A CLASS OF p-ADIC GALOIS REPRESENTATIONS ARISING FROM ABELIAN VARIETIES OVER $\mathbb{Q}_p$

MAJA VOLKOV

ABSTRACT. Let V be a p-adic representation of the absolute Galois group G of $\mathbb{Q}_p$ that becomes crystalline over a finite tame extension, and assume $p \neq 2$. We provide necessary and sufficient conditions for V to be isomorphic to the p-adic Tate module $V_p(\mathcal{A})$ of an abelian variety $\mathcal{A}$ defined over $\mathbb{Q}_p$. These conditions are stated on the filtered (φ, G)-module attached to V.

2000 *Mathematics Subject Classification*: Primary 14F30, 11G10; Secondary 11F80, 14G20, 14F20.

CONTENTS

Introduction

Fix a prime number p and an algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$. Let $\mathcal{A}$ be an abelian variety over $\mathbb{Q}_p$ of dimension d. Let $\mathcal{A}[p^n]$ be the group of p^n-torsion points with values in $\overline{\mathbb{Q}}_p$ and $T_p(\mathcal{A}) = \varprojlim \mathcal{A}[p^n]$ the p-adic Tate module of $\mathcal{A}$: it is a free $\mathbb{Z}_p$-module of rank $2d$ on which the Galois group $G = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ acts linearly and continuously. The p-adic representation of G attached to $\mathcal{A}$ (also called Tate module) is

$$V_p(\mathcal{A}) = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} T_p(\mathcal{A}).$$

A p-adic representation V of G arises from an abelian variety over $\mathbb{Q}_p$ if there exists an $\mathcal{A}/\mathbb{Q}_p$ such that $V \simeq V_p(\mathcal{A})$ as G-modules. Such representations are classical objects known to enjoy motivic properties. We want to consider an inverse problem, namely, to detect which p-adic representations V of G arise from abelian varieties. In this paper we solve this problem for the class of representations that become crystalline over a tame extension of $\mathbb{Q}_p$, and under the assumption $p \neq 2$. The solution is provided in terms of necessary and sufficient conditions on the filtered (φ, G)-module attached to V.

Being crystalline is the p-adic analogue of good reduction for ℓ-adic representations of G with $\ell \neq p$. Fontaine's theory shows that a potentially crystalline p-adic representation of G is determined by its associated filtered (φ, G)-module. The latter is a finite-dimensional vector space over an unramified extension of $\mathbb{Q}_p$ equipped with a semilinear Frobenius map φ, a semilinear action of a finite quotient of G commuting with φ, and a G-stable filtration. This association is functorial. We point out that we are using the contravariant version of Fontaine's functor. Also, a (φ, G)-module (unfiltered) may be replaced by its linearisation, which is a representation of the Weil group of $\mathbb{Q}_p$ over the same base field.

The Tate module $V_p(\mathcal{A})$ is potentially crystalline if and only if $\mathcal{A}$ has potential good reduction. Hence the above theory applies and the varieties involved have potential good reduction. As $V_p(\mathcal{A})$ is dual to $H^1_{\text{ét}}(\mathcal{A}_{\overline{\mathbb{Q}}_p}, \mathbb{Q}_p)$ our functor is covariant on the $H^1_{\text{ét}}$'s. Let $\mathcal{A}$ have good reduction over the finite Galois extension $K/\mathbb{Q}_p$ with maximal unramified subfield K_0. Let (D, Fil) be the filtered $\big(\varphi, \mathrm{Gal}(K/\mathbb{Q}_p)\big)$-module attached to $V_p(\mathcal{A})$ and Δ the Weil representation attached to D; both D and Δ are K_0-vector spaces. It is known that (D, Fil) enjoys the following "geometric" properties:

- (G1) A lifting of the geometric Frobenius acts semisimply on Δ with characteristic polynomial a p-Weil polynomial (see definition 2.1)
- (G2) Δ is defined over $\mathbb{Q}$
- (G3) There exists a nondegenerate skew form $(D, \mathrm{Fil}) \times (D, \mathrm{Fil}) \to K_0\{-1\}$
- (G4) (D, Fil) has Hodge-Tate type $(0, 1)$.

Property (G1) follows from the Weil conjectures for abelian varieties over $\mathbb{F}_p$. Property (G2) means that the traces of the action are in $\mathbb{Q}$ and is a consequence of the results of Serre and Tate on potential good reduction. They show more precisely that the descent datum furnished by the action of $\mathrm{Gal}(K/\mathbb{Q}_p)$ is geometric, that is, the inertia acts through automorphisms of $\mathcal{A}_K$'s special fibre. Property (G3) means there is a G-equivariant symplectic form $V_p(\mathcal{A}) \times V_p(\mathcal{A}) \to \mathbb{Q}_p(1)$, and indeed any polarisation on $\mathcal{A}$ induces such a form. Finally (G4) means that the filtration jumps in degrees 0 and 1, which follows from the Hodge decomposition of Tate modules of p-divisible groups and (G3).

Now let V be tamely potentially crystalline. Our result is that these four conditions are sufficient to garantee that a multiple of V comes from an abelian variety. Also, one can determine how many copies are needed to obtain a representation itself isomorphic to a $V_p(\mathcal{A})$.

Theorem. (see theorem 5.13) *Let $p \neq 2$. Let V be a p-adic representation of G that becomes crystalline over a finite tame extension. The following are equivalent:*

(i) *There exists an integer n and an abelian variety $\mathcal{A}/\mathbb{Q}_p$ such that $nV \simeq V_p(\mathcal{A})$*
(ii) *The filtered (φ, G)-module attached to V satisfies* (G1), (G2), (G3), *and* (G4).

Moreover there is a smallest integer n_V as in (i) *that can be computed explicitely.*

Given a V satisfying the conditions of the theorem we want to construct an abelian variety $\mathcal{A}/\mathbb{Q}_p$ and an integer n such that $nV \simeq V_p(\mathcal{A})$. Let V be crystalline over the tame Galois extension $K/\mathbb{Q}_p$ with residue field k. We first construct the relevant objects over finite fields. By the Honda-Tate theory we produce from (G1) an abelian variety $A_0/\mathbb{F}_p$ having the right Frobenius. Using Tate's theorems we produce essentially from (G2) a minimal n and an automorphism of $A^n = (A_0 \times_{\mathbb{F}_p} k)^n$ furnishing a geometric descent datum. Replace V by nV and A_0 by ${A_0}^n$. We then construct the relevant objects in characteristic zero. By a result of Breuil, which is why we assume p odd, (G4) furnishes a p-divisible group over the ring of integers O_K of K lifting $A(p)$. According to the Serre-Tate theory of liftings this produces a formal abelian scheme over O_K. Then (G3) enables us to lift some polarisation on A, which insures by Grothendieck's criterion that we obtain an algebraic scheme, hence an abelian variety over K with good reduction. Finally a Galois descent criterion, applicable thanks to the geometric nature of the descent, shows that this abelian variety is defined over $\mathbb{Q}_p$ and has the right Tate module.

The paper is organised as follows. Section 1 contains assorted facts on potential good reduction. We review the needed representation theory in 1.1 and potential good reduction of abelian varieties in 1.2. Section 2 deals with the Honda-Tate theory. It is reviewed in 2.1 and in 2.2 we prove a technical result on endomorphism algebras (proposition 2.5). In section 3 we introduce the appropriate objects yielding representations with geometric descent: they consist of an abelian variety over $\mathbb{F}_p$ together with a finite subgroup of $\overline{\mathbb{F}}_p$-automorphisms, subject to a condition of Galois nature. These objects, that we call Galois pairs, are defined in 3.1 (definition 3.1), their associated representations are constructed in 3.2, and a decomposition result (proposition 3.9) is proved in 3.3. In section 4 we describe such representations in the tame case. Some arithmetic properties of semisimple representations defined over $\mathbb{Q}$ are proved in 4.1. They enable the construction in 4.2 of a numerical invariant, namely the aforementioned integer n (definition 4.6). The determination of tame representations arising from Galois pairs is carried out in 4.3 (theorem 4.11), followed by some examples in 4.4. Section 5 deals with the lifting procedure. We review in 5.1 the needed facts on polarisations and Rosati involutions, and prove in 5.2 the existence of suitable polarisations on tame Galois pairs (proposition 5.3). In 5.3 we show that such polarisations may be lifted when the representation associated to a Galois pair lifts to a symplectic G-module (proposition 5.5). We then wrap everything up to prove the main theorem in 5.4 (theorem 5.13).

Acknowledgements. It is a pleasure to thank O. Bültel, E. Frossard, M. Kisin, N. Naumann, J. Nekovář, and A.J. Scholl for helpful conversations.

1. Potential good reduction

This section introduces notions related to potential good reduction. It reviews the relevant representation theory in 1.1 and Galois descent on abelian varieties in 1.2.

1.1. **Representations.** Let I be the inertia subgroup of $G = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. We have a short exact sequence

$$1 \longrightarrow I \longrightarrow G \xrightarrow{\upsilon} \hat{\mathbb{Z}} \longrightarrow 1$$

where υ sends a lifting of the arithmetic Frobenius to 1. The Weil group $W = \mathrm{Weil}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ is defined as $W = \upsilon^{-1}(\mathbb{Z})$. For algebraic extensions K of $\mathbb{Q}_p$ (assumed to be contained in $\overline{\mathbb{Q}}_p$) write $G_K = \mathrm{Gal}(\overline{\mathbb{Q}}_p/K)$, $I_K = I(\overline{\mathbb{Q}}_p/K)$, and $W_K = W \cap G_K = \mathrm{Weil}(\overline{\mathbb{Q}}_p/K)$. Let $\mathbb{Q}_p^{\mathrm{un}}$ be the maximal unramified extension of $\mathbb{Q}_p$ with residue field $\overline{\mathbb{F}}_p$, $W(k)$ the ring of Witt vectors with coefficients in $k \subseteq \overline{\mathbb{F}}_p$, and σ the absolute Frobenius acting on k, $W(k)$, and $\mathrm{Frac}\, W(k)$. We also fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ and an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$.

1.1.1. *Filtered (φ, G)-modules.* Let $K/\mathbb{Q}_p$ be a finite Galois extension and K_0 the maximal unramified subfield. A filtered $\big(\varphi, \mathrm{Gal}(K/\mathbb{Q}_p)\big)$-module (D, Fil) is a finite dimensional K_0-vector space D equipped with

- a σ-semilinear bijective Frobenius map $\varphi : D \xrightarrow{\sim} D$
- a σ-semilinear action of $\mathrm{Gal}(K/\mathbb{Q}_p)$ commuting with φ
- a decreasing filtration $\mathrm{Fil} = (\mathrm{Fil}^i D_K)_{i\in\mathbb{Z}}$ on $D_K = K \otimes_{K_0} D$ by $\mathrm{Gal}(K/\mathbb{Q}_p)$-stable subspaces such that $\mathrm{Fil}^i D_K = D_K$ for $i \ll 0$ and $\mathrm{Fil}^i D_K = 0$ for $i \gg 0$.

Such objects form a category ([Fo2]), the morphisms being K_0-linear maps commuting with the action of φ and $\mathrm{Gal}(K/\mathbb{Q}_p)$, and preserving the filtration after scalar extension to K. The dual of (D, Fil) is the K_0-linear dual D^* with $\varphi^* f = \sigma f \varphi^{-1}$ and $g^* f = g f g^{-1}$ for $f \in D^*$, $g \in \mathrm{Gal}(K/\mathbb{Q}_p)$, and $\mathrm{Fil}^i D_K^*$ consists of linear forms on D_K vanishing on $\mathrm{Fil}^j D_K$ for all $j > -i$. The Tate twist $D\{-1\}$ of (D, Fil) is D as a K_0-vector space with the same action of $\mathrm{Gal}(K/\mathbb{Q}_p)$ and $\varphi\{-1\} = p\varphi$, $\mathrm{Fil}^i(D\{-1\})_K = \mathrm{Fil}^{i-1} D_K$. The object (D, Fil) has Hodge-Tate type $(0, 1)$ if $\mathrm{Fil}^i D_K = D_K$ for $i \leq 0$, $\mathrm{Fil}^i D_K = 0$ for $i \geq 2$, and Fil^1 is a nontrivial subspace.

Now let V be a p-adic representation of G. Put

$$\mathbf{D}^*_{\mathrm{cris},K}(V) \underset{\mathrm{def}}{=} \mathrm{Hom}_{\mathbb{Q}_p[G_K]}(V, B_{\mathrm{cris}}).$$

Then $\mathbf{D}^*_{\mathrm{cris},K}(V) = (D, \mathrm{Fil})$ is a filtered $\big(\varphi, \mathrm{Gal}(K/\mathbb{Q}_p)\big)$-module ([Fo1], [Fo2]). We always have $\dim_{K_0} D \leq \dim_{\mathbb{Q}_p} V$ and V is said to be crystalline over K when equality holds. The contravariant functor $V \mapsto \mathbf{D}^*_{\mathrm{cris},K}(V)$ establishes an anti-equivalence between the category of p-adic representations of G crystalline over K and its essential image ([Fo2]). We have $\mathbf{D}^*_{\mathrm{cris},K}\big(V(1)\big) = \mathbf{D}^*_{\mathrm{cris},K}(V)\{-1\}$ where $V(1) = \mathbb{Q}_p(1) \otimes_{\mathbb{Q}_p} V$ is the usual Tate twist.

A representation is potentially crystalline if it is crystalline over some finite extension. Being crystalline depends only on the action of inertia ([Fo2] 5.1.5). Let $K \subseteq F$ be two finite Galois extensions of $\mathbb{Q}_p$ such that F/K is unramified, with respective maximal unramified subfields $K_0 \subseteq F_0$. Then V is crystalline over K if and only if it is crystalline over F. Let (D, Fil) be a filtered $\big(\varphi, \mathrm{Gal}(F/\mathbb{Q}_p)\big)$-module. Then $(D, \mathrm{Fil}) = (F_0 \otimes_{K_0} D_0, F \otimes_K \mathrm{Fil}_0)$

where (D_0, Fil_0) is the filtered $\big(\varphi, \mathrm{Gal}(K/\mathbb{Q}_p)\big)$-module obtained from (D, Fil) by taking $\mathrm{Gal}(F/K)$-invariants.

Let $\mathcal{A}_0$ be an abelian variety over $\mathbb{Q}_p$ having potential good reduction. Then $V_p(\mathcal{A}_0)$ is potentially crystalline, and it is crystalline over K if and only if $\mathcal{A}_0$ has good reduction over K ([Co-Io] Thm.4.7, see also [Br] Cor.5.3.4.). Then $\mathbf{D}^*_{\mathrm{cris},K}\big(V_p(\mathcal{A}_0)\big) = (D, \mathrm{Fil})$ has Hodge-Tate type $(0,1)$ and $\dim_K \mathrm{Fil}^1 D_K = \dim \mathcal{A}_0$.

1.1.2. *Dieudonné modules.* Let (D, Fil) be a filtered $\big(\varphi, \mathrm{Gal}(K/\mathbb{Q}_p)\big)$-module. Forgetting the filtration leads to the obvious notion of a $\big(\varphi, \mathrm{Gal}(K/\mathbb{Q}_p)\big)$-module D, and forgetting in addition the action of $\mathrm{Gal}(K/\mathbb{Q}_p)$ to a φ-module. Let k be the residue field of K. The contravariant Dieudonné functor $\Gamma \mapsto \mathbf{D}(\Gamma)$ establishes an anti-equivalence between the category of p-divisible groups over k up to isogeny and its essential image in the category of φ-modules (see e.g. [Fo4]).

Let $\mathcal{A}_0 \times_{\mathbb{Q}_p} K$ have good reduction, let A be the special fibre of the Néron model and $A(p)$ its associated p-divisible group over k. Put

$$D(A) \underset{\text{def}}{=} \mathbf{D}\big(A(p)\big).$$

If $\mathbf{D}^*_{\mathrm{cris},K}\big(V_p(\mathcal{A}_0)\big) = (D, \mathrm{Fil})$ there is a canonical isomorphism of φ-modules $D(A) \simeq D$ allowing us to identify these two objects ([Fo5] Thm.6.2). The Frobenius φ on $D(A)$ is induced by the Frobenius endomorphism of A. The filtration Fil is a lifting datum, that is, it carries the information that $A(p)$ is the special fibre of a p-divisible group over the ring of integers of K, namely the one of the Néron model. The action of $\mathrm{Gal}(K/\mathbb{Q}_p)$ is a descent datum reflecting the fact that we actually started with an object defined over $\mathbb{Q}_p$.

1.1.3. *Weil representations.* A $\big(\varphi, \mathrm{Gal}(K/\mathbb{Q}_p)\big)$-module is a semilinear object (unless $K_0 = \mathbb{Q}_p$) and it is convenient to have a linear one at hand naturally attached to it. The Weil group sits in the short exact sequence

$$1 \longrightarrow I \longrightarrow W \xrightarrow{\upsilon} \mathbb{Z} \longrightarrow 1.$$

A Weil representation over a characteristic zero field F is a finite dimensional F-linear representation of W that is trivial on an open subgroup of I. From a $\big(\varphi, \mathrm{Gal}(K/\mathbb{Q}_p)\big)$-module D we get a Weil representation $\mathbf{W}(D) = (\Delta, \rho)$ over K_0 as follows ([Fo3]): the K_0-vector space Δ is D, and the action is given by

$$\rho(w) = (w \bmod W_K)\varphi^{-\upsilon(w)} \in \mathrm{Aut}_{K_0}(\Delta), \quad w \in W.$$

We have $I_K \subseteq \mathrm{Ker}\,\rho$, that is, (Δ, ρ) has good reduction over K. It is tame if $I_p \subset \mathrm{Ker}\,\rho$ with I_p the maximal pro-p-group contained in I. The association $D \mapsto \mathbf{W}(D)$ is functorial (covariant), and we have a canonical isomorphism

$$K_0 \otimes_{\mathbb{Q}_p} \mathrm{Hom}_{\varphi,\mathrm{Gal}(K/\mathbb{Q}_p)}(D_1, D_2) \simeq \mathrm{Hom}_W\big(\mathbf{W}(D_1), \mathbf{W}(D_2)\big)$$

so that isomorphism classes are in bijection. We may always assume that K is a Galois extension of minimal degree over which Δ has good reduction ([Fo3] 1.3.7).

A semisimple Weil representation (Δ, ρ) is defined over $\mathbb{Q}$ if $\mathrm{Tr}\big(\rho(w)\big) \in \mathbb{Q}$ for all $w \in W$. For each prime $\ell \neq p$ let Δ_ℓ be a $\mathbb{Q}_\ell$-linear semisimple Weil representation defined over $\mathbb{Q}$ and let Δ_p be a K_0-linear one. The system $(\Delta_\ell)_\ell$ is compatible if the trace maps are

independent of ℓ. It is known that abelian varieties with potential good reduction give rise to such systems.

