Projective p-adic Representations of the K-rational Geometric Fundamental Group

G. Frey and E. Kani

Herrn E. Lamprecht zum 75. Geburtstag gewidmet

1 Introduction

Let C/K be a smooth, geometrically connected curve over a finitely generated field K, and let $F = \kappa(C)$ denote its function field. If C has a K-rational point $P \in C(K)$, then the *K-rational fundamental group $\pi_1(C, P)$ of C/K with base point P* is the Galois group

$$\pi_1(C, P) = \mathrm{Gal}(F_{nr,P}/F)$$

of the maximal unramified extension $F_{nr,P}$ of F in which P splits completely. Since the extension $F_{nr,P}/F$ is regular, it is clear that $\pi_1(C, P)$ is a quotient of the usual geometric fundamental group $\pi_1(C_{\bar{K}}, P)$ of $C_{\bar{K}} = C \otimes \bar{K}$ over the algebraic closure $\bar{K}$ of K with base point P.

The group $\pi_1(C, P)$, which is a special case of the groups $\mathrm{Gal}(F_S^{ur}/F)$ introduced by Ihara [Ih], was studied in some detail in [FKV]. It may be viewed as a natural analogue of the fundamental group $\pi_1(F)$ of a number field F, as the results of section 2 of [FKV] indicate. For example, the maximal abelian subextension $F_{nr,P}^{ab}$ of $F_{nr,P}$, which may be interpreted as an analogue of the Hilbert class field (cf. Rosen [Ro]), is always finite.

However, this picture changes if we look at p-adic representations if K has positive characteristic, particularly in view of the following consequence of *Fontaine-Mazur Conjecture* [FM]:

Conjecture 1 ([FM], Conjecture 5b) *If F is a number field, then any p-adic representation*

$$\rho : \pi_1(F) \to \mathrm{GL}_n(\mathbb{Q}_p)$$

factors through a finite *quotient group. In particular, any quotient group of the maximal unramified pro-p-group $\pi_1(F)^{(p)}$, which is a p-adic analytic group, is finite.*

Now the natural analogue of this conjecture for the group $\pi_1(C,P)$ is *false* if K has positive characteristic. This can be deduced from the work of Oort[Oo1] (as will be explained in section 4), but this approach does not lead to *explicit* counterexamples. We therefore present here the following result:

Theorem 1.1 *Suppose K is a field of characteristic* $\mathrm{char}(K) \equiv 3 \pmod 4$ *and that K contains the fourth roots of unity. Let $b \in K^\times, b^4 \neq \pm 1$, and put $c = 1 + b^4$ and $a = \frac{2b^2}{c}$. Let C/K be the curve defined by the equation*

$$s^4 = ct(t^2-1)(t-a)g(t),$$

where $g(t) \in K[t]$ is any polynomial with

$$g(a) = 1 \quad \textit{and} \quad g(0)g(1)g(-1) \neq 0,$$

and put $P = (a,0) \in C(K)$. Then the K-rational geometric fundamental group $\pi_1(C,P)$ is infinite*; more precisely, for every prime $p \equiv 5 \pmod{12}$ (with $p \neq char(K)$), the group $PSL_3(\mathbb{Z}_p)$ is a factor of $\pi_1(C,P)$, i.e. there is a surjection*

$$\tilde{\rho} : \pi_1(C,P) \to PSL_3(\mathbb{Z}_p).$$

Corollary 1.2 *In the above situation, let C_p denote the finite cover of C of degree $p+1$ corresponding to a pro-p-Sylow subgroup U_p of $PSL_3(\mathbb{Z}_p)$. Then for any point P' over P, the fundamental group $\pi_1(C_p, P')$ has a quotient which is isomorphic to the p-adic analytic group U_p.*

It should also be mentioned here that Ihara [Ih] has constructed other explicit counterexamples in the case that K is a finite field (of characteristic 3 or 5).

To construct such representations $\tilde{\rho}$, we shall actually follow the *spirit* of the *Main Conjecture* of Fontaine-Mazur[FM] which asserts that all "reasonable" p-adic representations of G_F come from geometry, i.e. they are subrepresentations of an étale cohomology group $H^q(X_{\bar{F}}, \mathbb{Q}_p(r))$ attached to some algebraic variety X/F.

In our case we shall take X to be a curve and $q = 1$, which means that we are considering representations which are closely related to the $\mathbb{Q}_p$-Tate module $V_p(A) := T_p(A) \otimes \mathbb{Q}_p$ of an abelian subvariety A/F of the Jacobian variety of X.

It is easily seen that the usual p-adic G_F-subrepresentations $V \subset V_p(A)$ do not lead to representations of $\pi_1(C,P)$ (cf. Proposition 2.2). We use instead the associated *projective* representations

$$\tilde{\rho}_V : G_F \to \mathrm{PGL}(V) = \mathrm{Aut}(\mathbb{P}(V)).$$

Since it seems difficult to find a *useful* (geometric) criterion that such a *single* representation $\tilde{\rho}_V$ factors over $\pi_1(C,P)$, we work instead with a complete system $\{\tilde{\rho}_{V_i}\}$ of subrepresentations belonging to a G_F-*decomposition* $V_p(A) = \oplus V_i$.

A first condition for the existence of such a system $\{\tilde{\rho}_{V_i}\}$ is given by the criterion of Néron-Ogg-Shafarevich: A has to have *good reduction everywhere*, i.e. at all points of C.

A second condition is that the fixed fields of (finite quotients of) the kernels of the $\tilde{\rho}_{V_i}$'s are *regular extensions* of F.

Note that by using group theoretical methods it not difficult to find examples of abelian varieties A/F and corresponding representations $\{\tilde{\rho}_{V_i}\}$ which satisfy these two conditions (cf. [FKV]).

The most difficult condition is the existence of a point $P \in C(K)$ which splits completely in $\mathrm{Fix}(\mathrm{Ker}(\tilde{\rho}_{V_i}))$. Of course this condition implies the second one but at present we have no "canonical" method for constructing abelian varieties A/F which satisfy the first and the third condition. (Actually, the "supersingular moduli constructions" discussed in section 4 do give such a method, but this method does not apply in characteristic 0.)

The aim of this paper is to analyze the arithmetical conditions for A which are imposed by these conditions.

In the case that the V_i are the eigenspaces of a suitable automorphism $\sigma \in \mathrm{Aut}(A)$ (this situation occurs in the constructions of [FKV]), we give in Theorem 2.5 a complete characterization of the case when *all* the $\tilde{\rho}_{V_i}$ factor over $\pi_1(C, P)$: under suitable hypotheses, this happens precisely when the reduction $\overline{A}_P$ of A at P has *complex multiplication* and the centre $Z(\mathrm{End}^0_K(\overline{A}_P))$ of the endomorphism algebra of $\overline{A}_P$ is contained in the algebra $\mathbb{Q}(\bar{\sigma}) \subset \mathrm{End}^0(\overline{A}_P)$ generated by the reduction $\bar{\sigma} \in \mathrm{Aut}(\overline{A}_P)$ of σ. The proof of this theorem is given in section 3.

In section 5 we apply this criterion to the example considered in the last section of [FKV]. Under the assumption that K contains the fourth roots of unity we obtain a three dimensional subvariety A of the Jacobian of a suitable curve of genus 4 and a point P on C such that $\overline{A}_P$ is (isogenous to) the product of three copies of the elliptic curve

$$E: \quad Y^2 = X^3 - X$$

(which has complex multiplication by $\mathbb{Q}(i)$). However, when we compute the centre $Z(\mathrm{End}^0_K(\overline{A}_P))$ it turns out that it is *not* contained in $\mathbb{Q}(\overline{\sigma})$ *unless* E is supersingular! Thus, we have to correct the statement of Theorem 5.22 of [FKV] by adding the condition that $\mathrm{char}(K) \equiv 3 \pmod 4$. It remains open whether there is a curve over a number field for which the analogue of Conjecture 1 is not true.

Acknowledgment: The authors gratefully acknowledge receipt of partial funding by both the DFG (Forschergruppe and Graduiertenkolleg Essen) and the Natural Science and Engineering Research Council of Canada (NSERC) (through an operating grant held by the second author) which made this joint research possible.

