and let $N = N(g)$ be as in Theorem 1.4.*

Let X be a g-dimensional abelian variety over a finite field k of characteristic p. Assume that there exist a positive integer n and a prime $\ell \neq p$ such *that the self-product X^n of X carries an exotic ℓ-adic Tate cohomology class.*

Then the self-product X^{2N} of X carries an exotic l-adic cohomology Tate class for all primes $l \neq p$.

Remark 1.9. — Theorem 1.8 gives a positive answer to a question of Kiran Kedlaya, who pointed out that this result is related to the algorithmic problem of deciding whether or not a given abelian variety (specified by its Weil polynomial) is *neat* in a sense of [21, Section 3], [22]).

Is it possible to get all Tate classes on all self-products of X, using only Tate classses of bounded dimension? In order to answer this question, we need the following result about nonnegative admissible functions.

Theorem 1.10. — *Let g be a positive integer. Then there exists a positive even integer $H = H(g)$ that enjoys the following property.*

Let X be a g-dimensional abelian variety over a finite field k. Then there exist a positive integer d and d nonnegative admissible functions $e_i\colon R_X \to \mathbb{Z}_+$ such that:

(i) *the weight of each e_i does not exceed $H(g)$;*
(ii) *each nonnegative admissible function $e\colon R_X \to \mathbb{Z}_+$ may be presented as a linear combination of $e_1, \ldots, e_d$ with nonnegative integer coefficients.*

Theorem 1.10 implies the following assertion.

Theorem 1.11. — *Let g be a positive integer. Let $H = H(g)$ be as in Theorem 1.10.*

Let X be a g-dimensional abelian variety over a finite field k. Assume that k is sufficiently large w.r.t X. Let ℓ be a prime different from $\mathrm{char}(k)$ *and n be a positive integer. Then every ℓ-adic Tate cohomology class on X^n may be presented as a linear conbination of products of ℓ-adic Tate cohomology classes of dimension $\leqslant H(g)$.*

The paper is organized as follows. In Section 2 we discuss basic useful results about R_X and related objects, including the Newton polygons. In addition, we discuss roots of unity in $\Gamma(X, k)$ (Lemma 2.2) and the structure and degree of L_X (Lemma 2.5). In Section 3 we study multiplicative relations between Weil numbers (i.e., admissible functions) and their weights; in particular, we prove Lemma 1.7 (see Lemma 3.7). In Sections 4 and 5 we prove Theorems 1.4 and 1.10 respectively. Section 6 contains certain constructions from multilinear algebra that we use in Section 7 in order to prove Theorems 1.8 and 1.11.

As usual, ℓ and l are primes different from p, and $\mathbb{N}, \mathbb{Z}, \mathbb{Z}_\ell, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Q}_\ell$ stand for the set of positive integers, the rings of integers and ℓ-adic integers, the fields of rational, real, complex, and ℓ-adic numbers respectively. We write $\mathbb{Z}_+$ and $\mathbb{R}_+$ for the additive semigroups of *nonnegative* integers and of *nonnegative* real numbers respectively. If z is a complex number then we write $\bar{z}$ for its complex-conjugate. Similarly, if $\phi\colon E \hookrightarrow \mathbb{C}$ is a field embedding then we write $\bar{\phi}$ for the corresponding complex-conjugate field embedding

$$\bar{\phi}\colon E \hookrightarrow \mathbb{C},\ x \mapsto \overline{\phi(x)}.$$

If M is a positive integer and v and w are two vectors in $\mathbb{R}^M$ then we write $v \cdot w$ for their scalar product. If A is a finite set then we write $\#(A)$ for the number of its elements. We write $\mathrm{rk}(\Delta)$ for the rank of a finitely generated commutative group Δ.

Acknowledgements

I am deeply grateful to Kiran Kedlaya for interesting stimulating questions and to the referee, whose comments helped to improve the exposition.

Part of this work was done during my stay at Centre Émile Borel (Institut Henri Poincaré, Paris) in June-July 2019, whose hospitality and support are gratefully acknowledged.

2. Preliminaries

In this section we discuss basic properties of $L = L_X, R_X, \Gamma(X,k)$. Let us start with the formal definition of $\mathcal{P}_X(t)$.

Throughout this paper k is a finite field of characteristic p that consists of q elements, $\bar{k}$ an algebraic closure of k and $\mathrm{Gal}(k) = \mathrm{Gal}(\bar{k}/k)$ the absolute Galois group of k. It is well known that the profinite group $\mathrm{Gal}(k)$ is procyclic and the *Frobenius automorphism*

$$\sigma_k\colon \bar{k} \to \bar{k},\ x \mapsto x^q$$

is a topological generator of $\mathrm{Gal}(k)$. If $\ell \neq p$ is a prime then we write

$$\chi_\ell\colon \mathrm{Gal}(k) \to \mathbb{Z}_\ell^*$$

for the ℓ-adic *cyclotomic character* that defines the Galois action on all ℓ-power roots of unity in $\bar{k}$. By definition,

$$\chi_\ell(\sigma_k) = q \in \mathbb{Z}_\ell^*.$$

Let X be an abelian variety of positive dimension over k. We write $\mathrm{End}(X)$ for the ring of its k-endomorphisms and $\mathrm{End}^0(X)$ for the corresponding (finite-dimensional semisimple) $\mathbb{Q}$-algebra $\mathrm{End}(X)\otimes\mathbb{Q}$. We write $\mathrm{Fr}_X = \mathrm{Fr}_{X,k}$ for the Frobenius endomorphism of X. We have

$$\mathrm{Fr}_X \in \mathrm{End}(X) \subset \mathrm{End}^0(X).$$

It is well known that

$$\sigma_k(x) = \mathrm{Fr}_X(x) \;\; \forall\, x \in X(\bar{k}). \tag{2.1}$$

By a theorem of Tate [15, Section 3, Theorem 2 on p. 140], the $\mathbb{Q}$-subalgebra $\mathbb{Q}[\mathrm{Fr}_X]$ of $\mathrm{End}^0(X)$ generated by Fr_X coincides with the center of $\mathrm{End}^0(X)$. In particular, if $\mathrm{End}^0(X)$ is a field then $\mathrm{End}^0(X) = \mathbb{Q}[\mathrm{Fr}_X]$.

If ℓ is a prime different from p then we write $T_\ell(X)$ for the $\mathbb{Z}_\ell$-Tate module of X and $V_\ell(X)$ for the corresponding $\mathbb{Q}_\ell$-vector space

$$V_\ell(X) = T_\ell(X) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell.$$

It is well known [8, Section 18] that $T_\ell(X)$ is a free $\mathbb{Z}_\ell$-module of rank $2\mathrm{dim}(X)$ that may be viewed as a $\mathbb{Z}_\ell$-lattice in the $\mathbb{Q}_\ell$-vector space $V_\ell(X)$ of dimension $2\mathrm{dim}(X)$. The Galois action on $X(\bar{k})$ induces the continuous group homomorphism [10, 11]

$$\rho_\ell = \rho_{\ell,X} \colon \mathrm{Gal}(K) \to \mathrm{Aut}_{\mathbb{Z}_\ell}\left(T_\ell(X)\right) \subset \mathrm{Aut}_{\mathbb{Q}_\ell}\left(V_\ell(X)\right).$$

In addition, there is a canonical isomorphism of $\mathrm{Gal}(k)$-modules $X[\ell] \cong T_\ell(X)/\ell$ where $X[\ell]$ is the kernel of multiplication by ℓ in $X(\bar{k})$.

By functoriality, $\mathrm{End}(X)$ and Fr_X acts on ($T_\ell(X)$ and) $V_\ell(X)$; it is well known that the action of Fr_X coincides with the action of $\rho_\ell(\sigma_k)$. By a theorem of A. Weil [8, Section 19 and Section 21], Fr_X acts on $V_\ell(X)$ as a semisimple linear operator, its characteristic polynomial

$$\mathbb{P}_X(t) = \mathbb{P}_{X,k}(t) = \det\left(t\,\mathrm{Id} - \mathrm{Fr}_X, V_\ell(X)\right) \in \mathbb{Z}_\ell[t]$$

lies in $\mathbb{Z}[t]$ and does not depend on a choice of ℓ. In addition, all eigenvalues of Fr_X (which are algebraic integers) have archimedean absolute value equal to $q^{1/2}$, and if an eigenvalue of Fr_X is a square root of q then its multiplicity is even (see [20, p. 267]). This implies that the constant term of $\mathbb{P}_{X,k}(t)$ is $q^{\mathrm{dim}(X)}$. In particular, Fr_X acts as an *automorphism* of the free $\mathbb{Z}_\ell$-module $T_\ell(X)$.

This means that if

$$L = L_X \subset \mathbb{C}$$

is the splitting field of $\mathbb{P}_X(t)$ and

$$R_X = R_{X,k} \subset L$$

is the set of roots of $P(t)$ then L is a finite Galois extension of $\mathbb{Q}$ such that for every field embedding $L \hookrightarrow \mathbb{C}$ we have $\mid \alpha \mid = q^{1/2}$ for all $\alpha \in R_X$. Let $\mathrm{Gal}(L/\mathbb{Q})$ be the Galois group of $L/\mathbb{Q}$. Clearly, R_X is a $\mathrm{Gal}(L/\mathbb{Q})$-invariant (finite) subset of L^*. It follows easily that if $\alpha \in R_X$ then $q/\alpha \in R_X$. Indeed, q/α is the *complex-conjugate* $\bar{\alpha}$ of α. We have

$$q^{-1}\alpha^2 = \frac{\alpha}{q/\alpha}.$$

Definition 2.1. — *Let ℓ be a prime and n a positive integer. We write $\mathbf{e}_\ell(n)$ for the largest order of elements of the general linear group* $\mathrm{GL}(n, \mathbb{F}_\ell)$*. We write* $\exp_\ell(n)$ *for the* exponent *of* $\mathrm{GL}(n, \mathbb{F}_\ell)$*.*

Recall that $\Gamma(X, k)$ is the multiplicative subgroup of L generated by R_X.

Lemma 2.2. — *If $\gamma \in \Gamma(X, k)$ is a root of unity then there is a positive integer $m \leqslant \max(2\mathbf{e}_2(2g), \mathbf{e}_3(2g))$ such that $\gamma^m = 1$. In addition, $\gamma^{D(g)} = 1$ where*

$$D(g) := \mathrm{LCM}\left(2\exp_2(2g), \exp_3(2g)\right), \quad \textit{and} \quad m|D(g).$$

Proof. — In what follows we choose a prime $\ell \neq p$ and view Fr_X as the automorphism of free $\mathbb{Z}_\ell$-module $T_\ell(X)$ of rank $2g$. Then Fr_X induces the automorphism $\mathrm{Fr}_X \bmod \ell$ of the $2g$-dimensional $\mathbb{F}_\ell$-vector space

$$T_\ell(X)/\ell = X[\ell].$$

Let r be the order of

$$\mathrm{Fr}_X \bmod \ell \in \mathrm{Aut}_{\mathbb{F}_\ell}\left(X[\ell]\right) \cong \mathrm{GL}\left(2g, \mathbb{F}_\ell\right).$$

Clearly,

$$r \leqslant \mathbf{e}_\ell(2g) \quad \text{and} \quad r \mid \exp_\ell(2g).$$

In addition,

$$\mathrm{Fr}_X^r \in \mathrm{Id} + \ell\,\mathrm{End}_{\mathbb{Z}_\ell}\left(T_\ell(X)\right).$$

Let Δ be the multiplicative group generated by all the eigenvalues of Fr_X^r. Clearly, $\delta = \gamma^r \in \Delta$. Applying a variant of Minkowski's Lemma [12, Lemma 2.4], we obtain that $\delta = 1$ if $\ell > 2$ and $\delta^2 = 1$ if $\ell = 2$. This implies that $\gamma^r = 1$ if $\ell > 2$ and $\gamma^{2r} = 1$ if $\ell = 2$. Now let us put $\ell = 2$ if $p \neq 2$ and $\ell = 3$ if $p = 2$. The rest is clear. □

Let $\mathcal{O}_L$ be the ring of integers in L. Clearly, $R_X \subset \mathcal{O}_L$. By a classical theorem of A. Weil (Riemann's hypothesis) [8], if $j\colon L_X = L \hookrightarrow \mathbb{C}$ is a field embedding then $j(\alpha)\overline{j(\alpha)} = q$. This implies that if $\mathfrak{B}$ is a maximal ideal in $\mathcal{O}_L$ such that $\mathrm{char}(\mathcal{O}_L/\mathfrak{B}) \neq p$ then all elements of R_X are $\mathfrak{B}$-adic units. The p-adic behaviour of R_X is described in terms of the set Slp_X of *slopes of the Newton polygon* of X [9] (see also [22, Section 4]). Recall that

Slp_X is a finite nonempty set of rational numbers that enjoys the following properties.

(i) $0 \leqslant c \leqslant 1$ for all $c \in \mathrm{Slp}_X$.
(ii) $c \in \mathrm{Slp}_X$ if and only if $1 - c \in \mathrm{Slp}_X$.
(iii) If $c \in \mathrm{Slp}_X$ then either $c = 1/2$ or there is a positive integer $h \leqslant g = \dim(X)$ such that $c \in \frac{1}{h}\mathbb{Z}$.
(iv) Let $\mathfrak{P}$ be any maximal ideal in $\mathcal{O}_L$ such that $\mathrm{char}(\mathcal{O}_L/\mathfrak{P}) = p$ and let

$$\mathrm{ord}_{\mathfrak{P}} \colon L^* \to \mathbb{Q}$$

be the discrete valuation map attached to $\mathfrak{P}$ that is normalized by the condition

$$\mathrm{ord}_{\mathfrak{P}}(q) = 1.$$

Then

$$\mathrm{ord}_{\mathfrak{P}}(R_X) = \mathrm{Slp}_X.$$

(v) If $\alpha \in R_X$ then

$$\mathrm{ord}_{\mathfrak{P}}(q/\alpha) = 1 - \mathrm{ord}_{\mathfrak{P}}(\alpha).$$

(vi) Let μ_L the multiplicative group of all roots of unity in L. Then its image $\mathrm{ord}_{\mathfrak{P}}(\mu_L) = \{0\}$.

Properties (i)-(vi) imply readily the following assertion.

Lemma 2.3. — *Let g be a positive integer. Let us consider the set* $\mathrm{Slp}(g)$ *of all rational numbers c that enjoy the following properties.*

(1) $0 \leqslant c \leqslant 1$.
(2) *Either $c = 1/2$ or there exists a positive integer $h \leqslant g$ such that $c \in \frac{1}{h}\mathbb{Z}$.*

Then $\mathrm{Slp}(g)$ *is a* finite nonempty *set that enjoys the following property.*

If X is a g-dimensional abelian variety over a finite field then Slp_X *lies in* $\mathrm{Slp}(g)$.

Remarks 2.4. — Let $S(p)$ be the set of all maximal ideals in $\mathcal{O}_L$ such that $\mathrm{char}(\mathcal{O}_L/\mathfrak{P}) = p$. Since $L/\mathbb{Q}$ is Galois, $\#(S(p))$ divides $[L:\mathbb{Q}]$; in particular, $\#(S(p))$ divides $g!2^g$ (see Lemma 2.5 (ii) below). Let us define a group homomorphism

$$w_X \colon \Gamma(X,K) \to \mathbb{Q}^{S(p)}, \gamma \mapsto \{\mathrm{ord}_{\mathfrak{P}}(\gamma)\}_{\mathfrak{P} \in S(p)}.$$

(a) Clearly, $w_X(q)$ is the vector $\mathbf{1} \in \mathbb{Q}^{S(p)}$, all whose coordinates equal 1, hence

$$w_X\left(\frac{q}{\alpha}\right) = \mathbf{1} - w_X(\alpha) \ \ \forall\, \alpha \in R_X.$$

(b) By Property (iv) and Lemma 2.3,

$$w_X(R_X) \subset \mathrm{Slp}_X^{S(p)} \subset \mathrm{Slp}(g)^{S(p)} \subset \mathbb{Q}^{S(p)}.$$

(c) It follows from Property (v) that a vector $\widetilde{c} \in \mathbb{Q}^{S(p)}$ lies in $w_X(R_X)$ if and only if $\mathbf{1} - \widetilde{c} \in w_X(R_X)$.

(d) In light of Property (vi), $w_X(\gamma) = 0$ if γ is a root of unity. The converse is also true: it is proven in [19, Proposition 2.1 on p. 249] (see also [17, Proposition 3.1.5]) that $\ker(w_X)$ *consists of roots of unity*.