1.2. **Abelian varieties.**

1.2.1. *The action of inertia.* Let $\mathcal{A}_0$ be an abelian variety over $\mathbb{Q}_p$ having potential good reduction. Recall ([Se-Ta], [Gr2]) that there is a smallest extension M of $\mathbb{Q}_p^{\mathrm{un}}$ over which $\mathcal{A}_0$ acquires good reduction. It is Galois over $\mathbb{Q}_p$, given by

$$G_M = I_M = I \cap \mathrm{Ker}(\rho_\ell)$$

where ℓ is any prime different from p and $\rho_\ell : G \to \mathrm{Aut}_{\mathbb{Q}_\ell}\big(V_\ell(\mathcal{A}_0)\big)$ the ℓ-adic representation. Since $M/\mathbb{Q}_p$ is Galois it can be descended to a finite totally ramified extension L of $\mathbb{Q}_p$, that is, $L\mathbb{Q}_p^{\mathrm{un}} = M$. Let K be the Galois closure of L and k the residue field of K. Then K/L is unramified, $K\mathbb{Q}_p^{\mathrm{un}} = M$, and $\mathrm{Gal}(K/\mathbb{Q}_p) = I(K/\mathbb{Q}_p) \rtimes \mathrm{Gal}(K/L)$ (semidirect product) with $\mathrm{Gal}(K/L) \simeq \mathrm{Gal}(k/\mathbb{F}_p)$. Furthermore $\mathcal{A}_0$ has good reduction over L and K is a Galois extension of minimal degree over which $\mathcal{A}_0$ acquires good reduction.

The group $\mathrm{Gal}(K/\mathbb{Q}_p)$ acts on $\mathcal{A} = \mathcal{A}_0 \times_{\mathbb{Q}_p} K$ via its action on K. This extends functorially to an action on the Néron model of $\mathcal{A}$, and on its special fibre A/k. The inertia subgroup acting trivially on k it acts on A by k-automorphisms, i.e. by an antimorphism

$$\nu : I(K/\mathbb{Q}_p) \to \mathrm{Aut}_k(A).$$

This map is injective because of the minimality of K. Indeed, $V_p(\mathcal{A}_0)$ is crystalline over $K^{\mathrm{Ker}(\nu)}$ so $\mathcal{A}_0$ has good reduction over this field. Hence ν identifies $I(K/\mathbb{Q}_p)$ with a finite subgroup of $\mathrm{Aut}_k(A)$.

Of course this is nothing else than the classical Weil criterion ([We]). For each $g \in \mathrm{Gal}(K/\mathbb{Q}_p)$ let $\mathcal{A}^g$ be the twisted abelian variety over K, with the usual relation $\mathcal{A}^{gh} = (\mathcal{A}^h)^g$. Since $\mathcal{A}$ is defined over $\mathbb{Q}_p$ there exists a system of K-isomorphisms

$$f_g : \mathcal{A} \xrightarrow{\sim} \mathcal{A}^g, \quad g \in \mathrm{Gal}(K/\mathbb{Q}_p)$$

satisfying the cocycle condition $f_{gh} = (f_h)^g \circ f_g$ for all $g, h \in \mathrm{Gal}(K/\mathbb{Q}_p)$. Now if $g \in I(K/\mathbb{Q}_p)$ the special fibre of $\mathcal{A}^g$ is A, so by restriction to the inertia subgroup and passing to special fibres we recover $\nu : I(K/\mathbb{Q}_p) \hookrightarrow \mathrm{Aut}_k(A)$.

Remark 1.1. Since $\mathcal{A}_0$ acquires good reduction over the totally ramified extension L we have $A = A_0 \times_{\mathbb{F}_p} k$, where $A_0/\mathbb{F}_p$ is the special fibre of the Néron model of $\mathcal{A}_0 \times_{\mathbb{Q}_p} L$.

Thus $\mathbf{D}^*_{\mathrm{cris},K}\big(V_p(\mathcal{A}_0)\big) = (D, \mathrm{Fil})$ is a $\big(\varphi, \mathrm{Gal}(K/\mathbb{Q}_p)\big)$-filtered module with an action of $I(K/\mathbb{Q}_p)$ coming from the composite morphism

$$I(K/\mathbb{Q}_p) \underset{\nu}{\hookrightarrow} \mathrm{Aut}_k(A) \underset{\mathrm{can}}{\hookrightarrow} \mathrm{Aut}_\varphi(D).$$

1.2.2. *Galois descent.* The following result is a converse to the situation explained in section 1.2.1. Let F be a finite extension of $\mathbb{Q}_p$.

Theorem 1.2 ([Vo] Thm.4.5)**.** *Let K/F be a totally ramified finite Galois extension with residue field k. Let $\mathcal{A}/K$ be an abelian variety having good reduction with special fibre A/k. Then $\mathcal{A}$ can be defined over F if and only if the action of G_K on $T_p(\mathcal{A})$ extends to an action of G_F such that the induced morphism $\mathrm{Gal}(K/F) = I(K/F) \to \mathrm{Aut}_\varphi\big(D(A)\big)$ factors through an an antimorphism $I(K/F) \to \mathrm{Aut}_k(A)$.*

Specifically, there is an abelian variety $\mathcal{A}_0/F$ and a K-isomorphism $\psi : \mathcal{A}_0 \times_F K \xrightarrow{\sim} \mathcal{A}$ inducing a G_F-equivariant isomorphism $T_p(\psi) : T_p(\mathcal{A}_0) \xrightarrow{\sim} T_p(\mathcal{A})$, with G_F acting naturally on $T_p(\mathcal{A}_0)$ and by the given extended action on $T_p(\mathcal{A})$. The pair $(\mathcal{A}_0, \psi)$ is unique up to F-isomorphism. Also, the smallest extension of F contained in K over which $\mathcal{A}_0$ acquires good reduction is the field fixed by $\operatorname{Ker}\nu$.

The proof of theorem 1.2 is written in [Vo] for elliptic curves but it clearly applies to abelian varieties without change. If we replace $T_p(\mathcal{A})$ by $V_p(\mathcal{A})$ the conclusion is that $\mathcal{A}$ is K-isogenous to an abelian variety defined over F.

Consider now the following situation. Let $F \subseteq L \subseteq K$ be finite extensions with K/F Galois, L/F totally ramified, and K/L unramified, so $\operatorname{Gal}(K/F) = I(K/F) \rtimes \operatorname{Gal}(K/L)$. Let K_0 be the maximal unramified subfield of K/F. Suppose we are given an abelian variety $\mathcal{A}$ over L having good reduction, and let A be the special fibre of the Néron model of $\mathcal{A} \times_L K$. It then follows from theorem 1.2 together with [Vo] Lemma 4.6 that $\mathcal{A}$ can be defined over F if and only if the action of G_K on $T_p(\mathcal{A})$ extends to an action of G_F such that:

(a) the action of G_L coincides with the natural action on $T_p(\mathcal{A})$, and
(b) the action of G_{K_0} induces an action of $I(K/F) = \operatorname{Gal}(K/K_0)$ on $D(A)$ that comes from k-automorphisms of A.

1.2.3. *Duality and polarisations.* We keep the hypotheses and notations of section 1.2.1. Let $\mathcal{A}_0^\vee$ be the dual abelian variety of $\mathcal{A}_0$. It also acquires good reduction over K (and L), being $\mathbb{Q}_p$-isogenous to $\mathcal{A}_0$, thus yielding an injective antimorphism

$$\nu' : I(K/\mathbb{Q}_p) \hookrightarrow \operatorname{Aut}_k(A^\vee).$$

Consider the system of K-isomorphisms furnished by the Weil criterion for $\mathcal{A}_0^\vee$

$$\hat{f}_g : \mathcal{A}^\vee \xrightarrow{\sim} (\mathcal{A}^\vee)^g = (\mathcal{A}^g)^\vee, \quad g \in \operatorname{Gal}(K/\mathbb{Q}_p).$$

On the other hand, by dualising the system f_g we had for $\mathcal{A}_0$ and taking inverses, we obtain a set of K-isomorphisms for $\mathcal{A}_0^\vee$ that satisfies the cocycle condition. By unicity the two systems must match, that is, $\hat{f}_g = \big((f_g)^\vee\big)^{-1}$ for all $g \in \operatorname{Gal}(K/\mathbb{Q}_p)$. Hence

$$\nu'(g) = (\nu(g)^\vee)^{-1} \quad \text{for all } g \in I(K/\mathbb{Q}_p).$$

Now take any $\mathbb{Q}_p$-polarisation $\Lambda_0 : \mathcal{A}_0 \to \mathcal{A}_0^\vee$. Put $\Lambda = \Lambda_0 \times_{\mathbb{Q}_p} K : \mathcal{A} \to \mathcal{A}^\vee$, and let $\lambda : A \to A^\vee$ be obtained from Λ by taking special fibres of Néron models.

Lemma 1.3. *We have $\nu\big(I(K/\mathbb{Q}_p)\big) \subseteq \operatorname{Aut}_k(A, \lambda)$ for any polarisation λ on A deduced from one on $\mathcal{A}_0$.*

Proof. Since Λ comes from the $\mathbb{Q}_p$-polarisation Λ_0, it is compatible with the descent systems of $\mathcal{A}_0$ and $\mathcal{A}_0^\vee$, that is, $\Lambda^g f_g = \hat{f}_g \Lambda$ for all $g \in \operatorname{Gal}(K/\mathbb{Q}_p)$. Knowing that $\hat{f}_g = \big((f_g)^\vee\big)^{-1}$ we obtain $(f_g)^\vee \Lambda^g f_g = \Lambda$ for all g, which in turn gives, by restriction to the inertia subgroup and taking special fibres, $\nu(g)^\vee \lambda\, \nu(g) = \lambda$ for all $g \in I(K/\mathbb{Q}_p)$. $\square$

2. Abelian varieties over finite fields

We have seen in section 1.2.1 how potential good reduction of abelian varieties involves automorphisms of their special fibre. This raises the question of describing abelian varieties over finite fields together with a finite group of automorphisms. This task is made possible, at least up to isogeny, by the Honda-Tate theory which is reviewed in section 2.1. In section 2.2 we investigate under what condition a simple endomorphism algebra contains a subalgebra that naturally arises in a situation of tame potential good reduction (as in section 3.3). We state this condition in terms of an arithmetic invariant in proposition 2.5.

2.1. **The Honda-Tate theory.** Let A be an abelian variety over $k = \mathbb{F}_q$ with $q = p^s$ and let Frob_A be its Frobenius endomorphism. The $\mathbb{Q}$-algebra $\mathrm{End}_k^\circ(A) = \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}_k(A)$ is finite dimensional semisimple ([Mi] §12) with centre $\mathbb{Q}(\mathrm{Frob}_A)$ ([Ta1] Thm.2), call it the Honda-Tate algebra of A/k. The action of Frob_A on $V_\ell(A)$ for $\ell \neq p$, or via φ^s on $D(A)$ for $\ell = p$, is semisimple with characteristic polynomial $P_A \in \mathbb{Z}[X]$ independent of ℓ and monic of degree $2 \dim A$ ([Mi] Prop.12.9). The splitting of A up to k-isogeny into powers of pairwise nonisogenous simple varieties corresponds to the Wedderburn decomposition of its Honda-Tate algebra, which itself is given by the factorisation of P_A into $\mathbb{Q}$-irreducibles. If $A \sim B^n$ (k-isogenous) then $\mathrm{End}_k^\circ(A) \simeq M_n\big(\mathrm{End}_k^\circ(B)\big)$ and if B is simple then $\mathrm{End}_k^\circ(B)$ is a skewfield. Tate's theorems assert that we have canonical isomorphisms

$$\mathbb{Q}_\ell \otimes_{\mathbb{Z}} \mathrm{Hom}_k(A,B) \simeq \mathrm{Hom}_{\mathrm{Gal}(\overline{\mathbb{F}}_p/k)}\big(V_\ell(A), V_\ell(B)\big)$$

for each $\ell \neq p$ ([Ta1]) and also

$$\mathbb{Q}_p \otimes_{\mathbb{Z}} \mathrm{Hom}_k(A,B) \simeq \mathrm{Hom}_{\varphi}\big(D(B), D(A)\big)$$

(see [Wa-Mi] §II for a proof). In particular $A \sim B$ if and only if $P_A = P_B$.

A *q-Weil number* is an algebraic integer such that all its conjugates have absolute value $\sqrt{q}$ in $\mathbb{C}$. It is known that the roots of P_A are q-Weil numbers ([Mi] §19). Thus the isogeny class of a simple A is determined by the conjugacy class of a root π of P_A. Conversely, if π is a q-Weil number then by Honda's theorem [Ho-Ta] there exists a simple abelian variety A over k such that $P_A = \mathrm{P}_{\min}(\pi)^\delta$, where δ is determined by the conjugacy class of π. The skewfield $D = \mathrm{End}_k^\circ(A)$ is central of degree δ over $F = \mathbb{Q}(\pi)$, and the invariant of D at a prime v of F is

$$\mathrm{inv}(F_v \otimes_F D) = \begin{cases} 0 & \text{if } v \mid \ell \text{ with } \ell \neq p \text{ a rational prime} \\ \frac{1}{2} & \text{if } v \text{ is real} \\ \frac{f_v \,\mathrm{ord}_v(\pi)}{s} & \text{if } v \mid p, \text{ where } f_v = f(F_v/\mathbb{Q}_p) = \text{residue degree} \end{cases}$$

([Wa-Mi] Thm.8). If $k = \mathbb{F}_p$ and π has no real conjugate then $\mathrm{End}_k^\circ(A) = F$. For a simple $A/\mathbb{F}_{p^s}$ the polynomial P_A has real roots in only two cases:

(a) s is even and $P_A(X) = (X + p^{s/2})^2$ or $(X - p^{s/2})^2$ (corresponding to a quadratic twist), then A is a supersingular elliptic curve with $\mathrm{End}^\circ_{\mathbb{F}_{p^s}}(A) = \mathcal{D}_{p,\infty}$ = the quaternion algebra over $\mathbb{Q}$ ramified only at p and ∞

(b) s is odd and $P_A(X) = (X^2 - p^s)^2$, then A is an abelian surface with $\mathrm{End}^\circ_{\mathbb{F}_{p^s}}(A) =$ the quaternion algebra over $\mathbb{Q}(\sqrt{p})$ ramified only at the two infinite primes. Over a quadratic extension A becomes isogenous to the product of two supersingular elliptic curves of the second type above.

So the invariant δ attached to the simple abelian variety A/k, or equivalently to the q-Weil number π such that $P_A(\pi) = 0$, is given by

$$\delta = \begin{cases} 2 & \text{if } \mathrm{P}_{\min}(\pi) \text{ has a real root} \\ \operatorname{lcm}\left[\operatorname{ord}_{\mathbb{Q}/\mathbb{Z}}\left(\frac{f_v \operatorname{ord}_v(\pi)}{s}\right)\ ,\ v \mid p \text{ in } F\right] & \text{otherwise.} \end{cases}$$

Definition 2.1. A monic polynomial $P \in \mathbb{Z}[X]$ is a *p-Weil polynomial* if all its roots in $\overline{\mathbb{Q}}$ are p-Weil numbers and its valuation at $X^2 - p$ is even.

Equivalently, all the roots are p-Weil numbers and $P(0) = p^{\deg P/2}$. Thus

$$P(X) = (X^2 - p)^{2n_0} P_1(X)^{n_1} \dots P_m(X)^{n_m}$$

with P_i irreducibles in $\mathbb{Z}[X]$ having no real root. If A is an abelian variety over $\mathbb{F}_p$ then P_A is a p-Weil polynomial, and for each p-Weil polynomial P there is an $A/\mathbb{F}_p$ such that $P_A = P$. Specifically, there is a simple abelian surface A_0 with $P_{A_0}(X) = (X^2 - p)^2$ and for each i there is a simple A_i with $P_{A_i} = P_i$, so that we can take $A = \prod_{0 \le i \le m} A_i^{n_i}$. We thus get a convenient correspondance between p-Weil polynomials and isogeny classes of abelian varieties over $\mathbb{F}_p$.

We conclude this section by an elementary remark on the behaviour under base change. For $P \in \mathbb{Q}[X]$ splitting over $\overline{\mathbb{Q}}$ as $P(X) = \prod_i (X - \lambda_i)$ and s a positive integer, put

$$P^{(s)}(X) \underset{\text{def}}{=} \prod_i (X - \lambda_i^s).$$

One checks that $P^{(s)} \in \mathbb{Q}[X]$, and if P is irreducible then $P^{(s)}$ is a power of an irreducible in $\mathbb{Q}[X]$. Now for $A = A_0 \times_{\mathbb{F}_p} \mathbb{F}_{p^s}$ we have $P_A = P_{A_0}^{(s)}$, consequently if $A_0/\mathbb{F}_p$ is simple then $A \sim B^n$ with $B/\mathbb{F}_{p^s}$ simple.

2.2. **Honda-Tate algebras.** We begin with a result on subalgebras, known to the experts as Schofield's Lemma, that will be used several times in this paper. The proof we present here for the reader's convenience is due to E. Frossard. Let K be any field and A, B two central simple algebras over K. Denote by $[\mathsf{A}]$ the class of A in the Brauer group of K.

Lemma 2.2 ([Sc] 5, Lemma 9.1)**.** *There is a K-algebra embedding $\mathsf{A} \hookrightarrow \mathsf{B}$ if and only if* $\operatorname{ind}\big([\mathsf{B}] - [\mathsf{A}]\big) \deg \mathsf{A}$ *divides* $\deg \mathsf{B}$.

Proof. Assume $\mathsf{A} \hookrightarrow \mathsf{B}$ and identify A with its image. Obviously $\deg \mathsf{A}$ divides $\deg \mathsf{B}$. Let C be the centraliser of A in B. Then $\mathsf{A} \otimes_K \mathsf{C} = \mathsf{B}$, so $[\mathsf{C}] = [\mathsf{B}] - [\mathsf{A}]$ and $\operatorname{ind}\big([\mathsf{C}]\big)$ divides $\deg \mathsf{C} = \deg \mathsf{B}/\deg \mathsf{A}$.