2 Projective p-adic Representations

As was mentioned in the introduction, we shall construct p-adic representations of the K-rational geometric fundamental group $\pi_1(C,P)$ by making use of the p-adic Galois representation

$$\rho_{A,p} : G_F = \mathrm{Gal}(F^{sep}/F) \to \mathrm{GL}(V_p(A)) \simeq \mathrm{GL}_{2d}(\mathbb{Q}_p)$$

induced by the natural action of G_F on the $\mathbb{Q}_p$-Tate module $V_p(A) := T_p(A) \otimes \mathbb{Q}_p$ of a suitable abelian variety A/F. (We shall always assume tacitly that $p \neq \mathrm{char}(F)$.)

Since we want this representation to factor over $\pi_1(C,P)$, the extension

$$F(V_p(A)) := (F^{sep})^{\mathrm{Ker}(\rho_{A,p})} = \bigcup_n F(A[p^n])$$

of all p^n-th torsion points has to lie in $F_{nr,P}$ and hence in particular has to be *unramified everywhere*. Now by the criterion of Néron-Ogg-Shafarevich (cf. [ST] or [FKV]) this latter condition is equivalent to

Assumption 2.1 A has *good reduction everywhere* over C.

Assuming this, we thus see that $F(V_p(A)) \subset F_{nr,P}$ if and only if P splits completely in $F(V_p(A))$, i.e. in each $F(A[p^n])$, for all $n \geq 1$. Now this in fact can *never* happen, for otherwise all the p^n-torsion points of the reduction $\overline{A}_P$ would be K-rational, which is impossible since $\overline{A}_P(K)$ is finitely generated by the Theorem of Mordell-Weil-Néron-Lang.

Moreover, a similar conclusion holds for any subrepresentation $\rho_V : G_F \to \mathrm{GL}(V)$ associated to a (non-zero) $\mathbb{Q}_p[G_F]$-submodule $V \subset V_p(A)$. Indeed, if we let

$$F(V) := (F^{sep})^{\mathrm{Ker}(\rho_V)} = \bigcup F(M/p^nM), \qquad \text{where } M = T_p(A) \cap V,$$

then the same argument shows that $F(V)$ cannot lie in $F_{nr,P}$, and hence we have

Proposition 2.2 *No non-trivial p-adic subrepresentation of $\rho_{A,p}$ factors over $\pi_1(C,P)$.*

Thus, none of the representations ρ_V induces a representation of $\pi_1(C,P)$. However, if we replace ρ_V by its associated *projective* representation

$$\tilde{\rho}_V : G_F \to \mathrm{PGL}(V) = \mathrm{Aut}(\mathbb{P}(V)),$$

then it turns out in some cases that $\tilde{\rho}_V$ does factor over $\pi_1(C,P)$, or equivalently, that P splits completely in the subfield

$$F(\mathbb{P}(V)) := F(V)^{Z(GL(V))} \subset F(V)$$

consisting of those elements of $F(V)$ which are fixed by all the Galois automorphisms lying in the centre $Z(GL(V))$ of $GL(V)$.

For our purposes it is useful to characterize this splitting property in terms of the Galois action on the Tate module of the reduction $\overline{A}_P/K$ of A at P. For this, let $\overline{V} \subset T_p(\overline{A}_P)$ denote the image of V under the natural identification $V_p(A) \simeq V_p(\overline{A}_P)$ induced by the reduction map; clearly $\overline{V}$ is a $\mathbb{Q}_p[G_K]$-module. Then we have

Proposition 2.3 *The projective p-adic representation $\tilde{\rho}_V : G_F \to PGL(V)$ factors over $\pi_1(C,P)$ if and only if G_K* acts centrally *on $\overline{V}$, i.e. if for every $g \in G_K$ we have*

$$\rho_{\overline{V}}(g) = c_g \, id_{\overline{V}}, \quad \text{for some } c_g \in \mathbb{Q}_p^{\times}. \tag{1}$$

Proof. By the discussion above, $\tilde{\rho}_V$ factors over $\pi_1(C,P)$ if and only if P splits completely in each $F(\mathbb{P}(M_n))$, for $n \geq 1$, where $M_n = M/p^n M \leq A[p^n]$ and $M = V \cap T_p(A)$. Now by the first part of Corollary 5.11 of [FKV] this holds if and only if $K(\mathbb{P}(\overline{M}_n)) = K \Leftrightarrow$ every $\sigma \in \mathrm{Gal}(K(\overline{M}_n)/K)$ acts centrally on $\overline{M}_n \Leftrightarrow$ every $\sigma \in G_K$ acts centrally on $\overline{M}_n$, and so the assertion follows.

Remark 2.4 Note that condition (1) holds (for any V) in the case that the reduction $\overline{A}_P/K$ of A/F at P is K-isogenous to a power of a supersingular elliptic curve E/K (with all endomorphisms defined over K), i.e. $\overline{A}_P \sim E^g$ and $\dim_{\mathbb{Q}} \mathrm{End}_K^0(E) = 4$.

Indeed, in this case we have $\mathrm{End}_K^0(\overline{A}_P) \otimes \mathbb{Q}_p = \mathrm{End}_{\mathbb{Q}_p}(V_p(A)) \simeq M_{2g}(\mathbb{Q}_p)$, and so $\mathrm{Im}(\rho_{\overline{A}_P,p}) \subset C_{V_p(A)}(\mathrm{End}_K^0(\overline{A}_P)) = Z(V_p(A)) = \mathbb{Q}_p$, which means that (1) holds.

In fact, as we shall see below, the above situation is the only case for which condition (1) holds for the full Tate module $V_p(A)$; cf. Corollary 2.6 below.

In order to be able to use the result of Proposition 2.3 for the construction of suitable projective representations, we need to translate condition (1) into a geometric property of the reduction $\overline{A}_P$. This seems to be difficult for a single subrepresentation $\tilde{\rho}_V$ of $\tilde{\rho}_{A,p}$, but if we consider instead a complete collection $\{\tilde{\rho}_{V_i}\}$ of subrepresentations attached to a $\mathbb{Q}_p[G_F]$-*decomposition*

$$V_p(A) = \bigoplus_{i=1}^{r} V_i, \tag{2}$$

then such a translation is possible, particularly if we assume that the decomposition is obtained as the eigenspace decomposition of an automorphism $\sigma \in \mathrm{Aut}(A)$.

Indeed, if condition (1) holds for each $\overline{V}_i$, then it follows in particular that G_K *acts diagonally* on $V_p(\overline{A}_P)$, and this imposes a very strong restriction on the abelian variety $\overline{A}_P/K$, for it implies (as we shall see below) that $\overline{A}_P/K$ *has complex multiplication (CM)* in the sense that for every K-simple abelian subvariety $B \leq \overline{A}_P$ we have

$$\dim_{\mathbb{Q}} \mathrm{End}_K^0(B) = \tfrac{4}{e}(\dim B)^2, \tag{3}$$

where $e = [Z(\mathrm{End}_K^0(B)) : \mathbb{Q}]$; cf. Mumford [Mu2], p. 183. (Note that this condition is equivalent to existence of a subfield $L \subset \mathrm{End}_K^0(B)$ of degree $[L : \mathbb{Q}] = 2 \dim B$, which is the definition used in Serre-Tate [ST].)

