1. An isogeny class of supersingular elliptic curves

Let p be a prime number, and k a finite field with p^2 elements. The Honda–Tate theory of abelian varieties over finite fields guarantees the existence of a k–isogeny class $\mathcal{C}_{-p}$ of elliptic curves over k whose objects A are those for which the equality

$$\pi_A = -p \tag{1}$$

holds in the ring $\mathrm{End}_k(A)$ (cf. [8], Théorème 1). Here $\pi_A : A \to A$ is the geometric Frobenius endomorphism of A relative to k, i.e., π_A is the identity on the topological space underlying A, and is given by $s \to s^{|k|}$ on sections. Furthermore, for any such A the division algebra $\mathrm{End}_k(A) \otimes \mathbf{Q}$ is "the" $\mathbf{Q}$–quaternion ramified at p and infinity (cf. Tate, loc. cit.), and the elliptic curve A is *supersingular*. In fact any supersingular elliptic curve over an algebraic closure $\bar{k}$ of k admits a canonical and functorial descent to $\mathcal{C}_{-p}$. It can be shown that (cf. [1], Lemma 3.21 for a brief sketch of the proof):

Theorem 1.1. *The base extension functor $A \to A \otimes_k \bar{k}$ induces an equivalence of categories between $\mathcal{C}_{-p}$ and the isogeny class of supersingular elliptic curves over $\bar{k}$.*

In this section we explain how isomorphism classes of objects of $\mathcal{C}_{-p}$, equipped with some extra structure, are parametrized by a certain double coset arising from the adelic points of the multiplicative group of the quaternion algebra above. To describe such correspondence we make essential use of results of Tate (cf. [12], Thm. 6), describing the local structure at every prime ℓ of the module $\mathrm{Hom}_k(A, B)$ of homomorphisms between two abelian varieties A, B over a finite field k.

Since the correspondence is classical, this section will probably not appear in a more definitive version of this paper. We first learnt of this correspondence in [7], what is included here is the outcome of our effort in understanding all the details of its proof. Ghitza in [4] explains, and generalizes, a correspondence very similar to the one considered here. Our method is similar to his.

The notation adopted throughout the section is as follows. The Galois group of a fixed algebraic closure $\bar{k}$ of k over k is denoted by G_k. For an object A of $\mathcal{C}_{-p}$, and a prime number ℓ, we let $T_\ell(A)$ denote the ℓ–adic Tate module of A for $\ell \neq p$, and the contravariant Dieudonné module attached to the p–divisible group $A[p^\infty]$ of A for $\ell = p$ (cf. [11], Ch. 1; [2], Ch. III). For any prime ℓ, we set $V_\ell(A) = T_\ell(A) \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell$. If $\ell \neq p$ then $V_\ell(A)/T_\ell(A)$ is identified with the Galois module $A[\ell^\infty]$ of $\bar{k}$–valued points of A of ℓ–power torsion. If $\psi : A \to B$ is a morphism in $\mathcal{C}_{-p}$, then $\psi_\ell : T_\ell(A) \to T_\ell(B)$ denotes the corresponding morphism of Tate modules

for $\ell \neq p$, and $\psi_p : T_p(B) \to T_p(A)$ that of Dieudonné modules. The morphism of $\mathbf{Q}_\ell$–vector spaces deduced from ψ_ℓ is denoted by $V_\ell(\psi)$, while $\psi[\ell^\infty]$ denotes, for $\ell \neq p$, the morphism from $A[\ell^\infty]$ to $B[\ell^\infty]$ induced by ψ. It is a basic fact that $\psi \neq 0$ if and only if ψ_ℓ is injective for some (all) ℓ, if and only if $V_\ell(\psi)$ is an isomorphism for some (all) ℓ. If ψ is an isogeny, then $\ker_\ell(\psi)$ denotes the finite subgroup of A given by the ℓ–primary part of $\ker(\psi)$. If $\ell \neq p$, then $\ker_\ell(\psi)$ will be identified with the Galois module given by $\mathrm{coker}(\psi_\ell)$, on the other hand $\mathrm{coker}(\psi_p)$ is the finite length Dieudonné module associated to $\ker_p(\psi)$.

1.1. **The endomorphism ring.** Let E be any object of $\mathcal{C}_{-p}$, denote the ring $\mathrm{End}_k(E)$ by R, and the $\mathbf{Q}$–algebra $\mathrm{End}_k(E) \otimes \mathbf{Q}$ by D. If ℓ is any prime number, set $R_\ell = R \otimes \mathbf{Z}_\ell$ and $D_\ell = D \otimes \mathbf{Q}_\ell$. As mentioned above, D is a central, division algebra over $\mathbf{Q}$ such that D_ℓ is isomorphic to the matrix algebra $M_2(\mathbf{Q}_\ell)$ when $\ell \neq p$, and to "the" central, division algebra over $\mathbf{Q}_\ell$ of rank four when $\ell = p$. In this section we show that R is a *maximal* order of D or, equivalently, that R_ℓ is a maximal $\mathbf{Z}_\ell$–order in D_ℓ, for all ℓ.