Conversely, assume $\deg \mathsf{B} = n \operatorname{ind}\big([\mathsf{B}] - [\mathsf{A}]\big) \deg \mathsf{A}$ for some integer n. Let D be the skewfield such that $[\mathsf{D}] = [\mathsf{B}] - [\mathsf{A}]$ and put $\mathsf{B}' = \mathsf{A} \otimes_K M_n(\mathsf{D})$. Then $[\mathsf{B}'] = [\mathsf{A}] + [\mathsf{D}] = [\mathsf{B}]$ and $\deg \mathsf{B}' = n \deg \mathsf{D} \deg \mathsf{A} = n \operatorname{ind}\big([\mathsf{B}] - [\mathsf{A}]\big) \deg \mathsf{A} = \deg \mathsf{B}$, hence $\mathsf{B} \simeq \mathsf{B}'$. □

Corollary 2.3. *Let K be a number field. Then $\mathsf{A} \hookrightarrow \mathsf{B}$ if and only if $K_v \otimes_K \mathsf{A} \hookrightarrow K_v \otimes_K \mathsf{B}$ for all places v of K.*

Proof. Since K is a number field the global index is the least common multiple of the local indices, whereas degrees are unchanged. □

Let $B/\mathbb{F}_{p^s}$ be a simple abelian variety with p^s-Weil number π, and D its Honda-Tate division algebra with centre $F = \mathbb{Q}(\pi)$ and index δ. Let $K_0 = \operatorname{Frac} W(\mathbb{F}_{p^s})$ and $\zeta_r \in \overline{\mathbb{Q}}$ a primitive rth root of unity.

Lemma 2.4. *Assume $r \geq 3$ is an integer prime to p such that s is the order of p in $(\mathbb{Z}/r\mathbb{Z})^\times$. Then $F(\zeta_r)$ splits D. Furthermore δ divides $[F(\zeta_r) : F]$ and $n = [F(\zeta_r) : F]/\delta$ is the smallest integer such that $F(\zeta_r)$ embeds in $M_n(D)$.*

Proof. Let v be a prime of F lying above p and f_v the residue degree of F_v. Our assumption on r implies that $F(\zeta_r)_v = K_0F_v$. We have $[K_0F_v : F_v] = s/(s, f_v)$, where $(s, f_v) = \gcd(s, f_v)$, thus

$$[K_0F_v : F_v] \operatorname{inv}(F_v \otimes_F D) = \frac{f_v}{(s, f_v)} \operatorname{ord}_v(\pi) \in \mathbb{Z}.$$

So $F(\zeta_r)_v$ splits $F_v \otimes_F D$. At primes above $\ell \neq p$ we are in a split situation to start with. At an archimedian prime ∞ we have $F(\zeta_r)_\infty = \mathbb{C}$ since $r \geq 3$. Therefore $F(\zeta_r)$ splits D. The rest follows from the index reduction theorem, see [Al] IV, §§9,10. Then $F(\zeta_r)$ is a maximal subfield of $M_{[F(\zeta_r):F]/\delta}(D)$. □

We use the standard notation $\big(K/L, \omega, \alpha\big)$ for the cyclic algebra defined by the cyclic extension K/L with $\operatorname{Gal}(K/L) = \langle\omega\rangle$ and $\alpha \in L^\times$ (see [Pi] 15.1). It is a simple algebra of degree $n = [K : L]$ over its centre L, and

$$\big(K/L, \omega, \alpha\big) = \bigoplus_{0 \leq i < n} Ku^i \quad \text{with } uxu^{-1} = \omega(x) \text{ for all } x \in K \text{ and } u^n = \alpha.$$

The element α is unique up to a norm from K to L. It follows from the Honda-Tate theory that for v lying above p the algebra $F_v \otimes_F D$ is Brauer equivalent to

$$\Big(K_0F_v/F_v, \sigma^{f_v}, \pi^{f_v/(s,f_v)}\Big) = \Big(K_0F_v/F_v, \sigma^{(s,f_v)}, \pi\Big).$$

Fix $r \geq 3$ prime to p such that $s = \operatorname{ord}\big(p \in (\mathbb{Z}/r\mathbb{Z})^\times\big)$. Let m be a multiple of δ and consider the central simple Honda-Tate algebra of degree m over F

$$M_{m/\delta}(D) = \operatorname{End}^\circ_{\mathbb{F}_{p^s}}(A) \quad \text{with } A \sim B^{m/\delta}.$$

We assume that $\operatorname{Gal}\big(F(\zeta_r)/F\big)$ contains an automorphism σ_p acting as $\zeta_r \mapsto \zeta_r{}^p$ (i.e. $F \cap \mathbb{Q}(\zeta_r)$ is contained in the subfield of $\mathbb{Q}(\zeta_r)$ fixed by $\zeta_r \mapsto \zeta_r{}^p$). Let L be the field fixed by σ_p. We want to state necessary and sufficient conditions for $M_{m/\delta}(D)$ to contain a subalgebra isomorphic to the cyclic algebra of degree s over L

$$C(\pi) \underset{\text{def}}{=} \big(F(\zeta_r)/L, \sigma_p, \pi\big).$$

Lemma 2.4 shows that $F(\zeta_r)$ embeds in $M_{m/\delta}(D)$ if and only if $[F(\zeta_r) : F]$ divides m. The algebra $M_{[F(\zeta_r):F]/\delta}(D)$ is then a crossed product $\big(F(\zeta_r)/F, \mathsf{c}\big)$ for some 2-cocycle $\mathsf{c} \in H^2\big(\operatorname{Gal}\big(F(\zeta_r)/F\big), F(\zeta_r)^\times\big)$ ([Pi] 14.1, 14.2). Pick an $a \in L^\times$ such that

$$\operatorname{Res}_{\langle\sigma_p\rangle}\big(F(\zeta_r)/F, \mathsf{c}\big) \simeq \big(F(\zeta_r)/L, \sigma_p, a\big) \underset{\text{def}}{=} C(a)$$

where $\operatorname{Res}_{\langle\sigma_p\rangle}$ is the algebra obtained by restriction to the subgroup $\langle\sigma_p\rangle$ of $\operatorname{Gal}\big(F(\zeta_r)/F\big)$ ([Pi] 14.7). The algebra $C(a)$ is Brauer equivalent to $L \otimes_F D$, being the centraliser

of L in $\big(F(\zeta_r)/F, \mathsf{c}\big)$. Note that $C(\pi)$ embeds in $M_{m/\delta}(D)$ if and only if it embeds in $M_{m/[F(\zeta_r):F]}\big(C(a)\big)$, the centraliser of L in $M_{m/\delta}(D)$.

For each place v of L define

$$n_v(r;\pi) \underset{\text{def}}{=} \begin{cases} \operatorname{ord}\Big(\pi \in L_v^\times \big/ N_{F(\zeta_r)_v/L_v}\big(F(\zeta_r)_v^\times\big)\Big) & \text{if } v \text{ lies above } \ell \neq p \text{ and } \ell \mid r \\ 2 & \text{if } L_v = \mathbb{R} \text{ and } \pi = p^{s/2} \text{ with } s \text{ even} \\ 1 & \text{otherwise.} \end{cases}$$

This integer is actually the order of π/a in $L_v^\times \big/ N_{F(\zeta_r)_v/L_v}\big(F(\zeta_r)_v^\times\big)$. Indeed, it follows from Honda-Tate that π/a is a local norm at each $v \mid p$ and that a is a local norm at each $v \mid \ell \neq p$. Since π is an ℓ-adic unit for $\ell \neq p$, it is a local norm at $v \mid \ell$ whenever $F(\zeta_r)/L$ is unramified at v, which is the case if ℓ does not divide r. Finally, L has a real place if and only if s is even, $\pi = \pm p^{s/2}$, and $p^{s/2} \equiv -1 \bmod r$; then $F = \mathbb{Q}$, $D = \mathcal{D}_{p,\infty}$ and a is not a norm from $\mathbb{C}$ to $\mathbb{R}$. Now put

$$n(r;\pi) \underset{\text{def}}{=} \operatorname{lcm}\Big(n_v(r;\pi),\ v \text{ place of } L\Big).$$

The extension $F(\zeta_r)/L$ being cyclic $n(r;\pi)$ is the order of π/a in $L^\times \big/ N_{F(\zeta_r)/L}\big(F(\zeta_r)^\times\big)$.

Proposition 2.5. *Let $r \geq 3$ be prime to p, $s = \operatorname{ord}\big(p \in (\mathbb{Z}/r\mathbb{Z})^\times\big)$, and $\operatorname{End}^\circ_{\mathbb{F}_{p^s}}(A)$ central simple over $F = \mathbb{Q}(\pi)$. There is an embedding $\big(F(\zeta_r)/L, \sigma_p, \pi\big) \hookrightarrow \operatorname{End}^\circ_{\mathbb{F}_{p^s}}(A)$ if and only if $[F(\zeta_r) : F]n(r;\pi)$ divides the degree of $\operatorname{End}^\circ_{\mathbb{F}_{p^s}}(A)$.*

Proof. By lemma 2.4 $[F(\zeta_r) : F]$ must divide $m =$ degree of $\operatorname{End}^\circ_{\mathbb{F}_{p^s}}(A)$. According to corollary 2.3 we have to show for each place v of L that

$$(\iota_v) \qquad L_v \otimes_L C(\pi) \hookrightarrow L_v \otimes_L M_{m/[F(\zeta_r):F]}\big(C(a)\big)$$

holds if and only if $n_v(r;\pi)$ divides $m/[F(\zeta_r) : F]$. For $v \mid p$ we have $F_v = L_v$ and $L_v \otimes_L C(\pi) \simeq \big(K_0F_v/F_v, \sigma^{(s,f_v)}, \pi\big) \simeq L_v \otimes_L C(a)$, so (ι_v) holds. For $v \mid \ell \neq p$ we have

$$L_v \otimes_L M_{m/[F(\zeta_r):F]}\big(C(a)\big) \simeq M_{m/[L:F]}(L_v) \quad \text{whereas} \quad L_v \otimes_L C(\pi) \simeq M_{s/n_v(r;\pi)}(D_v)$$

with D_v a skewfield of degree $n_v(r;\pi)$ over L_v. By lemma 2.2 (ι_v) holds if and only if $n_v(r;\pi)$ divides $m/[F(\zeta_r) : F]$. Finally, let v be archimedean. If $L_v = \mathbb{C}$ then (ι_v) holds. If $L_v = \mathbb{R}$ then s is even, $\pi = \pm p^{s/2}$, $D = \mathcal{D}_{p,\infty}$, and $\mathbb{R} \otimes_L C(a) \simeq M_{s/2}(\mathbb{H})$. For $\pi = -p^{s/2}$ we have $\mathbb{R} \otimes_L C(\pi) \simeq M_{s/2}(\mathbb{H})$ and (ι_v) holds. For $\pi = p^{s/2}$ we have $\mathbb{R} \otimes_L C(\pi) \simeq M_s(\mathbb{R})$, so by lemma 2.2 (ι_v) holds if and only if $n_v(r;\pi) = 2$ divides $m/[F(\zeta_r) : F]$. □

3. Galois pairs

We set the following notations. For an abelian variety $A_0/\mathbb{F}_p$ put $\mathsf{f}_0 = \operatorname{Frob}_{A_0}$, $A = A_0 \times_{\mathbb{F}_p} \mathbb{F}_{p^s}$, and $\mathsf{f} = \operatorname{Frob}_A = \mathsf{f}_0^{\,s}$. Further $K_0 = \operatorname{Frac} W(\mathbb{F}_{p^s})$ and $\Delta(A) = \mathbf{W}\big(D(A)\big)$.

Recall that $D(A_0)$ is a $\mathbb{Q}_p$-vector space of dimension $2 \dim A$ together with a $\mathbb{Q}_p$-linear isomorphism $\varphi_0 : D(A_0) \xrightarrow{\sim} D(A_0)$ such that $\mathrm{P}_{\mathrm{char}}(\varphi_0) = \mathrm{P}_{\mathrm{char}}(\mathsf{f}_0)$, that $D(A)$ is a K_0-vector space of the same dimension together with a σ-semilinear bijection $\varphi : D(A) \xrightarrow{\sim} D(A)$ such that $\mathrm{P}_{\mathrm{char}}(\varphi^s) = \mathrm{P}_{\mathrm{char}}(\mathsf{f})$, and that $w \in W$ acts on $\Delta(A)$ via $\varphi^{-v(w)}$ (see 1.1.3). We actually have

$$D(A) = K_0 \otimes_{\mathbb{Q}_p} D(A_0) \quad \text{and} \quad \varphi = \sigma \otimes \varphi_0.$$

Thus $D(A)$ has a natural structure of a $\big(\varphi, \mathrm{Gal}(K_0/\mathbb{Q}_p)\big)$-module. Indeed, $\sigma(\lambda \otimes x_0) = \sigma(\lambda) \otimes x_0$ for $\lambda \in K_0$, $x_0 \in D(A_0)$ defines a σ-semilinear action of $\mathrm{Gal}(K_0/\mathbb{Q}_p)$ commuting with φ, and then $D(A_0) = \{x \in D(A) \mid \sigma x = x\}$. We have

$$\mathbb{Q}_p \otimes_{\mathbb{Q}} \mathrm{End}^{\circ}_{\mathbb{F}_p}(A_0) \simeq \mathrm{End}_{\varphi_0}\big(D(A_0)\big) \simeq \mathrm{End}_{\varphi, \mathrm{Gal}(K_0/\mathbb{Q}_p)}\big(D(A)\big).$$

We want to mimic the situation considered in section 1.2.1 where a $\big(\varphi, \mathrm{Gal}(K/\mathbb{Q}_p)\big)$-module structure was obtained on $D(A)$ in a context of potential good reduction, with K a suitable Galois extension of $\mathbb{Q}_p$ containing K_0. We first define in 3.1 the appropriate notion, namely Galois pairs. In 3.2 we check that these objects yield the desired representations, be it $\big(\varphi, \mathrm{Gal}(K/\mathbb{Q}_p)\big)$-modules or Weil representations. We then specialise to the tame case in 3.3 where we prove a decomposition result (proposition 3.9).

3.1. **Definition of Galois pairs.** For an abelian variety A over $\mathbb{F}_{p^s}$ consider the set of $\mathbb{F}_{p^s}$-isomorphisms from A to its various $\mathrm{Gal}(\mathbb{F}_{p^s}/\mathbb{F}_p)$-twists

$$\mathrm{Ist}_{\mathbb{F}_{p^s}}(A) \underset{\text{def}}{=} \{\, \psi_g = (g, \psi) \mid g \in \mathrm{Gal}(\mathbb{F}_{p^s}/\mathbb{F}_p) \text{ and } \psi : A \xrightarrow{\sim} A^g \,\}.$$

For $\psi_g : A \xrightarrow{\sim} A^g$ and $\psi_h : A \xrightarrow{\sim} A^h$ in $\mathrm{Ist}_{\mathbb{F}_{p^s}}(A)$, set

$$\psi_g * \psi_h \underset{\text{def}}{=} (\psi_g)^h \circ \psi_h \ : A \xrightarrow{\sim} A^{gh} = A^{hg}.$$

This defines a group structure on $\mathrm{Ist}_{\mathbb{F}_{p^s}}(A)$ with identity Id_A; the inverse of ψ_g is $(\psi_g^{-1})^{g^{-1}}$. The natural projection $\mathrm{pr} : \mathrm{Ist}_{\mathbb{F}_{p^s}}(A) \to \mathrm{Gal}(\mathbb{F}_{p^s}/\mathbb{F}_p)$, $\psi_g \mapsto g$, is a group morphism. Its kernel is the normal subgroup $\mathrm{Aut}_{\mathbb{F}_{p^s}}(A)$ on which $*$ is the usual group law. Write $\psi^{[n]} = \psi * \cdots * \psi$ (n times) for $n \in \mathbb{Z}$. Now let A_0 be an abelian variety over $\mathbb{F}_p$ and put

$$f_\sigma \underset{\text{def}}{=} (\mathrm{Id}_{A_0} \otimes \sigma : A \xrightarrow{\sim} A^\sigma) \in \mathrm{Ist}_{\mathbb{F}_{p^s}}(A).$$

The projection $\mathrm{pr} : f_\sigma^{[n]} \mapsto \sigma^n$ induces an isomorphism $\langle f_\sigma \rangle \simeq \mathrm{Gal}(\mathbb{F}_{p^s}/\mathbb{F}_p)$ which provides a section for the short exact sequence

$$1 \longrightarrow \mathrm{Aut}_{\mathbb{F}_{p^s}}(A) \longrightarrow \mathrm{Ist}_{\mathbb{F}_{p^s}}(A) \xrightarrow{\mathrm{pr}} \mathrm{Gal}(\mathbb{F}_{p^s}/\mathbb{F}_p) \longrightarrow 1.$$

Therefore when $A = A_0 \times_{\mathbb{F}_p} \mathbb{F}_{p^s}$ we have $\mathrm{Ist}_{\mathbb{F}_{p^s}}(A) = \mathrm{Aut}_{\mathbb{F}_{p^s}}(A) \rtimes \langle f_\sigma \rangle$.

Definition 3.1. Let $K/\mathbb{Q}_p$ be a finite Galois extension with residue field $\mathbb{F}_{p^s}$. A *Galois pair* for $K/\mathbb{Q}_p$ is a triple (A_0, Γ, ν) where $A_0/\mathbb{F}_p$ is an abelian variety, Γ is a finite subgroup of $\mathrm{Aut}_{\mathbb{F}_{p^s}}(A)$, and $\nu : \mathrm{Gal}(K/\mathbb{Q}_p) \to \mathrm{Ist}_{\mathbb{F}_{p^s}}(A)$ is an antimorphism satisfying

(i) $(\mathrm{pr} \circ \nu)(g) = g \bmod I(K/\mathbb{Q}_p)$ for all $g \in \mathrm{Gal}(K/\mathbb{Q}_p)$
(ii) $\mathrm{Im}\,\nu = \Gamma \rtimes \langle f_\sigma \rangle$.

Observe that condition (i) is equivalent to the commutativity of the diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & I(K/\mathbb{Q}_p) & \longrightarrow & \mathrm{Gal}(K/\mathbb{Q}_p) & \longrightarrow & \mathrm{Gal}(\mathbb{F}_{p^s}/\mathbb{F}_p) & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle \nu} & & \downarrow{\scriptstyle \nu} & & \| & & \\
1 & \longrightarrow & \mathrm{Aut}_{\mathbb{F}_{p^s}}(A) & \longrightarrow & \mathrm{Ist}_{\mathbb{F}_{p^s}}(A) & \xrightarrow{\mathrm{pr}} & \mathrm{Gal}(\mathbb{F}_{p^s}/\mathbb{F}_p) & \longrightarrow & 1.
\end{array}$$

Condition (ii) further imposes $\nu\big(I(K/\mathbb{Q}_p)\big) = \Gamma$ and $f_\sigma \in \mathrm{Im}\,\nu$.

Remark 3.2. *Changing K.* Let (A_0, Γ, ν) be a Galois pair for $K/\mathbb{Q}_p$.

