Ordinary abelian varieties over a finite field

Pierre Deligne

1969

Translator's note

This page is a translation into English of the following:

Deligne, P. "Variétés abéliennes ordinaires sur un corps fini." *Inventiones Math.* **8** (1969), 238–243. publications.ias.edu/node/352

The translator (Tim Hosgood) takes full responsibility for any errors introduced, and claims no rights to any of the mathematical content herein.

Version: `94f6dce`

p. 238

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

1

Let p be a prime number, $\mathbb{F}_p$ the field $\mathbb{Z}/(p)$, and $\overline{\mathbb{F}}_p$ an algebraic closure of $\mathbb{F}_p$. For every power q of p, let $\mathbb{F}_q$ be the subfield of q elements of $\overline{\mathbb{F}}_p$. For every algebraic extension k of $\mathbb{F}_p$, we denote by $W_0(k)$ the discrete valuation Henselian 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 $W = W(\overline{F}_p)$, and let φ be an embedding of W into 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 $\mathbb{Z}_\ell(1)(\mathbb{C}) = \varprojlim \mu_{\ell^n}(\mathbb{C})$.

We denote by A^* the dual abelian variety of an abelian variety A. For every field k, we denote by $\overline{k}$ the 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 said to be *ordinary* if any of the following equivalent conditions are satisfied:

i. A has p^g points of order dividing p with values in $\overline{k}$.
ii. The "Hasse-Witte matrix" $F^*\colon H^1(A^{(p)}, \mathscr{O}_{A^{(p)}}) \to H^1(A, \mathscr{O}_A)$ is invertible.
iii. The neutral component of the group scheme A_p that is the kernel of multiplication by p is of multiplicative type (and thus geometrically isomorphic to a power of μ_p).

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

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

3

Let A be an ordinary abelian variety over $\overline{\mathbb{F}}_p$. We denote by $\widetilde{A}$ the canonical Serre–Tate covering [4] of A over W. Recall that $\widetilde{A}$ depends functorially on A, and is characterised by the fact that the p-divisible group $T_p(\widetilde{A})$ over W attached to $\widetilde{A}$ [5] is the product of the p-divisible groups (uniquely determined, by §2.iii) that cover, respectively, the neutral component and the largest étale quotient of $T_p(A)$. The canonical covering $\widetilde{A}$ is again the *p. 239* unique covering of A such that every endomorphism of A lifts to $\widetilde{A}$. We denote by $T(A)$ the integer homology of the complex abelian variety $A_{\mathbb{C}}$ induced by $\widetilde{A}$ and φ by the extension of scalars of W to $\mathbb{C}$:

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

We know that $\widetilde{A}$ descends uniquely to $W_0(\overline{F}_p)$, and so $A_{\mathbb{C}}$ depends only on A and on the restriction of φ to $W_0(\overline{F}_p)$. The free $\mathbb{Z}$-module $T(A)$ is of rank $2\dim(A)$; it is functorial in A. Furthermore, if $\ell \neq p$ is a prime number, then we have, functorially, that

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

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

$$T(A) \otimes T(A^*) \to \mathbb{Z}(1) \tag{3.2}$$

(it is necessary to use $\mathbb{Z}(1)$ instead of $\mathbb{Z}$ in order to obtain a theory that is invariant under complex conjugation). The pairings (3.2) are compatible, via (3.1), with the pairings

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

a morphism $\xi\colon A \to A^*$ defines a polarisation of A if and only if $\xi_{\mathbb{C}}\colon A_{\mathbb{C}} \to A^*_{\mathbb{C}}$ defines a polarisation of $A_{\mathbb{C}}$. Set

$$\begin{aligned} T'_p(A) &= \mathrm{Hom}(\mathbb{Q}_p/\mathbb{Z}_p, A(\overline{F}_p)) \\ T''_p(A) &= \mathrm{Hom}_{\mathbb{Z}_p}(T'_p(A^*), \mathbb{Z}(1) \otimes \mathbb{Z}_p) \end{aligned}$$

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

By definition of the canonical covering, the p-divisible group $T_p(\widetilde{A})$ is the sum of the constant proétale group $T'_p(A)$ and the Cartier dual of $T'_p(A^*)$. For every morphism $u\colon A \to B$, the induced morphism $u\colon T_p(\widetilde{A}) \to T_p(\widetilde{B})$ can be identified with the sum of $u|T'_p(A)\colon T'_p(A) \to T'_p(B)$ and the Cartier transpose of $u^t|T'_p(B^*)\colon T'_p(B^*) \to T'_p(A^*)$. Over $\mathbb{C}$, we canonically have that $\mathbb{Z}(1)/(p^n) \sim \mu_{p^n}$, whence an isomorphism of functors:

$$T_{(p)}(A) = T(A) \otimes \mathbb{Z}_p = T'_p(A) \oplus T''_p(A). \tag{3.3}$$

4

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

$$0 \to H_1(X) \to H_1(Y) \to \mathrm{Ker}(\varphi) \to 0.$$

The abelian varieties that are quotients of X by a finite subgroup, and these finite subgroups of X, correspond bijectively with the sub-lattice of $H_1(X) \otimes \mathbb{Q}$ containing $H_1(X)$. p. 240