If ℓ is a prime $\neq p$, then $T_\ell(E)$ is a free $\mathbf{Z}_\ell$–module of rank two on which G_k acts continuously and in a natural way. The action of the arithmetic Frobenius $\mathrm{Frob}_k \in G_k$ on $T_\ell(E)$ is the *same* as that given by $\pi_{E,\ell}$, i.e., that induced by π_E via functoriality of the Tate module. Therefore the Galois module structure of $T_\ell(E)$ is specified by the requirement that Frob_k act as multiplication by $-p$. In particular we see that

$$\mathrm{End}_{\mathbf{Z}_\ell[G_k]}(T_\ell(E)) = \mathrm{End}_{\mathbf{Z}_\ell}(T_\ell(E)). \tag{2}$$

The natural map $\iota_\ell : R \to \mathrm{End}_{\mathbf{Z}_\ell[G_k]}(T_\ell(E))$ sending $r \in R$ into the induced morphism r_ℓ of Tate modules extends by continuity to a map on R_ℓ, also denote by ι_ℓ. A special case of a theorem of Tate (cf. [9] or [12]) yields:

Theorem 1.2. *The map $\iota_\ell : R_\ell \to \mathrm{End}_{\mathbf{Z}_\ell}(T_\ell(E))$ is an isomorphism, and R_ℓ is a maximal order of D_ℓ.*

In order to study R_p it is customary to work with the contravariant Dieudonné module $T_p(E)$ attached to the p–divisible group $E[p^\infty]$ of E. If $W = W(k)$ is the ring of Witt vectors of k, recall that the Dieudonné ring $\mathcal{A} = \mathcal{A}_k$ over k is the non–commutative, polynomial ring in two variables $W[F, V]$ subject to the relations

$FV = VF = p$;

$F\lambda = \lambda^\sigma F$, $V\lambda^\sigma = \lambda V$;

where $\lambda \in W$ is any element, and $\lambda \to \lambda^\sigma$ is the automorphism of W inducing the absolute Frobenius on the residue field k. Notice that in this special case where $|k| = p^2$ we have that F and V have the same semi–linear behavior with respect to the action on W, since $\sigma = \sigma^{-1}$.

The Dieudonné module $T_p(E)$ is a left $\mathcal{A}$–module that is finite and free of rank two as W–module. Equation (1) implies that F^2 acts as multiplication by $-p$, therefore the k–semi–linear endomorphism of $T_p(E)/pT_p(E)$ induced by F is nonzero and nilpotent. Using this one shows that there exists a W–basis (e_1, e_2) of $T_p(E)$ such that

$F(e_1) = -pe_2$;

$F(e_2) = e_1$;

moreover we must have that $V = -F$ (cf. [5] for more details). The nonzero $\mathcal{A}$–submodules of $T_p(E)$ that are W–lattices of $V_p(E)$ are those given by $F^n T_p(E)$, for $n \geq 0$. In terms of the arithmetic of E, this implies that every finite, closed subgroup of E of p–power rank is the kernel of a chain of successive, alternating applications of the absolute Frobenius morphisms $F_E : E \to E^{(p)}$ and $F_{E^{(p)}} : E^{(p)} \to E^{(p^2)} = E$. Notice that equation (1) says that $F_{E^{(p)}} F_E = -p$.

The ring R acts on the right of $T_p(E)$ by functoriality, and determines a ring homomorphism $\iota_p : R^{\mathrm{op}} \to \mathrm{End}_{\mathcal{A}}(T_p(E))$ which extends by continuity to R_p^{op}. There is a version at p of Theorem (1.2), also due to Tate (cf. [12], Thm. 6):

Theorem 1.3. *The map $\iota_p : R_p^{\mathrm{op}} \to \mathrm{End}_{\mathcal{A}}(T_p(E))$ is an isomorphism.*

The ring R_p^{op} is thus identified with the ring of W–linear endomorphisms of $T_p(E)$ commuting with F. Using the coordinate system induced by the previous basis (e_1, e_2) of $T_p(E)$, we readily compute that R_p^{op} is described by matrices of the form

$$\begin{pmatrix} a^\sigma & -b \\ pb^\sigma & a \end{pmatrix},$$

where $a, b \in W$. Letting a and b vary in the degree two, unramified extension $L = W[1/p]$ of $\mathbf{Q}_p$, leads to a matrix description of $D_p^{\mathrm{op}} = R_p^{\mathrm{op}} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ whose trace (tr) and determinant (det) respectively give the reduced trace and reduced norm of D_p^{op} (cf. [10], I.1). The involution $x \to \mathrm{tr}(x) - x$ gives an isomorphism $D_p^{\mathrm{op}} \xrightarrow{\sim} D_p$, sending R_p^{op} to R_p. Its effect on the matrix description is

$$\begin{pmatrix} a^\sigma & -b \\ pb^\sigma & a \end{pmatrix} \longrightarrow \begin{pmatrix} a & b \\ -pb^\sigma & a^\sigma \end{pmatrix}.$$

The ring R_p is the unique *maximal* order of D_p as it consists of all the elements with both reduced trace and reduced norm valued in $\mathbf{Z}_p$. If $\nu_p : \mathbf{Q}_p \to \mathbf{Z} \cup \{\infty\}$ is the valuation of $\mathbf{Q}_p$, normalized in such a way that $\nu_p(p) = 1$, then the function $R \ni r \to \nu_p(\det(r)) \in \mathbf{Z} \cup \{\infty\}$ has the formal properties of a discrete valuation ([10], II.1). Therefore R has a unique, two–sided, maximal, principal ideal $\mathfrak{m}$ given by all the elements

whose determinant belongs to $(p) \subset \mathbf{Z}_p$, and generated by element whose determinant generates (p) in $\mathbf{Z}_p$. The residue field $R/\mathfrak{m}$ has order p^2.

1.2. **Isogenies in $\mathcal{C}_{-p}$ and ideals of** $\mathrm{End}_k(E)$**.** In this section we prove two theorems useful to describe a correspondece between isogenies of $\mathcal{C}_{-p}$ whose source is a fixed object E, and nonzero, left ideals of $R = \mathrm{End}_k(E)$. They both follow from the results of Tate that we already encountered.