1.Put $K' = K^{\operatorname{Ker}\nu}$. Since $\operatorname{Ker}\nu \subseteq I(K/\mathbb{Q}_p)$ the extension K/K' is totally ramified and $K'/\mathbb{Q}_p$ is Galois with residue field $\mathbb{F}_{p^s}$. The induced $\nu' : \operatorname{Gal}(K'/\mathbb{Q}_p) \hookrightarrow \operatorname{Ist}_{\mathbb{F}_{p^s}}(A)$ is injective and (A_0, Γ, ν') is a Galois pair for $K'/\mathbb{Q}_p$. The injectivity of ν' implies that $\operatorname{Gal}(K'/\mathbb{Q}_p) \simeq I(K'/\mathbb{Q}_p) \rtimes \operatorname{Gal}(\mathbb{F}_{p^s}/\mathbb{F}_p)$ (compare with section 1.2.1).

2. Assume ν injective. Let $\omega \in \operatorname{Gal}(K/\mathbb{Q}_p)$ such that $\nu(\omega) = f_\sigma$ and $L = K^{\langle\omega\rangle}$. The largest normal subgroup of $\operatorname{Gal}(K/\mathbb{Q}_p)$ contained in $\langle\omega\rangle$ is $\langle\omega^r\rangle$, where r is the least positive integer such that ω^r commutes with all elements in $I(K/\mathbb{Q}_p)$. As ν is injective the latter is equivalent to $f_\sigma^{[r]} * \gamma = \gamma * f_\sigma^{[r]}$ for all $\gamma \in \Gamma$. Therefore the Galois closure of L in K is $F = L \operatorname{Frac} W(\mathbb{F}_{p^r})$ with $\mathbb{F}_{p^r} \subseteq \mathbb{F}_{p^s}$ the smallest field of definition for Γ. Then ν induces $\bar\nu : \operatorname{Gal}(F/\mathbb{Q}_p) \hookrightarrow \operatorname{Ist}_{\mathbb{F}_{p^r}}(A)$ and $(A_0, \Gamma, \bar\nu)$ is a Galois pair for $F/\mathbb{Q}_p$.

Call a Galois pair (A_0, Γ, ν) for $K/\mathbb{Q}_p$ *minimal* when ν is injective and $\mathbb{F}_{p^s}$ minimal with respect to Γ.

Example 3.3. Let $e \in \{3, 4, 6\}$ prime to p. Let $L/\mathbb{Q}_p$ be totally ramified of degree e and K its Galois closure. Then K/L is unramified of degree s, with $s = 1$ or 2 according to $p \equiv 1$ or $-1 \bmod e\mathbb{Z}$, and $\operatorname{Gal}(K/\mathbb{Q}_p) = I(K/\mathbb{Q}_p) \rtimes \operatorname{Gal}(K/L) \simeq \mathbb{Z}/e\mathbb{Z} \rtimes \mathbb{Z}/s\mathbb{Z}$.

When $s = 1$ there is an ordinary elliptic curve $E_0/\mathbb{F}_p$ with $\operatorname{Ist}_{\mathbb{F}_p}(E_0) = \operatorname{Aut}_{\mathbb{F}_p}(E_0) = \langle -\zeta_e\rangle$, while when $s = 2$ there is a supersingular one with $\operatorname{Aut}_{\mathbb{F}_{p^2}}(E) = \langle -\zeta_e\rangle$, so $\operatorname{Ist}_{\mathbb{F}_{p^2}}(E) = \langle -\zeta_e\rangle \rtimes \langle f_\sigma\rangle$ with $f_\sigma \zeta_e = \zeta_e^{-1} f_\sigma$ ([Si] III§10 and V4.4,4.5). In both cases any injection $\nu : \operatorname{Gal}(K/\mathbb{Q}_p) \hookrightarrow \operatorname{Ist}_{\mathbb{F}_{p^s}}(E)$ sending a generator of $I(K/\mathbb{Q}_p)$ to ζ_e and the generator of $\operatorname{Gal}(K/L)$ to f_σ defines a minimal Galois pair $(E_0, \langle\zeta_e\rangle, \nu)$ for $K/\mathbb{Q}_p$.

Not all (A_0, Γ) give rise to a minimal Galois pair for some $K/\mathbb{Q}_p$.

Example 3.4. Let $A_0 = {B_0}^n$ so that $\operatorname{Aut}_{\mathbb{F}_p}(A_0)$ contains a subgroup isomorphic to the permutation group $\mathcal{S}_n$. Let Γ be a cyclic subgroup of $\mathcal{S}_n$ of order e prime to p. Then there exists a Galois extension $K/\mathbb{Q}_p$ for which (A_0, Γ, ν) is a minimal Galois pair for some ν if and only if $p \equiv 1 \bmod e\mathbb{Z}$.

Now fix $K/\mathbb{Q}_p$ finite Galois. All the Galois pairs considered below, starting with (A_0, Γ, ν) and (A_0', Γ', ν'), are assumed to be Galois pairs for $K/\mathbb{Q}_p$. They form the objects of a category.

Morphisms. A morphism of Galois pairs $\psi_0 : (A_0, \Gamma, \nu) \to (A_0', \Gamma', \nu')$ is an $\mathbb{F}_p$-morphism of abelian varieties $\psi_0 : A_0 \to A_0'$ such that the diagram

$$\begin{array}{ccc} A & \xrightarrow{\psi} & A' \\ {\scriptstyle \nu(g)}\big\downarrow\wr & & \wr\big\downarrow{\scriptstyle \nu'(g)} \\ A^{\bar g} & \xrightarrow[\psi^{\bar g}]{} & A'^{\bar g} \end{array}$$

commutes for all $g \in \operatorname{Gal}(K/\mathbb{Q}_p)$, with $\bar g = g \bmod I(K/\mathbb{Q}_p)$. There is an obvious notion of isogeny of Galois pairs, just require in addition ψ_0 to be an isogeny. Let $\operatorname{End}_{\mathbb{F}_p,\Gamma}(A_0)$ be the subring of $\operatorname{End}_{\mathbb{F}_p}(A_0)$ consisting of elements commuting with all elements in Γ (after base change to $\mathbb{F}_{p^s}$). We have

$$\operatorname{End}_{\text{Gal pair}}\big((A_0, \Gamma, \nu)\big) \simeq \operatorname{End}_{\mathbb{F}_p,\Gamma}(A_0).$$

Subobjects. Let $B_0 \subseteq A_0$ be an abelian subvariety such that Γ stabilises $B = B_0 \times_{\mathbb{F}_p} \mathbb{F}_{p^s}$. We have $f_\sigma(B) = B^\sigma$, so $\operatorname{Im}\nu = \Gamma \rtimes \langle f_\sigma \rangle$ is realised by restriction to B as a subgroup of $\mathrm{Ist}_{\mathbb{F}_{p^s}}(B)$. Then $(B_0, \Gamma_{|B}, g \mapsto \nu(g)_{|B})$ is a Galois pair and the inclusion $B_0 \hookrightarrow A_0$ a morphism of Galois pairs.

Duals. Put $\Gamma^\vee = \{\gamma^\vee, \gamma \in \Gamma\} \subseteq \mathrm{Aut}_{\mathbb{F}_{p^s}}(A^\vee)$. The dual of (A_0, Γ, ν) is

$$(A_0, \Gamma, \nu)^\vee \underset{\text{def}}{=} \big(A_0^\vee, \Gamma^\vee, g \mapsto \nu(g)^{\vee -1}\big).$$

Note that a morphism $\lambda_0 : A_0 \to A_0^\vee$ induces a morphism of Galois pairs if and only if $\gamma^\vee \lambda^\vee \gamma = \lambda$ for all $\gamma \in \Gamma$. When λ_0 is a polarisation this means $\Gamma \subseteq \mathrm{Aut}(A, \lambda)$ (compare with lemma 1.3), and we say that λ_0 is a polarisation on (A_0, Γ, ν).

*Products.*The fibre product of $\mathrm{Ist}_{\mathbb{F}_{p^s}}(A)$ and $\mathrm{Ist}_{\mathbb{F}_{p^s}}(A')$ over $\mathrm{Gal}(\mathbb{F}_{p^s}/\mathbb{F}_p)$ (relative to the projections pr and pr′) is a subgroup of $\mathrm{Ist}_{\mathbb{F}_{p^s}}(A \times A')$. Set

$$(A_0, \Gamma, \nu) \times (A_0', \Gamma', \nu') = (A_0'', \Gamma'', \nu'')$$

with $A_0'' = A_0 \times A_0'$, $\Gamma'' = \{\big(\nu(g), \nu'(g)\big),\ g \in I(K/\mathbb{Q}_p)\} \subseteq \Gamma \times \Gamma'$, and

$$\nu'' \ : \ \begin{cases} \mathrm{Gal}(K/\mathbb{Q}_p) & \to & \mathrm{Ist}_{\mathbb{F}_{p^s}}(A) \times_{\mathrm{Gal}(\mathbb{F}_{p^s}/\mathbb{F}_p)} \mathrm{Ist}_{\mathbb{F}_{p^s}}(A') \\ g & \mapsto & \big(\nu(g), \nu'(g)\big) \end{cases}$$

(which is well-defined since $\mathrm{pr} \circ \nu = \mathrm{pr}' \circ \nu'$). Then (A_0'', Γ'', ν'') is a Galois pair and the projections from $A_0 \times A_0'$ to each factor are morphisms of Galois pairs.

Decompositions. Let B_0 and C_0 be Γ-stable $\mathbb{F}_p$-subvarieties of A_0. Then the morphism $B_0 \times C_0 \to A_0$, $(b, c) \mapsto b + c$ induces a morphism of Galois pairs

$$\big(B_0, \Gamma_{|B}, g \mapsto \nu(g)_{|B}\big) \times \big(C_0, \Gamma_{|C}, g \mapsto \nu(g)_{|C}\big) \longrightarrow (A_0, \Gamma, \nu).$$

In particular, if A_0 is isogenous to a product of Γ-stable abelian varieties defined over $\mathbb{F}_p$ then (A_0, Γ, ν) is isogenous to the product of the Galois pairs associated to each factor. Hence the category of Galois pairs for $K/\mathbb{Q}_p$ up to isogeny is semisimple.

3.2. **The representations associated to Galois pairs.** The definition of a Galois pair (A_0, Γ, ν) for $K/\mathbb{Q}_p$ has been taylored so to provide a $\big(\varphi, \mathrm{Gal}(K/\mathbb{Q}_p)\big)$-module structure on $D(A)$, via ν. Indeed, passing to p-divisible groups and applying the functor $\mathbf{D}$ we get

$$\begin{array}{ccc} \mathrm{Gal}(K/\mathbb{Q}_p) & \xrightarrow{\ \nu\ } & \mathrm{Ist}_{\mathbb{F}_{p^s}}(A) \\ & \searrow^{\nu} & \big\downarrow \text{functor } D \\ & & \mathrm{Ist}^*_{\mathbb{F}_{p^s}}\big(D(A)\big). \end{array}$$

Here $\mathrm{Ist}^*_{\mathbb{F}_{p^s}}\big(D(A)\big)$ is the group of φ-module isomorphisms $D(A^g) \xrightarrow{\sim} D(A)$ for all $g \in \mathrm{Gal}(\mathbb{F}_{p^s}/\mathbb{F}_p)$, the group law being functorially deduced from the one on $\mathrm{Ist}_{\mathbb{F}_{p^s}}(A)$. Note that this time the diagonal ν is a genuine group morphism, thanks to contravariancy. This obviously defines a σ-semilinear action of $\mathrm{Gal}(K/\mathbb{Q}_p)$ on $D(A)$. Since $f_\sigma * \mathsf{f}_0 = f_\sigma \circ \mathsf{f}_0$ commutes with all elements in $\mathrm{Ist}_{\mathbb{F}_{p^s}}(A)$ and $D(f_\sigma * \mathsf{f}_0) = \sigma \otimes \varphi_0 = \varphi$ this action commutes with φ. We thus obtain the $\big(\varphi, \mathrm{Gal}(K/\mathbb{Q}_p)\big)$-module structure on $D(A)$ associated to the Galois pair (A_0, Γ, ν).

The association $(A_0,\Gamma,\nu)\mapsto D(A)$ from the category of Galois pairs for $K/\mathbb{Q}_p$ to that of $\big(\varphi,\mathrm{Gal}(K/\mathbb{Q}_p)\big)$-modules is functorial (contravariant). It is faithful, isogenies of Galois pairs yielding isomorphisms of $\big(\varphi,\mathrm{Gal}(K/\mathbb{Q}_p)\big)$-modules. The $(\varphi,\mathrm{Gal}(K/\mathbb{Q}_p))$-module $D(A^\vee)$ associated to $(A_0,\Gamma,\nu)^\vee$ is isomorphic to the twisted dual $D(A)^*\{-1\}$ of $D(A)$, since the dual action of an element in $I(K/\mathbb{Q}_p)$ is the inverse of the dual of its image in $\mathrm{Aut}_\varphi\big(D(A)\big)$. If $(A_0,\Gamma,\nu)=(A_0',\Gamma',\nu')\times(A_0'',\Gamma'',\nu'')$ then $D(A)=D(A')\oplus D(A'')$.

Remark 3.5. We have canonical isomorphisms

$$\mathbb{Q}_p\otimes_{\mathbb{Z}}\mathrm{End}_{\text{Gal pair}}\big((A_0,\Gamma,\nu)\big)\simeq\mathbb{Q}_p\otimes_{\mathbb{Q}}\mathrm{End}^\circ_{\mathbb{F}_p,\Gamma}(A_0)\simeq\mathrm{End}_{\varphi,\mathrm{Gal}(K/\mathbb{Q}_p)}\big(D(A)\big).$$

We now construct the associated Weil pair (A_0,Γ,ρ). Replacing K by the subfield fixed by $\mathrm{Ker}\,\nu$ we may assume that ν is injective. Recall that $\upsilon: W\twoheadrightarrow\mathbb{Z}$ sends a lifting of the absolute Frobenius to 1, and let $\sigma_0\in W$ be one such lifting with $\sigma_0 \bmod W_K=\nu^{-1}(f_\sigma)\in\mathrm{Gal}(K/\mathbb{Q}_p)$. Put

$$\rho\ :\ \begin{cases} W & \to & \mathrm{End}^\circ_{\mathbb{F}_{p^s}}(A)^\times \\ w & \mapsto & \Big((f_\sigma * \mathsf{f}_0)^{[\upsilon(w)]}\Big)^{-1}\nu(w \bmod W_K). \end{cases}$$

One checks that ρ is a well-defined antimorphism satisfying $\rho(\sigma_0^{-1})=\mathsf{f}_0$ and $\rho(I)=\Gamma$. If we let $M=K\mathbb{Q}_p^{\mathrm{un}}$ then $\mathrm{Weil}(M/\mathbb{Q}_p)=W/I_K=I(K/\mathbb{Q}_p)\rtimes\langle\sigma_0\rangle$ and ρ yields an injection

$$\rho:\mathrm{Weil}(M/\mathbb{Q}_p)\hookrightarrow\mathrm{Aut}_{\mathbb{F}_{p^s}}(A)\rtimes\langle\mathsf{f}_0\rangle\subseteq\mathrm{End}^\circ_{\mathbb{F}_{p^s}}(A)^\times$$

with image $\Gamma\rtimes\langle\mathsf{f}_0\rangle$. We thus obtain the associated Weil representation

$$\begin{array}{ccc} \mathrm{Weil}(M/\mathbb{Q}_p) & \xhookrightarrow{\ \rho\ } & \mathrm{End}^\circ_{\mathbb{F}_{p^s}}(A)^\times \\ & \searrow^{\rho} & \big\downarrow{\scriptstyle \text{functor }\Delta} \\ & & \mathrm{Aut}_{K_0}\big(\Delta(A)\big). \end{array}$$

Remark 3.6. View the anti-embedding $\mathrm{End}^\circ_{\mathbb{F}_{p^s}}(A)\hookrightarrow\mathrm{End}_{K_0}\big(\Delta(A)\big)$ as a faithful algebra representation. The action of a simple subalgebra E of $\mathrm{End}^\circ_{\mathbb{F}_{p^s}}(A)$ is $2d/f\delta$ times the direct sum of the reduced representation of E (tensored by K_0), where $d=\dim A$, $f=[Z(E):\mathbb{Q}]$ and $\delta=\deg E$ ([Mi] Prop.12.12, replacing $V_\ell(A)$ by $\Delta(A)$). Recall that the reduced representation of E is the direct sum of the f nonisomorphic representations of E over $\overline{\mathbb{Q}}$ furnished by the f distinct embeddings of $Z(E)$ in $\overline{\mathbb{Q}}$. It is defined over $\mathbb{Q}$.

Conversely, suppose $\rho: W\to\mathrm{End}^\circ_{\mathbb{F}_{p^s}}(A)^\times$ is an antimorphism such that $\rho(\sigma_0^{-1})=\mathsf{f}_0$ and $\rho(I)=\Gamma$. Then $\mathrm{Ker}\,\rho$ is a subgroup of I of finite index and determines a Galois extension M of $\mathbb{Q}_p$ containing $\mathbb{Q}_p^{\mathrm{un}}$. As in section 1.2.1 let K be the Galois closure of a totally ramified extension of $\mathbb{Q}_p$ generating M over $\mathbb{Q}_p^{\mathrm{un}}$. Define an injective antimorphism by

$$\nu\ :\ \begin{cases} \mathrm{Gal}(K/\mathbb{Q}_p) & \hookrightarrow & \mathrm{Ist}_{\mathbb{F}_{p^s}}(A)=\mathrm{Aut}_{\mathbb{F}_{p^s}}(A)\rtimes\langle f_\sigma\rangle \\ g & \mapsto & \eta\big(\rho(\tilde g) \bmod \langle\mathsf{f}\rangle\big) \end{cases}$$

where $\tilde{g}$ is any lifting of g in $\mathrm{Weil}(M/\mathbb{Q}_p)$ and η is $\big(\mathsf{f}_0 \bmod \langle \mathsf{f}\rangle\big)^n\gamma \mapsto f_\sigma^{[n]} * \gamma$ for $\gamma \in \mathrm{Aut}_{\mathbb{F}_{p^s}}(A)$. We then have a commutative diagram

$$\begin{array}{ccc}
\mathrm{Weil}(M/\mathbb{Q}_p) & \xrightarrow{\ \rho\ } & \mathrm{Aut}_{\mathbb{F}_{p^s}}(A) \rtimes \langle \mathsf{f}_0\rangle \\
\Big\downarrow{\scriptstyle \bmod W_K/I_K} & & \Big\downarrow{\scriptstyle \bmod \langle \mathsf{f}\rangle} \\
\mathrm{Gal}(K/\mathbb{Q}_p) & \xrightarrow{\ \nu\ } & \mathrm{Aut}_{\mathbb{F}_{p^s}}(A) \rtimes \langle \mathsf{f}_0 \bmod \langle \mathsf{f}\rangle\rangle \\
 & & \wr\Big\downarrow{\scriptstyle \eta} \\
 & & \mathrm{Ist}_{\mathbb{F}_{p^s}}(A).
\end{array}$$

Hence these constructions are inverse one to the other, and, when passing to representations, $\nu \mapsto \rho$ corresponds to $D \mapsto \mathbf{W}(D) = \Delta$ whereas $\rho \mapsto \nu$ corresponds to a "section" $\Delta \mapsto D$.