Conversely, if $\overline{A}_P$ has CM (and if $\mathbb{Q}_p$ splits $\mathrm{End}_K^0(\overline{A}_P)$), then G_K acts diagonally (cf. Proposition 3.1), although not necessarily via the given decomposition. However, if (2) is the eigenspace decomposition of an automorphism $\sigma \in \mathrm{Aut}(A)$, then we can give a complete characterization:

Theorem 2.5 *Let A/F be an abelian variety with good reduction everywhere, and suppose that A has an automorphism $\sigma \in \mathrm{Aut}(A)$ of order N such that for some prime*[1] *$p \equiv 1 \pmod N$ the eigenspace decomposition of $V_p(A)$ with respect to σ has the form*

$$V_p(A) = \bigoplus_{(i,N)=1} V_i, \tag{4}$$

where $V_i = V_p(A)_{\lambda^i} = \{v \in V_p(A) : \sigma v = \lambda(\sigma)^i v\}$ denotes the i-th eigenspace with respect to a fixed character $\lambda : \langle\sigma\rangle \to \mathbb{Q}_p^\times$ of order N. In addition, assume that all these spaces have the same dimension

$$\dim_{\mathbb{Q}_p} V_i = n. \tag{5}$$

Then each projective p-adic subrepresentation $\tilde{\rho}_{A,\lambda^i} := \tilde{\rho}_{V_i} : G_F \to \mathrm{PGL}(V_i)$ of $\tilde{\rho}_{A,p}$ factors over $\pi_1(C, P)$, i.e. $\tilde{\rho}_{A,\lambda^i}$ induces a homomorphism

$$\tilde{\rho}_{V_i} : \pi_1(C, P) \to \mathrm{PGL}(V_i), \quad \textit{for all } i \textit{ with } (i, N) = 1,$$

if and only if the reduction $\overline{A}_P$ has complex multiplication *and if the algebra $\mathbb{Q}(\bar{\sigma}) \subset \mathbb{E} := \mathrm{End}_K^0(\overline{A}_P)$ generated by the reduction $\bar{\sigma}$ of σ contains the centre $Z(\mathbb{E})$ of $\mathbb{E}$, i.e. if $\mathbb{Q}(\bar{\sigma}) \supset Z(\mathbb{E})$.*

Before proving this theorem in the next section, let us observe here that it also gives a complete answer to the question of when the "full" projective representation $\tilde{\rho}_{A,p}$ factors over $\pi_1(C, P)$. In particular, we see that $\tilde{\rho}_{A,p}$ *never* factors over $\pi_1(C, P)$ if $\mathrm{char}(F) = 0$.

Corollary 2.6 *The projective representation $\tilde{\rho}_{A,p}$ factors over $\pi_1(C, P)$ if and only the reduction $\overline{A}_P$ is K-isogenous to a power of a* supersingular *elliptic curve E/K (with all endomorphisms defined over K).*

Proof. If the reduction $\overline{A}_P$ satisfies these conditions, then by Remark 2.4 we know that $\tilde{\rho}_{A,p}$ factors over $\pi_1(C, P)$. Conversely, if the latter condition holds, then by Theorem 2.5 (with $\sigma = id_A$) we conclude that $\overline{A}_P$ has CM with centre $Z(\mathbb{E}) = \mathbb{Q}$. Thus $\overline{A}_P \simeq B^r$,

[1] Note that if (4) holds for one prime, then it holds for all primes $p \equiv 1$ (N) by [FKV], Corollary 5.4.

for some K-simple abelian variety B with CM. Since the centre of $D = \mathrm{End}_K^0(B)$ is $Z(D) = \mathbb{Q}$, it follows from the classification theory (cf. [Mu2], p. 201) that either $D = \mathbb{Q}$ or that D is a quaternion algebra over $\mathbb{Q}$. But since B has CM, equation (3) shows that this is only possible in the second case, and then $\dim B = 1$. But this means that B is a supersingular elliptic curve (with all endomorphisms defined over K); cf. [Mu2], p. 217.

3 The Splitting Condition

We now analyze the meaning of the splitting condition (1) in terms of geometric properties of the reduction $\overline{A}_P$, particularly in the case that we have a decomposition (4), and thereby prove Theorem 2.5. Since this analysis only involves the reduction $\overline{A}_P/K$ (and not A/F), we shall simplify the notation here by writing A in place of $\overline{A}_P$.

Thus, let A/K be an abelian variety over a finitely generated field K, and suppose that its $\mathbb{Q}_p$-Tate module $V_p(A)$ has a $\mathbb{Q}_p[G_K]$-decomposition

$$V_p(A) = \bigoplus_{i=1}^{r} V_i. \tag{6}$$

The aim here is to find necessary and sufficient conditions such that G_K acts centrally on each V_i; cf. (1). Since this condition is equivalent to requiring that V_i be contained in the χ_i-eigenspace

$$V_p(A)_{\chi_i} = \{v \in V_p(A) : v^g = \chi_i(g)v, \text{ for all } g \in G_K\}$$

for some character $\chi_i \in \mathrm{Hom}(G_K, \mathbb{Q}_p)$, we see that this condition implies in particular that G_K *acts diagonally* on $V_p(A)$, i.e. we have

$$V_p(A) = \bigoplus_{\chi \in \mathrm{Hom}(G_K, \mathbb{Q}_p)} V_p(A)_\chi. \tag{7}$$

This latter condition can be characterized geometrically as follows.

Proposition 3.1 *Let A/K be an abelian variety over a finitely generated field K, and let $p \neq \mathrm{char}(K)$ be a prime. Then G_K acts diagonally on $V_p(A)$ if and only if A/K has CM and $\mathbb{E} := \mathrm{End}_K^0(A)$ is split by $\mathbb{Q}_p$, i.e. $\mathbb{E} \otimes \mathbb{Q}_p$ is a direct sum of matrix rings over $\mathbb{Q}_p$.*

Proof. Since K is finitely generated, we have

$$\mathbb{E}_p := \mathbb{E} \otimes \mathbb{Q}_p = \mathrm{End}_{G_K}(V_p(A)) \tag{8}$$

by the Tate Conjecture for abelian varieties which was proved by Faltings [Fa]; cf. also Schappacher [Sch].

Let us suppose first that G_K acts diagonally on V. Then by (8) and (7) we have

$$\mathbb{E}_p = \mathrm{End}_{G_K}(V_p(A)) \overset{(7)}{\simeq} \bigoplus_{\chi} M_{n_\chi}(\mathbb{Q}_p), \tag{9}$$

where $n_\chi = \dim_{\mathbb{Q}_p}(V_p(A)_\chi)$. Thus $\mathbb{Q}_p$ splits $\mathbb{E}$, and hence in particular, p splits completely in the centre $Z = Z(\mathbb{E})$, i.e. $Z_\mathfrak{p} \simeq \mathbb{Q}_p$, for every prime $\mathfrak{p}|p$ in (the ring of integers of) Z.

Suppose now for the moment that A is simple, so $\mathbb{E}$ is a skewfield (and hence is simple). In this case all the $n_\chi \neq 0$ are equal; in fact, we have

$$n_\chi^2 = \dim_Z \mathbb{E}, \quad \text{if } n_\chi \neq 0; \tag{10}$$

here $Z = Z(\mathbb{E})$ denotes the centre of $\mathbb{E}$. To see this, note that since $\mathbb{E} \otimes \mathbb{Q}_p \simeq \prod_{\mathfrak{p}|p} \mathbb{E} \otimes_Z Z_\mathfrak{p}$, the $E \otimes_Z Z_\mathfrak{p}$ are precisely the simple factors of $\mathbb{E}_p$, and hence by (9) we have $\mathbb{E} \otimes_Z Z_\mathfrak{p} \simeq M_{n_\chi}(\mathbb{Q}_p)$. Since $Z_\mathfrak{p} \simeq \mathbb{Q}_p$, the assertion (10) follows by comparing dimensions.

Now from (10) (and (7)) it follows that $2 \dim A = \dim_{\mathbb{Q}_p} V_p(A) = ne$, where $n^2 = \dim_Z \mathbb{E}$, and so by (9) we have

$$\dim_{\mathbb{Q}} \mathbb{E} = \dim_{\mathbb{Q}_p} \mathbb{E}_p \overset{(9)}{=} n^2 e = \tfrac{4}{e}(\dim A)^2,$$

which means that (3) holds, i.e. that A has CM.

Now suppose that A/K is arbitrary abelian variety such that G_K acts diagonally on $V_p(A)$. Then the same is true for every abelian subvariety $B \leq A$, and so, if B is simple, then the above argument shows that B has CM, which means that A has CM.