(e) It follows readily from (d) that:
   (1) none of elements in R_X lies in $\ker(w_X)$;
   (2) if k is *not small* w.r.t X and α_1, α_2 are distinct elements of R_X then
$$w_X(\alpha_1) \neq w_X(\alpha_2).$$

Lemma 2.5.

(i) *The field L_X is either $\mathbb{Q}$ or $\mathbb{Q}(\sqrt{p})$ or a CM field.*

(ii) *The field L_X is a finite Galois extension of $\mathbb{Q}$ and its degree $[L_X : \mathbb{Q}]$ divides $g!2^g$.*

(iii) *$\#(S(p))$ divides $g!2^g$.*

Proof. — Let us prove ((i),(ii)). By definition of the splitting field, $L_X/\mathbb{Q}$ is Galois.

Suppose that X is simple. According to [15, 16], $\mathcal{P}_X(t)$ is a power $\mathcal{P}_{\mathrm{irr}}(t)^a$ of a $\mathbb{Q}$-irreducible monic polynomial $\mathcal{P}_{\mathrm{irr}}(t)$ where a is a positive integer dividing $2g$ and

$$\deg(\mathcal{P}_{\mathrm{irr}}) = \frac{2g}{a}.$$

Clearly, L_X is the normal closure of the degree $2g/a$ number field $E_X := \mathbb{Q}[t]/\mathcal{P}_{\mathrm{irr}}(t)$. According to [16, Exemples], E_X is either $\mathbb{Q}$ or $\mathbb{Q}(\sqrt{p})$ or a CM field.

In the first two cases $L_X = \mathbb{Q}$ or $\mathbb{Q}(\sqrt{p})$; in particular, it is a totally real number field, whose degree divides $2g = 2\dim(X)$.

In the third case let E_X^+ be the maximal totally real subfield of E_X; $[E_X^+ : \mathbb{Q}] = g/a$ and E_X is a purely imaginary quadratic extension $E_X^+(\sqrt{-\delta})$ of E_X^+. Here δ is a totally positive element of E_X^+. Let L_X^+ be the normal closure of E_X^+. Since E_X^+ is totally real, L_X^+ is totally real as well, and its degree $[L_X^+ : \mathbb{Q}]$ divides $[E_X^+ : \mathbb{Q}]! = (g/a)!$. Since $-\delta \in E_X^+ \subset L_X^+$, its Galois orbit in L_X^+ consists at most of $[E_X^+ : \mathbb{Q}] = g/a$ elements. This implies that $[L_X : L_X^+]$ divides $2^{g/a}$, since L_X is obtained from L_X^+ by adjoining square roots of all the (totally negative) Galois conjugates $-\delta$. This implies that

L_X is a CM field and $[L_X : \mathbb{Q}]$ divides $(g/a)! \cdot 2^{g/a}$, which in turn, divides $g! \cdot 2^g$.

Now let us consider the general case when X is isogenous to a product $\prod_{i=1}^m X_i$ of m nonzero simple abelian varieties X_i. It is well known that if we put

$$g_i := \dim(X_i), \quad \text{and} \quad L_i := L_{X_i}$$

then

$$g = \dim(X) = \sum_{i=1}^m g_i, \quad \mathcal{P}_X(t) = \prod_{i=1}^m \mathcal{P}_{X_i}(t).$$

Let $\bar{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$. We may and will view all L_i as subfields of $\bar{\mathbb{Q}}$. Then L_X is the **compositum** of m number fields $L_{X_i} = L_i$ in $\bar{\mathbb{Q}}$. Applying ((i),(ii)) to simple X_i's, we obtain that L_X is either $\mathbb{Q}$ or $\mathbb{Q}(\sqrt{p})$ or a CM field, which proves (i).

In order to prove (ii), recall that all $L_i/\mathbb{Q}$ and $L_X/\mathbb{Q}$ are finite Galois extensions. Let $\mathrm{Gal}(L_i/\mathbb{Q})$ and $\mathrm{Gal}(L_X/\mathbb{Q})$ be the corresponding (finite) Galois groups. Clearly, each L_i is a $\mathrm{Gal}(L_X/\mathbb{Q})$-invariant subfield of L_X, and the corresponding restriction map

$$\mathrm{Gal}\left(L_X/\mathbb{Q}\right) \to \mathrm{Gal}\left(L_i/\mathbb{Q}\right), \quad s \mapsto s_i$$

is a surjective group homomorphism. On the other hand, since all the L_i's generate L_X as a field, the product-map

$$\mathrm{Gal}\left(L_X/\mathbb{Q}\right) \to \prod_{i=1}^m \mathrm{Gal}\left(L_i/\mathbb{Q}\right), \quad s \mapsto \{s_i\}_{i=1}^m$$

is a *group embedding*. By Lagrange's theorem, $\#(\mathrm{Gal}(L_X/\mathbb{Q}))$ divides $\prod_{i=1}^m \#(\mathrm{Gal}(L_i/\mathbb{Q}))$. In other words, $[L_X : \mathbb{Q}]$ divides $\prod_{i=1}^m [L_i : \mathbb{Q}]$, which, in turn, divides

$$\prod_{i=1}^m g_i! 2^{g_i} = 2^g \prod_{i=1}^m g_i!.$$

Since $\sum_{i=1}^m g_i = g$, the product $\prod_{i=1}^m g_i!$ divides $g!$. This implies that $[L_X : \mathbb{Q}]$ divides $2^g g!$, which ends the proof of (ii).

Let us prove (iii). Since $L_X/\mathbb{Q}$ is Galois, $\#(S(p))$ divides $[L_X : \mathbb{Q}]$. Now (iii) follows readily from (ii). $\square$

3. Multiplicative relations between Weil numbers

This section contains auxiliary results that will be used in Section 4 in the proof of Theorem 1.4.

3.1. The involution

Recall that there is an involution map

$$\iota : R_X \to R_X,\ \alpha \mapsto \frac{q}{\alpha} = \bar{\alpha}. \tag{3.1}$$

Let R_X^ι be the subset of fixed points of ι. Its elements (if there are any) are square roots of q; hence,

$$\#(R_X^\iota) \leqslant 2. \tag{3.2}$$

In addition, if k is *not* small with respect to X then at most *one square root* of q lies in R_X, hence,

$$\#(R_X^\iota) \leqslant 1. \tag{3.3}$$

Remark 3.1. — Suppose that k is *not* small w.r.t X. If β is an element of R_X such that β^2/q is a root of unity then $q/\beta \in R_X$ and the ratio

$$\frac{\beta}{q/\beta} = \frac{q}{\beta^2}$$

is a root of unity. This implies that $\beta = q/\beta$, i.e., $\beta \in R_X^\iota$.

Let us consider the free abelian group $\mathbb{Z}^{R_X}$ of functions $e : R_X \to \mathbb{Z}$. The involution ι induces an automorphism (also an involution)

$$\iota^* : \mathbb{Z}^{R_X} \to \mathbb{Z}^{R_X},\ \iota^* e(\alpha) := e(\iota\alpha) = e(q/\alpha).$$

Let us consider the group homomorphism

$$\Pi \colon \mathbb{Z}^{R_X} \to \Gamma(X,k) \subset L_X^*,\ e \mapsto \prod_{\alpha \in R_X} \alpha^{e(\alpha)}.$$

We have

$$\Pi(\iota^* e) = \overline{\Pi(e)}.$$

Remarks 3.2.

(i) If $\iota^* e = e$ then $\Pi(e) = \overline{\Pi(e)}$ is (totally) real; it follows from Weil's theorem that $\Pi(e)^2$ is an integral power of q. In particular, if $\sum_{\alpha \in R_X} e(\alpha)$ is even then it follows from Weil's theorem that $\Pi(e)$ is $\pm$ integral power of q.

(ii) If f is a function $R_X \to \mathbb{Z}$ then the function $e := f + \iota^* f$ is obviously trivial.

Conversely, one may easily check that a function $e \colon R_X \to \mathbb{Z}$ is trivial if and only if there exists $f \colon R_X \to \mathbb{Z}$ such that $e = f + \iota^* f$.

(iii) Clearly, e is admissible if and only if $\Pi(e)$ lies in the cyclic multiplicative subgroup $q^{\mathbb{Z}}$ generated by q.

3.2. Ranks and Orbits

The complement $R_X \setminus R_X^\iota$ splits (if it is not empty) into a disjoint union of 2-element orbits of ι say $\{\alpha, q/\alpha\}$. Let r_X be the number of such orbits, which is a nonnegative integer that vanishes if and only if $R_X = R_X^\iota$. We have

$$\#\left(R_X \setminus R_X^\iota\right) = 2r_X; \quad r_X \leqslant \frac{\#(R_X)}{2} \leqslant \frac{2g}{2} = g. \tag{3.4}$$

If $r_X \geqslant 1$ (i.e., $R_X \neq R_X^\iota$) then we have r_X 2-elements ι-orbits $O_1, \ldots, O_{r_X}$ in $R_X \setminus R_X^\iota$. By choosing arbitrarily an element $\alpha_i \in O_i$ for all $i = 1, \ldots, r_X$, we get

$$\begin{gathered} O_i = \{\alpha_i, q/\alpha_i\} \quad \forall\, i = 1, \ldots, r_X; \\ R_X \setminus R_X^\iota = \{\alpha_1, q/\alpha_1, \ldots, \alpha_{r_X}, q/\alpha_{r_X}\}. \end{gathered} \tag{3.5}$$

Recall [21], that $\Gamma(X,k)$ always contains q. Since $\beta^2 = q$ for all $\beta \in R_X^\iota$, the subgroup $\Gamma_1(X,k)$ of $\Gamma(X,k)$ generated by q and all elements of $R_X \setminus R_X^\iota$ has finite index in $\Gamma(X,k)$. In particular,

$$\operatorname{rk}\left(\Gamma_1(X,k)\right) = \operatorname{rk}\left(\Gamma(X,k)\right). \tag{3.6}$$

Clearly, if $r_X = 0$ then $\Gamma_1(X,k) = q^{\mathbb{Z}}$ has rank 1, hence $\operatorname{rk}(\Gamma(X,k)) = 1$. It follows from (3.5) that if $r_X \geqslant 1$ then $\Gamma_1(X,k)$ is generated by $\{\alpha_1, \ldots, \alpha_{r_X}; q\}$. In particular,

$$\operatorname{rk}\left(\Gamma_1(X,k)\right) \leqslant r_X + 1. \tag{3.7}$$

Remark 3.3. — Suppose that k is *not small* w.r.t X. Then $\#(R_X^\iota) = 0$ or 1 and therefore $\#(R_X) = 2r_X$ or $2r_X + 1$ respectively. In both cases

$$r_X = \left\lfloor \frac{\#(R_X)}{2} \right\rfloor. \tag{3.8}$$

Combining (3.8) with (3.7) and (3.6), we obtain that

$$\operatorname{rk}\left(\Gamma(X,k)\right) = \operatorname{rk}\left(\Gamma_1(X,k)\right) \leqslant r_X + 1 = \left\lfloor \frac{\#(R_X)}{2} \right\rfloor + 1. \tag{3.9}$$

3.3. Nontrivial and reduced admissible functions

The existence of a nontrivial admissible function implies certain restrictions on R_X.

LEMMA 3.4. — *Suppose that there exists a nontrivial admissible function $e\colon R_X \to \mathbb{Z}$ of degree, say, d.*

Then the following conditions hold.

(i) $R_X \neq R^{\iota}_X$, *i.e.*, $R_X \setminus R^{\iota}_X$ *is a nonempty subset of* R_X.

(ii) *For each nonzero integer* m *the function*

$$m \cdot e\colon R_X \to \mathbb{Z}, \quad \alpha \mapsto m \cdot e(\alpha)$$

is also nontrivial admissible.

(iii) *Let us consider the function* $e_0\colon R_X \to \mathbb{Z}$ *that vanishes identically on* R^{ι}_X *(if this subset is nonempty) and coincides with* e *on* $R_X \setminus R^{\iota}_X$. *Then* e_0 *is nontrivial. In addition, for each nonzero even integer* m *the function*

$$m \cdot e_0 : R_X \to \mathbb{Z}, \quad \alpha \mapsto m \cdot e_0(\alpha)$$

is nontrivial admissible, and its weight

$$\mathbf{wt}(m \cdot e_0) = |m|\mathbf{wt}(e_0) \leqslant |m|\mathbf{wt}(e). \tag{3.10}$$

Proof. — If $R^{\iota}_X = \emptyset$ then all three assertions of Lemma are obviously true. So, let us assume that $R^{\iota}_X \neq \emptyset$.

(i) Suppose that $R_X = R^{\iota}_X$. Then

$$\prod_{\alpha \in R^{\iota}_X} \alpha^{e(\alpha)} = q^d \quad \text{and} \quad \sum_{\alpha \in R^{\iota}_X} e(\alpha) = 2d$$

is an even integer. Since R^{ι}_X consists of one or two elements and e is *nontrivial*, there is $\beta \in R^{\iota}_X$ such the $e(\beta)$ is odd. This implies that R^{ι}_X consists of two elements, say, β and $-\beta$,

$$e(\beta) + e(-\beta) = 2d$$

and both integers $e(\beta)$ and $e(-\beta)$ are *odd*. This implies that (recall that $\beta^2 = q$)

$$\begin{aligned} q^d = \beta^{e(\beta)} \cdot (-\beta)^{e(-\beta)} &= \beta^{e(\beta)} \cdot (-1) \cdot \beta^{e(-\beta)} \\ = -\beta^{e(\beta)+e(-\beta)} \qquad &= -\beta^{2d} = -q^d. \end{aligned}$$

So, $q^d = -q^d$, which is absurd. The obtained contradiction proves (i).

(ii) The admissibility of $m \cdot e$ is obvious. The nontriviality is also clear if there exists $\alpha \in R_X \setminus R^{\iota}_X$ with

$$e(\alpha) \neq e(q/\alpha).$$

So, we may assume that $m \cdot e$ is trivial (we are going to arrive to a contradiction), and

$$e(\alpha) = e(q/\alpha) \;\; \forall\, \alpha \in R_X \setminus R^{\iota}_X. \tag{3.11}$$

This implies that there is an integer n such that

$$\prod_{\alpha \in R_X^\iota} \alpha^{e(\alpha)} = q^n.$$

It follows that the sum

$$\sum_{\alpha \in R_X^\iota} e(\alpha) = 2n \in 2\mathbb{Z} \tag{3.12}$$

is an *even* integer. On the other hand, the nontriviality of e combined with (3.11) implies that there is $\beta \in R_X^\iota$ with *odd* $e(\beta)$. Since $\#(R_X^\iota) \leqslant 2$, it follows from (3.12) that integer $e(\alpha)$ is odd for all $\alpha \in R_X^\iota$. It follows that $\prod_{\alpha \in R_X^\iota} \alpha = q^d$ for some integer d. Therefore $\#(R_X^\iota) = 2d$ is a positive even integer, i.e., R_X^ι consists of two elements $\beta, -\beta$ with $\beta^2 = q$; in addition, both integers $e(\beta)$ and $e(-\beta)$ are odd. The same computations as in the proof of (i) give us that

$$q^d = \beta^{e(\beta)}(-\beta)^{e(-\beta)} = -q^d,$$

hence, $q^d = -q^d$. The obtained contradiction proves the nontriviality of $m \cdot e$.

(iii) Suppose that e_0 is trivial, i.e.,

$$e(\alpha) = e(q/\alpha) \ \ \forall\, \alpha \in R_X \setminus R_X^\iota.$$

Then it is admissible and therefore there is an integer h such that

$$\prod_{\alpha \in R_X \setminus R_X^\iota} \alpha^{e_0(\alpha)} = \prod_{\alpha \in R_X \setminus R_X^\iota} \alpha^{e(\alpha)} = q^h.$$

Since e is admissible of degree d,

$$\prod_{\beta \in R_X^\iota} \beta^{e(\beta)} = q^{d-h}.$$

The nontriviality of e implies that there is $\beta \in R_X^\iota$ such that integer $e(\beta)$ is *odd*. Now the same computations as in the proof of (i) give us that R_X^ι consists of two elements β and $-\beta$, both integers $e(\beta)$ and $e(-\beta)$ are odd and eventually, $q^{d-h} = -q^{d-h}$. The obtained contradiction proves that e is *nontrivial*, which is the first assertion of (iii).

