

Ordinary abelian varieties over a finite field

Pierre Deligne (Bures-sur-Yvette)

We give a down-to-earth description of the category of ordinary abelian varieties over a finite field $\mathbb{F}_q$. The result obtained was inspired by Ihara [2], ch. V (see also [3]).

1. Let p be a prime number, let $\mathbb{F}_p$ be the field $\mathbb{Z}/(p)$, let $\overline{\mathbb{F}_p}$ be an algebraic closure of $\mathbb{F}_p$, and, for each power q of p , let $\mathbb{F}_q$ be the subfield with q elements of $\overline{\mathbb{F}_p}$. For every algebraic extension k of $\mathbb{F}_p$, let $W_0(k)$ denote the henselian discrete valuation ring, essentially of finite type over $\mathbb{Z}$, absolutely unramified, with residue field k ; let $W(k)$ be the ring of Witt vectors over k , i.e. the completion of $W_0(k)$, let $W = W(\overline{\mathbb{F}_p})$, and let φ be an embedding of W in the field $\mathbb{C}$ of complex numbers. We denote by $\mathbb{Z}(1)$ the subgroup $2\pi i\mathbb{Z}$ of $\mathbb{C}$. The exponential map defines an isomorphism between $\mathbb{Z}(1) \otimes \mathbb{Z}_\ell$ and

$$\mathbb{Z}_\ell(1)(\mathbb{C}) = \varprojlim_n \mu_{\ell^n}(\mathbb{C}).$$

We denote by A^* the abelian variety dual to an abelian variety A . For every field k , let $\bar{k}$ denote an algebraic closure of k .

2. Let A be an abelian variety of dimension g , defined over a field k of characteristic p . Recall that A is called ordinary if the following equivalent conditions are satisfied:

(I) A has p^g points of order dividing p with values in $\bar{k}$.

(II) The “Hasse–Witt matrix”

$$F^* : H^1(A^{(p)}, \mathcal{O}_{A^{(p)}}) \longrightarrow H^1(A, \mathcal{O}_A)$$

is invertible.

(III) The neutral component of the group scheme A_p , the kernel of multiplication by p , is of multiplicative type, hence geometrically isomorphic to a power of μ_p .

If $k = \mathbb{F}_q$, if F is the Frobenius endomorphism of A , and if $P_{cA}(F; x)$ is its characteristic polynomial, these conditions are further equivalent to:

(IV) At least half of the roots of $P_{cA}(F; x)$ in $\overline{\mathbb{Q}_p}$ are p -adic units. In other words, if $n = \dim A$, the reduction modulo p of the polynomial $P_{cA}(F; x)$ is not divisible by x^{n+1} .

3. Let A be an ordinary abelian variety over $\overline{\mathbb{F}_p}$. Let $\tilde{A}$ denote the canonical Serre–Tate lift [4] of A over W . Recall that $\tilde{A}$ depends functorially on A and is characterized by the fact that the p -divisible group $T_p(\tilde{A})$ over W attached to $\tilde{A}$ [5] is the product of the p -divisible groups, uniquely determined by 2. (III), lifting respectively the neutral component and the largest étale quotient of $T_p(A)$. The canonical lift $\tilde{A}$ is also the unique lift of A such that every endomorphism of A lifts to $\tilde{A}$. Let $T(A)$ denote the integral homology of the complex abelian variety $A_{\mathbb{C}}$ deduced from $\tilde{A}$ and φ by extension of scalars from W to $\mathbb{C}$:

$$T(A) = H_1(\tilde{A} \otimes_{\varphi} \mathbb{C}).$$

It is known that $\tilde{A}$ descends uniquely to $W_0(\overline{\mathbb{F}_p})$, so that $A_{\mathbb{C}}$ depends only on A and on the restriction of φ to $W_0(\overline{\mathbb{F}_p})$. The free $\mathbb{Z}$ -module $T(A)$ has rank $2 \dim(A)$; it is functorial in A . Moreover, if ℓ is a prime number distinct from p , one has functorially

$$T(A) \otimes \mathbb{Z}_\ell = T_\ell(A). \quad (3.1)$$

The canonical lift of the abelian variety A^* dual to A is the dual of $\tilde{A}$, so that $(A_{\mathbb{C}})^* = A_{\mathbb{C}}^*$ and $T(A)$ and $T(A^*)$ are in perfect duality with values in $\mathbb{Z}(1)$:

$$T(A) \otimes T(A^*) \longrightarrow \mathbb{Z}(1). \quad (3.2)$$

It is indispensable to use $\mathbb{Z}(1)$ rather than $\mathbb{Z}$ in order to obtain a theory invariant under complex conjugation. The pairings (3.2) are compatible, via (3.1), with the pairings