Conversely, suppose that $\mathbb{E}$ is split by $\mathbb{Q}_p$ and that $A \sim B_1 \times \ldots \times B_r$ has CM, where each B_i is simple. Then by Serre-Tate [ST], Theorem 5, Corollary 2, the image of G_K in each $V_p(B_i)$ is abelian, and hence the same is true for the image of G_K on $V_p(A) = V_p(B_1) \oplus \ldots \oplus V_p(B_r)$. Let $R_p \subset \mathrm{End}(V_p(A))$ denote the $\mathbb{Q}_p$-algebra generated by G_K. Then by Faltings[Fa] R_p is semi-simple, so $R_p \simeq K_1 \oplus \ldots \oplus K_t$ is a direct sum of fields (with $[K_i : \mathbb{Q}_p] < \infty$). Now if any $K_i \neq \mathbb{Q}_p$, then $\mathrm{End}_{R_p}(V_p(A))$ cannot be a sum of matrix rings over $\mathbb{Q}_p$, i.e. $\mathbb{E}_p \overset{(8)}{=} \mathrm{End}_{R_p}(V_p(A))$ is not split, contrary to hypothesis. Thus $R_p \simeq \mathbb{Q}_p^e$ (for some e), and so all the characters of R_p are 1-dimensional, which means that $V_p(A)$ has a decomposition of the form (7).

Remark 3.2 a) As the above proof shows, we can also characterize the validity of (7) by the fact that we have an isomorphism $R_p \simeq \mathbb{Q}_p^e$, for some e, where, as above, $R_p \subset \mathrm{End}(V_p(A))$ denotes the $\mathbb{Q}_p$-algebra generated by the image of G_K.

b) A similar characterization of CM abelian varieties is given (without proof) in Serre[Se2], (2.2.6).

c) Note that if K is a finite field, then by Tate's theorem every abelian variety A/K has CM; cf. [Mu2], Theorem 3(b) on p. 256.

d) On the other hand, we observe that G_K acts *centrally* on $V_p(A)$ if and only A is K-isogenous to a power E^g of a supersingular elliptic curve E/K all of whose endomorphisms are defined over K. Indeed, one direction was proved in Remark 2.4 and the other in the course of the proof of Corollary 2.6. (If K is finite, then further characterizations of this condition can be found in [Mu2], Theorem 3(d) on p. 256.)

Let us now assume that A has an automorphism $\sigma \in \mathrm{Aut}(A)$ of order N and that $p \equiv 1 \pmod{N}$. Then there exists a character $\lambda : \langle\sigma\rangle \to \mathbb{Q}_p^\times$ of order N, and so $V_p(A)$ admits a decomposition $V_p(A) = \oplus V_i$ into σ-eigenspaces $V_i = V_p(A)_{\lambda^i}$. We assume that this decomposition has the following form:

$$(11)\quad V_p(A) = \bigoplus_{(i,N)=1} V_i, \quad \text{and} \quad n := \dim_{\mathbb{Q}_p} V_i \ \text{ does not depend on } i \ (\text{for } (i,N)=1).$$

Remark 3.3 The hypothesis (11) clearly implies that $\dim_{\mathbb{Q}_p} V_p(A) = \phi(N)n$ and hence we have $\dim A = \frac{1}{2}\phi(N)n$. In addition, it implies that

$$(12)\qquad \dim_{\mathbb{Q}_p} \mathrm{End}_{\mathbb{Q}_p[\sigma]}(V_p(A)) = \phi(N)n^2,$$

for $V_i \simeq W_i^n$, where W_i is the 1-dimensional $\mathbb{Q}_p[\sigma]$-module affording the character λ^i.

Furthermore, we observe that the subalgebra $\mathbb{Q}(\sigma) \subset \mathbb{E} = \mathrm{End}_K^0(A)$ generated by σ is isomorphic to the N-th cyclotomic field $\mathbb{Q}(\zeta_N)$. Indeed, $Q := \mathbb{Q}(\sigma)$ is a quotient algebra of the group ring $\mathbb{Q}[\sigma]$ with the property that in the faithful $Q \otimes \mathbb{Q}_p$-module V precisely the irreducible components W_i with $(i,N) = 1$ appear, and any such quotient is isomorphic to $\mathbb{Q}(\zeta_N)$.

For abelian varieties A/K satisfying property (11), we have the following geometric characterizations of the splitting condition (1):

Theorem 3.4 *If A/K and σ satisfy the above property (11), then the following conditions are equivalent:*

(i) G_K acts centrally on each V_i.

(ii) $Im(\rho_K) \subset \mathbb{Q}_p(\sigma)$, where $\rho_K : G_K \to \mathrm{Aut}(V_p(A))$ denotes the associated Galois representation.

(iii) A has CM and $Z(\mathbb{E}) \subset \mathbb{Q}(\sigma)$, where $\mathbb{E} = \mathrm{End}_K^0(A)$.

(iv) The centralizer $C_{\mathbb{E}}(\mathbb{Q}(\sigma))$ of $\mathbb{Q}(\sigma)$ in $\mathbb{E}$ has dimension $\dim_{\mathbb{Q}} C_{\mathbb{E}}(\mathbb{Q}(\sigma)) = \phi(N)n^2$.

(v) $\mathrm{End}_{\mathbb{Q}_p(\sigma)}(V_p(A)) \subset \mathbb{E} \otimes \mathbb{Q}_p$.

Proof. (i) $\Rightarrow$ (ii): Since $p \equiv 1 \pmod{N}$, the idempotent $\varepsilon_i := \frac{1}{N}\sum_k \lambda(\sigma^k)^i\sigma^{-k}$ lies in $\mathbb{Q}_p(\sigma)$; clearly $V_i = \varepsilon_i V$. Thus, if $g \in G_K$, then by hypothesis we have $\rho_K(g)_{|V_i} = c_{g,i}id_{V_i}$ for some $c_{g,i} \in \mathbb{Q}_p^\times$, and hence $\rho_K(g) = \sum_i c_{g,i}\varepsilon_i \in \mathbb{Q}_p(\sigma)$, i.e. condition (ii) holds.

(ii) $\Rightarrow$ (i): This is trivial, since by hypothesis (11) the automorphism σ and hence also all $x \in \mathbb{Q}_p(\sigma)$ act centrally on each V_i.

(ii) $\Rightarrow$ (iii): The hypothesis (ii) implies in particular that G_K acts diagonally on V, and hence by Proposition 3.1 we see that A has CM. In addition, the hypothesis (ii) implies that $R_p := \mathbb{Q}_p[\mathrm{Im}(\rho_K)] \subset \mathbb{Q}_p(\sigma)$. Now by Faltings' results [Fa] we have

$$Z(\mathbb{E}_p) = \mathbb{E}_p \cap R_p, \tag{13}$$

because $Z(\mathbb{E}_p) = C(\mathbb{E}_p) \cap \mathbb{E}_p \overset{(8)}{=} C(C(R_p)) \cap \mathbb{E}_p = R_p \cap \mathbb{E}_p$ by the double centralizer theorem Curtis-Reiner [CR], Theorem 59.6 (p. 405) or Exercise 26.1 (p. 178)). From this we therefore obtain that $Z(\mathbb{E}_p) \subset R_p \subset \mathbb{Q}_p(\sigma)$, and hence it follows that $Z(\mathbb{E}) \subset \mathbb{Q}(\sigma)$.

(iii) $\Rightarrow$ (iv): Since $\mathbb{Q}(\sigma)$ is a field (cf. Remark 3.3), so is $Z(\mathbb{E})$, and hence $\mathbb{E}$ is a simple algebra. This means that $A \sim B^r$, for some r, where B is K-simple. Thus $\mathbb{E} \simeq M_r(D)$, where $D = \mathrm{End}_K^0(B)$ is a skewfield with centre $Z(D) \simeq Z(\mathbb{E})$. Thus, by Remark 3.3 we have

$$r \dim B = \dim A = \tfrac{1}{2}\phi(N)n; \tag{14}$$

Furthermore, since B/K has CM by hypothesis, we have by (3) and (14) that

$$\dim_{\mathbb{Q}} \mathbb{E} = r^2 \dim_{\mathbb{Q}} D \overset{(3)}{=} \tfrac{1}{e}4r^2(\dim B)^2 \overset{(14)}{=} \tfrac{1}{e}\phi(N)^2n^2, \tag{15}$$

where as before $e = [Z(D) : \mathbb{Q}]$.