Let us prove the second asssertion of (iii). Since m is even, there is an integer n such that $m=2n$.We have

$$\begin{aligned} q^{md} &= \left(\prod_{\alpha\in R_X} \alpha^{e(\alpha)}\right)^m = \left(\prod_{\alpha\in R_X\setminus R_X^{\iota}} \alpha^{e(\alpha)}\right)^m \times \left(\prod_{\beta\in R_X^{\iota}} \beta^{e(\beta)}\right)^m \\ &= \left(\prod_{\alpha\in R_X} \alpha^{m\cdot e_0(\alpha)}\right) \times \left(\prod_{\beta\in R_X^{\iota}} \beta^{2n\cdot e(\beta)}\right) \\ &= \left(\prod_{\alpha\in R_X} \alpha^{m\cdot e_0(\alpha)}\right) \times \left(\prod_{\beta\in R_X^{\iota}} q^{n\cdot e(\beta)}\right). \end{aligned}$$

This implies that $\prod_{\alpha\in R_X} \alpha^{m\cdot e_0(\alpha)}$ is an integral power of q, i.e., $m\cdot e_0$ is *admissible*. The nontriviality of $m\cdot e_0$ follows from the nontriviality of e_0, because e_0 vanishes identically on R_X^{ι}. This ends the proof of (iii). The last assertion of (iii) about weights follows readily from obvious inequality $\mathbf{wt}(e_0)\leqslant \mathbf{wt}(e)$. □

It turns out that one may easily construct a reduced admissible function when k is *small* w.r.t X.

Lemma 3.5. — *Assume that there are distinct $\alpha_1,\alpha_2\in R_X$ such that $\gamma:=\alpha_2/\alpha_1$ is a root of unity. Then there is a reduced admissible function $e\colon R_X\to\mathbb{Z}$, whose weight w enjoys the following properties.*

$$w\leqslant 4\mathbf{e}_2(2g) \quad \textit{if} \quad p\neq 2;\ w\leqslant 2\mathbf{e}_3(2g)) \quad \textit{if} \quad p=2.$$

Proof. — Clearly, $\gamma\in\Gamma(X,k)$. By Lemma 2.2, there is a positive integer m such that

$$\gamma^m=1;\ m\leqslant 2\mathbf{e}_2(2g) \quad \text{if} \quad p\neq 2;\ m\leqslant \mathbf{e}_3(2g)) \quad \text{if} \quad p=2.$$

Hence, it suffices to produce a reduced multiplicative relation of weight $2m$. To this end, notice that $q/\alpha_1\in R_X$ and

$$\alpha_2^m\,(q/\alpha_1)^m=q^m.$$

If $\alpha_2\neq q/\alpha_1$ then we may define

$$e\colon R_X\to\mathbb{Z},\ e(\alpha_2):=m, e(q/\alpha_1):=m;\ e(\alpha):=0 \quad \text{for all other } \alpha.$$

Clearly, e is a *reduced admissible* function of weight $2m$.

Suppose that $\alpha_2=q/\alpha_1$. Since $\alpha_1\neq\alpha_2$,

$$\alpha_1\neq q/\alpha_1,\ \alpha_1^2\neq q.$$

Then we have

$$q^m = (\alpha_1\alpha_2)^m = \alpha_1^{2m}, \quad \text{i.e., } \alpha_1^{2m} = q^m.$$

Now let us consider

$$e\colon R_X \to \mathbb{Z},\ e(\alpha_1) := 2m;\ e(\alpha) := 0 \ \text{ for all other } \alpha.$$

Clearly, e is a *reduced admissible* function of weight $2m$. $\square$

The next Lemma 3.6 asserts that the existence of a nontrivial admissible function implies the existence of a reduced admissible function, whose weight we can control.

LEMMA 3.6. — *Let w be a positive integer. Suppose that k is not small w.r.t X and there exists a nontrivial admissible function of weight $\leqslant w$.*

Then there exist a nonempty subset $A_1 \subset R_X$, an integer-valued function $\widetilde{e}\colon A_1 \to \mathbb{Z}$, and a positive integer $s \leqslant w$ that enjoy the following properties.

(1) $\forall\, \alpha \in A_1$ *we have* $\frac{q}{\alpha} \notin A_1,\ \widetilde{e}(\alpha) > 0.$

(2)

$$\prod_{\alpha \,\in\, A_1} \alpha^{\tilde{e}(\alpha)} = q^s. \tag{3.13}$$

In particular, if we define

$$f\colon R_X \to \mathbb{Z},\ f(\alpha) := \widetilde{e}(\alpha)\ \ \forall\, \alpha \in A_1;\ f(\alpha) := 0\ \ \forall\, \alpha \notin A_1$$

then f is a reduced admissible function of weight $2s \leqslant 2w$ that vanishes identically on R_X^ι.

Proof. — By Lemma 3.4, $R_X \setminus R_X^\iota$ is *not* empty. Let $e\colon R_X \to \mathbb{Z}$ be a *nontrivial* admissible function e of weight $\leqslant w$. Let us consider (in the notation of Lemma 3.4) the function

$$h_2 = 2 \cdot e_0\colon R_X \to \mathbb{Z}.$$

It follows from Lemma 3.4 that h_2 is nontrivial admissible, it vanishes identically on R_X^ι and its weight does not exceed $2w$. This implies that

$$\prod_{\alpha \,\in\, R_X \setminus R_X^\iota} \alpha^{h_2(\alpha)} = q^d,\ 2w \geqslant \sum_{\alpha \,\in\, R_X} |h_2(\alpha)| \tag{3.14}$$

where d is an integer such that

$$|d| \leqslant \mathbf{wt}(h_2) \leqslant 2w.$$

The nontriviality and vanishing everywhere at R_X^ι of h_2 imply that the subset A of R_X defined by

$$A := \{\alpha \in R_X \mid h_2(\alpha) \neq h_2(q/\alpha)\}$$

is *nonempty*. It follows from the very definition that A is ι-invariant and does *not* meet R_X^ι. Let us define the subset A_1 of A by

$$A_1 := \{\alpha \in A \,|\, h_2(\alpha) > h_2(q/\alpha)\} \subset A \subset R_X.$$

Clearly, if $\alpha \in A$ then $\alpha \in A_1$ if and only if $\bar{\alpha} = q/\alpha \notin A_1$. This implies that A_1 is *nonempty* and A is the *disjoint union* of A_1 and $\iota(A_1)$. In particular, $\#(A) = 2\#(A_1)$.

On the other hand, if

$$B := \{\beta \in R_X \setminus R_X^\iota \,|\, h_2(\beta) = h_2(q/\beta)\} \subset \{R_X \setminus R_X^\iota\}$$

then B is ι-invariant, $R_X \setminus R_X^\iota$ is a disjoint union of A and B, and

$$\prod_{\beta \in B} \beta^{h_2(\beta)} = q^n$$

for some integer n with

$$|n| \leqslant \mathbf{wt}(h_2) \leqslant 2w.$$

Since $R_X \setminus R_X^\iota$ is a disjoint union of A and B, it follows from (3.14) that

$$\prod_{\alpha \in A} \alpha^{h_2(\alpha)} = \frac{q^d}{q^n} = q^{d-n}.$$

Since A is a disjoint union of A_1 and $\iota(A_1)$, we get

$$\begin{aligned} q^{d-n} &= \left(\prod_{\alpha \in A_1} \alpha^{h_2(\alpha)}\right) \times \left(\prod_{\alpha \in A_1} \iota(\alpha)^{h_2(\iota\alpha)}\right) \\ &= \left(\prod_{\alpha\in A_1} \alpha^{h_2(\alpha)}\right) \times \left(\prod_{\alpha\in A_1} (q/\alpha)^{h_2(q/\alpha)}\right) \\ &= \left(\prod_{\alpha \in A_1} \alpha^{h_2(\alpha)-h_2(q/\alpha))}\right) \times q^m \end{aligned}$$

where $m := \sum_{\alpha \in A_1} h_2(q/\alpha) \in \mathbb{Z}$. If we define the function

$$\widetilde{e}\colon A_1 \to \mathbb{Z},\ \alpha \mapsto h_2(\alpha) - h_2(q/\alpha)$$

then $\widetilde{e}(\alpha) > 0\ \ \forall\, \alpha \in A_1$,

$$\sum_{\alpha \in A_1} \widetilde{e}(\alpha) \leqslant \sum_{\alpha \in A_1} (|h_2(\alpha)| + |h_2(q/\alpha)|) = \sum_{\alpha \in A} |h_2(\alpha)| \leqslant \mathbf{wt}(h_2) \leqslant 2w,$$

and

$$q^{d-n} = \left(\prod_{\alpha \in A_1} \alpha^{\tilde{e}(\alpha)}\right) \times q^m,$$

i.e.,

$$\prod_{\alpha \in A_1} \alpha^{\tilde{e}(\alpha)} = q^{d-n-m}.$$

It remains to put $s := d - n - m$. This ends the proof of Lemma 3.6. $\square$

The following assertion contains Lemma 1.7. (Recall that $\Gamma_1(X, k)$ is defined in Subsection 3.2.)

Lemma 3.7. — *Suppose that k is not small w.r.t X.*

Then the following conditions are equivalent.

(1a) *There is a nontrivial admissible function on R_X.*

(1b) *There is a nontrivial admissible function on R_X that vanishes at R_X^ι.*

(2a) *There is a reduced admissible function on R_X.*

(2b) *There is a reduced admissible function on R_X that vanishes at R_X^ι.*

(3a) $\mathrm{rk}(\Gamma(X, k)) \leqslant \lfloor \#(R_X)/2 \rfloor$.

(3b) $\mathrm{rk}(\Gamma_1(X, k)) \leqslant \lfloor \#(R_X)/2 \rfloor$.

Proof. — Obviously, (1b) implies (1a), (2b) implies (2a) , (2a) implies (1a), and (2b) implies (1b). By Lemma 3.6, (1a) implies (2b). This implies that (1a), (1b), (2a), (2b) are equivalent.

In light of (3.6), conditions (3a) and (3b) are equivalent.

In order to handle conditions (3), let us discuss the parity of $\#(R_X)$, using the observations and notation of Subsection 3.1.

In order to check the equivalence of (1) and (3), let us start with the "degenerate" case $r_X = 0$, i.e., $R_X = R_X^\iota = \{\beta\}$. Then $\Gamma(X, k)$ is an infinite cyclic group generated by β containing the index 2 subgroup generated by $\beta^2 = q$. Therefore $\mathrm{rk}(\Gamma(X, k)) = 1 > 0$, i.e., (3a) does *not* hold. On the other hand, we have already seen (Lemma 3.4) that if $R_X = \{\beta\} = R_X^\iota$ then (1a) does *not* hold.

So, we may assume that $R_X \neq R_X^\iota$. Then the positive integer $r_X = \lfloor \#(R_X)/2 \rfloor$ is the number of all ι-orbits $O_1, \ldots, O_{r_X}$ in $R_X \setminus R_X^\iota$, see Subsection 3.2. If we choose any element α_i of O_i for all i then the $2r_X$-element set

$$R_X \setminus R_X^\iota = \{\alpha_1, q/\alpha_1, \ldots, \alpha_{r_X}, q/\alpha_{r_X}\}$$

and $\Gamma_1(X, k)$ is generated by q and $\{\alpha_1, \ldots, \alpha_{r_X}\}$, see Subsection 3.2.

Suppose that (3b) holds. This means that $\mathrm{rk}(\Gamma_1(X, k)) \leqslant r_X$. Hence, there are $(r_X + 1)$ integers $f_1, \ldots, f_{r_X}; d$ *not all* zeros, such that

$$\prod_{i=1}^{r_X} \alpha_i^{f_i} = q^d. \tag{3.15}$$

Clearly, *not all* $f_1, \ldots, f_{r_X}$ are zeros. Let us define the function

$$e\colon R_X \to \mathbb{Z},\ e(\alpha_i) = f_i\ \ \forall\, i = 1, \ldots, r_X;\ f(\alpha) = 0\ \text{ for all other } \alpha. \tag{3.16}$$

In light of (3.15) and (3.16), e is a nontrivial admissible function. Hence, (1a) holds.

Now assume that (1a) holds. Then (2b) holds, i.e., there are a *nonempty* subset $A_1 \subset R_X$, a function $\widetilde{e}\colon A_1 \to \mathbb{Z}$ and a positive integer s that enjoy the following properties.

(i) A_1 and $\iota(A_1)$ do not meet each other;
(ii) $\widetilde{e}(\alpha) > 0\ \ \forall\, \alpha \in A_1$;
(iii) $\prod_{\alpha \in A_1} \alpha^{\tilde{e}(\alpha)} = q^s$.

Let us put $n := \#(A_1)$ and let $A_1 = \{\alpha_1, \ldots \alpha_n\}$. Then all $O_i = \{\alpha_i, q/\alpha_i\}$ are disjoint 2-element orbits in $R_X \setminus R_X^{\iota}$. In particular, $n \leqslant r_X$.

If $n = r_X$ then $\{\alpha_1, \ldots, \alpha_{r_X}; q\}$ generate $\Gamma_1(X, k)$. The property (iii) implies that the rank of this group does not exceed r_X, i.e., (3b) holds.

Now assume that $n < r_X$. Then there are precisely $(r_X - n)$ *other* two-element ι-orbits O_j in R_X $(j = n+1, \ldots r_X)$. If we pick for all j an element $\delta_j \in O_j$ then $O_j = \{\delta_j, q/\delta_j\}$ $(n+1 \leqslant j \leqslant r_X)$. Then $\{\alpha_1, \ldots, \alpha_n; \delta_{n+1}, \ldots, \delta_{r_X}; q\}$ generate a subgroup of finite index in $\Gamma_1(X, k)$. The property (iii) implies that the rank of this group does not exceed r_X, i.e., (3b) holds. This ends the proof of Lemma 3.7. □

4. Frames and Skeletons of Abelian Varieties over Finite Fields

In the course of our proof of Theorem 1.4 we will need the following notion.

Definition 4.1. — *Let g be a positive integer. A g-frame is a triple (M, r, U) that consists of positive integers M and r, and a finite subset*

$$U \subset \mathbb{Q}^M$$

of nonzero *vectors that enjoy the following properties.*

(i) *M divides $2^g g!$, $r \leqslant g$, and $\#(U) = 2r$.*
(ii) *$U \subset \mathrm{Slp}(g)^M \subset \mathbb{Q}^M$ (see Lemma 2.3 for the definition of the finite subset $\mathrm{Slp}(g) \subset \mathbb{Q}$).*
(iii) *A vector $u \in \mathbb{Q}^M$ lies in U if and only if $\mathbf{1} - u$ lies in U. Here $\mathbf{1} = (1, \ldots, 1) \in \mathbb{Q}^M$ is the vector, all whose coordinates are 1.*
(iv) *Let $\Delta(U)$ be the additive subgroup of $\mathbb{Q}^M$ generated by $\mathbf{1}$ and all elements of U. Then the rank of $\Delta(U)$ does not exceed r.*

Remark 4.2. — The *finiteness* of $\mathrm{Slp}(g)$ implies that the set of all frames (for a given g) is finite.

4.1. Properties of frames

The map

$$\iota_F \colon \mathbb{Q}^M \to \mathbb{Q}^M,\ u \mapsto \mathbf{1} - u \tag{4.1}$$

is an involution, whose only fixed point is

$$\frac{1}{2} \cdot \mathbf{1} = (1/2, \dots, 1/2).$$

Notice that

$$\iota_F(U) = U.$$

Since $\#(U)$ is *even*, U does *not* contain the *fixed point* $\frac{1}{2} \cdot \mathbf{1}$ and therefore splits into a disjoint union of 2-element ι_F-orbits $O_1, \dots, O_r$. If we choose in each O_i a vector $u_i \in O_i$ then

$$\begin{aligned} O_i &= \{u_i, \mathbf{1} - u_i\} \quad \forall\ i = 1, \dots, r; \\ U &= \{u_1, \mathbf{1} - u_1, \dots, u_i, \mathbf{1} - u_i, \dots, \mathbf{1} - u_r\} \end{aligned} \tag{4.2}$$

Definition 4.1 (iv) combined with (4.2) implies that there exist integers $a_1, \dots, a_r$ not all zeros and an integer d such that

$$\sum_{i=1}^{r} a_i u_i = d \cdot \mathbf{1} = (d, \dots, d)\,. \tag{4.3}$$

Lemma 4.3. — *Let g be a positive integer. Then there is a positive integer $C(g)$ that depends only on g and enjoys the following property.*

Let (M, r, U) be a g-frame. Then there are exist r integers $a_1, \dots, a_r$ not all zeros, an integer d, and r distinct vectors $u_1, \dots, u_r$ in U such that:

(i) *the $2r$-element set $U = \{u_1, \mathbf{1} - u_1, \dots, u_i, \mathbf{1} - u_r\}$;*
(ii) $\sum_{i=1}^{r} a_i u_i = d \cdot \mathbf{1} = (d, \dots, d)$;
(iii) $\sum_{i=1}^{r} |a_i| \leqslant C(g)$.