Let A be an ordinary abelian variety over $\overline{\mathbb{F}}_p$. If n is an integer coprime to p, then the subschemes of finite groups of order n of A, of $\widetilde{A}$, and of $A_{\mathbb{C}}$, correspond bijectively, and also correspond to lattices R containing $T(A)$ such that $[R : T(A)] = n$.

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

All told, the finite subgroups of A^p, or the abelian varieties that are quotients of A, correspond bijectively to the lattices R containing $T(A)$ such that

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

5

In particular, $A^{(p)}$, the quotient of A by the largest infinitesimal subgroup of A that is annihilated by p (for ordinary A), is defined by the lattice $T(A)^{(p)}$ containing $T(A)$ that is p-isogenous to $T(A)$, and 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 $F\colon x \mapsto x^q$ its Frobenius endomorphism. Recall that A is uniquely determined by the pair $(\overline{A}, F)$ induced by (A, F) by extension of scalars from $\mathbb{F}_q$ to $\overline{\mathbb{F}}_q$; the endomorphism F of $\overline{A}$ factors as the relative Frobenius morphism $F_{\mathrm{r}}^{(q)}\colon \overline{A} \to \overline{A}^{(q)}$ followed by an isomorphism $F'\colon \overline{A}^{(q)} \to \overline{A}$. If A is ordinary, then we denote by $T(A)$ the $\mathbb{Z}$-module $T(\overline{A})$ endowed with the endomorphism F induced by the Frobenius endomorphism of A. By §5, the above, and (3.3), the lattices $T(A)$ and $F(T(A))$ are p-isogenous, and we have that

$$F(T'_p(A)) = T'_p(A), \tag{6.1}$$

$$F(T''_p(A)) = q T''_p(A). \tag{6.2}$$

7

Theorem.

The functor $A \mapsto (T(A), F)$ is an equivalence of categories between the category of ordinary abelian varieties over $\mathbb{F}_q$ and the category of free $\mathbb{Z}$-modules T of finite type endowed with an endomorphism F that satisfy the following conditions: p. 241

a. *F is semi-simple, and its eigenvalues have complex absolute value $q^{\frac{1}{2}}$,*
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 is of rank d, then the reduction $\bmod p$ of the polynomial $\mathrm{Pc}_T(F;x)$ is not divisible by $x^{[d/2]+1}$,*
c. *there exists an endomorphism V of T such that $FV = q$.*

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

d. *the module $T \otimes \mathbb{Z}_p$ admits a decomposition, stable under F, into two sub-$\mathbb{Z}_p$-modules T'_p and T''_p of equal dimension, and such that $F|T'_p$ is invertible, and $F|T''_p$ is divisible by q.*

Proof. A. We first prove that (a)+(b)+(c) $\Longrightarrow$ (d). If α is a complex eigenvalue of F, then $\overline{\alpha}$ is another, of the same multiplicity, and $\alpha\overline{\alpha} = q$. If we exclude those that are equal to $\pm q^{\frac{1}{2}}$, then the eigenvalues of F in $\mathbb{C}$, and thus in $\overline{\mathbb{Q}}_p$, can be grouped into pairs of roots α and q/α. The roots α and q/α can not simultaneously be p-adic units, and so it follows from (b) that $\pm q^{\frac{1}{2}}$ is not an eigenvalue of F, that half of the eigenvalues of F in $\overline{\mathbb{Q}}_p$ are p-adic units, say $\alpha_1, \ldots, \alpha_{d/2}$, and that the other half are of the form $\beta_1 = q/\alpha_1, \ldots, \beta_{d/2} = q/\alpha_{d/2}$. Let $T_{(p)} = T \otimes \mathbb{Z}_p$, $V_p = T \otimes \mathbb{Q}_p$, V'_p the subspace of V_p given by the kernel of $\prod_i (F - \alpha_i)$, and V''_p the kernel of the endomorphism $\varphi = \prod_i (F - \beta_i)$. We have that $V_p = V'_p \oplus V''_p$. Let T'_p be the projection from $T_{(p)}$ to V'_p, and let $T''_p = T_{(p)} \cap V''_p$. Since φ annihilates V''_p, and respects T, it sends T'_p to $T_{(p)} \cap V'_p \subset T'_p$. Also, $\det(\varphi|V'_p) = \prod_{i,j} (\alpha_i - \beta_j)$ is a p-adic unit, and so $\varphi(T'_p) = T'_p$, and $T_{(p)} \cap V'_p = T'_p$, and so $T_{(p)} = T'_p \oplus T''_p$.