Let $\psi : E \to E_\psi$ be any isogeny in $\mathcal{C}_{-p}$, consider the R–left ideal

$$I_\psi = \{r \in R : r = r'\psi, \text{ for some } r' \in \mathrm{Hom}_k(E_\psi, E)\}$$

consisting of all the endomorphisms of E trivial on the finite subgroup $\ker(\psi)$. Pull–back by ψ gives an isomorphism $\psi^* : \mathrm{Hom}(E_\psi, E) \xrightarrow{\sim} I_\psi$ of left R–modules. Notice that I_ψ is a $\mathbf{Z}$–lattice of D, since for example $\deg(\psi) \in I_\psi$. If ℓ is any prime, the module $I_\psi \otimes \mathbf{Z}_\ell$ will be denoted by $I_{\psi,\ell}$, it is a left ideal of R_ℓ that is also a $\mathbf{Z}_\ell$–lattice of D_ℓ. The isomorphism ψ^* above induces an isomorphism $\mathrm{Hom}(E_\psi, E) \otimes \mathbf{Z}_\ell \xrightarrow{\sim} I_{\psi,\ell}$, tacitly used in what follows.

Remark 1.4. From the maximality of R_ℓ, it follows that $I_{\psi,\ell}$ is *principal* for any prime ℓ (cf. [10] II.1, II.2). If $\ell \neq p$, there exists a $\mathbf{Z}_\ell$–lattice Λ_0 of $V_\ell(E)$ *containing* $T_\ell(E)$ such that the isomorphism ι_ℓ (cf. Thm. 1.2) sends $I_{\psi,\ell}$ to the left ideal $\mathrm{End}_{\mathbf{Z}_\ell}(\Lambda_0, T_\ell(E))$. In fact we will see that Λ_0 is the pull–back of $T_\ell(E_\psi)$ via $V_\ell(\psi)$ (cf. proof of Thm. 1.5). For $\ell = p$, there exists a W–lattice M_0 in $V_p(E)$ *contained* in $T_p(E)$ such that the isomorphism ι_p (cf. Thm. 1.3) sends $I_{\psi,p}$ to the right ideal $\mathrm{End}_{\mathcal{A}}(T_p(E), M_0)$. From the proof of Theorem 1.5 it will follow that M_0 is the isomorphic image of $T_p(E_\psi)$ with respect to $V_p(\psi) : V_p(E_\psi) \to V_p(E)$. For any ℓ, the left ideal $I_{\psi,\ell}$ is generated by any of its elements of reduced norm with minimal valuation.

Before showing that the isogeny ψ can essentially be recovered from I_ψ (cf. Thm. 1.5), we make a few observations. Let ℓ be a prime $\neq p$, from the isogeny $\psi : E \to E_\psi$ we can deduce a commutative diagram of G_k–modules with exact rows

$$\begin{array}{ccccccccc}
0 & \longrightarrow & T_\ell(E) & \longrightarrow & V_\ell(E) & \longrightarrow & E[\ell^\infty] & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \psi_\ell} & & \downarrow{\scriptstyle V_\ell(\psi)} & & \downarrow{\scriptstyle \psi[\ell^\infty]} & & \\
0 & \longrightarrow & T_\ell(E_\psi) & \longrightarrow & V_\ell(E_\psi) & \longrightarrow & E_\psi[\ell^\infty] & \longrightarrow & 0.
\end{array}$$

The pull–back of the Tate module $T_\ell(E_\psi)$ via the isomorphism $V_\ell(\psi)$ identifies the former with a $\mathbf{Z}_\ell$–lattice of $V_\ell(E)$ containing $T_\ell(E)$, and that will be denoted by Λ_{ψ_ℓ}. Under this identification, the map ψ_ℓ clearly corresponds to the inclusion $T_\ell(E) \subset \Lambda_{\psi_\ell}$. Since the two rows of the diagram are exact,

$V_\ell(\psi)$ induces an identification $\mathrm{coker}(\psi_\ell) \simeq \ker(\psi[\ell^\infty])$, or, equivalently,

$$\Lambda_{\psi_\ell}/T_\ell(E) \simeq \ker_\ell(\psi). \tag{3}$$

The $\mathbf{Z}_\ell$–lattice Λ_ψ depends on ψ in a functorial way, in a sense that can be made precise by working with the category $\mathcal{C}_E$ that will be introduced in the next section. We observe that if $\varphi : E \to E_\varphi$ is another isogeny, and $u : E_\psi \to E_\varphi$ is a morphism, then the map $V_\ell(\varphi)^{-1}V_\ell(u)V_\ell(\psi) : V_\ell(E) \to V_\ell(E)$ sends Λ_ψ to Λ_φ and there is a commutative diagram

$$\begin{array}{ccc} \Lambda_\psi & \xrightarrow{V_\ell(\varphi)^{-1}V_\ell(u)V_\ell(\psi)} & \Lambda_\varphi \\ \downarrow \simeq & & \downarrow \simeq \\ T_\ell(E_\psi) & \xrightarrow{u_\ell} & T_\ell(E_\varphi) \end{array}$$

where the vertical morphisms are the natural identifications. In particular, if u is an isogeny, the cokernel of the top horizontal map of the diagram is isomorphic to $\ker_\ell(u)$ in a natural way.