$$T_\ell(A) \otimes T_\ell(A^*) \longrightarrow \mathbb{Z}_\ell(1);$$

a morphism $\xi : A \rightarrow A^*$ defines a polarization of A if and only if $\xi_{\mathbb{C}} : A_{\mathbb{C}} \rightarrow A_{\mathbb{C}}^*$ defines a polarization of $A_{\mathbb{C}}$. Put

$$T'_p(A) = \text{Hom}(\mathbb{Q}_p/\mathbb{Z}_p, A(\overline{\mathbb{F}_p}))$$

and

$$T''_p(A) = \text{Hom}_{\mathbb{Z}_p}(T'_p(A^*), \mathbb{Z}(1) \otimes \mathbb{Z}_p).$$

These $\mathbb{Z}_p$ -modules are covariant functors of A .

By definition of the canonical lift, the p -divisible group $T_p(\tilde{A})$ is the sum of the constant pro-étale group $T'_p(A)$ and of the Cartier dual of $T'_p(A^*)$. For every morphism $u : A \rightarrow B$, the induced morphism

$$u : T_p(\tilde{A}) \rightarrow T_p(\tilde{B})$$

is identified with the sum of $u|_{T'_p(A)} : T'_p(A) \rightarrow T'_p(B)$ and the Cartier transpose of ${}^t u|_{T'_p(B^*)} : T'_p(B^*) \rightarrow T'_p(A^*)$. Over $\mathbb{C}$, one has canonically $\mathbb{Z}(1)/(p^n) \sim \mu_{p^n}$, whence an isomorphism of functors:

$$T_{(p)}(A) = T(A) \otimes \mathbb{Z}_p = T'_p(A) \oplus T''_p(A). \quad (3.2)$$

4. Recall that, if $\varphi : X \rightarrow Y$ is an isogeny between complex abelian varieties, the exact homotopy sequence reduces to a short exact sequence

$$0 \longrightarrow H_1(X) \longrightarrow H_1(Y) \longrightarrow \text{Ker}(\varphi) \longrightarrow 0.$$

The abelian varieties which are quotients of X by a finite subgroup, and these finite subgroups of X , correspond bijectively to the sublattices of $H_1(X) \otimes \mathbb{Q}$ containing $H_1(X)$.

Let A be an ordinary abelian variety over $\overline{\mathbb{F}_p}$. If n is an integer prime to p , the finite group subschemes of order n of A , of $\tilde{A}$, and of $A_{\mathbb{C}}$ correspond bijectively, and still correspond to the overlattices R of $T(A)$ such that $[R : T(A)] = n$.

Put

$$V'_p = T'_p(A) \otimes \mathbb{Q}_p, \quad V''_p(A) = T''_p(A) \otimes \mathbb{Q}_p.$$

The finite group subschemes of order p^k of A are products of an étale subgroup and an infinitesimal subgroup. The étale subgroups of order p^k of A correspond to those subgroups of order p^k of $A_{\mathbb{C}}$ for which the corresponding overlattice R of $T(A)$ is contained in $T_{(p)}(A) + V'_p(A)$. By duality, the infinitesimal subgroups of A correspond to the overlattices R of $T(A)$, p -isogenous to $T(A)$, i.e. such that $[R : T(A)]$ is a power of p , and contained in $T_{(p)}(A) + V''_p(A)$.

In all, the finite subgroups of A , or the abelian varieties quotient of A , correspond bijectively to the overlattices R of $T(A)$ such that

$$R \otimes \mathbb{Z}_p = (R \otimes \mathbb{Z}_p \cap V'_p) + (R \otimes \mathbb{Z}_p \cap V''_p). \quad (4.1)$$

5. In particular, $A^{(p)}$, the quotient of A by the largest infinitesimal subgroup of A killed by p for A ordinary, is defined by the overlattice $T(A)^{(p)}$ of $T(A)$, p -isogenous to $T(A)$, such that

$$T(A)^{(p)} \otimes \mathbb{Z}_p = T'_p(A) + \frac{1}{p}T''_p(A).$$

6. Let A be an abelian variety over $\mathbb{F}_q$ and let $F : x \mapsto x^q$ be its Frobenius endomorphism. Recall that A is uniquely determined by the pair $(\bar{A}, F)$ deduced from (A, F) by extension of scalars from $\mathbb{F}_q$ to $\overline{\mathbb{F}_q}$; the endomorphism F of $\bar{A}$ factors through the relative Frobenius