Now since $\mathbb{E}$ is a simple algebra and $\mathbb{Q}(\sigma)$ is a simple subalgebra containing the centre $Z = Z(\mathbb{E}) \simeq Z(D)$, we have (cf. Huppert [Hu], p. 542) that

$$\dim_Z C_{\mathbb{E}}(\mathbb{Q}(\sigma)) = \dim_Z \mathbb{E}/\dim_Z \mathbb{Q}(\sigma) = \tfrac{1}{e}\phi(N)n^2,$$

where the second equality follows from (15) (and from the fact that $\dim_Z \mathbb{Q}(\sigma) = [\mathbb{Q}(\sigma) : Z] = \phi(N)/e$). Thus $\dim_{\mathbb{Q}} C_{\mathbb{E}}(\mathbb{Q}(\sigma)) = e \dim_Z C_{\mathbb{E}}(\mathbb{Q}(\sigma)) = \phi(N)n^2$, as desired.

(iv) $\Leftrightarrow$ (v): By definition we have $C_{\mathbb{E}}(\mathbb{Q}(\sigma)) \otimes \mathbb{Q}_p = \mathrm{End}_{\mathbb{Q}_p(\sigma)}(V) \cap \mathbb{E}_p$, where $V = V_p(A)$, and so $\mathrm{End}_{\mathbb{Q}_p(\sigma)}(V) \subset \mathbb{E}_p \Leftrightarrow \dim_{\mathbb{Q}}(C_{\mathbb{E}}(\mathbb{Q}(\sigma))) = \dim_{\mathbb{Q}_p} \mathrm{End}_{\mathbb{Q}_p(\sigma)}(V) = \phi(N)n^2$, where the latter equality holds by (12).

(v) $\Rightarrow$ (ii): Since $\mathrm{End}_{\mathbb{Q}_p(\sigma)}(V) = C(\mathbb{Q}_p(\sigma))$ is the centralizer of $\mathbb{Q}_p(\sigma)$ in $\mathrm{End}_{\mathbb{Q}_p}(V)$ and $\mathbb{E}_p = C(R_p)$ is that of R_p (cf. (8)), we see that hypothesis (v) implies that

$$C(C(\mathbb{Q}_p(\sigma))) \supset C(E_p) = C(C(R_p)).$$

Now since $\mathbb{Q}_p(\sigma)$ and R_p are both semi-simple, the double centralizer theorem (cf. [CR], loc. cit.) shows that $C(C(\mathbb{Q}_p(\sigma))) = \mathbb{Q}_p(\sigma)$ and $C(C(R_p)) = R_p$, and so $R_p \subset \mathbb{Q}_p(\sigma)$, which means that (ii) holds.

Proof of Theorem 2.5. The G_F-decomposition (1) of $V_p(A)$ induces (via the reduction map) a G_K-decomposition (6) of the $\mathbb{Q}_p$-Tate module $\overline{V} = V_p(\overline{A}_P)$ reduction $\overline{A}_P$. Clearly, the image $\overline{V}_i$ of the i-th σ-eigenspace V_i is the i-th $\bar{\sigma}$-eigenspace of $\overline{V}$, and so the hypotheses imply that condition (11) holds for $\overline{A}_P/K$ and $\bar{\sigma}$.

Now by the splitting condition (Proposition 2.2) we know that all the $\tilde{\rho}_{A,\lambda^i}$ factor over $\pi_1(C,P)$ if and only if G_K acts centrally on each $\overline{V}_i$, and by the equivalence (i) $\Leftrightarrow$ (iv) of Theorem 3.4 this happens if and only if $\overline{A}_P/K$ has CM and $Z(\mathbb{E}) \subset \mathbb{Q}(\bar{\sigma})$.

4 Constructions via Moduli Spaces

Returning to the situation studied in section 2, we shall now use the geometry of the moduli spaces $\mathcal{A}_{g,d}$ and the results of Oort[Oo1] to construct (in every positive characteristic) examples of abelian varieties $A/F = \kappa(C)$ whose projective p-adic representations $\tilde{\rho}_{A,p} : G_F \to \mathrm{PGL}(V_p(A))$ factor over $\pi_1(C,P)$ (for suitable C and P).

As is explained below, all such examples arise from the existence of suitable morphisms $f : C \to \mathcal{A}_{g,d}$ to the (coarse) moduli space $\mathcal{A}_{g,d}$ which classifies isomorphism classes of pairs (A,λ) of g-dimensional abelian varieties $A/\overline{K}$ with a polarization $\lambda : A \to A^t$ of degree d^2 (cf. Mumford [Mu1] or Oort[Oo1]). To make this more precise, it is convenient to introduce the following terminology:

Definition. As usual, a point $x \in \mathcal{A}_{g,d}(\overline{K})$ is called *supersingular* if the abelian variety $A/\overline{K}$ corresponding to x is supersingular (i.e. A is $\overline{K}$-isogenous to a power of a supersingular elliptic curve $E/\overline{K}$).

Furthermore, if (C,P) is a pointed curve over K (i.e. C/K is a curve and $P \in C(K)$ is a K-rational point), then a *non-constant ss-morphism* $f : (C,P) \to \mathcal{A}_{g,d}$ is a morphism $f : C \to \mathcal{A}_{g,d}$ such that (a) $f(P)$ is a supersingular point and (b) the generic point of $f(C)$ is not supersingular (over $\overline{\kappa(C)}$).

Remark 4.1 In the above definition we could replace condition (b) by the (stronger) condition that some point $x' \in f(C) \subset \mathcal{A}_{g,d}(\overline{K})$ is not supersingular; this follows from a result of Oort (and Grothendieck/Katz) that the set of supersingular points in $\mathcal{A}_{g,d}$ is closed (cf. Oort[Oo2], (2.4)). Other equivalent conditions can be derived from the following proposition (which is required in the proof of Theorem 4.3 below).

Proposition 4.2 *If A/F is an abelian variety over a finitely generated field F, then the following conditions are equivalent:*

(i) $A \otimes \overline{F}$ (or $A \otimes F^{sep}$) is not supersingular;

(ii) for some (or for every) $p \neq \mathrm{char}(K)$, the image $\tilde{G}_{F,p} := \mathrm{Im}(\tilde{\rho}_{A,p})$ of the associated projective p-adic representation $\tilde{\rho}_{A,p} : G_F \to \mathrm{PGL}(V_p(A))$ is infinite;

(iii) for some (or for every) $p \neq \mathrm{char}(K)$, the image $\tilde{G}_{F,p}$ contains an infinite pro-p-subgroup of finite index.

Proof. (i) $\Rightarrow$ (ii): If (for some p) the image $\mathrm{Im}(\tilde{\rho}_{A,p})$ were finite, then there is a finite separable extension F'/F such that the restriction $\tilde{\rho}_{A\otimes F',p}$ of $\tilde{\rho}_{A,p}$ to $G_{F'} \leq G_F$ is trivial. This means that $G_{F'}$ acts centrally on $V_p(A)$, and so by Remark 3.2(d) we see that $A \otimes F'$ is supersingular, contradiction.

(ii) $\Rightarrow$ (i): Suppose $A \otimes \overline{F}$ is supersingular; then there is a finite extension F'/F such that $A \otimes F'$ is F'-isogenous to a power of a supersingular elliptic curve E/F' with all endomorphisms defined over F'. Then by Remark 3.2(d) we see that (for each $p \neq \mathrm{char}(K)$) the image $\tilde{G}_{F',p}$ of $G_{F'}$ is trivial, and hence the same is true for $\tilde{G}_{F'_{sep},p}$, where F'_{sep} is the separable closure of F in F'. Now $G_{F'_{sep}} \leq G_F$ is a subgroup of finite index, hence it follows that $\tilde{G}_{F'_{sep},p} = \{1\}$ is a subgroup of finite index in $\tilde{G}_{F,p}$, i.e. $\tilde{G}_{F,p}$ is finite.