If $\ell = p$, the situation is formally analogous, after replacing the covariant Tate module by the contravariant Dieudonné module. The morphism $\psi_p : T_p(E_\psi) \to T_p(E)$ identifies $T_p(E_\psi)$ with an $\mathcal{A}$–submodule M_{ψ_p} of $T_p(E)$ that is a W–lattice of $V_p(E)$. Moreover $T_p(E)/M_{\psi_p}$ is the Dieudonné module associated to the finite group $\ker_p(\psi)$. As before, if $\varphi : E \to E_\varphi$ is an isogeny and $u : E_\psi \to E_\varphi$ is any morphism, then the map $V_p(\psi)V_p(u)V_p(\varphi)^{-1} : V_p(E) \to V_p(E)$ sends M_{φ_p} to M_{ψ_p}, there is a commutative diagram

$$\begin{array}{ccc} M_{\psi_p} & \xleftarrow{V_p(\psi)V_p(u)V_p(\varphi)^{-1}} & M_{\varphi_p} \\ \downarrow \simeq & & \downarrow \simeq \\ T_p(E_\psi) & \xleftarrow{u_p} & T_p(E_\varphi) \end{array}$$

where the vertical morphisms are the natural identifications. Moreover the cokernel of the top horizontal map of the diagram is the Dieudonné module of $\ker_p(u)$.

Theorem 1.5. *For any isogeny $\psi : E \to E_\psi$ and any prime number ℓ, there exists an isogeny $r' : E_\psi \to E$ whose degree is prime to ℓ. Equivalently, there exists an isogeny $r \in I_\psi$ so that $\ker_\ell(r) = \ker_\ell(\psi)$. In particular, $\ker(\psi)$ coincides with the largest k–subgroup of E killed by every element of I_ψ.*

Proof. We begin by proving the theorem in the case $\ell \neq p$. Consider the commutative diagram

$$\begin{array}{ccc} \mathrm{Hom}(E_\psi, E) \otimes \mathbf{Z}_\ell & \longrightarrow & \mathrm{Hom}_{\mathbf{Z}_\ell}(T_\ell(E_\psi), T_\ell(E)) \\ \downarrow \simeq & & \downarrow \simeq \\ I_{\psi,\ell} & \longrightarrow & \mathrm{Hom}_{\mathbf{Z}_\ell}(\Lambda_{\psi_\ell}, T_\ell(E)) \end{array}$$

where the horizontal maps are induced by functoriality of the Tate module, and the vertical isomorphism on the right comes from the identification $T_\ell(E_\psi) \simeq \Lambda_{\psi_\ell}$ and is given by $u_\ell \to u_\ell V_\ell(\psi)|^{T_\ell(E_\psi)}_{\Lambda_{\psi_\ell}}$.

Since $\mathrm{Hom}_{\mathbf{Z}_\ell[G_k]}(T_\ell(E_\psi), T_\ell(E)) = \mathrm{Hom}_{\mathbf{Z}_\ell}(T_\ell(E_\psi), T_\ell(E))$, the main theorem of [9] says that the top horizontal map of the previous diagram is an isomorphism, thus so is the bottom one and the isomorphism ι_ℓ from Theorem 1.2 induces an identification of left ideals

$$I_{\psi,\ell} \simeq \mathrm{Hom}_{\mathbf{Z}_\ell}(\Lambda_{\psi_\ell}, T_\ell(E)). \tag{4}$$

In particular, $I_{\psi,\ell} = R_\ell g_\ell$, where $g_\ell \in D_\ell$ is any element of R_ℓ mapping Λ_{ψ_ℓ} isomorphically to $T_\ell(E)$. If we pick $r \in I_\psi$ such that its image $r_\ell \in I_{\psi,\ell}$ is a generator then $\ker_\ell(r) = \ker_\ell(\psi)$ by (3), since the lattices Λ_{r_ℓ} and Λ_{ψ_ℓ} in $V_\ell(E)$ coincide.

For $\ell = p$ consider, in an analogous way, the commutative diagram

$$\begin{array}{ccc} \mathrm{Hom}(E_\psi, E) \otimes \mathbf{Z}_p & \longrightarrow & \mathrm{Hom}_{\mathcal{A}}(T_p(E), T_p(E_\psi)) \\ \downarrow \simeq & & \downarrow \simeq \\ I_{\psi,p} & \longrightarrow & \mathrm{Hom}_{\mathcal{A}}(T_p(E), M_{\psi_p}) \end{array}$$

where the horizontal maps are induced by functoriality of T_p, and the vertical isomorphism on the right is given by $u_p \to \psi_p u_p$. Notice that the lower horizontal map is that induced by the anti–isomorphism $\iota_p : R_p \to \mathrm{End}_{\mathcal{A}}(T_p(E))$, where $\mathrm{Hom}_{\mathcal{A}}(T_p(E), M_{\psi_p})$ is regarded in a natural way as a right ideal of $\mathrm{End}_{\mathcal{A}}(T_p(E))$.

Since both horizontal maps are isomorphisms (cf. [12], Thm. 6), the principal left ideal $I_{\psi,p}$ of R_p is generated by any element r_p such that $\iota_p(r_p)$ defines an endomorphism of $T_p(E)$ sending $T_p(E)$ isomorphically to M_{ψ_p}. Choosing now $r \in I_\psi$ such that $r_p \in I_{\psi,p}$ is a generator, we see that $M_{r_p} = M_{\psi_p}$, therefore $\ker_p(r) = \ker_p(\psi)$ and the theorem follows. □

Let now I be a nonzero left ideal of R, consider the isogeny

$$\psi_I : E \longrightarrow E/H(I), \tag{5}$$

where

$$H(I) = \bigcap_{r \in I} \ker(r)$$

is the largest k–subgroup of E that is killed by every element of I, and ψ_I is the canonical isogeny. The ideal I can be recovered from ψ_I:

Theorem 1.6. *For any nonzero left ideal I of R we have $I = I_{\psi_I}$.*

Proof. Let $J = I_{\psi_I}$ be the left ideal of R given by the endomorphisms of E trivial on $H(I)$, certainly $I \subset J$. For any prime ℓ, denote by I_ℓ and J_ℓ the left ideals of R_ℓ obtained from I and J after tensoring with $\mathbf{Z}_\ell$. Since $I_\ell \subset J_\ell$, it will be enough to show that $J_\ell \subset I_\ell$ for any ℓ.