$$\text{Fr}^{(q)} : \bar{A} \longrightarrow \bar{A}^{(q)}$$

and an isomorphism

$$F' : \overline{A}^{(q)} \longrightarrow \overline{A}.$$

If A is ordinary, $T(A)$ will denote the $\mathbb{Z}$ -module $T(\overline{A})$ endowed with the endomorphism F induced by the Frobenius endomorphism of A . By 5, by what precedes, and by (3.2), the lattices $T(A)$ and $F(T(A))$ are p -isogenous and one has

$$F(T'_p(A)) = T'_p(A), \quad (6.1)$$

$$F(T''_p(A)) = qT''_p(A). \quad (6.2)$$

7. Theorem. The functor

$$A \longmapsto (T(A), F)$$

is an equivalence of categories between the category of ordinary abelian varieties over $\mathbb{F}_q$ and the category of finite-type free $\mathbb{Z}$ -modules T endowed with an endomorphism F satisfying the following conditions:

- (a) F is semisimple, and its eigenvalues have complex absolute value $q^{1/2}$.
- (b) At least half of the roots in $\overline{\mathbb{Q}}_p$ of the characteristic polynomial of F are p -adic units; in other words, if T has rank d , the reduction modulo p of the polynomial $P_{cT}(F; x)$ is not divisible by $x^{\lfloor d/2 \rfloor + 1}$.
- (c) There exists an endomorphism V of T such that $FV = q$.

If condition (a) is satisfied, conditions (b) and (c) are equivalent to:

- (d) The module $T \otimes \mathbb{Z}_p$ admits a decomposition, stable under F , into two $\mathbb{Z}_p$ -submodules T'_p and T''_p of the same dimension, such that $F|_{T'_p}$ is invertible and $F|_{T''_p}$ is divisible by q .

Proof. (A) We prove that (a)+(b)+(c) imply (d). If α is a complex eigenvalue of F , then $\bar{\alpha}$ is another, with the same multiplicity, and $\alpha\bar{\alpha} = q$. Apart from those equal to $\pm q^{1/2}$, the eigenvalues of F in $\mathbb{C}$, hence in $\overline{\mathbb{Q}}_p$, fall into pairs of roots α and q/α . The roots α and q/α cannot both be p -adic units; it follows from (b) that $\pm q^{1/2}$ is not an eigenvalue of F , that half of the eigenvalues of F in $\overline{\mathbb{Q}}_p$ are p -adic units, say $\alpha_1, \dots, \alpha_{d/2}$, and that the other half consists of $\beta_1 = q/\alpha_1, \dots, \beta_{d/2} = q/\alpha_{d/2}$. Let

$$T_{(p)} = T \otimes \mathbb{Z}_p, \quad V_p = T \otimes \mathbb{Q}_p,$$

let V'_p be the subspace of V_p which is the kernel of $\prod_i (F - \alpha_i)$, and let V''_p be the kernel of the endomorphism $\varphi = \prod_i (F - \beta_i)$. One has

$$V_p = V'_p \oplus V''_p.$$

Let T'_p be the projection of $T_{(p)}$ onto V'_p and let $T''_p = T_{(p)} \cap V''_p$. Since φ kills V''_p and preserves T , it sends T'_p into $T_{(p)} \cap V'_p \subset T'_p$. On the other hand,

$$\det(\varphi|_{V'_p}) = \prod_{i,j} (\alpha_i - \beta_j)$$

is a p -adic unit, hence $\varphi(T'_p) = T'_p$ and $T_{(p)} \cap V'_p = T'_p$, so that

$$T_{(p)} = T'_p \oplus T''_p.$$

(B) *Full faithfulness.* Let A and B be two abelian varieties over $\mathbb{F}_q$, and let ψ be the map

$$\psi : \text{Hom}(A, B) \longrightarrow \text{Hom}_F(T(A), T(B)).$$

By Tate's theorem [7] and (3.1), the map

$$\psi_\ell : \text{Hom}(A, B) \otimes \mathbb{Z}_\ell \longrightarrow \text{Hom}_F(T(A), T(B)) \otimes \mathbb{Z}_\ell$$

is an isomorphism for $(\ell, p) = 1$, so that $\psi \otimes \mathbb{Q}$ is an isomorphism. It is known that $\text{Hom}(A, B)$ is torsion-free, hence ψ is injective. Let $u : A \rightarrow B$ be a morphism such that $T(u)$ is divisible by n . The induced morphism

$$u_{\mathbb{C}} : \overline{A}_{\mathbb{C}} \longrightarrow \overline{B}_{\mathbb{C}}$$

is then divisible by n , hence so is $\tilde{u} : \tilde{A} \rightarrow \tilde{B}$ at the generic point of W . The kernel of multiplication by n is flat over W ; thus $\tilde{u}$ vanishes on this kernel, $\tilde{u}$ and u are divisible by n , and ψ is bijective.