(ii) $\Leftrightarrow$ (iii) Since $\tilde{G}_{F,p}$ is an infinite compact p-adic Lie group, this equivalence follows from standard facts of p-adic Lie groups (cf. [Bou], §III.7, particularly Th. 4 and Prop. 5, Cor.). Alternatively, we can deduce this directly here by observing that $\mathrm{Gal}(F(A[p^\infty])/F(A[p^2])]$ is always a pro-p-group of finite index in $\mathrm{Gal}(F(A[p^\infty])/F)$.

As was suggested above, there is a close connection between non-constant ss-morphisms $f : (C, p) \to \mathcal{A}_{g,d}$ and projective p-adic representations $\tilde{\rho}_{A,p}$ which factor over $\pi_1(C, P)$; more precisely, we have

Theorem 4.3 *Let K be a finitely generated field of positive characteristic and let C/K be a (smooth, projective) curve with function field F and K-rational point P.*

(a) If A/F is an abelian variety of dimension g with good reduction everywhere such that the projective p-adic representation $\tilde{\rho}_{A,p}$ factors over $\pi_1(C, P)$ and has infinite image, then there is a non-constant ss-morphism $f : (C, P) \to \mathcal{A}_{g,d}$ for some $d \geq 1$.

(b) Conversely, if we have a non-constant ss-morphism $f : (C, P) \to \mathcal{A}_{g,d}$, then there is a finite extension K'/K, a finite cover $\varphi : C' \to C \otimes K'$ with $\varphi^{-1}(P) \subset C'(K')$, and an abelian variety $A/F' = \kappa(C')$ with good reduction everywhere such that the associated projective p-adic representation $\tilde{\rho}_{A,p}$ has infinite image and factors over $\pi(C', P')$, for all $P' \in \varphi^{-1}(P)$.

(c) For every $g \geq 3$ and $d \geq 1$ there exists a pointed curve (C, P) (defined over some finite extension K'/K) and a non-constant ss-morphism $f : (C, P) \to \mathcal{A}_{g,d}$.

Proof. (a) Since A/F has good reduction everywhere, the Néron model $\mathbf{A}/C$ is an abelian scheme. Furthermore, since $\mathbf{A}/C$ is projective, there exists a polarization λ on $\mathbf{A}/C$ of

some degree d. Thus, by the modular interpretation of $\mathcal{A}_{g,d}$, the pair $(\mathbf{A}, \lambda)$ gives rise to a unique morphism $f : C \to \mathcal{A}_{g,d}$. Since the projective p-adic representation $\tilde{\rho}_{A,p}$ factors over $\pi_1(C, P)$, we know by Corollary 2.6 that the reduction $\overline{A}_P$ is supersingular, and so (by the modular interpretation), $f(P)$ is a supersingular point. Furthermore, since the $\tilde{\rho}$ has infinite image, we have by Proposition 4.2 that $A \otimes \overline{F}$ is not supersingular; i.e. the generic point of $f(C)$ is not supersingular. Thus f is a non-constant ss-morphism as desired.

(b) Let $\mathcal{A}_{g,d}^{(n)}$ be the fine moduli space with level n-structure (where $n \geq 3$ and $\mathrm{char}(K) \nmid n$), and let $p_n : \mathcal{A}_{g,d}^{(n)} \to \mathcal{A}_{g,d}$ be the associated (finite) covering map. Let $C_{\overline{K}} = C \otimes \overline{K}$, and let C_0 be an irreducible component of $p_n^{-1}(f(C_{\overline{K}}))$ and let C_1 be a component of the fibre product $C_{\overline{K}} \times_{f,p_n} C_0$. Thus, if $\nu : C' \to C_1$ is the desingularization of C_1, then C' is a smooth, projective curve over $\overline{K}$ which has surjective morphisms $\varphi : C' \to C_{\overline{K}}$ and $f' : C' \to C_0$ such that $\pi_n \circ f' = f \circ \varphi$, and there is a finite extension K'/K such that C' and f' are defined over K' and such that all points $P' \in \varphi^{-1}(P)$ are K'-rational.

Since $\mathcal{A}_{g,n}^{(n)}$ is a fine moduli space, there exists a universal abelian scheme (with level structure) $\mathbf{A}^{univ}/\mathcal{A}_{g,d}^{(n)}$, and so its pullback $\mathbf{A} = \mathbf{A}^{univ} \times_{f'} C'$ via f' is an abelian scheme over C' or, equivalently, the generic fibre $A = \mathbf{A} \otimes F'$ is an abelian variety over $F' = \kappa(C')$ of dimension g which has good reduction everywhere. Furthermore, since $p_n(f'(P')) = f(P)$ is supersingular for each $P' \in \varphi^{-1}(P)$, it follows from the modular interpretation (and by enlarging K' if necessary) that the reduction $\overline{A}_{P'}$ of A at P' satisfies $\overline{A}_{P'} \sim E^g$, for some supersingular elliptic curve E/K' with $\dim \mathrm{End}_K^0(E) = 4$. Thus, by the above Remark 2.4 and Proposition 2.3 it follows that the projective p-adic representation $\tilde{\rho}_{A,p}$ factors over $\pi_1(C', P')$. Furthermore, the image $\tilde{G}_{F',p} := \mathrm{Im}(\tilde{\rho}_{A,p})$ is infinite, for otherwise $A \otimes \overline{F}$ would be supersingular by Proposition 4.2, which contradicts the fact that f is a non-constant ss-morphism.

(c) Let $x \in \mathcal{A}_{g,d}(\overline{K})$ be a supersingular point. Then $x \in W_{g,d}$, where (as in Oort [Oo1]) $W_{g,d}$ denotes the subset of points of $\mathcal{A}_{g,d}(\overline{K})$ of p-rank 0. Furthermore, since $g \geq 3$, there exists an abelian variety $A/\overline{K}$ which has p-rank 0 but which is not supersingular; for example, one can choose A such that its formal group $\hat{A} \sim G_{g-1,1} + G_{1,g-1}$; cf. Lenstra/Oort [LO]. (Such an A has p-rank 0 since $G_{1,0}$ does not occur as an isogeny factor of $\hat{A}$ (cf. Manin [Ma], Th. 2) but is not supersingular since $\hat{A} \not\sim gG_{1,1}$; cf. [Oo1], Th. 4.2.) Furthermore, by replacing A by an isogenous abelian variety if necessary, we may assume that A has a polarization λ of degree d^2, and so (A, λ) corresponds to a point $x' \in W_{g,d} \subset \mathcal{A}_{g,d}(\overline{K})$. By the proof of Theorem (1.1) of [Oo1] (cf. p. 96ff), $W_{g,d}$ is a projective subvariety of $A_{g,d}$ of dimension $\dim W_{g,d} \geq \frac{1}{2}g(g-1) \geq 1$, so there exists a projective irreducible curve $C_0 \subset W_{g,d}$ through x and x'(cf. [Mu2], p. 56). Let $f : C \to C_0$ denote the normalization/desingularization of $C_0/\overline{K}$; then f and C are defined over some extension field K'/K; by construction, $f : C \to C_0 \subset \mathcal{A}_{g,d}$ is a non-constant ss-morphism.

(Note that the generic point of $f(C) = C_0$ cannot be supersingular, for otherwise every specialization (i.e. every point of C_0) would be supersingular.)

Corollary 4.4 *For any finitely generated field K of positive characteristic and any $g \geq 3$ there exists a finite extension K'/K, a curve C/K' and an abelian variety $A/F = \kappa(C)$ of dimension g with good reduction everywhere such that the projective p-adic Galois representation $\tilde{\rho}_{A,p} : G_F \to PGL_2(V_p(A))$ factors over $\pi_1(C, P)$ and has an infinite image $\tilde{G}_{F,p} := \mathrm{Im}(\tilde{\rho}_{A,p})$ (which therefore contains an infinite pro-p-subgroup of finite index).*

Proof. The first statement follows by combining parts (c) and (a) of Theorem 4.3, and the last assertion follows from Proposition 4.2.

Remark 4.5 It seems more difficult (if not impossible) to characterize the more general situation studied in section 2 in terms of moduli spaces. Clearly, if the conditions of Theorem 2.5 hold, then we have a morphism $f : C \to A_{g,d}$ (for some d) such that $f(P)$ is a CM-point (i.e. the reduction $\overline{A}_P \otimes \overline{K}$ is an abelian variety with CM), but the converse need not hold, even if we assume the existence of an automorphism $\sigma \in \mathrm{Aut}(A/F)$; cf. Remark 5.2 below.