For $\ell \neq p$, as explained at the beginning of the section, the Tate module $T_\ell(E/H(I))$ is identified with the $\mathbf{Z}_\ell$–lattice $\Lambda_{\psi_{I,\ell}}$ of $V_\ell(E)$ containing $T_\ell(E)$ and such that the equality

$$\Lambda_{\psi_{I,\ell}}/T_\ell(E) = \ker_\ell(\psi_I),$$

holds in the ℓ–divisible group $E[\ell^\infty]$. Moreover, the isomorphism $\iota_\ell : R_\ell \xrightarrow{\sim} \mathrm{End}_{\mathbf{Z}_\ell}(T_\ell(E))$ induces an identification $J_\ell \simeq \mathrm{Hom}_{\mathbf{Z}_\ell}(\Lambda_{\psi_{I,\ell}}, T_\ell(E))$, as was shown in the proof of Theorem 1.5.

On the other hand, I_ℓ is a nonzero left ideal of $R_\ell = \mathrm{End}_{\mathbf{Z}_\ell}(T_\ell(E))$ and there exists a $\mathbf{Z}_\ell$–lattice Λ_0 of $V_\ell(E)$, containing $T_\ell(E)$, such that $I_\ell = \mathrm{Hom}_{\mathbf{Z}_\ell}(\Lambda_0, T_\ell(E))$; since $I_\ell \subset J_\ell$, we have $\Lambda_0 \supset \Lambda_{\psi_{I,\ell}}$.

Now, by definition of ψ_I we have

$$\ker_\ell(\psi_I) = \bigcap_{0 \neq r \in I} \ker_\ell(r),$$

or, reformulating,

$$\Lambda_{\psi_{I,\ell}} = \bigcap_{0 \neq r \in I} V_\ell(r)^{-1}(T_\ell(E)). \tag{6}$$

The right hand side of (6) certainly contains Λ_0, therefore $\Lambda_0 \subset \Lambda_{(\psi_I)_\ell}$ and $I_\ell \supset J_\ell$.

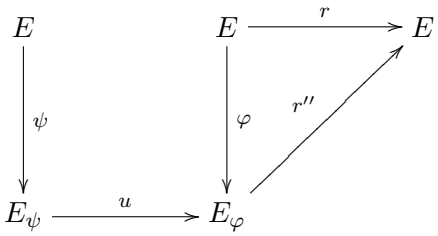
For $\ell = p$ the proof is similar and is omitted. As in the case $\ell \neq p$, the key fact is that I_p is known *a priori* to be principal, thanks to the maximality of R_p (cf. Remark 1.4). □

Remark 1.7. Theorem 1.6 is a special case of a more general result of Waterhouse (cf. [11], Thm. 3.15).

1.3. **An equivalence of categories.** We interpret the result of the previous section in a formal way, by showing the existence of an anti–equivalence of categories (cf. Thm. 1.8).

Let E be a fixed object of $\mathcal{C}_{-p}$, and let $\mathcal{C}_E$ be the category of *isogenies* of $\mathcal{C}_{-p}$ with source E, that is the category whose objects are isogenies in $\mathcal{C}_{-p}$ of the form $\psi : E \to E_\psi$, and whose sets of morphisms $\mathrm{Hom}(\psi, \varphi)$ between two objects is simply $\mathrm{Hom}(E_\psi, E_\varphi)$.

Let $\psi : E \to E_\psi$ be any object of $\mathcal{C}_E$, the natural identification $I_\psi = \mathrm{Hom}(E_\psi, E) = \mathrm{Hom}(\psi, \mathrm{id}_E)$ makes clear that I_ψ depends functorially on ψ; more precisely the assignment $\psi \to I_\psi$ defines a contravariant functor $\mathcal{I}$ from $\mathcal{C}_{-p}$ to the category $\mathcal{P}_R^{(1)}$ of projective left R–modules of rank one. We clarify that if $u \in \mathrm{Hom}(\psi, \varphi)$ is a morphism in $\mathcal{C}_E$, then $\mathcal{I}(u) : I_\varphi \to I_\psi$ is constructed as follows. If $r = r''\varphi \in I_\varphi$, consider the commutative diagram



the value of $\mathcal{I}(u)$ on r is the composition $r''u\psi \in I_\psi$.

From the results of the previous section we can draw the following consequence:

Theorem 1.8. *The functor $\mathcal{I}$ sending ψ to I_ψ induces an anti–equivalence of categories between $\mathcal{C}_E$ and $\mathcal{P}_R^{(1)}$.*

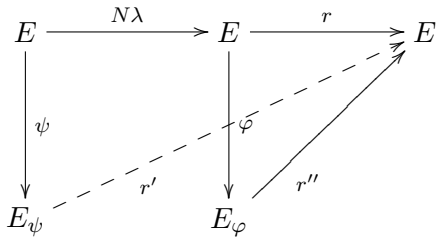
Proof. We show that any object of $\mathcal{P}_R^{(1)}$ is isomorphic to one of the form $\mathcal{I}(\psi)$, and that $\mathcal{I}$ is fullyfaithful.

Any nonzero projective left R–module P of rank one is isomorphic to a finitely generated, left R–submodule of D, therefore to a nonzero left ideal I of R, after multiplication by a suitable integer $N \geq 1$. From Theorem 1.6 we see that every nonzero left ideal I of R is of the form $\mathcal{I}(\psi)$, for some ψ in $\mathcal{C}_E$.