Proof. — The assertions follow readily from the construction of Subsection 4.1 combined with Remark 4.2. $\square$

4.2. Skeletons of abelian varieties

Let X be a g-dimensional abelian variety over a finite field k of characteristic p. Suppose that k is *not small* with respect to X and there exists a nontrivial admissible function $R_X \to \mathbb{Z}$. The aim of this subsection is to assign to X a certain g-frame that we call the *skeleton* of X.

First, let us put $r := r_X$ and $M := M_X := \#(S(p))$ where $S(p)$ is the set of maximal ideals in $\mathcal{O}_{L_X}$ that lie above p (see Remark 2.4). It follows from Lemma 2.5 that M divides $2^g \cdot g!$. By Lemma 3.4, the existence of a nontrivial admissible function implies that $R_X \neq R_X^\iota$ and $r = r_X$ is a positive integer. In addition (see (3.4)),

$$r \leqslant g,\ 2r = \#\left(R_X \setminus R_X^\iota\right).$$

Let us choose an order on the M-element set $S(p)$. This allows us to identify $S(p)$ with $\{1, \dots, M\}$ and $\mathbb{Q}^{S(p)}$ with $\mathbb{Q}^M$. Let us put

$$U = U_X := w_X\left(R_X \setminus R_X^\iota\right) \subset \mathbb{Q}^{S(p)} = \mathbb{Q}^M$$

(where homomorphism w_X is defined in Remark 2.4). It follows from Remark 2.4(d) that the map

$$R_X \setminus R_X^\iota \to U_X, \quad \alpha \mapsto w_X(\alpha) \tag{4.4}$$

is *injective*; in particular,

$$2r = 2r_X = \#\left(R_X \setminus R_X^\iota\right) = \#(U_X).$$

Since $\ker(w_X)$ consists of roots of unity (see Remark 2.4(d)), the rank of $\Delta(U_X)$ coincides with the rank of multiplicative $\Gamma_1(X,k)$ generated by $R_X \setminus R_X^\iota$. The existence of a nontrivial admissible function implies (thanks to Lemma 3.7) that

$$\mathrm{rk}\left(\Delta(U_X)\right) = \mathrm{rk}\left(\Gamma_1(X,k)\right) \leqslant r_X. \tag{4.5}$$

I claim that (M_X, r_X, U_X) is a g-frame. Indeed, it follows from Remarks 2.4 that

$$w_X(q) = \mathbf{1}; w_X(\alpha) \neq 0,\ w_X(q/\alpha) = \mathbf{1} - w_x(\alpha)\ \ \forall\, \alpha \in R_X \setminus R_X^\iota. \tag{4.6}$$

This implies that (M_X, r_X, U_X) enjoys the properties (i)-(iii). As for (iv), its validity follows from (4.5).

Proof of Theorem 1.4. — Let g be a positive integer. In light of Lemma 3.5, we may and will assume that k is *not small* w.r.t. X. In light of Lemma 3.6, it suffices to prove the following assertion.

Claim 4.4. — *There exists a positive integer $E(g)$ that depends only on g and enjoys the following property. Suppose that X is a g-dimensional abelian variety over a finite field k such that k is not small w.r.t. X and there exists a nontrivial admissible function $R_X \to \mathbb{Z}$.*

Then there exists a nontrivial admissible function $R_X \to \mathbb{Z}$ of weight $\leqslant E(g)$.

Proof of Claim. — Let X be an g-dimensional abelian variety over a finite field k such that k is not small w.r.t. X and there exists a nontrivial admissible function $R_X \to \mathbb{Z}$. Let us consider the corresponding g-frame (M_X, r_X, U_X). It follows from the injectiveness of the map (4.4) combined with Lemma 4.3 that there exist r_X distinct elements $\alpha_1, \dots, \alpha_{r_X} \in R_X \setminus R_X^{\iota}$, r_X integers $a_1, \dots, a_{r_X}$, and an integer d that enjoys the following properties.

(1) $R_X \setminus R_X^{\iota} = \{\alpha_1, q/\alpha_1 \dots, \alpha_{r_X}, q/\alpha_{r_X}\}$.
(2) Not all $a_1, \dots a_{r_X}$ are zero.
(3) $\sum_{i=1}^{r_X} a_i w_X(\alpha_i) = d \cdot \mathbf{1} = (d, \dots, d)$.
(4) $\sum_{i=1}^{r} |a_i| \leqslant C(g)$. (Here $C(g)$ is as in Lemma 4.3.)

It follows from Remark 2.4(d) that there exists a root of unity $\gamma \in \Gamma(X, k)$ such that

$$\prod_{i=1}^{r_X} \alpha_i^{a_i} = q^d \gamma.$$

According to Lemma 2.2, there exists a positive integer $m \leqslant D(g)$ such that $\gamma^m = 1$. (See Lemma 2.2 for the explicit formula of $D(g)$.) This implies that

$$\prod_{i=1}^{r_X} \alpha_i^{m a_i} = q^{md}.$$

This implies that the function

$$e \colon R_X \to \mathbb{Z},\ e(\alpha_i) = m \cdot a_i\ \ \forall\, \alpha_i,\ e(\alpha) = 0 \quad \text{forall other } \alpha$$

is admissible. On the other hand, it follows from properties (1) and (2) that e is *nontrivial*. In order to finish the proof of Claim, one has only to notice that

$$\mathbf{wt}(e) = \sum_{i=1}^{r_X} |a_i| = m \sum_{i=1}^{r_X} |a_i| \leqslant D(g) \cdot C(g) =: E(g). \qquad \square$$

This ends the proof of Theorem 1.4. $\square$

5. Applications of Gordan's Lemma

In order to prove Theorem 1.10, we need the following variant of a classical result of P. Gordan.

Lemma 5.1. — *Let m and s be positive integers and $v_1, \dots v_s$ be elements of $\mathbb{Q}^m$. Let us consider the addditive semigroup*

$$W = \left\{u \in \mathbb{Z}_+^m \,\middle|\, u \cdot v_j = 0 \ \ \forall\, j = 1, \dots, s\right\} \subset \mathbb{Z}_+^m.$$

Then W is a finitely generated semigroup of $\mathbb{Z}_+^m$.

Proof. — Replacing all v_j by Nv_j, where N is a sufficiently divisible positive integer, we may and will assume that $v_j \in \mathbb{Z}^m$ for all $j = 1, \dots, s$.

Let us consider the rational polyhedral cone $\sigma \subset \mathbb{R}^m$ that is generated by the standard basis of $\mathbb{R}^m$ and all the vectors $\{v_1, \dots v_s\}$. Then the dual cone is

$$\sigma^\vee = \left\{u \in \mathbb{R}_+^m \,\middle|\, u \cdot v_j \geqslant 0 \ \ \forall\, j = 1, \dots, s\right\}.$$

By Gordan's Lemma [3, Chapter 1, Proposition 1.2.17], $\sigma^\vee \cap \mathbb{Z}^m$ is a finitely generated additive semigroup. Let G be a finite subset of $\sigma^\vee \cap \mathbb{Z}^m$ that contains 0 and generates $\sigma^\vee \cap \mathbb{Z}^m$. Then the intersection $G \cap W$ is a finite subset of W that contains 0. I claim that $G \cap W$ generates W as a semigroup. Indeed, if $w \in W$ then $w \in \sigma^\vee \cap \mathbb{Z}^m$ and therefore there exists a positive integer r and (not necessarily distinct) r elements $g_1, \dots g_r \in G$ such that $w = \sum_{i=1}^r g_i$. We have for all $j = 1, \dots, s$

$$0 = w \cdot v_j = \sum_{i=1}^r g_i \cdot v_j, \ \ g_i \cdot v_j \geqslant 0 \ \ \forall\, i = 1, \dots, s.$$

This implies that all $g_i \cdot v_j = 0$ and therefore all $g_i \in W$, i.e., $g_i \in G \cap W$. It follows that $G \cap W$ generates W as a semigroup. □

We also need the following elementary observation.

Lemma 5.2. — *Suppose that X is an abelian variety of positive dimension g over a finite field k with q elements. Suppose that k is sufficiently large w.r.t. X. Then a nonnegative integer-valued function $e\colon R_X \to \mathbb{Z}_+$ of even weight is admissible if and only if*

$$w_X\left(\prod_{\alpha \,\in\, R_X} \left(\alpha^2/q\right)^{e(\alpha)}\right) = 0 \in \mathbb{Q}^{S(p)}. \tag{5.1}$$

Remark 5.3. — Let $e\colon R_X \to \mathbb{Z}_+$ be an admissible nonnegative integer-valued function. Then its weight is twice its degree and therefore is *even*.

Proof of Lemma 5.2. — Since e is nonnegative, its weight coincides with

$$\sum_{\alpha\,\in\,R_X} e(\alpha) =: n.$$

Since this weight is even, there is a nonnegative integer d such that $n = 2d$.

Now notice that in light of Remark 2.4(d), (5.1) holds if and only if $\prod_{\alpha\,\in\,R_X}(\alpha^2/q)^{e(\alpha)}$ is a root of unity. This means that $\prod_{\alpha\,\in\,R_X}(\alpha^2/q)^{e(\alpha)} = 1$, because k is sufficiently large w.r.t. X. Hence, (5.1) means that

$$\left(\prod_{\alpha\,\in\,R_X} \alpha^{e(\alpha)}\right)^2 = q^n \quad \text{with} \quad n = \sum_{\alpha\,\in\,R_X} e(\alpha) = 2d.$$

This means that

$$\prod_{\alpha\,\in\,R_X} \alpha^{e(\alpha)} = \pm q^d. \tag{5.2}$$

Since torsion-free $\Gamma(X,k)$ does not contain -1, (5.2) is equivalent to

$$\prod_{\alpha\,\in\,R_X} \alpha^{e(\alpha)} = q^d,$$

i.e, e is admissible. □

Proof of Theorem 1.10. — Let X be an abelian variety of positive dimension g over a finite field k of characteristic p. Suppose that k is sufficiently large w.r.t. X. Let us put $s := \#(S(p))$. By Lemma 2.5, s divides $2^g \cdot g!$. Let us choose an order in $S(p)$. This allows us to identify $S(p)$ with $\{1, \ldots, s\}$ and $\mathbb{Q}^{S(p)}$ with $\mathbb{Q}^s$. Let us choose an order on R_X: it allows us to list elements of R_X as $\{\alpha_1, \ldots, \alpha_m\}$ with $m = \#(R_X)$. We have $m \leqslant 2g$. Let us consider an additive group homomorpism

$$\begin{aligned}\widetilde{w}_X \colon \mathbb{Z}^m \to \mathbb{Q}^{S(p)} = \mathbb{Q}^s,&\\ u = (a_1, \ldots\, a_m) \mapsto w_X&\left(\prod_{i=1}^m \left(\alpha_i^2/q\right)^{a_i}\right)\\ &= 2\sum_{i=1}^m a_i w_X(\alpha_i) - \left(\sum_{i=1}^m a_i\right)\cdot \mathbf{1}.\end{aligned}$$

Clearly, there is a unique collection of s vectors $v_1, \ldots v_s \in \mathbb{Q}^m$ such that

$$\widetilde{w}_X(u) = (u\cdot v_1, \ldots, u\cdot v_s) \ \ \forall\, u \in \mathbb{Z}^m.$$

It is also clear that all the coordinates of all v_j's lie in the same finite set

$$2\cdot S(g) - 1 := \{2c-1 | c \in S(g)\} \subset \mathbb{Q}$$

that depends only on g. This implies that all the v_j's lie in the same finite subset

$$(2 \cdot S(g) - 1)^m \subset \mathbb{Q}^m$$

of $\mathbb{Q}^m$ that depends only on g and m. Combining this assertion with Lemma 5.1, we obtain that for each positive integers $m \leqslant 2g$ and s dividing $2^g \cdot g!$ there is a *finite subset* $F_0(g, m, s) \in \mathbb{Z}_+^m$ that depends only on g, m, s and enjoys the following property.

If $\#(R_X) = m$ *and* $\#(S(p)) = s$ *then the additive semigroup* $\ker(\widetilde{w}_X) \cap \mathbb{Z}_+^m$ *of* $\mathbb{Z}_+^m$ *is generated by a certain subset of* $F_0(g, m, s)$.

Now let as define the weight $\mathbf{wt}(u)$ of any $u = (a_1, \ldots, a_m) \in \mathbb{Z}_+^m$ as $\sum_{i=1}^m a_i$. It follows from Remark 5.3 combined with Lemma 5.2 that an integer-valued nonnegative function

$$\mathbf{b}_u \colon R_X \to \mathbb{Z}_+, \ \alpha_i \mapsto a_i$$

is *admissible* if and only if $u \in \ker(\widetilde{w}_X) \cap \mathbb{Z}_+^m$ and $\mathbf{wt}(u)$ is *even*. (It is also clear that each admissible nonnegative function $e : R_X \to \mathbb{Z}_+$ coincides with $\mathbf{b}_u$ for exactly one vector $u \in \mathbb{Z}_+^m$.) Then such u may be presented as a sum of (not necessarily distinct) elements of $F_0(g, m, s)$. It may happen that some elements of $F_0(g, m, s)$ in this sum have odd weight. Since the weight of u is even, the number of such summands is even. By grouping them in pairs, we obtain that u is a finite sum of some even weight elements from $F_0(g, m, s)$ and even weight elements from $F_0(g, m, s) + F_0(g, m, s) \subset \mathbb{Z}_+^m$. Now let $F(g, m, s) \subset \mathbb{Z}_+^m$ be the (finite) set of all even weight vectors from $F_0(g, m, s)$ and from $F_0(g, m, s) + F_0(g, m, s)$. Clearly, each $\mathbf{u} \in F(g, m, s)$ gives rise to nonnegative admissible $\mathbf{b}_{\mathbf{u}} \colon R_X \to \mathbb{Z}_+$ and each nonnegative admissible $e \colon R_X \to \mathbb{Z}_+$ may be presented as a linear combination of such $\mathbf{b}_{\mathbf{u}}$'s with nonnegative integer coefficients. Now one only has to choose as $H(g)$ the largest of the weights of $\mathbf{b}$ among all $\mathbf{u}$ (with *even weight*) in the union of all $F(g, m, s)$ where $1 \leqslant m \leqslant 2g$ and $s \mid 2^g \cdot g!$. $\square$

Theorem 1.10 implies readily the following assertion.

Corollary 5.4. — *Let g be a positive integer and $H(g)$ be as in Theorem 1.10.*

Let X an abelian variety of positive dimension g over a finite field k. Let $e : R_X \to \mathbb{Z}_+$ be a nonnegative admissible function. If $\mathbf{wt}(e) > H(g)$ then e may be presented as a sum $e = f_1 + f_2$ of two nonnegative admissible functions

$$f_1 \colon R_X \to \mathbb{Z}_+, \ f_2 \colon R_X \to \mathbb{Z}_+$$

such that $2 \leqslant \mathbf{wt}(f_2) \leqslant H(g)$.