Remark 3.7. $K/\mathbb{Q}_p$ is a Galois extension of minimal degree over which $\Delta(A)$ acquires good reduction if and only if (A_0, Γ, ν) is minimal.

3.3. **Tame Galois pairs.** Let (A_0, Γ, ν) be a Galois pair for $K/\mathbb{Q}_p$ such that Γ is of order e prime to p. Then $K^{\mathrm{Ker}\,\nu}/\mathbb{Q}_p$ is tame and we say that (A_0, Γ, ν) is a tame Galois pair. In this case Γ is a cyclic group generated by an element τ satisfying the relation

$$\mathsf{f}_0\tau = \tau^p\mathsf{f}_0 \quad \text{ in } \mathrm{End}_{\mathbb{F}_{p^s}}(A).$$

We may assume that $\mathbb{F}_{p^s}$ is the smallest field of definition for Γ (remark 3.2), which implies that s is the order of p in $(\mathbb{Z}/e\mathbb{Z})^\times$. Consider the semisimple subalgebra $\mathbb{Q}[\mathsf{f}_0, \tau]$ of $\mathrm{End}^\circ_{\mathbb{F}_{p^s}}(A)$ generated over $\mathbb{Q}$ by f_0 and τ.

Definition 3.8. The Galois pair $(A_0, \langle\tau\rangle, \nu)$ is *cyclic* if $\mathbb{Q}[\mathsf{f}_0, \tau]$ is a cyclic algebra.

Note that $\mathrm{End}^\circ_{\mathbb{F}_{p^s}}(A)$ is central simple over $\mathbb{Q}(\mathsf{f})$ when $(A_0, \langle\tau\rangle, \nu)$ is cyclic, as $\mathrm{P}_{\min}(\mathsf{f})$ is then irreducible in $\mathbb{Q}[X]$.

Proposition 3.9. *A tame Galois pair is isogenous to a product of cyclic ones. A cyclic tame Galois pair $(A_0, \langle\tau\rangle, \nu)$ with $r = \mathrm{ord}(\tau)$ and $s = \mathrm{ord}\big(p \in (\mathbb{Z}/r\mathbb{Z})^\times\big)$ satisfies*

$$\mathbb{Q}[\mathsf{f}_0, \tau] \simeq \big(F(\zeta_r)/L, \sigma_p, \pi\big)$$

where π is the associated p^s-Weil number, $\zeta_r \in \overline{\mathbb{Q}}$ is a primitive rth root of unity, $F = \mathbb{Q}(\pi)$, $\sigma_p(\pi) = \pi$, $\sigma_p(\zeta_r) = {\zeta_r}^p$, and $L = F(\zeta_r)^{\langle\sigma_p\rangle}$.

Proof. Let $(A_0, \langle\tau\rangle, \nu)$ be a tame Galois pair with $e = \mathrm{ord}(\tau)$ and $s = \mathrm{ord}\big(p \in (\mathbb{Z}/e\mathbb{Z})^\times\big)$. Recall from section 3.1 that a splitting of A_0 up to isogeny into a product of $\mathbb{F}_p$-defined, τ-stable abelian varieties yields a splitting of $(A_0, \langle\tau\rangle, \nu)$ up to isogeny accordingly. The minimal polynomial in $\mathbb{Q}[X]$ annihilating τ writes as

$$\mathrm{P}_{\min}(\tau) = \prod_{r\in S} \Phi_r$$

where Φ_r is the rth cyclotomic polynomial, and S is a set of positive integers dividing e such that $\mathrm{lcm}(r \in S) = e$. For $r \in S$ the connected component of $\mathrm{Ker}\big(\Phi_r(\tau)\big)$ containing the identity is an abelian subvariety A_r of A, and $A \sim \prod_{r\in S} A_r$ over $\mathbb{F}_{p^s}$. The A_r's are stable

by τ which restricts to an automorphism with $\mathrm{P}_{\min}$ equal to Φ_r. As r is prime to p we have $\mathrm{P}_{\min}(\tau^p) = \mathrm{P}_{\min}(\tau)$. The relation $\mathsf{f}_0\Phi_r(\tau) = \Phi_r(\tau^p)\mathsf{f}_0$ implies that $\Phi_r(\tau^p)\big(\mathsf{f}_0(A_r)\big) = 0$, which shows that $\mathsf{f}_0(A_r) \subseteq A_r$ and therefore A_r is defined over $\mathbb{F}_p$.

So assume $\mathrm{P}_{\min}(\tau) = \Phi_r$ and $s = \mathrm{ord}\big(p \in (\mathbb{Z}/r\mathbb{Z})^\times\big)$. The centre $Z(\mathbb{Q}[\mathsf{f}_0, \tau])$ is a product of number fields containing $\mathbb{Q}[\mathsf{f}]$. As above this decomposition splits A into the product of abelian varieties over $\mathbb{F}_{p^s}$ each of which is stable by τ and by f_0, hence defined over $\mathbb{F}_p$.

Now $(A_0, \langle\tau\rangle, \nu)$ is a tame Galois pair such that

$$\mathrm{P}_{\min}(\tau) = \Phi_r \quad \text{and} \quad Z(\mathbb{Q}[\mathsf{f}_0, \tau]) = L \text{ is a field.}$$

It follows that $\mathbb{Q}[\mathsf{f}, \tau]$ is a field. Indeed, as an étale algebra $\mathbb{Q}[\mathsf{f}, \tau]$ is a product of number fields $\prod_j K_j$, on which f_0 acts by conjugation $c_0 : x \mapsto \mathsf{f}_0 x \mathsf{f}_0^{-1}$. Since $c_0(\mathsf{f}) = \mathsf{f}$ and $c_0(\tau) = \tau^p$ this action preserves the direct factors, thus $\mathbb{Q}[\mathsf{f}, \tau]^{\langle c_0\rangle} = \prod_j L_j$ with L_j the subfield of K_j fixed by c_0. But the centre of $\mathbb{Q}[\mathsf{f}_0, \tau]$ is the intersection of the centraliser $\mathbb{Q}[\mathsf{f}, \tau]$ of τ and that of f_0, so $L = \mathbb{Q}[\mathsf{f}, \tau]^{\langle c_0\rangle}$ and $\mathbb{Q}[\mathsf{f}, \tau]$ is a field.

Let $\pi \in \overline{\mathbb{Q}}$ be a root of the $\mathbb{Q}$-irreducible polynomial $\mathrm{P}_{\min}(\mathsf{f})$ and let $F = \mathbb{Q}(\pi)$. We have an isomorphism $\mathbb{Q}[\mathsf{f}, \tau] \simeq F(\zeta_r)$ given by $\mathsf{f} \mapsto \pi$ and $\tau \mapsto \zeta_r$. The conjugation c_0 on $\mathbb{Q}[\mathsf{f}, \tau]$ translates to an element $\sigma_p \in \mathrm{Gal}\big(F(\zeta_r)/F\big)$ acting as $\sigma_p(\zeta_r) = {\zeta_r}^p$, and L is the subfield of $F(\zeta_r)$ fixed by it, so that $F(\zeta_r)/L$ is cyclic of degree s. Finally we obtain an isomorphism

$$\mathbb{Q}[\mathsf{f}_0, \tau] \xrightarrow{\sim} \big(F(\zeta_r)/L, \sigma_p, \pi\big)$$

by $\tau \mapsto \zeta_r$ and $\mathsf{f}_0 \mapsto u_p$ such that $u_p x u_p^{-1} = \sigma_p(x)$ for all $x \in F(\zeta_r)$ and $u_p^s = \pi$. □

4. Representations arising from abelian varieties over $\mathbb{F}_p$

We now aim to describe the tame representations arising from Galois pairs. Some general facts on semisimple representations defined over $\mathbb{Q}$ are proved in section 4.1. Corollary 4.2 is important as it shows how to decompose such a Δ into subobjects, that is, subrepresentations defined over $\mathbb{Q}$. Lemma 4.3 deals with the arithmetic of Δ in the abelian case; it is used in section 4.4 where some explicit examples are given in dimension 1 and 2. In section 4.2 we restrict to the tame case. The decomposition of Δ is carried out in detail in proposition 4.4. It leads to the introduction of an arithmetic invariant (definition 4.6), that is trivial when Δ comes from a Galois pair (proposition 4.9). This gives a new condition for a $\big(\varphi, \mathrm{Gal}(K/\mathbb{Q}_p)\big)$-module to arise from a Galois pair. In section 4.3 we show that requiring this condition to hold in addition to the classical ones (Weil numbers, symplectic structure) is enough to guarantee that a $\big(\varphi, \mathrm{Gal}(K/\mathbb{Q}_p)\big)$-module comes from a Galois pair (theorem 4.11).

4.1. Semisimple representations defined over $\mathbb{Q}$.

Let L/K be a characteristic zero field extension and V a finite dimensional L-vector space. A subgroup H of $\mathrm{Aut}_L(V)$ is defined over K if $\mathrm{P}_{\mathrm{char}}(u) \in K[X]$ for all $u \in H$. When H consists of semisimple elements this is equivalent to $\mathrm{Tr}(u) \in K$ for all $u \in H$.

Lemma 4.1. *Let f and g be two semisimple elements in $\mathrm{End}_L(V)$ such that $\mathrm{Tr}(g^n) \in K$ and $\mathrm{Tr}(fg^n) \in K$ for all integers n. Let W be a subspace of the form $W = \mathrm{Ker}\, P(g)$ for some $P \in K[X]$ and assume $f(W) \subseteq W$. Then $\mathrm{Tr}(f_{|W}) \in K$.*

Proof. Put $h = P(g) \in \mathrm{End}_L(V)$: it is a semisimple element such that $\mathrm{Tr}(fh^n) \in K$ for all n, and $W = \mathrm{Ker}\, h$. Moreover, $\mathrm{P}_{\mathrm{char}}(h) \in K[X]$ because $P \in K[X]$ and $\mathrm{P}_{\mathrm{char}}(g) \in K[X]$ by assumption. Write $\mathrm{P}_{\mathrm{char}}(h)(X) = X^m R(X)$ with $R(X) \in K[X]$ and $R(0) \neq 0$, which gives the decomposition $V = W \oplus \mathrm{Ker}\, R(h)$. Now $fR(h)$ stabilises W with

$$\big(fR(h)\big)_{|W} = R(0) f_{|W}$$

and vanishes on $\mathrm{Ker}\, R(h)$, so that

$$\mathrm{Tr}\big(fR(h)\big) = R(0)\,\mathrm{Tr}(f_{|W}).$$

Since $\mathrm{Tr}\big(fR(h)\big) \in K$ and $R(0) \in K^\times$ we get $\mathrm{Tr}(f_{|W}) \in K$. □

Corollary 4.2. *Let (Δ, ρ) be a Weil representation over L that is semisimple and defined over $\mathbb{Q}$. Let $u \in \mathrm{Im}\,\rho$ and $P \in \mathbb{Q}[X]$ such that $P(u) = 0$. Assume $P = P_1 P_2$ with $P_i \in \mathbb{Q}[X]$ coprime and each $\Delta_i = \mathrm{Ker}\, P_i(u)$ stable by ρ. Then $\Delta = \Delta_1 \oplus \Delta_2$ with Δ_i defined over $\mathbb{Q}$.*

Proof. Since elements in $\mathrm{Im}\,\rho$ have either finite order or generate a subgroup of finite index, the semisimplicity assumption implies that they are semisimple. Then apply lemma 4.1 to $K = \mathbb{Q}$, $f \in \mathrm{Im}\,\rho$, $g = u$ and $W = \Delta_i$. □

For $u \in \mathrm{End}_L(V)$ let $\mathrm{Spec}\, u$ be the set of u's eigenvalues in an algebraic closure $\overline{L}$ of L.

Lemma 4.3. *Let u and v be two semisimple commuting elements in $\mathrm{Aut}_L(V)$ such that $\langle u, v\rangle$ is defined over K and $\mathrm{P}_{\mathrm{char}}(u) = \mathrm{P}_{\min}(u)$. Then $\mathrm{Spec}\, v \subset K(\mathrm{Spec}\, u)$.*

Proof. The assumptions imply that u and v are codiagonalisable in $\overline{L} \otimes_L V$ and that $\mathrm{P}_{\mathrm{char}}(u)$ has distinct roots. Let $d = \dim_L V$. By semisimplicity $\langle u, v\rangle$ is defined over K if and only if $\mathrm{Tr}(u^i v^j) \in K$ for all $0 \leq i, j \leq d-1$. For $x_1, \ldots, x_d \in \overline{L}$ let $\mathrm{V}(x_1, \ldots, x_d)$ be the Vandermonde matrix

$$\mathrm{V}(x_1, \ldots, x_d) = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ x_1 & x_2 & \ldots & x_d \\ x_1^2 & x_2^2 & \ldots & x_d^2 \\ \vdots & \vdots & & \vdots \\ x_1^{d-1} & x_2^{d-1} & \ldots & x_d^{d-1} \end{pmatrix}$$

Pick a basis of $\overline{L} \otimes_L V$ over which the matrices of u and v are respectively $\mathrm{Diag}(\alpha_1, \ldots, \alpha_d)$ and $\mathrm{Diag}(\beta_1, \ldots, \beta_d)$. Let $T = \big(\mathrm{Tr}(u^i v^j)\big)_{i,j} \in M_d(K)$. We have

$$\mathrm{V}(\alpha_1, \ldots, \alpha_d)\mathrm{V}(\beta_1, \ldots, \beta_d)^t = T$$

where M^t is the transpose of M. But $\mathrm{V}(\alpha_1, \ldots, \alpha_d)$ is invertible as the α_i's are distinct. So $\mathrm{V}(\beta_1, \ldots, \beta_d)^t = \mathrm{V}(\alpha_1, \ldots, \alpha_d)^{-1} T$, hence $\beta_r \in K(\alpha_1, \ldots, \alpha_d)$ for all $1 \leq r \leq d$. □

4.2. **An arithmetic invariant.** *All the Weil representations considered in this section are over a finite unramified extension of $\mathbb{Q}_p$ and assumed to be semisimple, defined over $\mathbb{Q}$, and tame.* By subobjects we mean subrepresentations defined over $\mathbb{Q}$. For such an object $\Delta = (\Delta, \rho)$ over K_0 we fix the following notations. Let ϕ_0 be the image by ρ of a lifting of the geometric Frobenius and θ a generator of $\rho(I)$. Then $\mathrm{Im}\,\rho = \langle \phi_0, \theta\rangle$ with the relation $\phi_0 \theta = \theta^p \phi_0$. The algebra $\mathbb{Q}[\phi_0, \theta] \subset \mathrm{End}_{K_0}(\Delta)$ spanned over $\mathbb{Q}$ by $\mathrm{Im}\,\rho$ is finite dimensional over $\mathbb{Q}$ (because Δ is defined over $\mathbb{Q}$) and semisimple (because Δ is).

As usual $\zeta_r \in \overline{\mathbb{Q}}$ is a primitive rth root of unity and Φ_r is the rth cyclotomic polynomial. The following result is a representation analogue of proposition 3.9.

Proposition 4.4. *An object Δ decomposes as*

$$\Delta = \bigoplus_{(r;\pi)\in S(\Delta)} \Delta(r;\pi)$$

where $S(\Delta)$ is a finite set of elements $(r;\pi)$ with r an integer prime to p, $\pi \in \overline{\mathbb{Q}}$ a root of $\mathrm{P}_{\min}(\phi_0^s)$, $s = \mathrm{ord}\big(p \in (\mathbb{Z}/r\mathbb{Z})^\times\big)$, and $\Delta(r;\pi)$ is a subobject enjoying the following properties:

(a) $\mathrm{P}_{\min}(\theta) = \Phi_r$ *and* $Z(\mathbb{Q}[\phi_0,\theta]) \simeq L =$ *a number field,*
(b) $[F(\zeta_r):\mathbb{Q}]$ *divides* $\dim \Delta(r;\pi)$, *with* $F = \mathbb{Q}(\pi)$,
(c) $\mathrm{Gal}(F(\zeta_r)/F)$ *contains an element σ_p such that $\sigma_p(\zeta_r) = {\zeta_r}^p$, and*
(d) $\mathbb{Q}[\phi_0,\theta] \simeq \big(F(\zeta_r)/L, \sigma_p, \pi\big)$ *by $\theta \mapsto \zeta_r$, $\phi_0 \mapsto u_p$ such that $u_p x u_p^{-1} = \sigma_p(x)$ for all $x \in F(\zeta_r)$ and $u_p^s = \pi$.*

Proof. Δ being semisimple and defined over $\mathbb{Q}$ we have $\mathrm{P}_{\min}(\theta) = \prod_r \Phi_r$ with $r \mid \mathrm{ord}(\theta)$ and $\mathrm{lcm}(\text{all } r) = \mathrm{ord}(\theta)$. As r is prime to p we see that ϕ_0 stabilises each $\mathrm{Ker}\,\Phi_r(\theta)$, and by corollary 4.2 the representation restricted to $\mathrm{Ker}\,\Phi_r(\theta)$ is defined over $\mathbb{Q}$. So we may assume that $\mathrm{P}_{\min}(\theta) = \Phi_r$ for some r. Let s be the order of p in $(\mathbb{Z}/r\mathbb{Z})^\times$. Then we take $K_0 = \mathrm{Frac}\,W(\mathbb{F}_{p^s})$ and $\phi = \phi_0^s$ is the smallest power of ϕ_0 commuting with θ. Again by corollary 4.2 we may assume that $\mathrm{P}_{\min}(u)$ is irreducible in $\mathbb{Q}[X]$ for all u in $Z(\mathbb{Q}[\phi_0,\theta])$, i.e. that the centre of $\mathbb{Q}[\phi_0,\theta]$ is a field. The element ϕ_0 acts by conjugation $c_0 : u \mapsto \phi_0 u \phi_0^{-1}$ on $\mathbb{Q}[\phi,\theta]$ and the same argument as in the proof of proposition 3.9 shows that $\mathbb{Q}[\phi,\theta]$ is a field as well.