To see that $\mathcal{I}$ is fullyfaithful, let ψ and φ be two objects of $\mathcal{C}_E$, and $f : I_\varphi \to I_\psi$ any morphism of left R–modules. We have to show that there exists $u \in \mathrm{Hom}(\psi, \varphi)$ such that $f = \mathcal{I}(u)$. Since I_φ and I_ψ are lattices of D, f extends uniquely to an endomorphism of D, as left D–module, thus there is $\lambda \in D$ such that $f(x) = x\lambda$, for all $x \in I_\varphi$. Let N be an integer ≥ 1 such that $N\lambda \in R$. Right multiplication by $N\lambda$ on D clearly induces the morphism

$Nf : I_\varphi \to I_\psi$ and we will first show that there exists $u' \in \mathrm{Hom}(E_\psi, E_\varphi)$ such that $\mathcal{I}(u') = Nf$.

For $r = r''\varphi \in I_\varphi$ consider the commutative diagram



The existence of the dotted arrow r' follows from the fact that $rN\lambda$ belongs to I_ψ (in fact even to NI_ψ), and hence factors as $r'\psi$, for some $r' \in \mathrm{Hom}(E_\psi, E)$. Showing that there exists $u' \in \mathrm{Hom}(E_\psi, E_\varphi)$ with $\mathcal{I}(u') = Nf$ amounts to proving that $\varphi N\lambda$ factors as $u'\psi$, for a certain $u' \in \mathrm{Hom}(E_\psi, E_\varphi)$.

If $N\lambda = 0$ this is clear, therefore we may assume that $\varphi N\lambda$ is an isogeny. By Theorem 1.5 we have that

$$\ker(\varphi N\lambda) = \bigcap_{r'' \in \mathrm{Hom}(E_\varphi, E)} \ker(r''\varphi N\lambda),$$

but $r''\varphi N\lambda = r'\psi$, therefore

$$\ker(\psi) \subset \bigcap_{r'' \in \mathrm{Hom}(E_\varphi, E)} \ker(r''\varphi N\lambda).$$

The two equations readily imply $\ker(\psi) \subset \ker(\varphi N\lambda)$, which gives the desired factorization of $\varphi N\lambda$ as $u'\psi$.

A further application of Theorem 1.5 gives that u' is divisible by N in $\mathrm{Hom}(E_\psi, E_\varphi)$. In fact since $r''u'\psi \in NI_\psi$, for $r'' \in \mathrm{Hom}(E_\varphi, E)$, we have that $r''u' : E_\psi \to E$ is trivial on the subgroup $E_\psi[N]$. Since this happens for *all* $r'' \in \mathrm{Hom}(E_\varphi, E)$ we see that, by Theorem 1.5, u' is itself trivial on $E_\psi[N]$, and $u' = Nu$ for a unique $u \in \mathrm{Hom}(E_\psi, E_\varphi)$. Therefore $\mathcal{I}(u) = N^{-1}\mathcal{I}(u') = f$, this completes the proof of the theorem. □

1.4. **Adelic description of $\mathcal{C}_{-p}$.** The functor $\mathcal{I}$ introduced in the previous section admits an adelic description, thanks to the fact that I_ψ is locally principal, for any ψ in $\mathcal{C}_E$ (cf. Remark 1.4). Let $\hat{R}$ denote $R \otimes \hat{\mathbf{Z}}$ and, similarly, $\hat{D}$ denote $D \otimes \hat{\mathbf{Z}}$, we have $\hat{R} = \prod R_\ell$ and $\hat{D} = \prod D_\ell$, where the product is taken over all the primes ℓ.

If ψ is any object of $\mathcal{C}_E$, and ℓ is any prime, then $I_{\psi,\ell} = R_\ell g_\ell$, for some $g_\ell \in R_\ell$; observe that $g_\ell \in D_\ell^*$, since $I_{\psi,\ell}$ is a $\mathbf{Z}_\ell$–lattice of D_ℓ. The image of the adelic element $(g_\ell)_\ell \in \hat{R} \cap \hat{D}^*$ in the coset space $\hat{R}^* \backslash \hat{R} \cap \hat{D}^*$ depends only on ψ, and not on the choices of the g_ℓ, and is denoted by a_ψ.

Vicerversa, if $a \in \hat{R}^*\backslash\hat{R} \cap \hat{D}^*$ is represented by $(g_\ell)_\ell \in \hat{R} \cap \hat{D}^*$, then $R_\ell g_\ell = R_\ell$ for almost all ℓ, and there is a unique left ideal I_a of R such that $I_{a,\ell} = I_a \otimes \mathbf{Z}_\ell$ is equal to $R_\ell g_\ell$, for all ℓ. The isogeny corresponding to I_a will simply be denoted by $\psi_a : E \to E_{\psi_a}$, it defines an element of $\mathcal{C}_E$.

If Σ is the set of isomorphism classes of objects of $\mathcal{C}_E$, or of $\mathcal{C}_{-p}$, a consequence of Theorem 1.8 is:

Theorem 1.9. *The assignment $\psi \to a_\psi$ induces a correspondence*

$$\tau : \Sigma \xrightarrow{\sim} \hat{R}^*\backslash\hat{D}^*/D^*.$$

The surjectivity of τ follows from the fact that the inclusion $\hat{R}\cap\hat{D}^* \subset \hat{D}^*$ induces a bijection $\hat{R}^*\backslash\hat{R} \cap \hat{D}^*/D^* = \hat{R}^*\backslash\hat{D}^*/D^*$.