5 Explicit Constructions via Cyclic Coverings

We now apply the results of section 2 to the abelian varieties A/F associated to certain cyclic coverings of curves which were studied in [FKV].

For this, we first observe that the conditions of Theorem 2.5 are applicable to the general situation considered in [FKV], which therefore yields a general criterion for factorizability of the projective p-adic representations $\{\tilde{\rho}_{\lambda_i}\}$ over $\pi_1(C, P)$.

Proposition 5.1 *Let $F_0 = K(t)$, where t is transcendental over K and K contains the N-th roots of unity. Suppose that $t_1, \ldots, t_{n+1}$ are $n+1$ distinct elements in K, and put $t_{n+2} = t$. In addition, suppose that $m_1, \ldots, m_{n+2}$ are integers with $1 \leq m_i < N$ such that $\gcd(m_1, \ldots, m_{n+2}, N) = 1$, $m_1 + \ldots + m_{n+2} \equiv 0 \bmod N$ and $m_i \neq N - m_{n+2}$, for $1 \leq i \leq n+1$. Let $\pi : X \to \mathbb{P}^1_{F_0}$ denote the cyclic covering of degree N defined by the equation*

$$y^N = c(x - t_1)^{m_1} \cdots (x - t_{n+2})^{m_{n+2}}, \tag{16}$$

where $c \in K^*$, and let $\sigma \in \mathrm{Aut}(\pi)$ be a generator, which we view as an automorphism of the Jacobian J_X of X.

a) There is a σ-stable abelian subvariety $A_0 := J_X^{new} \leq J_X$ of dimension $\dim A_0 = \frac{1}{2}\phi(N)n$ such that condition (4) holds for every prime $p \equiv 1 \pmod N$.

b) A_0 has potentially stable reduction over F_0; more precisely, for every cyclic covering $F/K(t)$ which is ramified of order N at $t_1, \ldots, t_{n+1}$, the abelian variety $A = A_0 \otimes F$ has good reduction everywhere.

c) If A/F is as in b) and $P \in C(K)$, where C/K is the smooth curve with function field $\kappa(C) = F$, then all the projective representations $\{\tilde{\rho}_{A,\lambda^i}\}_{(i,N)=1}$ factor over $\pi_1(C,P)$ if and only if the reduction $\overline{A}_P$ has CM and if $Z(\mathrm{End}^0(\overline{A}_P)) \subset \mathbb{Q}(\bar{\sigma})$.

d) Suppose that the condition of d) holds, and that in addition we have $p > 3$ and $(n, p-1) = 1$ (and also $N \nmid 6$ if $n = 3$). Then for each i with $(i, N) = 1$ the projective representation $\tilde{\rho}_{A,\lambda^i}$ yields a surjection

$$\tilde{\rho}_{A,\lambda^i} : \pi_1(C,P) \twoheadrightarrow \mathrm{PGL}_n(\mathbb{Z}_p).$$

Proof. a) The abelian subvariety $A_0 = J_X^{new}$ defined in section 5.1 of [FKV] has this property (cf. [FKV], Theorem 5.5(a)).

b) This is (a special case of) Theorem 5.15 of [FKV].

c) In view of a) and b), this follows directly from Theorem 2.5.

d) By construction, $\mathrm{Im}(\tilde{\rho}_{A,\lambda^i}) \subset \mathrm{PGL}_n(\mathbb{Z}_p) = \mathrm{PSL}_n(\mathbb{Z}_p)$. If $r_p : \mathrm{PSL}_n(\mathbb{Z}_p) \to \mathrm{PSL}_n(\mathbb{F}_p)$ denotes the homomorphism induced by reduction modulo p, then by Theorem 5.5(d) of [FKV], the map $r_p \circ \tilde{\rho}_{A,\lambda^i} : \pi_1(C,P) \to \mathrm{PGL}_n(\mathbb{F}_p) = \mathrm{PSL}_n(\mathbb{F}_p)$ is surjective, and hence the same is true for $\tilde{\rho}_{A,\lambda^i}$ by Serre [Se1], Lemma 3 (and exercise 1) of section IV.3.4 (pp. IV-23 and IV-27).

Proof of Theorem 1.1. By the results of [FKV], section 5.3, we know that there is an abelian variety A/F of dimension 3 which has good reduction everywhere and which has an automorphism $\sigma \in \mathrm{Aut}(A)$ of order 4 such that (11) holds. Furthermore, we know by that its reduction $\overline{A}_P \sim E^3$, where E/K is an elliptic curve with $\mathbb{Q}(i) \subset \mathrm{End}_K^0(E)$, and hence $\overline{A}_P$ has CM. Furthermore, since the assumption $\mathrm{char}(K) \equiv 3 \pmod 4$ means that E/K is supersingular, we have $Z(\mathrm{End}_K^0(\overline{A}_P)) \simeq \mathrm{End}_K^0(E) = \mathbb{Q}$, and so we have automatically that $\mathbb{Z}(\mathrm{End}_K^0(\overline{A}_P)) \leq \mathbb{Q}(\bar{\sigma})$. Thus, by Theorem 2.5 we see that $\tilde{\rho}_{A,\lambda}$ and $\tilde{\rho}_{A,\lambda^{-1}}$ both factor over $\pi_1(C,P)$, and by the same argument as in Proposition 5.1 we have that their image is $\mathrm{PSL}_3(\mathbb{Z}_p) = \mathrm{PGL}_3(\mathbb{Z}_p)$, if $p \equiv 5$ (12).

Remark 5.2 Unfortunately, if we assume that $\mathrm{char}(K) \not\equiv 3$ (4), which means (in the situation of Theorem 1.1) that $\mathrm{End}_K^0(E) = \mathbb{Q}(i)$, then the condition $Z(\mathrm{End}_K^0(\overline{A}_P)) \subset \mathbb{Q}(\bar{\sigma})$ *does not hold*, and so $\tilde{\rho}_{A,\lambda_i}$ *does not factor* over $\pi_1(C,P)$, even though the reduction $\overline{A}_P$ is a CM-variety (in fact, $\overline{A}_P$ is isogenous to the third power of an elliptic curve with CM by $\mathbb{Q}(i)$, as was mentioned in the above proof).

Indeed, in this case we have that $Z(\overline{A}_P) \simeq \mathbb{Q}(i)$, so the desired containment holds if and only if $Z(\overline{A}_P) = \mathbb{Q}(\bar{\sigma})$, i.e. if and only if $\bar{\sigma} \in Z(\overline{A}_P)$. But the following lemma shows that this is *never* the case:

Lemma 5.3 *The reduction $\overline{A}_P$ contains three isomorphic elliptic curves $E_i \leq \overline{A}_P$ such that $\overline{A}_P \sim E_1 \times E_2 \times E_3$. Furthermore, for each $i = 1, 2, 3$, the automorphism $\bar{\sigma}$ restricts to an automorphism $\bar{\sigma}_i = \bar{\sigma}_{|E_i} \in \mathrm{Aut}(E_i)$ with the property that there exist isomorphisms $f_i : E_1 \xrightarrow{\sim} E_i$ with $f_i \circ \bar{\sigma}_1 = \bar{\sigma}_i^{-1} \circ f_i$, for $i = 2, 3$.*

Proof. As we shall see, we can use the elliptic curves E_i constructed in the proof of Lemma 5.21 of [FKV]. However, since we have to keep track of the induced σ-action, we need to review their construction from the very beginning.

Thus, let $F = K(t, s)$ be as in Theorem 1.1, and let X/F denote (the normalization of) the curve defined by the equation

$$y^4 = cx(x-1)(x+1)(x-a)^3(x-t)^2.$$

Recall that $A = J_X^{new}$ is the new part of the Jacobian J_X of X with respect to the automorphism $\sigma_J \in \mathrm{Aut}(J_X)$ which is induced by the curve automorphism $\sigma \in \mathrm{Aut}_F(X)$ defined by $\sigma^*(x) = x$, $\sigma^*(y) = iy$, where $i \in K$ is a fixed primitive fourth root of unity.