(C) *Necessity.* That $(T(A), F)$ satisfies (a) follows from Weil; condition (d), which implies (b) and (c), follows from 6.

(D) *Isogenies.* Let (T_0, F) satisfy (a) (d) and let T be a lattice in $T_0 \otimes \mathbb{Q}$, stable under F , still satisfying (d). Suppose that (T_0, F) is the image of an abelian variety A over $\mathbb{F}_q$ and let us prove that (T, F) comes from an isogenous abelian variety. Replacing T by $\frac{1}{k}T$, which is isomorphic to it, one may suppose that $T \supset T_0$. Condition (d) implies that T satisfies (4.1), and T defines a subgroup H of $\overline{A}$, which is defined over $\mathbb{F}_q$, and

$$(T, F) = T(A/H).$$

(E) *Surjectivity.* The functor T induces a functor $T_{\mathbb{Q}}$ from the category of ordinary abelian varieties up to isogeny over $\mathbb{F}_q$ to the category of finite-rank $\mathbb{Q}$ -vector spaces endowed with an automorphism F satisfying (a) (b). By (D), it is enough to prove that this functor $T_{\mathbb{Q}}$ is essentially surjective. It is even enough to show that every simple object (V, F) of the image category is attained. By Honda [1] (see also [6]), there exists an abelian variety A over $\mathbb{F}_q$ such that the characteristic polynomial of the Frobenius F_A of A is a power of that of F . The third characterization in 2.¹ of ordinary abelian varieties shows that A is ordinary. Moreover, $(T(A) \otimes \mathbb{Q}, F)$ is a sum of copies of (V, F) , hence, by (B), the abelian variety up to isogeny $A \otimes \mathbb{Q}$ is a sum of copies of an abelian variety B satisfying

$$T(B) \otimes \mathbb{Q} = (V, F).$$

8. Let (T, F) be a pair satisfying the hypotheses of the theorem, let $2g$ be the rank of T , let A be the corresponding abelian variety over $\mathbb{F}_q$, and let $A_{\mathbb{C}}$ be the complex abelian variety deduced from it (3.). One has

$$T = H_1(A_{\mathbb{C}}),$$

so that $T \otimes \mathbb{R}$ is identified with the Lie algebra of $A_{\mathbb{C}}$ and, as such, is endowed with a complex structure. Here is, according to J.-P. Serre, how to reconstruct this complex structure in terms of T , F , and the restriction of φ to $W_0(\overline{\mathbb{F}_p})$.

Proposition. The complex structure defined above on $T \otimes \mathbb{R}$ is characterized by the following properties:

- (I) The endomorphism F is $\mathbb{C}$ -linear.
- (II) If v is the valuation of the algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ in $\mathbb{C}$ extending the valuation of $W_0(\overline{\mathbb{F}_p})$, the valuations of the g eigenvalues of this endomorphism are strictly positive.

Condition (I) is evident, and condition (II) follows from the fact that the action of F on the Lie algebra of A is congruent to zero modulo p . The uniqueness of the complex structure satisfying (I) and (II) follows easily from condition (b) satisfied by (T, F) .

Bibliography

1. Honda, T.: Isogeny classes of abelian varieties over finite fields. J. Math. Soc. Jap. **20**, 83–95 (1968).
2. Ihara, Y.: On congruence monodromy problems, vol. I. University of Tokyo, 1968.
3. — The congruence monodromy problems. J. Math. Soc. Jap. **20**, 107–121 (1968).
4. Lubin, J., J.-P. Serre, and J. Tate: Elliptic curves and formal groups. Woods Hole Summer Institute 1964 (mimeographed, printed in a restricted number of copies).
5. Serre, J.-P.: Groupes p -divisibles (d’après J. Tate). Séminaire Bourbaki 318, Novembre 1966.
6. Tate, J.: Classes d’isogénies de variétés abéliennes sur un corps fini (d’après T. Honda). Séminaire Bourbaki 352, Novembre 1968.
7. — Endomorphisms of abelian varieties over finite fields. Inventiones Math. **2**, 134–144 (1966).

¹The printed source refers here to 1.; the characterizations of ordinarity are stated in 2., and that reference is restored here.

Pierre Deligne
I.H.E.S.
91, Bures-sur-Yvette, France

(Received July 3, 1969)