6. Linear Algebra

Throughout this section, V is a nonzero vector space of finite dimension n over a field K of characteristic 0, and E is an overfield of K. We write V_E for the E-vector space $V \otimes_K E$ of the E-dimension n. Let us put

$$V^* = \mathrm{Hom}_K(V, K),\ V_E^* = \mathrm{Hom}_E\left(V_E, E\right).$$

Let $A\colon V \to V$ be a K-linear operator and

$$A^*\colon V^* \to V^*, \quad \phi \mapsto \phi \circ A \quad \forall\, \phi \in V^*.$$

As usual, let us define

$$A_E \in \mathrm{End}(V_E), \quad A_E(v \otimes e) = Av \otimes e \quad \forall\, v \in V, e \in E.$$

Clearly,

$$(A_E)^* = \left(A^*\right)_E : V_E^* \to V_E^*.$$

Remark 6.1. — Let $a \in K \subset E$ and $V(a)$ (resp. $V_E(a)$) be the eigenspace of A (resp. of A_E) attached to eigenvalue a. It is well known that the natural E-linear map

$$V(a) \otimes_K E \to V_E(a)$$

is an isomorphism of E-vector spaces; in particular,

$$\dim_K(V(a)) = \dim_E\left(V_E(a)\right)\ \forall\, a \in K \subset E.$$

There are well known natural isomorphisms [2, Chapter III, Section 7, Proposition 7] of graded K-algebras

$$\wedge\left(V^*\right) = \oplus_{j=0}^{n} \wedge_K^j\left(V^*\right) = \oplus_{j=0}^{n}\mathrm{Hom}_K\left(\wedge_K^j(V), K\right)$$

and of graded E-algebras [2, Chapter III, Section 7, Proposition 8]

$$\begin{aligned}\wedge\left(V_E^*\right) = \oplus_{j=0}^{n} \wedge_E^j\left(V_E^*\right) &= \oplus_{j=0}^{n}\mathrm{Hom}_E\left(\wedge_E^j(V_E), E\right)\\ &= \oplus_{j=0}^{n}\mathrm{Hom}_K\left(\wedge_K^j(V), K\right) \otimes_K E,\end{aligned}$$

which give rise to the natural isomorphisms of E-vector spaces

$$\wedge_K^j\left(V^*\right)_E \cong \wedge_E^j\left(V_E^*\right). \tag{6.1}$$

6.1. Wedge products

Let i and j be nonnegative integers. The multiplication in $\wedge(V^*)$ (resp. in $\wedge(V^*_E)$) gives rise to the surjective K-linear map

$$(6.2)\qquad \Lambda_{i,j,K}:\ \wedge^i_K(V^*)\otimes_K \wedge^j_K(V^*) \twoheadrightarrow \wedge^{i+j}_K(V^*),\ \psi_i\otimes\psi_j\mapsto \psi_i\wedge\psi_j$$

and to the surjective E-linear map

$$(6.3)\qquad \Lambda_{i,j,E}:\ \wedge^i_E(V^*_E)\otimes_E \wedge^j_E(V^*_E) \twoheadrightarrow \wedge^{i+j}_E(V^*_E),\quad \psi_i\otimes\psi_j\mapsto \psi_i\wedge\psi_j.$$

Let U be a K-vector subspace in $\wedge^i_K(V^*)$ and W be a K-vector subspace in $\wedge^j_K(V^*)$. Then obviously the images $\Lambda_{i,j,K}(U\otimes_K W)\subset \wedge^{i+j}_K(V^*)$ and $\Lambda_{i,j,E}(U_E\otimes_E W_E)\subset \wedge^{i+j}_E(V^*_E)$ are related by

$$(6.4)\qquad \Lambda_{i,j,E}(U_E\otimes_E W_E) = \Lambda_{i,j,K}(U\otimes_K W)_E\,.$$

Here we identify U_E (resp. W_E) with its isomorphic image in $\wedge^i_K(V^*)_E = \wedge^i_E(V^*_E)$ (resp. in $\wedge^j_K(V^*)_E = \wedge^j_E(V^*_E)$).

The equality (6.4) implies readily its own generalization. Namely, let n be a positive integer and suppose that for each positive integer $r\leqslant n$ we are given K-vector subspaces

$$U_r\subset \wedge^i_K(V^*),\quad W_r\subset \wedge^j_K(V^*)\,.$$

Then

$$(6.5)\qquad \sum_{r=1}^n \Lambda_{i,j,E}(U_{r,E}\otimes_E W_{r,E}) = \left(\sum_{r=1}^n \Lambda_{i,j,K}(U_r\otimes_K W_r)\right)_E.$$

Here

$$U_{r,E} = U_r\otimes_K E,\quad W_{r,E} = W_r\otimes_K E.$$

6.2. Wedge products of eigenspaces

The operators A^* and A^*_E give rise to the graded K-algebra and graded E-algebra *endomorphisms*

$$\wedge(A^*):\ \wedge(V^*)\to\wedge(V^*),\quad \wedge(A^*_E):\wedge(V^*_E)\to\wedge(V^*_E)$$

[2, Chapter III, Section 7, Proposition 2], whose homogeneous components are K-linear and E-linear operators

$$\wedge^j(A^*):\ \wedge^j_K(V^*)\to\wedge^j_K(V^*),\quad \wedge^j_E(A^*_E)\ :\ \wedge^j_E(V^*_E)\to\wedge^j_E(V^*_E)$$

respectively, such that

$$(6.6)\qquad \wedge^j(A^*_E) = \wedge^j(A^*)_E\,.$$

Since $\wedge(A)$ and $\wedge(A_E^*)$ respect the multiplication in $\wedge(V^*)$ and $\wedge(V_E^*)$ respectively,

$$\begin{aligned}(6.7)\quad & \wedge^i(A^*)(\psi_i)\wedge\ \wedge^j(A^*)(\psi_j)\\ &= \wedge^{i+j}(A^*)(\psi_i\wedge\psi_j)\in\wedge^{i+j}(V^*)\ \ \forall\,\psi_i\in\wedge^i(V^*),\psi_j\in\wedge^j(V^*);\end{aligned}$$

$$\begin{aligned}&\wedge^i(A_E^*)(\psi_{i,E})\wedge\ \wedge^j(A_E^*)(\psi_{j,E})\\ &\qquad= \wedge^{i+j}(A_E^*)(\psi_{i,E}\wedge\psi_{j,E})\in\wedge^{i+j}(V_E^*)\\ &\qquad\qquad\forall\,\psi_{i,E}\in\wedge^i(V_E^*),\psi_{j,E}\in\wedge^j(V_E^*).\end{aligned}$$

The following assertion is an immediate corollary of (6.7) and (6.6).

Lemma 6.2. — *Let j_1, j_2 be positive integers such that $j_1+j_2\leqslant\dim(V)$. Let λ_1,λ_2 be elements of K. Let $\wedge_K^{j_r}(V^*)(\lambda_r)\subset\wedge_K^{j_r}(V^*)$ be the eigenspace of $\wedge_r^j(A^*)$ attached to λ_r $(r=1,2)$. Then the image of the K-linear map*

$$\wedge_K^{j_1}(V^*)(\lambda_1)\otimes_K\wedge_K^{j_2}(V^*)(\lambda_2)\to\wedge_K^{j_1+j_2}(V^*),\quad \psi_{j_1}\otimes\psi_{j_2}\mapsto\psi_{j_1}\wedge\psi_{j_2}$$

lies in the eigenspace $\wedge_K^{j_1+j_2}(V^*)(\lambda_1\lambda_2)$ of $\wedge^{j_1+j_2}(A^*)$ attached to $\lambda_1\lambda_2$.

Remark 6.3. — The K-linear map in Lemma 6.2 is the restriction of $\Lambda_{j_1,j_2,K}$ defined in Subsection 6.1.

Remark 6.4. — Applying Remark 6.1 to $\wedge^j(A^*)\colon\ \wedge_K^j(V^*)\to\wedge_K^j(V^*)$ (instead of $A\colon V\to V$), we obtain that if $\lambda\in K\subset E$ and $\wedge_K^j(V^*)(\lambda)$ (resp. $\wedge^j(V_E^*)(\lambda)$) is the attached to λ eigenspace of $\wedge^j(V^*)$ (resp. of $\wedge^j(V_E^*)$) then the natural E-linear map

$$\wedge_K^j(V^*)(\lambda)\otimes_K E\to\wedge^j(V_E^*)(\lambda)$$

induced by (6.1) is an isomorphism. Combining this assertion with Lemma 6.2 applied twice (over K and over E), we get immediately the following assertion.

Lemma 6.5. — *Let j_1, j_2 be positive integers such that $j_1+j_2\leqslant\dim(V)$. Let $\lambda_1,\lambda_2\in K\subset E$. We keep the notation and assumptions of Lemma 6.2.*

The E-linear map

$$\wedge_E^{j_1}(V_E^*)(\lambda_1)\otimes_E\wedge_E^{j_2}(V_E^*)(\lambda_2)\to\wedge_E^{j_1+j_2}(V^*)(\lambda_1\lambda_2),\ \ \psi_1\otimes\psi_1\mapsto\psi_1\wedge\psi_2$$

is not surjective if and only if the K-linear map

$$\wedge_K^{j_1}(V^*)(\lambda_1)\otimes_K\wedge_K^{j_2}(V^*)(\lambda_2)\to\wedge_K^{j_1+j_2}(V^*)(\lambda_1\lambda_2),\ \ \psi_1\otimes\psi_1\mapsto\psi_1\wedge\psi_2$$

is not surjective. Here $\wedge_E^j(V_E^*)(\lambda)\subset\wedge_E^j(V_E^*)$ is the eigensubspace of $\wedge^j(A_E^*)$ attached to λ.

6.3. Main construction

We keep the notation of Remark 6.4. Suppose that $A_E\colon V_E \to V_E$ is *diagonalizable*, $\operatorname{spec}(A) \subset E$ is the set of its *eigenvalues*, and mult_A : $\operatorname{spec}(A) \to \mathbb{Z}_+$ is the integer-valued function that assigns to each eigenvalue of A_E its multiplicity.

Let $\lambda \in K$ and $j \leqslant \dim(V)$ be a positive integer. Let us consider an integer-valued function $e\colon \operatorname{spec}(A) \to \mathbb{Z}_+$ that enjoys the following properties.

(i) $e(\alpha) \leqslant \operatorname{mult}_A(\alpha) \ \ \forall\, \alpha \in \operatorname{spec}(A)$;
(ii) $\sum_{\alpha \in \operatorname{spec}(A)} e(\alpha) = j$;
(iii) $\prod_{\alpha \in \operatorname{spec}(A)} \alpha^{e(\alpha)} = \lambda$.

Let us choose an *eigenbasis* B of E-vector space V_E w.r.t. A_E and let

$$\pi\colon B \twoheadrightarrow \operatorname{spec}(A)$$

be the surjective map that assigns to each eigenvector $x \in B$ the corresponding eigenvalue of A_E. Clearly, for every eigenvalue $\alpha \in \operatorname{spec}(A)$ the preimage $\pi^{-1}(\alpha)$ consists of $\operatorname{mult}_A(\alpha)$ elements of B. Let

$$B^* = \{x^* \mid x \in B\}$$

be the basis of V_E^* that is dual to B. Let us choose an order on B and define for each j-element subset $C \subset B$ an element

$$y_C := \wedge_{x \in C} x^* \in \wedge^j \left(V_E^*\right).$$

Clearly, all y_C's constitute an eigenbasis of $\wedge^j(V_E^*)$ w.r.t. $\wedge^j(A^*)$. Actually,

$$\wedge^j \left(A^*\right)(y_C) = \left(\prod_{x \in C} \pi(x)\right) y_C.$$

Let us assign to C the integer-valued function

$$e_C\colon \operatorname{spec}(A) \to \mathbb{Z}_+,\ \alpha \mapsto \#\big(\{x \in C \mid \pi(x) = \alpha\}\big). \tag{6.8}$$

Clearly, y_C is an eigenvector of $\wedge^j(A^*)$ with eigenvalue λ if and only if $e = e_C$ enjoys the properties (i)-(iii). This implies that the set of y_C's such that e_C satisfies (i)-(iii) is a E-basis of the eigenspace $\wedge^j(V_E^*)(\lambda)$.

Conversely, suppose that $e\colon \operatorname{spec}(A) \to \mathbb{Z}_+$ is an integer-valued function that enjoys the properties (i)-(iii). I claim that there exists a j-element subset $C \subset B$ such that $e = e_C$. Indeed, let us choose a $e(\alpha)$-element subset $C_\alpha \subset \pi^{-1}(\alpha) \subset B$ for all $\alpha \in \operatorname{spec}(A)$ with $e(\alpha) > 0$. The property (i) guarantees that such a choice is possible (but not necessarily unique). Now define C as the (disjoint) union of all these C_α's. Property (ii) implies that B is a j-element subset of B. It follows from (iii) that $y_C \in \wedge^j(V_E^*)(\lambda)$.

The following assertion will be used in the proof of Theorem 1.8 (with $K = \mathbb{Q}_\ell, V = V_\ell(X^n), A = \mathrm{Fr}_{X^n}$).

Proposition 6.6. — *We keep the notation and assumptions of Subsection 6.3, Remark 6.1 and Lemma 6.5. In particular, $A_E\colon V_E \to V_E$ is diagonalizable. Assume additionally that $A\colon V \to V$ is invertible, $j_1 = j-2$ and $j_2 = 2$. Suppose that λ_1 and λ_2 are nonzero elements of K and $j > 2$, i.e., $j_1 \geqslant 1$. Then the following conditions are equivalent.*

(a) *The K-linear map*

$$\wedge_K^{j-2}(V^*)(\lambda_1) \otimes_K \wedge_K^2 (V^*)(\lambda_2) \to \wedge_K^j (V^*)(\lambda_1\lambda_2)\,, \psi\otimes\phi \mapsto \psi\wedge\phi \tag{6.9}$$

is not surjective.

(b) *There exists a function $e\colon \mathrm{spec}(A) \to \mathbb{Z}_+$ that enjoys the following properties.*
   (i) $e(\alpha) \leqslant \mathrm{mult}_A(\alpha)\ \ \forall\, \alpha \in \mathrm{spec}(A)$;
   (ii) $\sum_{\alpha\,\in\,\mathrm{spec}(A)} e(\alpha) = j$;
   (iii) $\prod_{\alpha\,\in\,\mathrm{spec}(A)} \alpha^{e(\alpha)} = \lambda_1\lambda_2$.
   (iv) *If $\alpha \in \mathrm{spec}(A)$ and $e(\alpha) \neq 0$ then $e(\alpha) \geqslant 1$ and one of the following conditions holds.*
      (1) $\lambda_2/\alpha \notin \mathrm{spec}(A)$;
      (2) $\lambda_2/\alpha \in \mathrm{spec}(A)$ *but* $e(\lambda_2/\alpha) = 0$.
      (3) $\alpha = \lambda_2/\alpha$ *(i.e., $\alpha^2 = \lambda_2$) and* $e(\alpha) = 1$.

Remark 6.7. — The invertibility of A means that $0 \notin \mathrm{spec}(A)$.

Remark 6.8. — In light of Lemma 6.5, it suffices to check that condition (b) is equivalent (in the obvious notation) to the *non-surjectiveness* of the E-linear map

$$\wedge_E^{j-2}(V_E^*)(\lambda_1) \otimes_E \wedge_E^2 (V_E^*)(\lambda_2) \to \wedge^j (V^*)(\lambda_1\lambda_2), \psi\otimes\phi \mapsto \psi\wedge\phi. \tag{6.10}$$

Proof of Proposition 6.6. — We start with the following lemma that describes the image of map (6.10).

Lemma 6.9. — *The image of map* (6.10) *is generated by all y_C's where C is any j-element subset of B that enjoys the following properties.*

The set C is a disjoint union of a $(j-2)$-element subset S and a 2-element subset T such that the corresponding functions

$$e_S\colon \mathrm{spec}(A) \to \mathbb{Z}_+,\ \ e_T\colon \mathrm{spec}(A) \to \mathbb{Z}_+$$

defined by(6.8) *enjoy the following properties.*

$$\prod_{\alpha \in \operatorname{spec}(A)} \alpha^{e_S(\alpha)} = \lambda_1, \quad \prod_{\alpha \in \operatorname{spec}(A)} \alpha^{e_T(\alpha)} = \lambda_2. \tag{6.11}$$

Proof of Lemma 6.9. — It follows from arguments of Subsection 6.3 that all the y_S's (resp. all the y_T's) where S is any $(j-2)$-element subset of B (resp. where T is any 2-element subset of B) that satisfies (6.11) constitute a basis of $\wedge_E^{j-2}(V_E^*)(\lambda_1)$ (resp. a basis of $\wedge_E^2(V_E^*)(\lambda_2)$. This implies that the image of map (6.10) is generated by all $y_S \wedge y_T$. If S meets T then it follows from the very definition of y_S and y_T and basic properties of wedge products that $y_S \wedge y_T = 0$. On the other hand, if S does *not* meet T then $C := S \cup T = S \sqcup T$ is a j-element subset of B and $y_S \wedge y_T = \pm y_C$. This ends the proof. □

Now let us start to prove Proposition 6.6. Suppose that condition (b) holds. In light of Remark 6.8, it suffices to check that map (6.10) is *not* surjective. To this end, choose an eigenbasis B of V_E w.r.t. A_E, and choose an order on B. Using arguments of Subsection 6.3, choose a j-element subset $\widetilde{C} \subset B$ such that the function

$$e_{\tilde{C}} \colon \operatorname{spec}(A) \to \mathbb{Z}_+$$

coincides with e and therefore enjoys properties (bi)-(biv). Then

$$y_{\tilde{C}} \in \wedge^j \left(V^*\right) \left(\lambda_1 \lambda_2\right).$$

I claim that $y_{\tilde{C}}$ does *not* lie in the image of map (6.10). Indeed, $\wedge_E^{j-2}(V_E^*)$ (λ_1) is generated as the E-vector space by elements of the form y_S, where S are $(j-2)$-element subsets of B such that $\prod_{b \in S} \pi(b) = \lambda_1$. On the other hand, $\wedge_E^2(V_E^*)(\lambda_2)$ is generated as the E-vector space by elements of the form y_T, where T are 2-element subsets of B such that $\prod_{b \in T} \pi(b) = \lambda_2$. This implies that the image of map (6.10) is generated as the E-vector space by all $y_B \wedge y_T$. If S meets T then (as we have already seen) $y_S \wedge y_T = 0$. If S does *not* meet T then $S \cup T = S \sqcup T$ is a j-element subset of B and $y_S \wedge y_T = \pm y_{S \cup T}$.