Codiagonalise ϕ and θ in $\overline{\mathbb{Q}}_p \otimes_{K_0} \Delta$ and let $\pi \in \overline{\mathbb{Q}}$ be such that π and ζ_r are the eigenvalues, for ϕ and θ respectively, of some common eigenvector. Put $F = \mathbb{Q}(\pi)$. If $u \in \mathbb{Q}[\phi,\theta]$ writes as $u = P(\phi,\theta)$ for some $P \in \mathbb{Q}[X,Y]$ then $\xi = P(\pi,\zeta_r) \in \mathrm{Spec}\,u$. Since $\mathrm{P}_{\min}(u)$ is irreducible in $\mathbb{Q}[X]$ we have

$$\mathrm{P}_{\min}(u) = \mathrm{P}_{\min}(\xi)$$

the right-hand side being the minimal polynomial over $\mathbb{Q}$ of an algebraic number. Pick a primitive element ξ_0 for $F(\zeta_r)/\mathbb{Q}$, i.e. such that $F(\zeta_r) = \mathbb{Q}(\xi_0)$. Let $P_0 \in \mathbb{Q}[X,Y]$ be such that $P_0(\pi,\zeta_r) = \xi_0$ and put $u_0 = P_0(\phi,\theta)$. Then $\mathrm{P}_{\min}(u_0) = \mathrm{P}_{\min}(\xi_0)$, so $\dim_{\mathbb{Q}} \mathbb{Q}[u_0] = [F(\zeta_r):\mathbb{Q}]$ which divides $\dim_{K_0}\Delta$, and $\mathbb{Q}[\phi,\theta] = \mathbb{Q}[u_0]$. The choice of ξ_0 yields a $\mathbb{Q}$-algebra isomorphism

$$\mathbb{Q}[\phi,\theta] \xrightarrow{\sim} F(\zeta_r)$$

mapping u_0 to ξ_0 (thus $\phi \mapsto \pi$ and $\theta \mapsto \zeta_r$). By transport of structure the automorphism c_0 is carried to an element $\sigma_p \in \mathrm{Gal}(F(\zeta_r)/F)$ acting as $\zeta_r \mapsto {\zeta_r}^p$. Hence the above isomorphism identifies $Z(\mathbb{Q}[\phi_0,\theta])$ with the subfield L of $F(\zeta_r)$ fixed by σ_p. Finally we get an isomorphism

$$\mathbb{Q}[\phi_0,\theta] \xrightarrow{\sim} \big(F(\zeta_r)/L, \sigma_p, \pi\big)$$

by sending ϕ_0 to an element u_p such that $u_p x u_p^{-1} = \sigma_p(x)$ for all $x \in F(\zeta_r)$ and $u_p^s = \pi$. □

Remark 4.5. The object $\Delta(r;\pi)$ is determined up to isomorphism by its dimension together with property (d) in proposition 4.4.

Call such a $\Delta(r;\pi)$ $\mathbb{Q}$-*elementary* and $\Delta = \bigoplus_{(r;\pi)\in S(\Delta)} \Delta(r;\pi)$ the $\mathbb{Q}$-*elementary decomposition* of Δ. The $\mathbb{Q}$-elementary decomposition of Δ is unique up to isomorphism.

Now assume that the roots of $\mathrm{P}_{\mathrm{char}}(\phi_0)$ are p-Weil numbers, hence π is a p^s-Weil number. We proceed to define a numerical invariant $n(\Delta)$ attached to Δ. Consider first an invariant attached to a $\mathbb{Q}$-elementary object $\Delta(r;\pi)$ with associated cyclic algebra $\big(F(\zeta_r)/L, \sigma_p, \pi\big)$ as in proposition 4.4. Put $n(1;\pi) = n(2;\pi) = 1$, and for $r \geq 3$ recall that we have introduced in section 2.2 the integer

$$n(r;\pi) \underset{\text{def}}{=} \mathrm{lcm}\Big(\, n_v(r;\pi), \, v \text{ place of } L \, \Big)$$

with $n_v(r;\pi) =$ order of π modulo the norm group of $F(\zeta_r)_v/L_v$ if v lies above $\ell \neq p$ and ℓ divides r, $n_v(r;\pi) = 2$ if $L_v = \mathbb{R}$ and $\pi = p^{s/2}$, s even, and $n_v(r;\pi) = 1$ otherwise. We further define

$$n(\Delta) \underset{\text{def}}{=} \mathrm{lcm}\left(\, \frac{n(r;\pi)}{\gcd\Big(n(r;\pi), \, \frac{\dim \Delta(r;\pi)}{[\mathbb{Q}(\zeta_r,\pi):\mathbb{Q}]}\Big)} \, , \quad (r;\pi) \in S(\Delta) \, \right).$$

It is an invariant of the isomorphism class of Δ.

Definition 4.6. The object Δ is of *Tate type* if $n(\Delta) = 1$.

Equivalently, Δ is of Tate type if each object $\Delta(r;\pi)$ of its $\mathbb{Q}$-elementary decomposition has dimension divisible by $[\mathbb{Q}(\zeta_r,\pi):\mathbb{Q}]n(r;\pi)$.

Remark 4.7. Any Δ on which I acts trivially is of Tate type.

Remark 4.8. The object $n\Delta = \Delta \oplus \cdots \oplus \Delta$ (n times) is of Tate type if and only if n divides $n(\Delta)$. In particular $n(\Delta)$ is the smallest integer n such that $n\Delta$ is of Tate type.

The introduction of the invariant $n(\Delta)$ and definition 4.6 are motivated by the following result.

Proposition 4.9. *Let $(A_0, \langle\tau\rangle, \nu)$ be a tame Galois pair and $\Delta(A)$ its associated Weil representation. Then $\Delta(A)$ is of Tate type.*

Proof. The splitting of $(A_0, \langle\tau\rangle, \nu)$ up to isogeny into a product of cyclic Galois pairs as in propsition 3.9 corresponds to the $\mathbb{Q}$-elementary decomposition of $\Delta(A)$ up to isomorphism. If $(A_0, \langle\tau\rangle, \nu)$ is cyclic with $\mathbb{Q}[\mathsf{f}_0, \tau] \simeq \big(F(\zeta_r)/L, \sigma_p, \pi\big)$ then $\Delta(A)$ is isomorphic to a $\mathbb{Q}$-elementary $\Delta(r;\pi)$. It then follows from proposition 2.5 that $[F(\zeta_r) : \mathbb{Q}]n(r;\pi)$ divides $[F:\mathbb{Q}] \deg \mathrm{End}^{\circ}_{\mathbb{F}_{p^s}}(A) = \dim \Delta(A)$. □

Remark 4.10. Say Δ is ℓ-*adically realisable* if there exists a compatible system $(\Delta_\ell)_\ell$ of ℓ-adic Weil representations (see 1.1.3), ℓ running over all rational primes, such that $\Delta \simeq \Delta_p$. Using lemma 2.2, one checks that Δ is of Tate type if and only if it is ℓ-adically realisable and $2\,\mathrm{ord}(\mathbb{Z}/r\mathbb{Z})^\times$ divides $\dim \Delta(r;p^{s/2})$ for each $\mathbb{Q}$-elementary subobject $\Delta(r;p^{s/2})$ with $r \geq 3$ and L totally real.

4.3. **Tame representations arising from Galois pairs.** Let $K/\mathbb{Q}_p$ be a finite tame Galois extension with maximal unramified subfield K_0. We have $\mathrm{Gal}(K/\mathbb{Q}_p) \simeq I(K/\mathbb{Q}_p) \rtimes \mathrm{Gal}(K_0/\mathbb{Q}_p)$. Let D be a $\big(\varphi, \mathrm{Gal}(K/\mathbb{Q}_p)\big)$-module. Recall that the restriction of φ on the sub-$\mathbb{Q}_p$-vector space of D consisting of elements fixed by $\mathrm{Gal}(K_0/\mathbb{Q}_p)$ is a $\mathbb{Q}_p$-linear isomorphism φ_0. Consider the following conditions on D:

(1) φ_0 acts semisimply and $\mathrm{P}_{\mathrm{char}}(\varphi_0)$ is a p-Weil polynomial
(2) $\mathbf{W}(D)$ is defined over $\mathbb{Q}$ and of Tate type
(3) There exists a nondegenerate skew form $D \times D \to K_0\{-1\}$.

The skew form in (3) is to be understood in the category of $\big(\varphi, \mathrm{Gal}(K/\mathbb{Q}_p)\big)$-modules: φ_0 is a p-similitude (i.e. $\langle \varphi x, \varphi y\rangle = p\langle x, y\rangle$ for all $x, y \in D$) and $I(K/\mathbb{Q}_p)$ acts by isometries. The semisimplicity condition in (1) is equivalent to $\mathbf{W}(D)$ being semisimple.

Theorem 4.11. *Let $K/\mathbb{Q}_p$ be a finite tame Galois extension and D a $\big(\varphi, \mathrm{Gal}(K/\mathbb{Q}_p)\big)$-module. The following are equivalent:*

(i) *There exists a Galois pair $(A_0, \langle\tau\rangle, \nu)$ for $K/\mathbb{Q}_p$ such that $D \simeq D(A)$*
(ii) *D satisfies conditions* (1), (2), *and* (3).

In other words, a tame $\big(\varphi, \mathrm{Gal}(K/\mathbb{Q}_p)\big)$-module satisfying (1) is "geometric" if and only if it also satisfies (2) and (3). There is an obvious equivalent description for Weil representations.

Proof. Let $D(A)$ be the $\big(\varphi, \mathrm{Gal}(K/\mathbb{Q}_p)\big)$-module attached to a tame Galois pair for $K/\mathbb{Q}_p$. It is known that $D(A)$ satisfies (1) (cf. 2.1) and is defined over $\mathbb{Q}$ ([Se-Ta] Cor. to Thm.3). Proposition 4.9 shows that it is of Tate type and proposition 5.3 that it satisfies (3).

Now let D be a $\big(\varphi, \mathrm{Gal}(K/\mathbb{Q}_p)\big)$-module satisfying conditions (1), (2), and (3). Clearly we may work with Weil representations, i.e. it is enough to show the existence of a tame Galois pair $(A_0, \langle\tau\rangle, \nu)$ for $K/\mathbb{Q}_p$ such that $\mathbf{W}(D) = \Delta \simeq \Delta(A)$. Recall that $\phi_0 = \mathbf{W}(\varphi_0)$. Let $\Delta = \bigoplus \Delta(r;\pi)$ be the $\mathbb{Q}$-elementary decomposition as in proposition 4.4. The W-equivariant nondegenerate skew form $\Delta \times \Delta \to K_0\{-1\}$ furnished by condition (3) yields a linear automorphism ψ of Δ such that $p\psi\phi_0^{-1} = \phi_0\psi$ and $\psi\theta = \theta\psi$ (and conversely ψ determines the skew form). These relations show that $\psi\big(\Delta(r; p^s\pi^{-1})\big) = \Delta(r;\pi)$, with $s = \mathrm{ord}\big(p \in (\mathbb{Z}/r\mathbb{Z})^\times\big)$, and so the restriction of the skew form to each $\Delta(r;\pi)$ is nondegenerate. In particular the restriction of ϕ_0 is a symplectic p-similitude, which implies that $\mathrm{P}_{\mathrm{char}}(\phi_0)$ remains a p-Weil polynomial on $\Delta(r;\pi)$. Indeed, all we have to check is that its valuation at $X^2 - p$ stays even (see definiton 2.1); but if it wasn't the case the determinant would be $-p^n$ for some n, a contradiction. Hence we may assume that $\Delta = \Delta(r;\pi)$ and $K_0 = \mathrm{Frac}\, W(\mathbb{F}_{p^s})$ with $s = \mathrm{ord}\big(p \in (\mathbb{Z}/r\mathbb{Z})^\times\big)$.

Condition (1) implies the existence of an abelian variety A_0 over $\mathbb{F}_p$ such that $\mathrm{P}_{\mathrm{char}}(\mathsf{f}_0) = \mathrm{P}_{\mathrm{char}}(\phi_0)$. If $r = 1$ or 2 we obviously take $\tau = 1$ and $\tau = -1$ respectively, so we may assume $r \geq 3$. We have $\mathrm{P}_{\mathrm{char}}(\mathsf{f}) = \mathrm{P}_{\mathrm{char}}(\phi_0^s) = \mathrm{P}_{\min}(\pi)^m$ for some integer m. Put $F = \mathbb{Q}(\pi)$ and let δ be the invariant attached to the p^s-Weil number π (see 2.1). By lemmas 2.4 and 4.4 (b) we have the chain divisibility

$$\delta \;\mid\; [F(\zeta_r) : F] \;\mid\; m = \frac{\dim \Delta}{[F : \mathbb{Q}]}.$$

Since $\mathrm{P}_{\min}(\pi)$ is irreducible A is isogenous to the (m/δ)th power of some simple abelian variety over $\mathbb{F}_{p^s}$ with Honda-Tate division algebra D of degree δ over F. Thus

$$\mathrm{End}^\circ_{\mathbb{F}_{p^s}}(A) = M_{m/\delta}(D).$$

Condition (2) means that $[F(\zeta_r) : F]n(r;\pi)$ divides m, the degree of $\mathrm{End}^\circ_{\mathbb{F}_{p^s}}(A)$. Proposition 2.5 then implies the existence of an embedding

$$\iota : \big(F(\zeta_r)/L, \sigma_p, \pi\big) \hookrightarrow \mathrm{End}^\circ_{\mathbb{F}_{p^s}}(A)$$

such that $\iota(u_p) = \mathsf{f}_0$, where $u_p \in \big(F(\zeta_r)/L, \sigma_p, \pi\big)$ satisfies $u_p x u_p^{-1} = \sigma_p(x)$ for all $x \in F(\zeta_r)$ and $u_p^s = \pi$. Let $\tau = \iota(\zeta_r)$. By Waterhouse's result [Wa] Thm.3.13 any maximal order in $\mathrm{End}^\circ_{\mathbb{F}_{p^s}}(A)$ containing both f_0 and τ is the endomorphism ring over $\mathbb{F}_{p^s}$ of an abelian variety, which is defined over $\mathbb{F}_p$ and isogenous to A_0. Replacing A_0 by it we obtain $\tau \in \mathrm{Aut}_{\mathbb{F}_{p^s}}(A)$. Define an antimorphism $\rho : W \to \mathrm{End}^\circ_{\mathbb{F}_{p^s}}(A)^\times$ by setting $\rho(I_K) = 1$ and sending an element of W acting on Δ as θ (resp. ϕ_0) to τ (resp. f_0). Let $\nu : \mathrm{Gal}(K/\mathbb{Q}_p) \to \mathrm{Ist}_{\mathbb{F}_{p^s}}(A)$ be deduced from ρ (as in section 3.2). Then $(A_0, \langle\tau\rangle, \nu)$ is a (minimal) Galois pair for $K/\mathbb{Q}_p$ such that $\Delta(A) \simeq \Delta$. □

Consider now a condition weaker than (2) on a $\big(\varphi, \mathrm{Gal}(K/\mathbb{Q}_p)\big)$-module D:

$$(2') \quad \mathbf{W}(D) \text{ is defined over } \mathbb{Q}.$$

Writting $n(D)$ for the invariant $n\big(\mathbf{W}(D)\big)$ of definition 4.6, the remark 4.8 leads to an alternate formulation of theorem 4.11.

Corollary 4.12. *Let D be a tame $\big(\varphi, \mathrm{Gal}(K/\mathbb{Q}_p)\big)$-module. The following are equivalent:*

(i) *There exists a positive integer n such that $nD \simeq D(A)$ for some Galois pair $(A_0, \langle\tau\rangle, \nu)$ for $K/\mathbb{Q}_p$*
(ii) *D satisfies conditions* (1), (2′), *and* (3).

Moreover when (ii) *holds the integers n as in* (i) *are the multiples of $n(D)$.*

4.4. **Some examples in low dimension.** We keep the notations of section 4.3 and let Δ be a tame Weil representation satisfying conditions (1), (2), and (3). In each of the cases below we exhibit an abelian variety A_0 with automorphism τ, from which one deduces as in the proof of theorem 4.11 a minimal Galois pair $(A_0, \langle\tau\rangle, \nu)$ such that $\Delta(A) \simeq \Delta$.

4.4.1. *Elliptic curves.* Let Δ be 2-dimensional with $\mathrm{P}_{\mathrm{char}}(\theta) = \Phi_e$ and $e \in \{3, 4, 6\}$. The order of p in $(\mathbb{Z}/e\mathbb{Z})^\times$ is either 1 or 2. Let $A_0 = E/\mathbb{F}_p$ be an elliptic curve whose Frobenius has characteristic polynomial $\mathrm{P}_{\mathrm{char}}(\phi_0)$. Recall that E is ordinary if $\mathrm{Tr}(\phi_0)$ is prime to p and supersingular otherwise.

If $p \equiv 1 \bmod e\mathbb{Z}$ the representation is abelian and lemma 4.3 implies $\mathrm{End}^\circ_{\mathbb{F}_p}(E) = \mathbb{Q}(\zeta_e)$. This is a quadratic extension of $\mathbb{Q}$ unramified at p, so $\mathrm{Tr}(\phi_0)$ is prime to p and E is ordinary. Then $\tau = \zeta_e$ or ζ_e^{-1} (yielding nonisomorphic representations).

If $p \equiv -1 \bmod e\mathbb{Z}$ the relation $\phi_0\theta = \theta^{-1}\phi_0$ implies $\mathrm{Tr}(\phi_0) = 0$. Thus E is supersingular with $\zeta_e \in \mathrm{End}^\circ_{\mathbb{F}_{p^2}}(E) = \mathcal{D}_{p,\infty}$. Then we may take $\tau = \zeta_e$ (taking ζ_e^{-1} yields an isomorphic representation).

An explicit description of the Weil representations arising from elliptic curves over $\mathbb{F}_p$ when $p > 3$ can be found in [Vo] 2.1.

4.4.2. *The product of two supersingular elliptic curves.* Let Δ be 4-dimensional with $\mathrm{P}_{\mathrm{char}}(\theta) = \Phi_8$ (so $p \neq 2$) and $\mathrm{P}_{\mathrm{char}}(\phi_0)(X) = (X^2 + p)^2$. Let $E/\mathbb{F}_p$ be a supersingular elliptic curve whose Frobenius has characteristic polynomial $X^2 + p$. We have $\mathrm{End}^\circ_{\mathbb{F}_p}(E) = \mathbb{Q}(\sqrt{-p})$ and $\mathrm{End}^\circ_{\mathbb{F}_{p^2}}(E) = \mathcal{D}_{p,\infty}$. Take $A_0 = E \times E$, so $\mathrm{End}^\circ_{\mathbb{F}_{p^2}}(A_0) = M_2(\mathcal{D}_{p,\infty})$.

If $p \equiv 1 \bmod 8$ then lemma 4.3 implies $\mathbb{Q}(\sqrt{-p}) \subset \mathbb{Q}(\zeta_8)$, which is impossible since $\mathbb{Q}(\zeta_8)$ is unramified at p.

If $p \equiv 3 \bmod 8$ then $\zeta_4 \in \mathcal{D}_{p,\infty}$ and we may take $\tau = \begin{pmatrix} 0 & -\frac{1}{2}+\frac{1}{2}\zeta_4 \\ 1-\zeta_4 & 0 \end{pmatrix}$.