Let now $N \geq 1$ be a fixed integer not divisible by p. If $\psi : E \to E_\psi$ is an object of $\mathcal{C}_E$, the tangent space $\mathbf{t}_0(E_\psi)$ of E_ψ at the origin is a one–dimensional k–vector space, and its dual $\mathbf{t}_0(E_\psi)^*$ is identified with the space of invariant 1–form on E_ψ (defined over k). Consider the set $\Sigma(1, N)$ of isomorphism classes of triples (ψ, ω, x) given by an object $\psi : E \to E_\psi$ of $\mathcal{C}_E$, a nonzero invariant 1–form $\omega \in \mathbf{t}_0(E_\psi)^*$, and a point $x \in E_\psi[N](\bar{k})$ of order N. The notion of isomorphism between two such triples is clear: (ψ, ω, x) is isomorphic to (φ, η, y) if and only if there exists an isomorphism $u : E_\psi \xrightarrow{\sim} E_\varphi$ such that $u^*(\eta) = \omega$ and $u(x) = y$. Notice that k^* acts on $\Sigma(1, N)$ via homotheties on the second entry of the triples.

Choose now a nonzero 1–form $\omega_0 \in \mathbf{t}_0(E)^*$, and an element $x_0 \in E[N](\bar{k})$ of order N. The ring $\hat{R} = \prod R_\ell$ acts on the left of the product

$$\mathbf{t}_0(E)^* \times \prod_{\ell\neq p} E[\ell^\infty]$$

by considering the natural action of R_ℓ on $E[\ell^\infty]$ for $\ell \neq p$, and on $\mathbf{t}_0(E)^*$ for $\ell = p$. Notice that the action of R_p on $\mathbf{t}_0(E)^*$ is given by a canonical ring homomorphism $R_p \to k$, necessarily surjective because of the structure of R_p, that will be used to identify the residue field $R_p/\mathfrak{m}$ with k. The kernel of the corresponding character $R_p^* \to k^*$ is given by $R_p^*(1)$, the subgroup of units congruent to 1 modulo the maximal, two sided ideal $\mathfrak{m}$.

Let $K(1, N)$ be the open subgroup of $\hat{R}^*$ which stabilizes the pair (ω_0, x_0). We have a decomposition

$$K(1, N) = R_p^*(1) \times \prod_{\ell\neq p} K_\ell(N),$$

for a certain collection $K_\ell(N)$ of open subgroups of R_ℓ^*, with $\ell \neq p$. The subgroup R_p^* of $\hat{R}^*$ normalizes $K(1, N)$ and left translation induces an action of $R_p^*/R_p^*(1) = k^*$ on the coset space $K(1, N)\backslash\hat{D}^*/D^*$.

Remark 1.10. There is a $\mathbf{Z}_\ell$–basis (e_1, e_2) of $T_\ell(E)$, for $\ell \neq p$, such that the corresponding identification $R_\ell^* \simeq \mathrm{GL}_2(\mathbf{Z}_\ell)$ sends $K_\ell(N)$ to the subgroup

$$U_\ell(N) = \left\{ x \in \mathrm{GL}_2(\mathbf{Z}_\ell) | x \equiv \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \bmod \ \mathrm{N} \right\}.$$

If ℓ^e is the exact power of ℓ dividing N, the basis above should be chosen in such a way that the element of $T_\ell(E)/(N) = E[\ell^e](\bar{k})$ defined by e_1 (mod N) is equal to the ℓ–primary component of x_0.

Theorem 1.11. *There is a natural bijection*

$$\tau_N : \Sigma(1, N) \xrightarrow{\sim} K(1, N) \backslash \hat{D}^* / D^*.$$

The permutation action of k^* on $\Sigma(1, N)$ corresponds via τ_N to the action induced by left translation of R_p^* on $K(1, N) \backslash \hat{D}^* / D^*$.

Proof. Let $a \in K(1, N) \backslash \hat{R} \cap \hat{D}^*$ be any element, we begin by showing how to construct a triple (ψ_a, ω_a, x_a) of the type considered out of a. Let I_a be the left ideal of R defined by the adelic coset $\bar{a} \in \hat{R}^* \backslash \hat{R} \cap \hat{D}^*$ deduced from a. The isogeny $\psi_a : E \to E_{\psi_a}$ is that obtained from the I_a using the construction (5) from section 1.2.

Let $g = (g_\ell)_\ell \in \hat{R} \cap \hat{D}^*$ be any element representing a, i.e., such that $a = K(1, N)g$. Recall that for $\ell \neq p$ the module $T_\ell(E_{\psi_a})$ is identified with a $\mathbf{Z}_\ell$–lattice $\Lambda_{\psi_{a,\ell}}$ of $V_\ell(E)$ containing $T_\ell(E)$, moreover $g_\ell \in D_\ell^*$ is a generator of the principal, R_ℓ–left ideal $\mathrm{Hom}_{\mathbf{Z}_\ell}(\Lambda_{\psi_{a,\ell}}, T_\ell(E))$, and defines an isomorphism of $V_\ell(E)$ that maps $\Lambda_{\psi_{a,\ell}}$ isomorphically to $T_\ell(E)$. Therefore we deduce, for any $n \geq 0$, an identification

$$E_\psi[\ell^n](\bar{k}) = \Lambda_{\psi_{a,\ell}}/(\ell^n) \simeq T_\ell(E)/(\ell^n) = E[\ell^n](\bar{k}) \tag{7}$$

depending on the choice of the generator g_ℓ of $I_{\psi,\ell}$.