Lemma 6.10. — *The j-element $\widetilde{C}$ does* not *coincide with any of $S \cup T$.*

Proof of Lemma 6.10. — Suppose $\widetilde{C} = S \cup T$. This implies that $\widetilde{C}$ contains a subset T that consists of two distinct elements say $x_1, x_2 \subset B$ with $\pi(x_1)\pi(x_2) = \lambda_2$. So, $\widetilde{C}$ contains these x_1, x_2. It follows from the definition of $e_{\tilde{C}}$ (6.8) that if we put

$$\alpha_1 = \pi(x_1), \ \alpha_2 = \pi(x_2)$$

then $\alpha_1, \alpha_2 \in \operatorname{spec}(A)$ and

$$\alpha_1\alpha_2 = \lambda_2,\ e(\alpha_1) \geqslant 1, e(\alpha_2) \geqslant 1,\ e(\alpha_1) + e(\alpha_2) \geqslant 2.$$

If $\alpha_1 \neq \alpha_2 = \lambda_2/\alpha_1$ then $e(\alpha_1) \geqslant 1, e(\lambda_2/\alpha_1) \geqslant 1$, which violates property (biv). If $\alpha_1 = \alpha_2$ then $\alpha_2 = \lambda_2/\alpha_1$. It follows that $\alpha_1 = \pi(x_1) = \pi(x_2)$ and therefore $e(\alpha_1) \geqslant 2$, which also contradicts property (biv). This ends the proof. □

End of Proof of Proposition 6.6. — Taking into account that the set of all y_C's where C runs through all j-element subsets of B is *linearly independent*, we conclude that $y_{\tilde{C}}$ cannot be presented as a E-linear combination of $y_{S \cup T}$'s and therefore does *not* lie in the image of map (6.10). Hence, (a) holds. We proved that (b) implies (a).

Suppose that map (6.10) is *surjective*, i.e., (a) does not hold. We need to prove that (b) does not hold as well. Let $e\colon \operatorname{spec}(A) \to \mathbb{Z}_+$ be a function that enjoys the properties (i)-(iii) of Subsection 6.3. We need to check that e does not enjoy property 6.6(biv). Using arguments of Subsection 6.3, choose a j-element subset $\widetilde{C} \subset B$ such that the function

$$e_{\tilde{C}}\colon \operatorname{spec}(A) \to \mathbb{Z}_+$$

coincides with e and therefore enjoys properties (bi)-(biii). This implies that

$$y_{\tilde{C}} \in \wedge^j(V^*)(\lambda_1\lambda_2).$$

Let us check that $e = e_{\tilde{C}}$ does *not* enjoy property (biv). Indeed, we know that $y_{\tilde{C}}$ lies in the image of map (6.10). It follows from Lemma 6.9 that there is a positive integer m, m pairs of subsets $(S_1, T_1), \ldots, (S_m, T_m)$ in B, and m elements $a_1, \ldots, a_m \in E$ such that each $S = S_r$ and $T = T_r$ are disjoint $(j-2)$-element and 2-element subsets of B that satisfy (6.11) for all $r = 1, \ldots, m$, and such that

$$y_{\tilde{C}} = \sum_{r=1}^{m} a_r y_{S_r \sqcup T_r}.$$

Let us choose such a presentation for $y_{\tilde{C}}$ with smallest possible m. In this case all the j-element subsets $S_r \sqcup T_r$ are distinct. Now the linear independence of all y_C (where $C \subset B$ is a j-element subset) implies that $m = 1$ and $\widetilde{C}$ coincides with $S_1 \sqcup T_1$.

So, T_1 consists of two distinct elements say, x_1, x_2. Let us put

$$\alpha_1 := \pi(x_1) \in \operatorname{spec}(A), \alpha_2 = \pi(x_2) \in \operatorname{spec}(A).$$

It follows from (6.11) that $\alpha_1\alpha_2 = \lambda_2$. This implies that

$$e(\alpha_1) = e_{\tilde{C}}(\alpha_1) \geqslant 1,\ e(\alpha_2) = e_{\tilde{C}}(\alpha_2) \geqslant 1.$$

If $\alpha_1 \neq \alpha_2$ then property (biv) does not hold for e. If $\alpha_1 = \alpha_2$ then

$$\pi(x_1) = \alpha_1 = \lambda/\alpha_1 = \alpha_2 = \pi(x_2)$$

and therefore $e(\alpha_1) \geqslant 2$, hence, property (biv) does not hold for e. This ends the proof of Proposition 6.6. □

The following assertion will be used in the proof of Theorem 1.11 (with $K = \mathbb{Q}_\ell, V = V_\ell(X^n), A = \mathrm{Fr}_{X^n}$).

Proposition 6.11. — *We keep the notation and assumption of Subsection 6.3. Assume additionally that* $\mathrm{char}(K) = 0$, $\dim_K(V)$ *is even, and* $A : V \to V$ *is invertible. Let* q *be a nonzero element of* K *that is not a root of unity. Let* h *and* m *be positive integers that enjoy the following properties.*

(i) $h < m \leqslant \dim_K(V)/2$.

(ii) *If* $e\colon \mathrm{spec}(A) \to \mathbb{Z}_+$ *is any nonnegative integer-valued function such that*

$$\sum_{\alpha \,\in\, \mathrm{spec}(A)} e(\alpha) = 2m, \qquad \prod_{\alpha \,\in\, \mathrm{spec}(A)} \alpha^{e(\alpha)} = q^m$$

then there exist positive integers j_1, j_2 *and nonnegative integer-valued functions*

$$f_1\colon \mathrm{spec}(A) \to \mathbb{Z}_+, f_2\colon \mathrm{spec}(A) \to \mathbb{Z}_+$$

such that

$$\begin{gathered} m = j_1 + j_2,\ \ j_2 \leqslant h; \\ e(\alpha) = f_1(\alpha) + f_2(\alpha)\ \ \forall\, \alpha \in \mathrm{spec}(A); \end{gathered}$$

$$\begin{aligned} \sum_{\alpha \,\in\, \mathrm{spec}(A)} f_1(\alpha) = 2j_1, \qquad \prod_{\alpha \,\in\, \mathrm{spec}(A)} \alpha^{f_1(\alpha)} = q^{j_1}, \\ \sum_{\alpha \,\in\, \mathrm{spec}(A)} f_2(\alpha) = 2j_2, \qquad \prod_{\alpha \,\in\, \mathrm{spec}(A)} \alpha^{f_2(\alpha)} = q^{j_2}. \end{aligned}$$

Then

$$\sum_{j=1}^{h} \Lambda_{2(m-j),2j,K} \left(\wedge_K^{2(m-j)} \left(V^*\right) \left(q^{m-j}\right) \otimes_K \wedge_K^{2j} \left(V^*\right) \left(q^{j}\right)\right) = \wedge_K^{2m} \left(V^*\right) \left(q^{m}\right). \tag{6.12}$$

Proof. — In light of Remark 6.3 and arguments of Subsection 6.1, it suffices to check that

$$\sum_{j=1}^{h} \Lambda_{2(m-j),2j,E}\left(\wedge_E^{2(m-j)}\left(V_E^*\right)\left(q^{m-j}\right)\otimes_E \wedge_E^{2j}\left(V_E^*\right)\left(q^j\right)\right) = \wedge_E^{2m}\left(V_E^*\right)\left(q^m\right). \tag{6.13}$$

Recall that (in the notation of Subsection 6.3) that B is an (ordered) eigenbasis of V_E and all the $2m$-element subsets $C \subset \operatorname{spec}(A)$ with $\prod_{\alpha \in C} \alpha = q^m$ give rise to the base $\{y_C = \wedge_{x \in C} x^*\}$ of $\wedge_E^{2m}(V_E^*)(q^m)$. So, it suffices to prove that each such y_C lies in one of the summands in LHS of (6.13). To this end, let us consider the nonnegative integer-valued function

$$e_C\colon \operatorname{spec}(A) \to \mathbb{Z}_+,\ e(\alpha) = \#(C(\alpha)) \quad \text{where } C(\alpha) := \{x \in C \subset B | \pi(x) = \alpha\}.$$

(see (6.8)). Clearly,

$$\sum_{\alpha \in \operatorname{spec}(A)} e_C(\alpha) = \#(C) = 2m, \quad \prod_{\alpha \in \operatorname{spec}(A)} \alpha^{e_C(\alpha)} = \prod_{\alpha \in C} \alpha = q^m.$$

By property (ii), there exist positive integers j_1, j_2 and nonnegative integer-valued functions

$$f_1\colon \operatorname{spec}(A) \to \mathbb{Z}_+, f_2\colon \operatorname{spec}(A) \to \mathbb{Z}_+$$

such that

$$\begin{gathered} m = j_1 + j_2,\ j_2 \leqslant h; \\ e(\alpha) = f_1(\alpha) + f_2(\alpha)\ \ \forall\, \alpha \in \operatorname{spec}(A); \\ \sum_{\alpha \in \operatorname{spec}(A)} f_1(\alpha) = 2j_1, \quad \prod_{\alpha \in \operatorname{spec}(A)} \alpha^{f_1(\alpha)} = q^{j_1}, \\ \sum_{\alpha \in \operatorname{spec}(A)} f_2(\alpha) = 2j_2, \quad \prod_{\alpha \in \operatorname{spec}(A)} \alpha^{f_2(\alpha)} = q^{j_2}. \end{gathered}$$

Let us partition each $C(\alpha)$ into a *disjoint union* of two sets

$$C(\alpha) = C(\alpha)_1 \cup C(\alpha)_2 \quad \text{with} \quad C(\alpha)_1 \cap C(\alpha)_2 = \emptyset,$$
$$\#(C(\alpha)_1) = f_1(\alpha), \qquad \#(C(\alpha)_2) = f_2(\alpha)$$

and define C_1 (resp. C_2) as the (disjoint) union of all $C(\alpha_1)$ (resp. of all $C(\alpha_2)$). Then C becomes a *disjoint union* of C_1 and C_2, and

$$f_1 = e_{C_1}, f_2 = e_{C_2}.$$

It follows that

$$\sum_{\alpha \in \mathrm{spec}(A)} e_{C_1}(\alpha) = 2j_1, \quad \prod_{\alpha \in \mathrm{spec}(A)} \alpha^{e_{C_1}(\alpha)} = q^{j_1},$$
$$\sum_{\alpha \in \mathrm{spec}(A)} e_{C_2}(\alpha) = 2j_2, \quad \prod_{\alpha \in \mathrm{spec}(A)} \alpha^{e_{C_2}(\alpha)} = q^{j_2}.$$

This implies that

$$y_{C_1} \in \wedge_E^{2(j_1)}(V_E^*)\left(q^{j_1}\right) = \wedge_E^{2(m-j_2)}(V_E^*)\left(q^{m-j_2}\right), y_{C_2} \in \wedge_E^{2(j_2)}(V_E^*)\left(q^{j_2}\right).$$

Since C is a disjoint union of C_1 and C_2,

$$y_C = \pm y_{C_1} \wedge y_{C_2} \in \Lambda_{2(m-j_2),2j_2,E}\left(\wedge_E^{2(m-j_2)}(V_E^*)\left(q^{m-j_2}\right) \otimes_E \wedge_E^{2j_2}(V_E^*)\left(q^{j_2}\right)\right).$$

In order to finish the proof, one has only to recall that $j \leqslant h_2$. □

7. Tate forms

7.1. Tate modules and Frobenius

Recall that X is an abelian variety of positive dimension g over a finite field k with $\mathrm{char}(k) = p$ and $\#(k) = q$. Let $\ell \neq p$ be a prime and $T_\ell(X)$ the ℓ-adic Tate module of X. Let us consider the corresponding $\mathbb{Q}_\ell$-vector space

$$V_\ell(X) = T_\ell(X) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell,$$

which is a $2g$-dimensional vector space over $\mathbb{Q}_\ell$. The action of Fr_X extends by $\mathbb{Q}_\ell$-linearity to $V_\ell(X)$. So, we may view Fr_X as a $\mathbb{Q}_\ell$-linear automorphism of $V_\ell(X)$, whose characteristic polynomial coincides with $\mathcal{P}_X(t)$. A theorem of Weil [8, 15] asserts that Fr_X acts as a *semisimple* linear operator in $V_\ell(X)$. Let $\bar{\mathbb{Q}}_\ell$ be an algebraic closure of $\mathbb{Q}_\ell$. Let us choose a field embedding

$$L_X = \mathbb{Q}(R_X) \hookrightarrow \bar{\mathbb{Q}}_\ell.$$

Further we will identify L_X with its image in $\bar{\mathbb{Q}}_\ell$. We have

$$R_X \subset L_X \subset \bar{\mathbb{Q}}_\ell.$$

Let us consider the $2\dim(X)$-dimensional $\bar{\mathbb{Q}}_\ell$-vector space

$$\bar{V}_\ell(X) := V_\ell(X) \otimes_{\mathbb{Q}_\ell} \bar{\mathbb{Q}}_\ell.$$

Extending the action of Fr_X by $\bar{\mathbb{Q}}_\ell$-linearity, we get a $\bar{\mathbb{Q}}_\ell$-linear operator

$$\overline{\mathrm{Fr}}_X \colon \bar{V}_\ell(X) \to \bar{V}_\ell(X),\ v \otimes \lambda \mapsto \mathrm{Fr}_X(v) \otimes \lambda\ \ \forall\, v \in V_\ell(X), \lambda \in \bar{\mathbb{Q}}_\ell.$$

In the notation of Section 6, let us put

$$K = \mathbb{Q}_\ell, V = V_\ell(X), A = \mathrm{Fr}_X \colon V_\ell(X) \to V_\ell(X), E = \bar{\mathbb{Q}}_\ell. \tag{7.1}$$

Then

$$\begin{aligned} V_E = \bar{V}_\ell(X), A_E = \overline{\mathrm{Fr}}_X; \\ \mathrm{spec}(A) = R_X, \mathrm{mult}_A = \mathrm{mult}_X : R_X \to \mathbb{Z}_+. \end{aligned} \tag{7.2}$$

Remark 7.1. — If m is a positive integer and $Y = X^m$ then it is well known that there is a canonical isomorphism of $\mathbb{Q}_\ell$-vector spaces

$$V_\ell(Y) = \oplus_{i=1}^m V_\ell(X)$$

such that Fr_Y acts on $V_\ell(Y)$ as

$$\begin{aligned} &\mathrm{Fr}_Y\,(x_1, \dots x_m) \\ &\quad = (\mathrm{Fr}_X x_1, \dots, \mathrm{Fr}_X x_m) \ \ \forall\,(x_1, \dots x_m) \in \oplus_{i=1}^m V_\ell(X) = V_\ell(Y). \end{aligned}$$

This implies that

$$\begin{aligned} \mathcal{P}_Y(t) = \mathcal{P}_X(t)^m, \qquad\qquad & R_Y = R_X, L_X = L_Y, \\ \mathrm{mult}_Y(\alpha) = m \cdot \mathrm{mult}_X(\alpha) \ \ \forall\, \alpha \in R_X = R_Y. & \end{aligned} \tag{7.3}$$

In particular,

$$\mathrm{mult}_Y(\alpha) \geqslant m \ \ \forall\, \alpha \in R_Y = R_X. \tag{7.4}$$

Any invertible sheaf/divisor class $\mathcal{L}$ on X gives rise to (defined up to multiplication by an element of $\mathbb{Q}_\ell^*$) a $\mathbb{Q}_\ell$-bilinear alternating *Riemann form* (the first ℓ-adic Chern class of $\mathcal{L}$) [8]

$$\phi = \phi_{\mathcal{L}} \colon V_\ell(X) \times V_\ell(X) \to \mathbb{Q}_\ell$$

such that

$$\phi\big(\mathrm{Fr}_X(x), \mathrm{Fr}_X(y)\big) = q \cdot \phi(x, y) \ \ \forall\, x, y \in V_\ell(X). \tag{7.5}$$

7.2. Tate forms

A theorem of Tate [15] asserts that every alternating $\mathbb{Q}_\ell$-bilinear form ϕ on $V_\ell(X)$ that satisfies (7.5) is a $\mathbb{Q}_\ell$-linear combination of forms of type $\phi_{\mathcal{L}}$. We call such a form an ℓ-adic Tate form of degree 2 and denote by

$\mathrm{tate}_2(X,\ell)$ the subspace of all such forms in $\mathrm{Hom}_{\mathbb{Q}_\ell}(\Lambda^2 V_\ell(X), \mathbb{Q}_\ell)$. In other words,

$$\begin{aligned}\mathrm{tate}_2(X,\ell) :& \\ = \big\{\phi \in \mathrm{Hom}_{\mathbb{Q}_\ell}&\left(\Lambda^2 V_\ell(X), \mathbb{Q}_\ell\right) \,\big|\, \phi\left(\mathrm{Fr}_X(x), \mathrm{Fr}_X(y)\right) \\ &= q \cdot \phi(x,y)\ \forall\, x,y \in V_\ell(X)\big\}.\end{aligned}$$

More generally, let us define for each nonnegative integer $d \leqslant \dim(X) = g$ the subspace $\mathrm{tate}_{2d}(X,\ell)$ of all alternating $2d$-forms $\psi \in \mathrm{Hom}_{\mathbb{Q}_\ell}(\Lambda^{2d} V_\ell(X), \mathbb{Q}_\ell)$ such that

$$\psi\big(\mathrm{Fr}_X(v_1), \ldots, \mathrm{Fr}_X(v_{2d})\big) = q^d \cdot \psi\left(v_1, \ldots, v_{2d}\right)\ \ \forall\, x_1, \ldots, x_{2d} \in V_\ell(X).$$

We call elements of $\mathrm{tate}_{2d}(X,\ell)$ *Tate forms of degree* $2d$ [1] .