If $p \equiv 5 \bmod 8$ then $\xi \in \mathcal{D}_{p,\infty}$ with $\xi^2+2=0$ and we may take $\tau = \begin{pmatrix} \xi^{-1} & \xi^{-1} \\ -\xi^{-1} & \xi^{-1} \end{pmatrix}$.

If $p \equiv -1 \bmod 8$ then $\zeta_4 \in \mathcal{D}_{p,\infty}$ and we may take $\tau = \begin{pmatrix} 0 & \frac{1}{2}+\frac{1}{2}\zeta_4 \\ 1+\zeta_4 & 0 \end{pmatrix}$.

5. Representations arising from abelian varieties over $\mathbb{Q}_p$

We now proceed to describe the p-adic representations of G arising from abelian varieties with tame potential good reduction. In order to achieve this we want to lift abelian varieties over finite fields to characteristic 0 and then descend them to $\mathbb{Q}_p$. As the appropriate descent theory is available (see 1.2.2), we are here mainly concerned by the lifting procedure, which involves polarisations. Polarisations over finite fields are handled via Rosati involutions, as explained in section 5.1. In section 5.2 we show that a tame Galois pair can be polarised (proposition 5.3). In section 5.3 we show that when the $\big(\varphi, \mathrm{Gal}(K/\mathbb{Q}_p)\big)$-module attached to a tame Galois pair admits a symplectic lift, there exists a polarisation λ on the Galois pair and an isomorphic lift of the pair (D,λ) (proposition 5.5). We finally prove our main result in section 5.4 (theorem 5.7).

5.1. **Polarisations and Rosati involutions.** Let k be a finite extension of $\mathbb{F}_p$ and A/k an abelian variety. Fix a polarisation $\lambda = \lambda_{\mathcal{L}} : A \to A^\vee$ induced by an ample invertible sheaf $\mathcal{L}$ on A ([Mi] Rmk.13.2). The associated Rosati involution $\dagger$ on $\mathrm{End}_k^\circ(A)$ is

$$\alpha \mapsto \alpha^\dagger = \lambda^{-1}\alpha^\vee\lambda.$$

It is positive definite, i.e. the bilinear form $(\alpha,\beta) \mapsto \mathrm{Tr}(\alpha^\dagger\beta)$ is. If $\alpha^\dagger = \alpha$ then all the roots of its reduced characteristic polynomial $\mathrm{Prd}(\alpha)$ lie in $\mathbb{R}$. Write $\mathrm{End}_k^\circ(A)^\dagger$ for the sub-$\mathbb{Q}$-vector space of $\mathrm{End}_k^\circ(A)$ consisting of elements fixed by $\dagger$ and define

$$\mathrm{Pol}(A) \underset{\text{def}}{=} \{\alpha \in \mathrm{End}_k^\circ(A)^\dagger \mid \mathrm{Roots}\big(\mathrm{Prd}(\alpha)\big) \subset \mathbb{R}_{>0}\}.$$

All polarisations in $\mathrm{Hom}_k^\circ(A,A^\vee)$, i.e. elements μ such that $m\mu$ is a polarisation on A for some positive integer m, have the form

$$\mu = \lambda\,\alpha \quad \text{for some } \alpha \in \mathrm{Pol}(A).$$

Indeed, an isogeny $\mu : A \to A^\vee$ is induced by an invertible sheaf $\mathcal{M}$ if and only if $\lambda^{-1}\mu$ is fixed by $\dagger$ ([Mi] Prop.17.2); this is equivalent to μ being symmetric, i.e. $\mu^\vee = \mu$ under $A^{\vee\vee} \simeq A$. Then $\mathcal{M}$ is ample if and only if all the roots of $\mathrm{Prd}(\lambda^{-1}\mu)$ are positive ([Mu] 21, application III, top of p.210).

If $D = D(A)$ then $D(A^\vee) = D^*\{-1\}$ and λ yields an isomorphism of φ-modules

$$\delta = D(\lambda) : D^*\{-1\} \xrightarrow{\sim} D \quad \text{such that} \quad \delta^*\{-1\} = -\delta$$

(under the canonical identification $\big(D^*\{-1\}\big)^*\{-1\} \simeq D$). Indeed, a symmetric morphism such as λ becomes antisymmetric when passing to p-divisible groups, since $A^\vee(p)$ is the Cartier dual of $A(p)$. Thus Tate's isomorphism restricts to

$$\mathbb{Q}_p \otimes_{\mathbb{Q}} \mathrm{Hom}_k^{\mathrm{s}}(A,A^\vee) \simeq \mathrm{Hom}_\varphi^{\mathrm{a}}(D^*\{-1\}, D)$$

where the superscripts "s" and "a" stand respectively for "symmetric" in $\mathrm{Hom}_k^\circ(A, A^\vee)$ and "antisymmetric". As usual δ defines a nondegenerate alternating form in the category of φ-modules $b : D \times D \to K_0\{-1\}$, with $K_0 = \mathrm{Frac}\, W(k)$ and $b(\varphi x, \varphi y) = (\#k)b(x, y)$, and conversely b determines δ.

The Rosati involution extends by linearity to $\mathbb{Q}_p \otimes_{\mathbb{Q}} \mathrm{End}_k^\circ(A)$ and yields an involution also denoted $\dagger$ on $\mathrm{End}_\varphi(D)$, given by $\alpha^\dagger = \delta\alpha^*\{-1\}\delta^{-1}$. The sub-$\mathbb{Q}_p$-vector space $\mathrm{End}_\varphi(D)^\dagger$ of elements fixed by $\dagger$ is equipped with the p-adic topology.

Lemma 5.1. *The image of* $\mathrm{Pol}(A)$ *in* $\mathrm{End}_\varphi(D)^\dagger$ *is dense.*

Proof. If $x \in \mathrm{End}_k^\circ(A)^\dagger$ then $x + p^n \,\mathrm{Id} \in \mathrm{Pol}(A)$ for a sufficiently large integer n. Therefore $\mathrm{Pol}(A)$ is dense in $\mathrm{End}_k^\circ(A)^\dagger$ with respect to the p-adic topology. The lemma then follows from Tate's theorem $\mathbb{Q}_p \otimes_{\mathbb{Q}} \mathrm{End}_k^\circ(A)^\dagger \simeq \mathrm{End}_\varphi(D)^\dagger$. □

Let E be a finite dimensional semisimple $\mathbb{Q}_p$-algebra and $\dagger$ any involution on E fixing $\mathbb{Q}_p$. The group $E^\times$ acts on the $\mathbb{Q}_p$-vector space $E^\dagger$ by $\gamma \mapsto \alpha\gamma\alpha^\dagger$, $\gamma \in E^\dagger$, $\alpha \in E^\times$. The proof of the following lemma is left to the reader.

Lemma 5.2. *The orbit of an invertible element in* $E^\dagger$ *under the above action of* $E^\times$ *is open in the p-adic topology.*

5.2. **Polarisable Galois pairs.** Let $K/\mathbb{Q}_p$ be a finite Galois extension with residue field $\mathbb{F}_{p^s}$ and (A_0, Γ, ν) a Galois pair for $K/\mathbb{Q}_p$. Recall from section 3.1 that a polarisation on (A_0, Γ, ν) is an $\mathbb{F}_p$-polarisation on A_0 such that $\Gamma \subseteq \mathrm{Aut}(A, \lambda)$. A Galois pair is polarisable when there exists a polarisation on it.

Proposition 5.3. *A tame Galois pair is polarisable.*

Proof. Let $(A_0, \langle\tau\rangle, \nu)$ be a tame Galois pair for $K/\mathbb{Q}_p$. By proposition 3.9 we may assume it to be cyclic, so $\mathrm{End}_{\mathbb{F}_{p^s}}^\circ(A)$ is central simple over F. Pick any $\mathbb{F}_p$-polarisation λ_0 on A_0 with associated Rosati involution $\dagger$. Define $\mathcal{I}_0^+$ to be the set of positive definite involutions on $\mathrm{End}_{\mathbb{F}_{p^s}}^\circ(A)$ coinciding with $\dagger$ on F (thus having same kind), having same type as $\dagger$ (in case it is of the first kind), and stabilising $\mathrm{End}_{\mathbb{F}_p}^\circ(A_0)$. We have a map

$$\begin{cases} \mathrm{Pol}(A_0) & \to & \mathcal{I}_0^+ \\ \alpha & \mapsto & I_\alpha : x \mapsto \alpha^{-1}x^\dagger\alpha \text{ for all } x \in \mathrm{End}_{\mathbb{F}_{p^s}}^\circ(A) \end{cases}$$

The involution I_α is the Rosati involution associated to the $\mathbb{F}_p$-polarisation $\lambda_0\alpha$. The map $\alpha \mapsto I_\alpha$ is surjective by the Skolem-Noether theorem. Now set

$$\mathrm{Pol}(A_0, \tau) \underset{\text{def}}{=} \{\alpha \in \mathrm{Pol}(A_0) \mid \tau \in \mathrm{Aut}(A, \lambda\alpha)\}.$$

We want to show that $\mathrm{Pol}(A_0, \tau)$ is not empty, since for α in this set $\lambda_0\alpha$ is an appropriate polarisation. Put

$$\mathcal{I}_{0,\tau}^+ \underset{\text{def}}{=} \{ \text{ involutions } \ddagger \in \mathcal{I}_0^+ \mid \tau^\ddagger\tau = 1\}.$$

Obviously the above map carries $\mathrm{Pol}(A_0, \tau)$ onto $\mathcal{I}_{0,\tau}^+$, hence it is enough to show that $\mathcal{I}_{0,\tau}^+$ is nonempty. Define a positive definite involution $'$ on $\mathbb{Q}[\mathsf{f}_0, \tau] \subseteq \mathrm{End}_{\mathbb{F}_{p^s}}^\circ(A)$ by setting

$$\mathsf{f}_0' = p\mathsf{f}_0^{-1} \quad \text{and} \quad \tau' = \tau^{-1}.$$

Clearly † and $'$ have the same restriction to F. We claim that by Theorem 4.14 of [BI] the involution $'$ can be extended to an involution on $\mathrm{End}^\circ_{\mathbb{F}_{p^s}}(A)$ belonging to $\mathcal{I}^+_{0,\tau}$. Indeed, since $\mathsf{f}'_0 = p\mathsf{f}_0^{-1}$ any extension of $'$ stabilises $\mathrm{End}^\circ_{\mathbb{F}_p}(A_0)$, and since it is positive definite it can be extended to a positive definite one on $\mathrm{End}^\circ_{\mathbb{F}_{p^s}}(A)$. It remains to check that, in case $'$ is of the first kind (and thus † as well), it can be extended to an involution of the same type as †. So assume $'$ to be of the first kind. Then s must be even and $\mathsf{f} = \pm p^{s/2}$, so $F = \mathbb{Q}$, $\mathbb{Q}[\mathsf{f}_0, \tau] \simeq \big(\mathbb{Q}(\zeta_r)/L, \sigma_p, \pm p^{s/2}\big)$ with the notations of proposition 3.9, and

$$\mathrm{End}^\circ_{\mathbb{F}_{p^s}}(A) = M_n(\mathcal{D}_{p,\infty}) \quad \text{for some integer } n.$$

The involution † on $M_n(\mathcal{D}_{p,\infty})$ has symplectic type. On the other hand $'$ is symplectic if $\mathsf{f} = -p^{s/2}$ and orthogonal if $\mathsf{f} = p^{s/2}$. According to Theorem 4.14 of [BI] we need to check in the latter case that the degree of the centraliser C of $\big(\mathbb{Q}(\zeta_r)/L, \sigma_p, p^{s/2}\big)$ in $M_n(\mathcal{D}_{p,\infty})$ is even, for then $'$ can be extended to a symplectic involution. Writting $\boldsymbol{\varphi}$ for the Euler function, we have $\deg_L C = 2n/\boldsymbol{\varphi}(r)$. Now L is totally real of degree $\boldsymbol{\varphi}(r)/s$ over $\mathbb{Q}$ and $p^{s/2}$ is positive, so

$$\mathbb{R} \otimes_{\mathbb{Q}} \big(\mathbb{Q}(\zeta_r)/L, \sigma_p, p^{s/2}\big) \simeq \Big(\mathbb{R} \otimes_L \big(\mathbb{Q}(\zeta_r)/L, \sigma_p, p^{s/2}\big)\Big)^{\boldsymbol{\varphi}(r)/s} \simeq M_s(\mathbb{R})^{\boldsymbol{\varphi}(r)/s}.$$

Therefore there is an embedding $M_s(\mathbb{R})^{\boldsymbol{\varphi}(r)/s} \hookrightarrow M_n(\mathbb{H}) \simeq \mathbb{R} \otimes_{\mathbb{Q}} M_n(\mathcal{D}_{p,\infty})$, which by lemma 2.2 implies that $\frac{\boldsymbol{\varphi}(r)}{s} s = \boldsymbol{\varphi}(r)$ divides n. Thus $\deg_L C$ is even. □

5.3. **Lifting polarisations.** Let $(A_0, \langle\tau\rangle, \nu)$ be a tame Galois pair for $K/\mathbb{Q}_p$. Proposition 5.3 allows us to pick a polarisation μ_0 on $(A_0, \langle\tau\rangle, \nu)$. Let † be the Rosati involution attached to μ_0. These data will be fixed throughout the rest of this section, as well as the notations $\mathrm{End}^\circ_{\mathbb{F}_p,\tau}(A_0) = \{\, x_0 \in \mathrm{End}^\circ_{\mathbb{F}_p}(A_0) \mid x\tau = \tau x \,\}$, $D_0 = D(A_0)$, $D = D(A)$, $K_0 = \mathrm{Frac}\, W(\mathbb{F}_{p^s})$, superscripts "s" and "a" for "symmetric" and "antisymmetric".

The relation $\tau^\dagger\tau = 1$ implies that $\mathrm{End}^\circ_{\mathbb{F}_p,\tau}(A_0)$ and $\mathrm{End}_{\varphi,\mathrm{Gal}(K/\mathbb{Q}_p)}(D)$ are stable by †. Put

$$\mathrm{Hom}^{\mathrm{s}}_{\mathbb{F}_p,\tau}(A_0, A_0^\vee) \underset{\text{def}}{=} \{\, f \in \mathrm{Hom}^{\mathrm{s}}_{\mathbb{F}_p}(A_0, A_0^\vee) \mid f\tau^{-1} = \tau^\vee f \,\}.$$

The isomorphism $\mathrm{End}^\circ_{\mathbb{F}_p}(A_0)^\dagger \xrightarrow{\sim} \mathrm{Hom}^{\mathrm{s}}_{\mathbb{F}_p}(A_0, A_0^\vee)$ given by $x \mapsto \mu_0 x$ carries $\mathrm{End}^\circ_{\mathbb{F}_p,\tau}(A_0)^\dagger$ into $\mathrm{Hom}^{\mathrm{s}}_{\mathbb{F}_p,\tau}(A_0, A_0^\vee)$, again because $\tau^\dagger\tau = 1$. We have a commutative diagram

$$\begin{array}{ccccc}
\mathrm{End}^\circ_{\mathbb{F}_p,\tau}(A_0)^\dagger & \xhookrightarrow[\text{can}]{} & \mathbb{Q}_p \otimes_{\mathbb{Q}} \mathrm{End}^\circ_{\mathbb{F}_p,\tau}(A_0)^\dagger & \xrightarrow{\sim} & \mathrm{End}_{\varphi,\mathrm{Gal}(K/\mathbb{Q}_p)}(D)^\dagger \\
\downarrow\wr & & \downarrow\wr & & \downarrow\wr \\
\mathrm{Hom}^{\mathrm{s}}_{\mathbb{F}_p,\tau}(A_0, A_0^\vee) & \xhookrightarrow[\text{can}]{} & \mathbb{Q}_p \otimes_{\mathbb{Q}} \mathrm{Hom}^{\mathrm{s}}_{\mathbb{F}_p,\tau}(A_0, A_0^\vee) & \xrightarrow{\sim} & \mathrm{Hom}^{\mathrm{a}}_{\varphi,\mathrm{Gal}(K/\mathbb{Q}_p)}(D^*\{-1\}, D)
\end{array}$$

where the right-hand side vertical isomorphism is given by $\alpha \mapsto \alpha\eta_0$ with $\eta_0 = D(\mu_0)$. The following lemma has been pointed out by O. Bültel.

Lemma 5.4. *Assume there is an antisymmetric isomorphism $\delta : D^*\{-1\} \xrightarrow{\sim} D$ of $\big(\varphi, \mathrm{Gal}(K/\mathbb{Q}_p)\big)$-modules. Then there exists an $\alpha \in \mathrm{Aut}_{\varphi,\mathrm{Gal}(K/\mathbb{Q}_p)}(D)$ and a polarisation λ_0 on $(A_0, \langle\tau\rangle, \nu)$ such that $\alpha\delta\alpha^* = D(\lambda)$.*

Proof. Write $\delta = \gamma\eta_0$ with $\gamma \in \mathrm{Aut}_{\varphi,\mathrm{Gal}(K/\mathbb{Q}_p)}(D)^\dagger$. Recall that $\mathrm{Pol}(A_0,\tau)$ is the set of $\alpha \in \mathrm{Pol}(A_0)$ such that $\tau \in \mathrm{Aut}(A, \mu_0\alpha)$, so that the map $\beta \mapsto \mu_0\beta$ identifies $\mathrm{Pol}(A_0,\tau)$ with the set of polarisations λ_0 on $(A_0, \langle\tau\rangle, \nu)$ (up to a positive integer). Now since $\tau^\dagger = \tau^{-1}$ we have

$$\mathrm{Pol}(A_0,\tau) = \mathrm{Pol}(A_0) \cap \mathrm{End}^\circ_{\mathbb{F}_p,\tau}(A_0) \subseteq \mathrm{End}^\circ_{\mathbb{F}_p,\tau}(A_0)^\dagger.$$

The same argument as in lemma 5.1 shows that the image of $\mathrm{Pol}(A_0,\tau)$ is dense in $\mathrm{End}_{\varphi,\mathrm{Gal}(K/\mathbb{Q}_p)}(D)^\dagger$. Also, the group $\mathrm{Aut}_{\varphi,\mathrm{Gal}(K/\mathbb{Q}_p)}(D)$ acts on $\mathrm{End}_{\varphi,\mathrm{Gal}(K/\mathbb{Q}_p)}(D)^\dagger$ by $\xi \mapsto \alpha\xi\alpha^\dagger$, $\xi \in \mathrm{End}_{\varphi,\mathrm{Gal}(K/\mathbb{Q}_p)}(D)^\dagger$, $\alpha \in \mathrm{Aut}_{\varphi,\mathrm{Gal}(K/\mathbb{Q}_p)}(D)$, and by lemma 5.2 the orbit of γ is open. These two facts imply the existence of an $\alpha \in \mathrm{Aut}_{\varphi,\mathrm{Gal}(K/\mathbb{Q}_p)}(D)$ such that

$$\alpha\gamma\alpha^\dagger = D(\beta) \quad \text{for some } \beta \in \mathrm{Pol}(A_0,\tau).$$

Then $\lambda_0 = \mu_0\beta$ is the required polarisation as $D(\lambda) = \alpha\gamma\alpha^\dagger\eta_0 = \alpha\delta\alpha^*$. □

Let (D, Fil) be a filtered $\big(\varphi, \mathrm{Gal}(K/\mathbb{Q}_p)\big)$-module of Hodge-Tate type $(0,1)$. A nondegenerate skew form on (D, Fil) is one such form $D \times D \to K_0\{-1\}$ that is a morphism of $\big(\varphi, \mathrm{Gal}(K/\mathbb{Q}_p)\big)$-modules and for which $\mathrm{Fil}^1 D_K$ is totally isotropic (after extending the scalars to K). Equivalently it is given by an antisymmetric isomorphism of filtered $\big(\varphi, \mathrm{Gal}(K/\mathbb{Q}_p)\big)$-modules

$$\delta : D^*\{-1\} \xrightarrow{\sim} D$$

since $D^*\{-1\}$ has Hodge-Tate type $(0,1)$ with $\mathrm{Fil}^1(D^*\{-1\})_K = (\mathrm{Fil}^1 D_K)^\perp$. Now for $D = D(A)$, say that a polarisation λ_0 on A_0 lifts to (D, Fil) if it induces a (necessarily antisymmetric) isomorphism of filtered $\big(\varphi, \mathrm{Gal}(K/\mathbb{Q}_p)\big)$-modules $D(\lambda) : D^*\{-1\} \xrightarrow{\sim} D$.