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

$$\psi\colon \mathrm{Hom}(A,B) \to \mathrm{Hom}_F(T(A), T(B)).$$

By the theorem of Tate [7] and by (3.1), the arrow

$$\psi_\ell\colon \mathrm{Hom}(A,B) \otimes \mathbb{Z}_\ell \to \mathrm{Hom}_F(T(A), T(B)) \otimes \mathbb{Z}_\ell$$

is an isomorphism for $(\ell, p) = 1$, and so $\psi \otimes \mathbb{Q}$ is an isomorphism. We know that $\mathrm{Hom}(A,B)$ is torsion free, and so ψ is injective. Let $u\colon A \to B$ be a morphism such that $T(u)$ is divisible by n. The induced morphism $u_{\mathbb{C}}\colon \overline{A}_{\mathbb{C}} \to \overline{B}_{\mathbb{C}}$ is thus divisible by n, and thus so too is $\widetilde{u}\colon \widetilde{\overline{A}} \to \widetilde{\overline{B}}$ at the generic point of W. The kernel of multiplication by n is flat over W; $\widetilde{u}$ thus disappears on this kernel, $\widetilde{u}$ and u are divisible by n, and ψ is bijective.

C. *Necessity.* The fact that $(T(A), F)$ satisfies (a) follows from Weil; condition (d), which implies (b) and (c), follows from §6. p. 242

D. *Isogenies.* Let (T_0, F) satisfy (a) and (d), and let T be a lattice in $T_0 \otimes \mathbb{Q}$, stable under F, that also satisfies (d). Suppose that (T_0, F) is the image of an abelian variety A over $\mathbb{F}_q$;

we will prove that (T,F) comes from an isogenous abelian variety. By T with $\frac{1}{k}T$, which is isomorphic to T, we can suppose that $T \supset T_0$. Condition (d) implies that T satisfies (4.1), and that T defines a subgroup H of $\overline{A}$, defined over $\mathbb{F}_q$, and such that $(T,F) = T(A/H)$.

E. *Surjectivity.* The functor T induces a functor $T_{\mathbb{Q}}$ from the category of isogeny classes of ordinary abelian varieties over $\mathbb{F}_q$ to the category of finite-dimensional $\mathbb{Q}$-vector spaces endowed with an automorphism F that satisfies (a) and (b). By (D), it suffices to prove that this functor $T_{\mathbb{Q}}$ is essentially surjective. It even suffices to show that every simple object (V,F) in the codomain is in the image. 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 characterisation in §2 of ordinary abelian varieties shows that A is ordinary. Furthermore, $(T(A) \otimes \mathbb{Q}, F)$ is the sum of copies of (V,F), and thus, by (B), the isogeny class of the abelian variety $A \otimes \mathbb{Q}$ is the sum of copies of an abelian variety B that satisfies $T(B) \otimes \mathbb{Q} = (V,F)$. □

8

Let (T,F) be a pair satisfying the hypotheses of the theorem, $2g$ the rank of T, A the corresponding abelian variety over $\mathbb{F}_q$, and $A_{\mathbb{C}}$ the induced complex abelian variety (§3). We have that

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

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

Proposition.

The complex structure on $T \otimes \mathbb{R}$ defined above is characterised 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 $\mathbb{C}$ that extends the valuation of $W_0(\mathbb{F}_p)$, then the valuations of the g eigenvalues of this endomorphism are strictly positive.

Proof. 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 $\bmod p$. The uniqueness of a structure satisfying (i) and (ii) follows easily from condition (b), satisfied by (T,F). □

Bibliography

[1] T. Honda. "Isogeny classes of abelian varieties over finite fields." *J. Math. Soc. Jap.* **20** (1968), 83–95.

[2] Y. Ihara. *On congruence monodromy problems*. University of Tokyo, 1968. **1**.

[3] Y. Ihara. "The congruence monodromy problems." *J. Math. Soc. Jap.* **20** (1968), 107–121.

[4] J. Lubin, J.-P. Serre, J. Tate. *Elliptic curves and formal groups*. Woods Hole Summer Institute, 1964.

[5] J.-P. Serre. "Groups p-divisibles (d'après J. Tate)." *Séminaire Bourbaki*. **10** (1966-67).

[6] J. Tate. "Classes d'isogénies de variétés abéliennes sur un corps fini (d'après T. Honda)." *Séminaire Bourbaki*. **11** (1968-69).

[7] J. Tate. "Endomorphisms of abelian varieties over finite fields." *Inventiones Math.* **2** (1966), 134–144.