Remark 7.2. — Clearly, $\mathrm{tate}_{2d}(X,\ell)$ consists of all $\psi \in \mathrm{Hom}_{\mathbb{Q}_\ell}(\Lambda^{2d} V_\ell(X), \mathbb{Q}_\ell)$ such that

$$\psi\big(\mathrm{Fr}_X^{-1}(v_1), \ldots, \mathrm{Fr}_X^{-1}\left(v_{2d}\right)\big) = q^{-d} \cdot \psi\left(v_1, \ldots, v_{2d}\right)\ \forall\, v_1, \ldots, v_{2d} \in V_\ell(X).$$

Since Fr_X acts on $V_\ell(X)$ as $\rho_\ell(\sigma_k)$, the subspace $\mathrm{tate}_{2d}(X,l)$ consists of all $\psi \in \mathrm{Hom}_{\mathbb{Q}_\ell}(\Lambda^{2d} V_\ell(X), \mathbb{Q}_\ell)$ such that

$$\begin{aligned}&\psi\big(\rho_\ell(\sigma_k)^{-1}(v_1), \ldots, \rho_\ell(\sigma_k)^{-1}(v_{2d})\big) \\ &\qquad = \chi_\ell(\sigma_k)^{-d} \cdot \psi\left(v_1, \ldots, v_{2d}\right)\ \ \forall\, v_1, \ldots, v_{2d} \in V_\ell(X).\end{aligned}$$

Since σ_k is a topological generator of $\mathrm{Gal}(k)$, the subspace $\mathrm{tate}_{2d}(X,l)$ consists of all $\psi \in \mathrm{Hom}_{\mathbb{Q}_\ell}(\Lambda^{2d} V_\ell(X), \mathbb{Q}_\ell)$ such that

$$\begin{aligned}&\psi\left(\rho_\ell(\sigma)^{-1}(v_1), \ldots, \rho_\ell(\sigma)^{-1}\left(v_{2d}\right)\right) \\ &\quad = \chi_\ell(\sigma)^{-d} \cdot \psi\left(v_1, \ldots, v_{2d}\right) \quad \forall\, \sigma \in \mathrm{Gal}(k), v_1, \ldots, v_{2d} \in V_\ell(X).\end{aligned}$$

Remark 7.3. — In the notation of Section 6, (7.1) and (7.2),

$$\mathrm{tate}_{2d}(X,\ell) = \wedge_K^{2d}\left(V^*\right)\left(q^d\right)$$

is the eigenspace of K-linear operator $\wedge^{2d}(A^*)\colon\ \wedge_K^{2d}\left(V^*\right) \to \wedge_K^{2d}(V^*)$ attached to the eigenvalue q^d.

[1] In [21] we called them admissible forms.

7.3. Wedge products of Tate forms

For each integer $d \geqslant 3$ the exterior product map

$$\begin{aligned}\mathrm{Hom}_{\mathbb{Q}_\ell}\left(\Lambda^{2(d-1)}V_\ell(X),\mathbb{Q}_\ell\right)\otimes_{\mathbb{Q}_\ell}\mathrm{Hom}_{\mathbb{Q}_\ell}\left(\Lambda^{2}V_\ell(X),\mathbb{Q}_\ell\right)&\\ \to \mathrm{Hom}_{\mathbb{Q}_\ell}\left(\Lambda^{2d}V_\ell(X),\mathbb{Q}_\ell\right),&\\ \phi\otimes\psi\mapsto\phi\wedge\psi&\end{aligned}$$

induces the $\mathbb{Q}_\ell$-linear map

$$\mathrm{tate}_{2(d-1)}(X,\ell)\otimes_{\mathbb{Q}_\ell}\mathrm{tate}_2(X,\ell)\to\mathrm{tate}_{2d}(X,\ell),\ \phi\otimes\psi\mapsto\phi\wedge\psi. \tag{7.6}$$

Definition 7.4. — *Let $d > 1$ be an integer. An ℓ-adic* Tate form *of degree $2d$ is called* exceptional *if it does* not *lie in the image of map* (7.6).

Lemma 7.5. — *Let d be a positive integer such that*

$$2 \leqslant d \leqslant \dim(X).$$

Let $\ell \neq p$ be a prime. Then the following conditions are equivalent.

(a) *There exists an exceptional ℓ-adic Tate form on X of degree $2d$.*
(b) *There exists an admissible reduced function $e\colon R_X \to \mathbb{Z}$ of weight $2d$ such that*

$$0 \leqslant e(\alpha) \leqslant \mathrm{mult}_X(\alpha)\ \ \forall\, \alpha \in R_X.$$

Proof. — In the notation of (6.9), (7.1) and (7.2), it follows from Remark 7.3 that property (b) is equivalent to the *non-surjectiveness* of

$$\wedge_K^{j-2}(V^*)(\lambda_1)\otimes_K\wedge_K^2(V^*)(\lambda_2)\to\wedge_K^j(V^*)(\lambda_1\lambda_2),\ \psi\otimes\phi\mapsto\psi\wedge\phi$$

with

$$j=2d, \lambda_1=q^{d-1}, \lambda_2=q, \lambda_1\lambda_2=q^d.$$

By Proposition 6.6, the non-surjectiveness of this map is equivalent to the existence of a function $e\colon \mathrm{spec}(A)\to\mathbb{Z}_+$ that enjoys properties (bi)-(biv) of Proposition 6.6. Since $\mathrm{spec}(A)=R_X$, we may view e as a function $e\colon R_X\to\mathbb{Z}_+$. Now property (bii) means that e has weight $2d$, property (biii) that e is admisible, and property (biv) that e is reduced. As for property (bi), it means that

$$e(\alpha)\leqslant\mathrm{mult}_A(\alpha)=\mathrm{mult}_X(\alpha)\ \ \forall\,\alpha\in\mathrm{spec}(A)=R_X.$$

This implies that properties (bi)-(biv) of Proposition 6.6 are equivalent to property (b) of Lemma 7.5. It follows that properties (a) and (b) of Lemma 7.5 are equivalent. ☐

7.4. Twists and Tate classes

7.4.1. Twists and Tate classes

Consider an abelian variety $\bar{X} = X \times_k \bar{k}$ over the algebraic closure $\bar{k}$ of k and its étale ℓ-adic cohomology groups $\mathrm{H}^j(\bar{X}, \mathbb{Q}_\ell)$ [1, 4, 5, 14]. Here ℓ is any prime different from $\mathrm{char}(k)$, j any nonnegative integer, and $\mathrm{H}^j(\bar{X}, \mathbb{Q}_\ell)$ is a certain finite-dimensional $\mathbb{Q}_\ell$-vector space endowed with a continuous linear action of the absolute Galois group $\mathrm{Gal}(k) := \mathrm{Gal}(\bar{k}/k)$ of k. We write

$$\chi_\ell \colon \mathrm{Gal}(k) \to \mathbb{Z}_\ell^* \subset \mathbb{Q}_\ell^*$$

for the ℓ-adic *cyclotomic character* (see Section 2 above). There exists a certain "naturally defined" one-dimensional $\mathbb{Q}_\ell$-vector space $\mathbb{Q}_\ell(1)$ (that was denoted by W in [14, Section 2]) endowed with the natural continuous linear action of $\mathrm{Gal}(k)$ defined by the cyclotomic character

$$\chi_\ell \colon \mathrm{Gal}(k) \to \mathbb{Q}_\ell^* = \mathrm{Aut}_{\mathbb{Q}_\ell}(\mathbb{Q}_\ell(1))$$

(see [4, 5, 7, 14]). Namely, $\mathbb{Q}_\ell(1) = \mathbb{Z}_\ell(1) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ where $\mathbb{Z}_\ell(1)$ is the projective limit of multiplicative groups (finite Galois modules) μ_{ℓ^n} of $\ell^{n\ \mathrm{th}}$ roots of unity in $\bar{k}$.

Let us fix once and for all an *ℓ-adic orientation*, i.e., an isomorphism of $\mathbb{Q}_\ell$-vector spaces

$$\mathbb{Q}_\ell(1) \cong \mathbb{Q}_\ell,$$

which allows us to identify $\mathbb{Q}_\ell$ not only with $\mathbb{Q}_\ell(1)$ but also with all *tensor powers* $\mathbb{Q}_\ell(i)$ [1, 4, 5, 13, 14] of $\mathbb{Q}_\ell(1)$.

Let i be an integer. Let us consider the *twist* $\mathrm{H}^j(\bar{X}, \mathbb{Q}_\ell)(i)$ of the Galois module $\mathrm{H}^j(\bar{X}, \mathbb{Q}_\ell)$ by character χ_ℓ^i of $\mathrm{Gal}(k)$ [4, 5, 13, 14]. In other words, $\mathrm{H}^j(\bar{X}, \mathbb{Q}_\ell)(i)$ coincides with $\mathrm{H}^j(\bar{X}, \mathbb{Q}_\ell)$ as the $\mathbb{Q}_\ell$-vector space but if

$$\sigma, c \mapsto \sigma(c) \ \ \forall\, \sigma \in \mathrm{Gal}(k),\ c \in \mathrm{H}^j\left(\bar{X}, \mathbb{Q}_\ell\right)$$

is the Galois action on $\mathrm{H}^j(\bar{X}, \mathbb{Q}_\ell)$ then in $\mathrm{H}^j(\bar{X}, \mathbb{Q}_\ell)(i)$ a Galois automorphism σ sends c to $\chi_\ell(\sigma)^i \sigma(c)$.

If W is a Galois-invariant $\mathbb{Q}_\ell$-vector subspace in $\mathrm{H}^j(\bar{X}, \mathbb{Q}_\ell)$ then we write $W(i)$ for the same $\mathbb{Q}_\ell$-vector subspace in $\mathrm{H}^j(\bar{X}, \mathbb{Q}_\ell)(i)$. Clearly, $W(i)$ is a Galois-invariant subspace of $\mathrm{H}^j(\bar{X}, \mathbb{Q}_\ell)(i)$ but *not* necessarily isomorphic to W as Galois module.

Remarks 7.6.

(i) If j_1, j_2 are any nonnegative integers then the Galois-equivariant $\mathbb{Q}_\ell$-bilinear cup product in the cohomology of $\bar{X}$ leads to a Galois-equivariant $\mathbb{Q}_\ell$-linear map

$$\mathrm{H}^{j_1}\left(\bar{X}, \mathbb{Q}_\ell\right) \otimes_{\mathbb{Q}_\ell} \mathrm{H}^{j_2}\left(\bar{X}, \mathbb{Q}_\ell\right) \to \mathrm{H}^{j_1+j_2}\left(\bar{X}, \mathbb{Q}_\ell\right), \ c_1 \otimes c_2 \mapsto c_1 \cup c_2, \tag{7.7}$$

which, in turn, gives rise to the natural Galois-equivariant $\mathbb{Q}_\ell$-linear map [5, 14]

$$\begin{aligned}\mathrm{H}^{j_1}\left(\bar{X}, \mathbb{Q}_\ell\right)(i_1) \otimes_{\mathbb{Q}_\ell} \mathrm{H}^{j_2}\left(\bar{X}, \mathbb{Q}_\ell\right)(i_2) \\ \to \mathrm{H}^{j_1+j_2}\left(\bar{X}, \mathbb{Q}_\ell\right)(i_1+i_2), \ c_1 \otimes c_2 \mapsto c_1 \cup c_2.\end{aligned} \tag{7.8}$$

(ii) Let W_1 (resp. W_2) is s a Galois-invariant $\mathbb{Q}_\ell$-vector subspace in $\mathrm{H}^{j_1}(\bar{X}, \mathbb{Q}_\ell)$ (resp. in $\mathrm{H}^{j_2}(\bar{X}, \mathbb{Q}_\ell)$) and $W \subset \mathrm{H}^{j_1+j_2}(\bar{X}, \mathbb{Q}_\ell)$ be the image of subspace

$$W_1 \otimes_{\mathbb{Q}_\ell} W_2 \subset \mathrm{H}^{j_1}\left(\bar{X}, \mathbb{Q}_\ell\right) \otimes_{\mathbb{Q}_\ell} \mathrm{H}^{j_2}\left(\bar{X}, \mathbb{Q}_\ell\right)$$

under the map (7.7). It follows readily that the twist

$$W(i_1+i_2) \subset \mathrm{H}^{j_1+j_2}\left(\bar{X}, \mathbb{Q}_\ell\right)(i_1+i_2)$$

coincides with the image of subspace

$$W_1(i_1) \otimes_{\mathbb{Q}_\ell} W_2(i_2) \subset \mathrm{H}^{j_1}\left(\bar{X}, \mathbb{Q}_\ell\right)(i_1) \otimes_{\mathbb{Q}_\ell} \mathrm{H}^{j_2}\left(\bar{X}, \mathbb{Q}_\ell\right)(i_2)$$

under the map (7.8).

DEFINITION 7.7. — *Let d be a nonnegative integer. Let us consider the $\mathbb{Q}_\ell$-vector subspace*

$$\mathcal{T}_{\ell,d}(X) := \mathrm{H}^{2d}\left(\bar{X}, \mathbb{Q}_\ell\right)(d)^{\mathrm{Gal}(k)}$$

of Galois invariants *in* $\mathrm{H}^{2d}(\bar{X}, \mathbb{Q}_\ell)(d)$ *and a* weight *$\mathbb{Q}_\ell$-vector subspace*

$$W_{\ell,d}(X) := \left\{c \in \mathrm{H}^{2d}(\bar{X}, \mathbb{Q}_\ell) \,\middle|\, \sigma(x) = \chi_\ell(\sigma)^{-d} c \ \ \forall\, \sigma \in \mathrm{Gal}(k)\right\}$$

in $\mathrm{H}^{2d}(\bar{X}, \mathbb{Q}_\ell)$. *It follows from the very definitions that*

$$\mathcal{T}_{\ell,d}(X) = W_{\ell,d}(X)(d). \tag{7.9}$$

Remark 7.8. — Let d_1 and d_2 be nonnegative integers. It follows from the Galois equivariance of maps (7.7) and (7.8) combined with Remark 7.6(ii) that the image $W_{\ell,d_1,d_2}(X)$ of

$$W_{\ell,d_1}(X) \otimes W_{\ell,d_2}(X) \to \mathrm{H}^{2(d_1+d_2)}\left(\bar{X}, \mathbb{Q}_\ell\right), \ c_1 \otimes c_2 \to c_1 \cup c_2$$

lies in $W_{\ell,d_1+d_2}(X)$. Similarly, the image $\mathcal{T}_{\ell,d_1,d_2}(X)$ of

$$\mathcal{T}_{\ell,d_1}(X) \otimes \mathcal{T}_{\ell,d_2}(X) \to \mathrm{H}^{2(d_1+d_2)}\left(\bar{X}, \mathbb{Q}_\ell\right)(d_1+d_2), \ c_1 \otimes c_2 \to c_1 \cup c_2$$

lies in $\mathcal{T}_{\ell,d_1+d_2}(X)$. In addition, it follows from (7.9) that

$$\mathcal{T}_{\ell,d_1,d_2}(X) = W_{\ell,d_1,d_2}(X)\,(d_1+d_2)\,.$$

Definition 7.9. — *Let $\ell \neq \mathrm{char}(k)$ be a prime and d a nonnegative integer.*

(i) *Elements of $\mathcal{T}_{\ell,d}(X)$ are called ℓ-adic* Tate classes of dimension $2d$ *on X.*
(ii) *A nonzero $2d$-dimensional Tate class c is called* exotic *if $d \geqslant 1$ and c cannot be presented as a linear combination of products of d Tate classes of dimension 2 with coefficients in $\mathbb{Q}_\ell$.*
(iii) *A Tate class c of dimension $2d$ is called* very exotic *if $d \geqslant 1$ and c cannot be presented as a linear combination with coefficients in $\mathbb{Q}_\ell$ of products of Tate classes of dimension $2d-2$ and 2, i.e., c does* not *belong to $\mathcal{T}_{\ell,d-1,1}(X)$.*

Remarks 7.10.