Proposition 5.5. *Let $(A_0, \langle\tau\rangle, \nu)$ be a tame Galois pair for $K/\mathbb{Q}_p$ and $D = D(A)$ the associated $\big(\varphi, \mathrm{Gal}(K/\mathbb{Q}_p)\big)$-module. Let $\mathrm{Fil} = (\mathrm{Fil}^i D_K)_{i\in\mathbb{Z}}$ be a Hodge-Tate $(0,1)$ filtration on D_K stable by $\mathrm{Gal}(K/\mathbb{Q}_p)$. Assume there is a nondegenerate skew form on (D, Fil). Then there exists*

(a) *a filtration Fil' on D_K such that $(D, \mathrm{Fil}) \simeq (D, \mathrm{Fil}')$, and*
(b) *a polarisation λ_0 on $(A_0, \langle\tau\rangle, \nu)$ lifting to (D, Fil').*

Proof. The given form induces an antisymmetric isomorphism of filtered $\big(\varphi, \mathrm{Gal}(K/\mathbb{Q}_p)\big)$-modules $\delta : D^*\{-1\} \xrightarrow{\sim} D$. By lemma 5.4 there is a polarisation λ_0 on $(A_0, \langle\tau\rangle, \nu)$ and an $\alpha \in \mathrm{Aut}_{\varphi,\mathrm{Gal}(K/\mathbb{Q}_p)}(D)$ such that $D(\lambda) = \alpha\delta\alpha^*$. Put

$$\mathrm{Fil}' = (\alpha_K \mathrm{Fil}^i D_K)_{i\in\mathbb{Z}}.$$

Obviously α induces an isomorphism $(D, \mathrm{Fil}) \xrightarrow{\sim} (D, \mathrm{Fil}')$ of filtered $\big(\varphi, \mathrm{Gal}(K/\mathbb{Q}_p)\big)$-modules. Furthermore we have

$$(\alpha\delta\alpha^*)_K(\alpha_K \mathrm{Fil}^1 D_K)^\perp = \alpha_K\delta_K(\mathrm{Fil}^1 D_K)^\perp \subseteq \alpha_K \mathrm{Fil}^1 D_K,$$

so $\alpha\delta\alpha^* : D^*\{-1\} \xrightarrow{\sim} D$ is an isomorphism of $\big(\varphi, \mathrm{Gal}(K/\mathbb{Q}_p)\big)$-modules preserving Fil'. □

Remark 5.6. We actually do not need the Hodge-Tate type to be $(0,1)$. However, the existence of an antisymmetric isomorphism of filtered modules $\delta : D^*\{-1\} \xrightarrow{\sim} D$ forces the Hodge-Tate type to be $(-n, n+1)$ for some nonnegative integer n.

5.4. **The main theorem.** Let $K/\mathbb{Q}_p$ be a finite tame Galois extension with maximal unramified subfield K_0 and (D, Fil) a filtered $\big(\varphi, \mathrm{Gal}(K/\mathbb{Q}_p)\big)$-module. As in section 4.3 write φ_0 for the $\mathbb{Q}_p$-linear restriction of φ to the subspace of D consisting of elements fixed by $\mathrm{Gal}(K_0/\mathbb{Q}_p)$. Consider the following conditions on (D, Fil):

(1) φ_0 acts semisimply and $\mathrm{P}_{\mathrm{char}}(\varphi_0)$ is a p-Weil polynomial
(2) $\mathbf{W}(D)$ is defined over $\mathbb{Q}$ and is of Tate type
(3) There exists a nondegenerate skew form $(D, \mathrm{Fil}) \times (D, \mathrm{Fil}) \to K_0\{-1\}$
(4) It has Hodge-Tate type $(0, 1)$.

When $(D, \mathrm{Fil}) \simeq \mathbf{D}^*_{\mathrm{cris},K}(V)$ condition (3) means there exists a G-equivariant symplectic form $V \times V \to \mathbb{Q}_p(1)$. Hence $\bigwedge^{2d} V = \mathbb{Q}_p(d)$ where $\dim V = 2d$, that is, the determinant on V is the the d-th power of the p-adic cyclotomic character.

Theorem 5.7. *Let $p \neq 2$. Let V be a p-adic representation of G that becomes crystalline over a finite tame Galois extension $K/\mathbb{Q}_p$. The following are equivalent:*

(i) *There exists an abelian variety $\mathcal{A}_0$ over $\mathbb{Q}_p$ such that $V \simeq V_p(\mathcal{A}_0)$*
(ii) *$\mathbf{D}^*_{\mathrm{cris},K}(V)$ satisfies conditions* (1), (2), (3), *and* (4).

Proof. Let $(D, \mathrm{Fil}) = \mathbf{D}^*_{\mathrm{cris},K}\big(V_p(\mathcal{A}_0)\big)$ with $\mathcal{A}_0/\mathbb{Q}_p$ an abelian variety having good reduction over K. Theorem 4.11 shows that the $\big(\varphi, \mathrm{Gal}(K/\mathbb{Q}_p)\big)$-module D satisfies (1) and (2). The existence of a polarisation on $\mathcal{A}_0$ implies that (D, Fil) satisfies (3), and it is well-known that the filtration satisfies (4).

Now let $(D, \mathrm{Fil}) = \mathbf{D}^*_{\mathrm{cris},K}(V)$ be a filtered $\big(\varphi, \mathrm{Gal}(K/\mathbb{Q}_p)\big)$-module satisfying (1), (2), (3), and (4). We may assume K to be the Galois closure of a totally ramified tame extension $L/\mathbb{Q}_p$ of minimal degree over which V becomes crystalline. Let $\mathbb{F}_{p^s}$ be the residue field of K and $K_0 = \mathrm{Frac}\, W(\mathbb{F}_{p^s})$. By theorem 4.11 conditions (1), (2), and (3) imply the existence of a Galois pair $(A_0, \langle\tau\rangle, \nu)$ for $K/\mathbb{Q}_p$ such that $D(A) \simeq D$. We may assume $D = D(A)$. By proposition 5.5 condition (3) implies the existence of a polarisation λ_0 on $(A_0, \langle\tau\rangle, \nu)$ lifting to (D, Fil), possibly after replacing the filtration by an isomorphic one. If $\psi_0 : (A_0', \langle\tau'\rangle, \nu') \to (A_0, \langle\tau\rangle, \nu)$ is an isogeny then $\lambda_0' = \psi_0^\vee \lambda_0 \psi_0$ is a polarisation on $(A_0', \langle\tau'\rangle, \nu')$ lifting to $D(\psi)_K(\mathrm{Fil})$. By Breuil's theorem ([Br] Thm.5.3.2) condition (4) and $p \neq 2$ imply the existence of a p-divisible group $\mathcal{G}$ over the ring of integers O_L of L such that $V \simeq V_p(\mathcal{G})$ as G_L-modules, and a by result of Raynaud [Ra] every G_L-stable lattice in V comes from a p-divisible group as well. Therefore, replacing $(A_0, \langle\tau\rangle, \nu)$ by an isogenous Galois pair if necessary, we may assume that $A_0(p)$ lifts to such a p-divisible group over O_L. Let T be a G-stable lattice in V such that

$$T = T_p(\mathcal{G}) \quad \text{with} \quad \mathcal{G} \times_{O_L} \mathbb{F}_p \simeq A_0(p).$$

The polarisation λ_0 induces an antisymmetric isomorphism of G-modules $\xi : V \xrightarrow{\sim} V^*(1)$. Multiplying λ_0 by a suitable power of p we may assume that the restriction of ξ on T yields an injection $\xi : T \hookrightarrow T^*(1)$. By Tate's full faithfulness theorem [Ta2] we have

$$\mathrm{Hom}_{p\text{-div}/O_L}\big(\mathcal{G}, \mathcal{G}^D\big) \simeq \mathrm{Hom}_{\mathbb{Z}_p[G_L]}\big(T, T^*(1)\big)$$

where $\mathcal{G}^D$ is the Cartier dual of $\mathcal{G}$, so $T_p\big(\mathcal{G}^D\big) = T^*(1)$. It follows that the isogeny $\lambda_0(p) : A_0(p) \to A_0^\vee(p) = A_0(p)^D$ induced by λ_0 lifts to a quasipolarisation

$$\Lambda(p) : \mathcal{G} \to \mathcal{G}^D.$$

By the Serre-Tate theory of liftings together with Grothendieck's theorem on algebraisation of formal schemes ([Gr1] 5.4.5) the data $\big(A_0, \lambda_0, \mathcal{G}, \Lambda(p)\big)$ defines an abelian scheme over O_L lifting A_0. Its generic fibre base-changed to K is an abelian variety $\mathcal{A}/K$ with special fibre $A/\mathbb{F}_{p^s}$ and $T \simeq T_p(\mathcal{A})$ as G_K-modules. The action of G_K extends to an action of G on $T_p(\mathcal{A})$ such that G_L acts naturally and G_{K_0} induces an action of $I(K/\mathbb{Q}_p)$ on $D(A)$ coming from $\langle\tau\rangle \subseteq \mathrm{Aut}_{\mathbb{F}_{p^s}}(A)$. Therefore, by theorem 1.2 together with the subsequent comments, $\mathcal{A}$ is defined over $\mathbb{Q}_p$, say $\mathcal{A} = \mathcal{A}_0 \times_{\mathbb{Q}_p} K$, and $V \simeq V_p(\mathcal{A}_0)$ as G-modules. □

Remark 5.8. The compatibility of λ with the descent datum implies in addition that the O_L-polarisation deduced from $\big(\lambda_0, \Lambda(p)\big)$ descends to a $\mathbb{Q}_p$-polarisation on $\mathcal{A}_0$.

Corollary 5.9. *Let $p \neq 2$. A crystalline p-adic representation of G is isomorphic to the Tate module of an abelian variety over $\mathbb{Q}_p$ if and only if its associated filtered module satisfies conditions* (1)*,* (3)*, and* (4) *of theorem* 5.7*.*

Proof. By remark 4.7 a crystalline representation satisfying (1) is of Tate type. □

Corollary 5.10. *Let d be a positive integer and assume $p > 2d+1$. A $2d$-dimensional potentially crystalline p-adic representation of G is isomorphic to the Tate module of an abelian variety over $\mathbb{Q}_p$ if and only if its associated filtered module satisfies conditions* (1)—(4) *of theorem* 5.7*.*

Proof. According to [Se-Ta] §2 Cor.2(a) the action of inertia is tame when $p > 2d+1$. □

Remark 5.11. When V is 2-dimensional conditions (2) and (3) may be replaced respectively by the weaker

(2′) $\mathbf{W}(D)$ is defined over $\mathbb{Q}$
(3′) $\bigwedge^2(D, \mathrm{Fil}) = K_0\{-1\}$

the latter meaning $\bigwedge^2 V = \mathbb{Q}_p(1)$, see [Vo] Thm.5.1. An explicit list of the filtered (φ, G)-modules arising from elliptic curves over $\mathbb{Q}_p$ when $p > 3$ is given in [Vo] 2.2.

Remark 5.12. Let V_ℓ be an ℓ-adic representation of G, $\ell \neq p$, with good reduction over the finite Galois extension $K/\mathbb{Q}_p$. It is determined by its associated contravariant ℓ-adic Weil representation $\Delta_\ell = \mathrm{Hom}_{\mathbb{Q}_\ell[I_K]}(V_\ell, \mathbb{Q}_\ell)$ ([Fo3]). Then V_ℓ is isomorphic to the ℓ-adic Tate module of an abelian variety over $\mathbb{Q}_p$ if and only if there exists an admissible filtered $\big(\varphi, \mathrm{Gal}(K/\mathbb{Q}_p)\big)$-module (D, Fil) satisfying the conditions of theorem 5.7 such that $\mathbf{W}(D) = \Delta_p$ and Δ_ℓ are compatible. This follows from the compatibility of the system $\big(V_\ell(\mathcal{A}_0)\big)_\ell$ where ℓ runs over all primes. Obviously this criterion is not handy. However the results in [No] give some hints in this direction, under the assumption that the ramification degree of K is less than $p-1$ (in particular it is tame and $p \neq 2$).

Finally we derive from corollary 4.12 the following equivalent formulation of theorem 5.7. Recall that condition (2′) is as in remark 5.11.

Theorem 5.13. *Let $p \neq 2$. Let V be a p-adic representation of G that becomes crystalline over a finite tame Galois extension $K/\mathbb{Q}_p$. The following are equivalent:*

(i) *There exists an integer n such that $nV \simeq V_p(\mathcal{A}_0)$ for some abelian variety $\mathcal{A}_0/\mathbb{Q}_p$*
(ii) $\mathbf{D}^*_{\mathrm{cris},K}(V) = (D, \mathrm{Fil})$ *satisfies conditions* (1)*,* (2′)*,* (3)*, and* (4)*.*

Moreover when (ii) *holds the integers n as in* (i) *are the multiples of the invariant $n(D)$ of definition* 4.6*.*

References

[Al] A.A. Albert, *Structure of Algebras*, AMS Coll. Publ. **24** (1939).

[BI] M.-A. Knus, A. Merkurjev, M. Rost and J.-P. Tignol, *The book of involutions*, AMS Coll. Publ. **44** (1998).

[Br] C. Breuil, *Groupes p-divisibles, groupes finis et modules filtrés*, Annals of Math. **152** (2000), 489-549.

[Co-Io] R. Coleman and A. Iovita, *The Frobenius and Monodromy operators for Curves and Abelian Varieties*, Duke Math. J. **97** (1999), 171-215.

[Fo1] J.-M. Fontaine, *Le corps des périodes p-adiques*, in Périodes p-adiques, Astérisque **223**, Soc. Math. de France (1994).

[Fo2] J.-M. Fontaine, *Représentations p-adiques semi-stables*, in Périodes p-adiques, Astérisque **223**, Soc. Math. de France (1994).

[Fo3] J.-M. Fontaine, *Représentations ℓ-adiques potentiellement semi-stables*, in Périodes p-adiques, Astérisque **223**, Soc. Math. de France (1994).

[Fo4] J.-M. Fontaine, *Groupes p-divisibles sur les corps locaux*, Astérisque **47-48**, Soc. Math. de France (1977).

[Fo5] J.-M. Fontaine, *Sur certains types de représentations p-adiques du groupe de Galois d'un corps local ; construction d'un anneau de Barsotti-Tate*, Annals of Math. **115** (1982), 529-577.

[Gr1] A. Grothendieck, *EGA III*, Inst. Hautes Études Sci. Publ. Math. **11** (1961).

[Gr2] A. Grothendieck, *Modèles de Néron et monodromie*, exposé IX in Groupes de monodromie en géométrie algébrique, SGA7 I, Lect. Notes Math. **288**, Springer-Verlag (1972), 313-523.

[Ho-Ta] J. Tate, *Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda)*, Séminaire Bourbaki **352** (1968), 15p.

[Mi] J.S. Milne, *Abelian Varieties*, in Arithmetic Geometry, G. Cornell and J.H. Silverman eds., Springer-Verlag (1986).

[Mu] D. Mumford, *Abelian Varieties*, Oxford Univ. Press (1970).

[No] P. Norman,*Lifting Abelian Varieties*, Invent. Math. **64** (1981), 431-443.

[Pi] R.S. Pierce, *Associative Algebras*, GTM **88**, Springer-Verlag (1982).

[Ra] M. Raynaud, *Schémas en groupes de type* $(p, \dots, p)$, Bull. Soc. Math. de France **102** (1974), 241-280.

[Sc] A.H. Schofield, *Representations of rings over skew fields*, L.M.S. Lect. Notes Series **92**, Cambridge University Press (1985).

[Se-Ta] J.-P. Serre and J. Tate, *Good reduction of abelian varieties*, Annals of Math. **88** (1968), 492-517.

[Si] J.H. Silverman, *The Arithmetic of Elliptic Curves*, GTM **106**, Springer-Verlag (1986).

[Ta1] J. Tate, *Endomorphisms of Abelian Varieties over Finite Fields*, Invent. Math. **2** (1966), 134-144.

[Ta2] J. Tate, *p-Divisible groups*, in Proceedings of a Conference on Local Fields, Driebergen 1966, Springer-Verlag (1967), 158-183.

[Vo] M. Volkov, *Les représentations ℓ-adiques associées aux courbes elliptiques sur* $\mathbb{Q}_p$, J. reine angew. Math. **535** (2001), 65-101.

[Wa] W.C. Waterhouse, *Abelian Varieties over Finite Fields*, Ann. scient. École Norm. Sup. **2** (1969), 521-560.

[Wa-Mi] W.C. Waterhouse and J.S. Milne, *Abelian Varieties over Finite Fields*, in AMS Proceedings of Symposia in Pure Mathematics **XX** (1971), 53-64.

[We] A. Weil, *The Field of Definition of a Variety*, Am. J. of Math. **78** (1956), 509-524.

Université de Caen, Laboratoire de Mathématiques Nicolas Oresme, Campus II, B.P. 5186, 14032 Caen cedex, France.

E-mail address: volkov@math.unicaen.fr