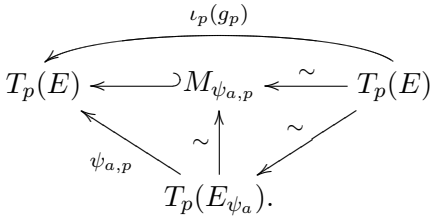
If now ℓ^e is the exact power of ℓ dividing N, then the ℓ–th primary component $x_{0,\ell}$ of x_0 is a point of order ℓ^e in $T_\ell(E)/(\ell^e)$. The inverse image $x_{a,\ell} \in \Lambda_{\psi_{a,\ell}}/(\ell^e)$ of $x_{0,\ell}$ by the identification (7) for $n = e$ is a point $E_{\psi_a}[\ell^e](\bar{k})$ of order ℓ^e that depends only on the coset $K_\ell(N)g_\ell$, as one can easily check. The point $x_a \in E_{\psi_a}[N](\bar{k})$ is the one whose ℓ–th primary component is $x_{a,\ell}$, and depends only on a, and not on g.

To construct the invariant k–form ω_a, we use the fact that for any object X of $\mathcal{C}_{-p}$ there is a canonical identification of k–vector spaces (cf. [3], II, Prop. 4.3)

$$T_p(X)/FT_p(X) = \mathbf{t}_0(X)^*. \tag{8}$$

Recall that the Dieudonné module $T_p(E_{\psi_a})$ is identified, via $\psi_{a,p}$, to a $\mathcal{A}$–submodule $M_{\psi_{a,p}}$ of $T_p(E)$, moreover the component $g_p \in D_p^*$ at p of g defines a generator $\iota_p(g_p)$ of $\mathrm{Hom}_{\mathcal{A}}(T_p(E), M_{\psi_{a,p}})$ as a right ideal of $\mathrm{End}_{\mathcal{A}}(T_p(E))$.

We have a commutative diagram of morphisms of $\mathcal{A}$–modules



The diagonal isomorphism to the right of the diagram is induced by the composition of $\iota_p(g_p)$ corestricted to $M_{\psi_{a,p}}$, followed by the inverse of the corestriction of $\psi_{p,a}$ to the same lattice of $V_p(E)$. Notice that it is not independent on the choice of g_p. From this isomorphism, using (8), we can deduce an isomorphism of k–vector spaces

$$\xi_a : \mathbf{t}_0(E)^* \xrightarrow{\sim} \mathbf{t}_0(E_{\psi_a})^*$$

that depend only on the coset $R_p^*(1)g_p$, and not on the choice of g_p, as one can easily check. Setting ω_a to be equal to $\xi_a(\omega_0)$ completes the construction of the triple (ψ_a, ω_a, x_a) attached to $a = K(1,N)g \in K(1,N)\backslash\hat{R} \cap \hat{D}^*$.

We are left with showing that, for a, $b \in K(1,N)\backslash\hat{R} \cap \hat{D}^*$, the triples (ψ_a, ω_a, x_a) and (ψ_b, ω_b, x_b) are isomorphic if and only if $a = b\lambda$, for some $\lambda \in D^*$. One way to proceed is to observe that in order for the two triples to be isomorphic certainly we must have that there exists an isomorphism $u : E_{\psi_a} \to E_{\psi_b}$, equivalently, by Proposition 1.9, if $\bar{a}$, $\bar{b}$ denote the elements of $\hat{R}^*\backslash\hat{R}\cap\hat{D}^*$ deduced from, respectively, a and b, then there must be $\lambda \in D^*$ such that $\bar{a} = \bar{b}\lambda$. We leave to the reader the task of showing, with the help of section 1.2, that the isomorphism u induces an isomorphism between (ψ_a, ω_a, x_a) and (ψ_b, ω_b, x_b) if and only if $a = b\lambda$. □

Remark 1.12. If d is an integer ≥ 1, the natural map $K(1,Nd)\backslash\hat{D}^*/D^* \to K(1,N)\backslash\hat{D}^*/D^*$ corresponds, under the identifications τ_{Nd} and τ_N to the map sending a given triple $(\psi, \omega, x) \in \Sigma(1,Nd)$ to $(\psi, \omega, dx) \in \Sigma(1,N)$.

References

[1] Baker, Gonzlez–Jimnez, Gonzlez, Poonen, *Finiteness theorems for modular curves of genus at least 2*, Amer. J. Math. 127 (2005), 1325–1387.

[2] M. Demazure, *Lectures on p–divisible groups*, Lecture Notes in Mathematics, Vol. 302. Springer–Verlag, Berlin–New York, 1972.

[3] J.–M. Fontaine, *Groupes p–divisibles sur les corps locaux*, Astérisque 47-48, Société Mathématique de France, (1977).

[4] A. Ghitza, *Hecke eigenvalues of Siegel modular forms (mod p) and of algebraic modular forms*, Journal of Number Theory 106, no. 2 (2004), 345–384.

[5] A. Ghitza, *Siegel modular forms (mod p) and algebraic modular forms*, PhD thesis.

[6] B. H. Gross, *Heights and special values of L-series*, CMS Proceedings, Vol. 7, AMS (1986), 115–187.

[7] J.–P. Serre, *Two letters on Quaternions and Modular Forms (mod p)*. With introduction, appendix and references by R. Livné. Israel J. Math. **95**, 281–299 (1996).

[8] J. Tate, *Classes d'isogénie des variétés abéliennes sur un corps fini*, Sém. Bourbaki 21e année, 1968/69, no 352.

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

[10] M.–F. Vignéras, *Artihmétiques des algèbres de quaternions*, Lecture Notes in Mathematics, Vol. 800. Springer–Verlag, Berlin–New York, 1980.

[11] W.C. Waterhouse, *Abelian varieties over finite fields*, Ann. scient. Éc. Norm. Sup., 4^e série, t. 2, 1969, 521–560.

[12] W.C. Waterhouse, J.S. Milne, *Abelian varieties over finite fields*, 1969 Number Theory Institute (Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, N.Y., 1969), pp. 53–64. Amer. Math. Soc., Providence, R.I., 1971.