(i) Let Z be a closed irreducible subvariety of codimension d in X. The choice of the ℓ-adic orientation allows us to define the ℓ-adic class $\mathrm{cl}(Z) \in \mathcal{T}_{\ell,d}(X) \subset \mathrm{H}^{2d}(\bar{X},\mathbb{Q}_\ell)(d)$ of Z [13, 14]. Tate [13, 14] conjectured that for all nonnegative integer d the subspace $\mathcal{T}_{\ell,d}(X)$ is spanned by all $\mathrm{cl}(Z)$ and proved it for $d=1$ [15].
(ii) If d is a nonnegative integer and $d \leqslant g$ then it is known [13, 14] that $\mathcal{T}_{\ell,d}(X) \neq \{0\}$.
(iii) Clearly, all 2-dimensional Tate classes are neither exotic nor very exotic. Hence, the existence of an exotic (or very exotic) Tate class of dimension $2d$ implies readily that

$$2 \leqslant d \leqslant g = \dim(X),$$

because $\mathrm{H}^{2d}(\bar{X},\mathbb{Q}_\ell) = \{0\}$ for all $d > g$, and, therefore, all $2d$-dimensional Tate classes are just zero. (Actually, it is known that $\mathrm{H}^{2g}(\bar{X},\mathbb{Q}_\ell)(g)$ is a one-dimensional $\mathbb{Q}_\ell$-vector space generated by the gth self-product of the class of a hyperplane section of X [14]. Therefore, there are no non-exotic Tate classes of dimension $2g$.)
(iv) Clearly, every *very exotic* Tate class is *exotic*.

Conversely, suppose that there exists an *exotic* $2d$-dimensional ℓ-adic Tate class on X. I claim that there is a positive integer $d' \leqslant d$ such that there exists a *very exotic* $2d'$-dimensional ℓ-adic Tate class on X. Indeed, decreasing d if necessary, we may and will assume that d is the smallest positive integer such that there is an exotic

ℓ-adic $2d$-dimensional Tate class on X. Let c be such a class. Then $d > 1$.

Assume that c is *not* very exotic. Then c is a linear combination of cup products $h_i \cup c_i$ where all c_i are nonzero Tate classes of dimension 2 and all h_i are nonzero Tate classes of dimension $2(d-1)$. Since c is exotic, there is an index i such that h_i is exotic. But exotic h_i is $2(d-1)$-dimensional, which contradicts the minimality of d. The obtained contradiction implies that c itself is very exotic, which ends the proof.

It follows that *X carries an ℓ-adic exotic Tate class if and only if it carries a very exotic ℓ-adic Tate class* (may be, of different dimension).

7.5. Étale cohomology of abelian varieties

7.5.1. Étale cohomology of abelian varieties

Let us consider the abelian variety $\bar{X} = X \times_k \bar{k}$ over $\bar{k}$. Let j be a nonnegative integer and let $\mathrm{H}^j(\bar{X}, \mathbb{Q}_\ell)$ be the j^{th} étale ℓ-adic cohomology group of $\bar{X}$, which is a finite-dimensional $\mathbb{Q}_\ell$-vector space endowed with the canonical continuous linear action of $\mathrm{Gal}(k)$ [5, 7, 14]. There is a canonical $\mathrm{Gal}(k)$-equivariant isomorphism of graded $\mathbb{Q}_\ell$-algebras ([1, 5, 14], [7, Section 12])

$$\oplus_{j=0}^{2\dim(X)} \mathrm{H}^j\left(\bar{X}, \mathbb{Q}_\ell\right) \cong \oplus_{j=0}^{2\dim(X)} \mathrm{Hom}_{\mathbb{Q}_\ell}\left(\Lambda^j_{\mathbb{Q}_\ell} V_\ell(X), \mathbb{Q}_\ell\right). \tag{7.10}$$

Its Galois equivariance combined with Remark 7.2 imply that (in the notation of Definition 7.7) map (7.10) induces for all nonnegative integers $d \leqslant \dim(X)$ a $\mathbb{Q}_\ell$-linear isomorphism between

$$\begin{aligned} W_{\ell,d}(X) &= \left\{c \in \mathrm{H}^{2d}\left(\bar{X}, \mathbb{Q}_\ell\right) \middle| \sigma(c) = \chi_\ell(\sigma)^{-d} c \ \ \forall \sigma \in \mathrm{Gal}(k)\right\} \\ &= \left\{c \in \mathrm{H}^{2d}\left(\bar{X}, \mathbb{Q}_\ell\right) \middle| \sigma_k(c) = \chi_\ell\left(\sigma_k\right)^{-d} c\right\} \subset \mathrm{H}^{2d}\left(\bar{X}, \mathbb{Q}_\ell\right) \end{aligned}$$

and the subspace

$$\mathrm{tate}_{2d}(X, \ell) \subset \mathrm{Hom}_{\mathbb{Q}_\ell}\left(\Lambda^{2d}_{\mathbb{Q}_\ell} V_\ell(X), \mathbb{Q}_\ell\right)$$

of ℓ-adic Tate forms of degree $2d$ on X. Recall (see Definitions 7.7 and 7.9) that the twist $W_{\ell,d}(X)(d) \subset \mathrm{H}^{2d}(\bar{X}, \mathbb{Q}_\ell)(d)$ coincides with the subspace $\mathcal{T}_{\ell,d}(X)$ of $2d$-dimensional ℓ-adic Tate classes on X. Recall that map (7.10) is a $\mathbb{Q}_\ell$-algebra isomorphism. Applying Remark 7.8 to $d_1 = d - 1$ and $d_2 = 1$, we obtain that *the existence of a very exotic a ℓ-adic Tate class of* *dimension $2d$ on X is equivalent to the existence of an exceptional ℓ-adic Tate form of degree $2d$ on X.*

We will need to state explicitly the following useful assertion.

Lemma 7.11. — *Let X be an abelian variety over k. Let $\ell \neq \mathrm{char}(k)$ be a prime. Then the following three conditions are equivalent.*

(i) *X carries an exotic ℓ-adic Tate class.*

(ii) *X carries a very exotic ℓ-adic Tate class.*

(iii) *There exists an exceptional ℓ-adic Tate form on X.*

In addition, the validity of equivalent conditions (i)-(iii) *does not depend on a choice of ℓ.*

Proof of Lemma 7.11. — The equivalence of (ii) and (iii) follows readily from the arguments at the end of Subsection 7.5. The equivalence of (i) and (ii) was already proven in Remark 7.10 (iv).

Notice that property (b) of Lemma 7.5 does not depend on the choice of ℓ. Now Lemma 7.5 implies that the validity of (iii) does *not* depend on the choice of ℓ. □

Proof of Theorem 1.8. — By a theorem of Tate [15], if Y is any abelian variety over k (e.g., $Y = X^n$) then every element of $\mathcal{T}_{\ell,1}(Y)$ is a linear combination of divisor classes on Y with coefficients in $\mathbb{Q}_\ell$.

Suppose that there is an exotic ℓ-adic Tate class on X^n for some positive integer n. It follows from Lemma 7.11 (applied to $Y = X^n$ instead of X) that there is an exceptional ℓ-adic Tate form on X^n. In light of Lemma 7.5 (applied to Y instead of X), there exists an admissible reduced function $R_X = R_Y \to \mathbb{Z}_+$. In light of Theorem 1.4, there exists an admissible reduced function $e\colon R_X \to \mathbb{Z}_+$ of weight $\leqslant N(g)$. This means that

$$\mathbf{wt}(e) = \sum_{\alpha \in R_X} e(\alpha) \leqslant 2N(g);$$

in particular,

$$0 \leqslant e(\alpha) \leqslant 2N(g) \ \ \forall\, \alpha \in R_X.$$

Let us put $Z = X^{2N(g)}$ and consider e as the reduced admissible function

$$R_Z = R_X \to \mathbb{Z}_+,\ \alpha \mapsto e(\alpha).$$

In light of Remark 7.1 applied to $m = 2N(g)$,

$$e(\alpha) \leqslant 2N(g) \leqslant \mathrm{mult}_Z(\alpha) \ \ \forall\, \alpha \in R_Z = R_X.$$

It follows from Lemma 7.5 that there is an exceptional ℓ-adic Tate form on $X^{2N(g)} = Z$. Applying Lemma 7.11 to Z, we obtain that there is an exotic ℓ-adic Tate class on $Z = X^{2N(g)}$. Now the last assertion of Lemma 7.11

implies that there is an exotic l-adic Tate class on $Z = X^{2N(g)}$ for all primes $l \neq \mathrm{char}(k)$. This ends the proof. $\square$

Proof of Theorem 1.11. — In light of arguments of Subsection 7.5 combined with Remark 7.8, it suffices to check that each ℓ-adic Tate form of any even degree $2m$ on X^n can be presented as a linear combination of exterior products of ℓ-adic Tate forms of degree at most $H(g)$. Let us prove it, using induction by m.

The assertion is obviously true for all $m \leqslant H(g)/2$. Suppose that $m > H(g)/2$. First, notice that

$$R_{X^n} = R_X \quad \forall\, n.$$

Applying Theorem 1.10, we conclude that the conditions of Proposition 6.11 are fulfilled for

$$K = \mathbb{Q}_\ell, V = V_\ell\left(X^n\right), \quad A = \mathrm{Fr}_{X^n} : V_\ell\left(X^n\right) \to V_\ell\left(X^n\right),$$
$$\mathrm{spec}(A) = R_{X^n} = R_X,\ h = H(g)/2.$$

Applying Proposition 6.11, we conclude that each ℓ-adic Tate form of degree $2m$ on X^n can be presented as a linear combination of wedge products

$$\psi_{m-j} \wedge \phi_j \ \ (j = 1, \dots, H(g)/2))$$

where ψ_{m-j} is an ℓ-adic Tate form of degree $2(m-j)$ on X^n and ϕ_j is an ℓ-adic Tate form of degree $2j \leqslant H(g)$ on X^n. Applying the induction assumption to all ψ_{m-j}'s, we conclude that each ℓ-adic Tate form of degree $2m$ on X^n can be presented as a linear combination of exterior products of Tate forms of degree at most $H(g)$. This ends the proof. $\square$

BIBLIOGRAPHY

[1] V. G. Berkovich, "The Brauer group of abelian varieties", *Funct. Anal. Appl.* **6** (1973), p. 180-184.

[2] N. Bourbaki, *Elements of mathematics. Algebra I, Chapters 1-3*, Springer, 1989.

[3] D. A. Cox, J. B. Little & H. K. Schenk, *Toric varieties*, Graduate Studies in Mathematics, vol. 124, American Mathematical Society, 2011.

[4] N. M. Katz, "Review of l-adic cohomology", in *Motives, part 1. Proceedings of the summer research conference on motives, (Seattle, WA, 1991)* (U. Jannsen, S. Kleiman & J.-P. Serre, eds.), Proceedings of Symposia in Pure Mathematics, vol. 55, American Mathematical Society, 1994, p. 21-30.

[5] S. L. Kleiman, "Algebraic cycles and the Weil conjecture", in *Dix Exposés sur la Cohomologie des Schémas* (A. Grothendieck & N. H. Kuiper, eds.), Advanced Studies in Pure Mathematics, vol. 3, North-Holland, 1968, p. 359-386.

[6] H. W. J. Lenstra & Y. G. Zarhin, "The Tate conjecture for almost ordinary abelian varieties over finite fields", in *Advances in Number Theory (CNTA 91 Conference Proceedings, Kingston, ON, 1991)* (F. Q. Gouvea & N. Yui, eds.), Oxford University Press, 1993, p. 179-194.

[7] J. S. Milne, "Abelian Varieties, version 2.0", 2008, `https://www.jmilne.org/math/CourseNotes/av.html`.

[8] D. Mumford, *Abelian varieties*, 2nd ed., Tata Institute of Fundamental Research Studies in Mathematics, vol. 5, Oxford University Press, 1974.

[9] F. Oort, "Abelian varieties over finite fields", in *Higher-dimensional varieties over finite fields* (D. Kaledin & Y. Tschinkel, eds.), NATO Science for Peace and Security Series D: Information and Communication Security, vol. 16, IOS Press, 2008, p. 123-188.

[10] J.-P. Serre, *Abelian ℓ-adic representations and elliptic curves*, 2nd ed., Advanced Book Classics, Addison-Wesley Publishing Group, 1989.

[11] ———, "Lettres á Ken Ribet du 1/1/1981 et du 29/1/1981", in *Œuvres, IV, 1985–1998*, Springer, 2000, p. 1-20.

[12] A. Silverberg & Y. G. Zarhin, "Connectedness results for ℓ-adic representations associated to abelian varieties", *Compos. Math.* **97** (1995), no. 1-2, p. 273-284.

[13] J. T. Tate, "Conjectures on algebraic cycles in ℓ-adic cohomology", in *Motives, part 1. Proceedings of the summer research conference on motives, (Seattle, WA, 1991)* (U. Jannsen, S. Kleiman & J.-P. Serre, eds.), Proceedings of Symposia in Pure Mathematics, vol. 55, American Mathematical Society, 1994, p. 71-83.

[14] J. T. Tate, "Algebraic cycles and poles of zeta functions", in *Arithmetical Algebraic Geometry (Proc. Conf. Purdue Univ., 1963)* (O. F. G. Schilling, ed.), Harper & Row, 1965, p. 93-110.

[15] ———, "Endomorphisms of abelian varieties over finite field", *Invent. Math.* **2** (1966), p. 134-144.

[16] ———, "Classes d'isogénie de variétés abéliennes sur un corps fini (d'après T. Honda)", in *Séminaire Bourbaki: Vol. 1968/69. Exposés 347 - 363* (N. Bourbaki, ed.), Lecture Notes in Mathematics, vol. 179, Springer, 1971, p. 95-110.

[17] Y. G. Zarhin, "Abelian varieties, ℓ-adic representations and Lie algebras. Rank independence on ℓ", *Invent. Math.* **55** (1979), p. 165-176.

[18] ———, "Abelian varieties, ℓ-adic representations and SL_2", *Math. USSR Izv.* **14** (1980), p. 275-288.

[19] ———, "Abelian varieties of K3 type and ℓ-adic representations", in *Algebraic Geometry and Analytic Geometry, (Tokyo,1990)* (A. Fujiki, K. Kato, T. Katsura, Y. Kawamata & Y. Miyaoka, eds.), Springer, 1991, p. 231-255.

[20] ———, "Abelian varieties of K3 type", in *Séminaire de Théorie des Nombres, Paris, 1990-91* (D. Sinnou, ed.), Progress in Mathematics, Birkhäuser, 1993, p. 263-279.

[21] ———, "The Tate conjecture for non-simple abelian varieties over finite fields", in *Algebra and Number Theory. Proceedings of a conference held at the Institute of Experimental Mathematics, University of Essen, Germany, December 2-4, 1992* (G. Frey & J. Ritter, eds.), Walter de Gruyter, 1994, p. 267-296.

[22] ———, "Eigenvalues of Frobenius Endomorphisms of Abelian varieties of low dimension", *J. Pure Applied Algebra* **219** (2015), no. 6, p. 2076-2098.

Manuscrit reçu le 22 juin 2020,
révisé le 6 mars 2021,
accepté le 8 avril 2021.

Yuri G. ZARHIN
Department of Mathematics, Pennsylvania State University, University Park, PA 16802, USA
E-mail address (Y. Zarhin):
zarhin@math.psu.edu