Now by [FKV], Proposition 5.18, the reduction $\overline{X}_P$ at $P = (a, 0)$ (of the associated stable model) of X/F has precisely two (smooth) irreducible components $\overline{X}_1$ and $\overline{X}_2$ given by the equations

$$y_1^2 = x_1(x_1^2 - d) \quad \text{and} \quad y_2^4 = cx_2(x_2^2 - 1)(x_2 - a), \tag{17}$$

respectively, where $d = c/g(a)$. Since $\overline{X}_1$ is an elliptic curve and $\overline{X}_2$ is a curve of genus 3, it is clear that the reduction $\bar{\sigma}$ of σ maps each component $\overline{X}_k$ into itself, and so the induced automorphism $\bar{\sigma}_J$ on the reduction $(\overline{J}_X)_P \simeq J_{\overline{X}_1} \times J_{\overline{X}_2}$ has the form $\bar{\sigma} = \bar{\sigma}_1 \times \bar{\sigma}_2'$.

We now claim that these automorphisms (viewed as automorphisms of $\overline{X}_k$) satisfy the relations

$$\bar{\sigma}_1^* x_1 = -x_1,\ \bar{\sigma}_1^* y_1 = -iy_1, \quad \text{and} \quad (\bar{\sigma}_2')^*(x_2) = x_2,\ (\bar{\sigma}_2')^* y_2 = iy_2. \tag{18}$$

Indeed, if $\bar{x}_2$ and $\bar{y}_2$ denote the images of x and y under the second reduction map (corresponding to the component $\overline{X}_2$), then the proof of [FKV], Proposition 5.18, shows that $x_2 = \bar{x}_2$ and $y_2 = \bar{y}_2/(\bar{x}_2 - a)$. Since $(\bar{\sigma}_2')^*\bar{x}_2 = \bar{x}_2$ and $(\bar{\sigma}_2')^*\bar{y}_2 = i\bar{y}_2$, the relation (18) is clear for $\bar{\sigma}_2'$. On the other hand, if $\bar{x}_1$ and $\bar{y}_1$ denote the images of $(x-a)/s^4$ and y/s^5 with respect to the first reduction map, then we have by the proof of Proposition 5.18 that $x_1 = \bar{y}_1^2/(\bar{x}_1(\bar{x}_1 - b_0))$ and $y_1 = a_0\bar{y}_1/x_1$, where $a_0 = ca(a^2-1)$ and $b_0 = d/a_0$. Thus, since $\bar{\sigma}_1^*\bar{x}_1 = \bar{x}_1$ and $\bar{\sigma}_1^*\bar{y}_1 = i\bar{y}_1$, we see that $\bar{\sigma}_1^* x_1 = (i\bar{y}_1)^2/(\bar{x}_1(\bar{x}_1 - b_0)) = -x_1$ and $\bar{\sigma}_1^* y_1 = a_0(\bar{\sigma}_1^*\bar{y}_1)/(\bar{\sigma}_1^* x_1) = a_0(i\bar{y}_1)/(-x_1) = -iy_1$, which means that (18) holds for $\bar{\sigma}_1$ as well.

Next, by Lemma 5.20 of [FKV] we know that $J_{\overline{X}_2} \sim E_2 \times E_3 \times E'$, where the elliptic curves belong respectively to the three elliptic subfields F_2, F_3 and F' of index 2 of the function field $K(x_2, y_2)$ of $\overline{X}_2$, and that these subfields are given by

$$F_2 = K(z_2, v_2), \quad F_3 = K(z_3, v_3) \quad \text{and} \quad F' = K(x_2, y_2^2),$$

where $z_2 = y_2(1-b^2x_2)/(x_2^2-1)$, $z_3 = z_2(x_2-b^2)/(b^3(1-b^2x_2))$, $v_2 = z_2^2/(u-1)$, and $v_3 = v_1/b^2$ with $u := cx_2(x_2-1)$). These elements satisfy the relation

$$z_k^2 = v_k(v_k^2-1) \quad \text{for } k = 2,3,$$

and so we have an isomorphism $f : E_2 \xrightarrow{\sim} E_3$ such that $f^*v_3 = v_2$ and $f^*z_3 = z_2$.

Furthermore, if $\bar{\sigma}_k^* = (\bar{\sigma}_2')^*_{|F_k}$ denotes the restriction of $(\bar{\sigma}_2')^*$ to the subfield F_k for $k = 2,3$, then we have from (18)

$$\bar{\sigma}_k^* z_k = iz_k,\ \bar{\sigma}_k^* v_k = -v_k, \quad \text{for } k = 2,3, \tag{19}$$

and so we have $f \circ \bar{\sigma}_2 = \bar{\sigma}_3$.

On the other hand, since $d = d_1^4$ is a fourth power in K (by hypothesis), we have an isomorphism $f_2 : E_1 := \overline{X}_1 \xrightarrow{\sim} E_2$ such that $f_2^*v_1 = d_1^2x_1$, $f_2^*z_1 = d_1^3y_1$. Comparing (18) with (19) shows that $f_2 \circ \bar{\sigma}_1 = \bar{\sigma}_2^{-1} \circ f_2$, and hence a similar relation holds for $f_3 := f \circ f_2 : E_1 \xrightarrow{\sim} E_3$.

Since $\bar{\sigma}^2$ acts non-trivially on E_k, we see that $E_k \leq \overline{A}_P = (\overline{J}_X^{new})_P$, for $k = 1,2,3$, and so $\overline{A}_P = E_1 + E_2 + E_3$ since $\dim \overline{A}_P = 3$ and by the above E_1, E_2, E_3 generate an abelian subvariety of dimension 3. Thus $\overline{A}_P \sim E_1 \times E_2 \times E_3$.

Remark 5.4 Note that the above lemma also shows that Lemma 5.21(b) of [FKV] is *false* if $\mathrm{char}(K) \not\equiv 3 \pmod 4$, and hence the same is true for Theorem 5.22 (and for the consequence on p. 87). Thus, in both cases one has to add the condition that $\mathrm{char}(K) \equiv 3 \pmod 4$.

Explicitly, the error occurs in the second paragraph of the proof (of part (b)) where it is asserted (without proof) that there exist isomorphisms $f_{1i} : E_1 \to E_i$ such that $f_{1i} \circ \alpha_1 = \alpha_i \circ f_{1i}$, where the $\alpha_i \in \mathrm{End}(E_i)$ are a certain endomorphisms of degree p.

References

[Bou] N. Bourbaki, *Lie Groups and Lie Algebras, chs. 1–3*, Springer-Verlag, Berlin, 1989.

[CR] C. Curtis, I. Reiner, *Representation Theory of Finite Groups and Associative Algebras.* Interscience Publ., New York, 1962.

[Fa] G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Inv. Math.* **73** (1983), 349–366.

[FM] J.-M. Fontaine, B. Mazur, Geometric Galois representations. In: *Conf. on Elliptic Curves and Modular Forms*, Hong Kong, Intern. Press, Cambridge, 1995, pp. 41–78.

[FKV] G. Frey, E. Kani, H. Völklein, *Curves with infinite K-rational geometric fundamental group.* In: *Aspects of Galois Theory* (H. Völklein et al., eds.), LMS Lecture Notes **256** (1999), 85–118.

[Hu] B. Huppert, *Endliche Gruppen I.* Springer-Verlag, Berlin, 1967.

[Ih] Y. Ihara, On unramified extensions of function fields over finite fields. In: *Galois Groups and their Representations*, Adv. Sudies in Pure Math. 2 (1983), pp. 89-97.

[LO] H.W. Lenstra, F. Oort, Simple abelian varieties having prescribed formal isogeny type. *J. Pure Appl. Alg.* **4** (1974), 47-53.

[Ma] Ju. Manin, On the theory of abelian varieties over a field of finite characteristic. *Izv. Akad. Nauk SSSR Ser. Mat.* **26** (1962), 281–292 = AMS Translations (2) **50** (1966), 127–140.

[Mu1] D. Mumford, *Geometric Invariant Theory.* Springer-Verlag, Berlin, 1966.

[Mu2] D. Mumford, *Abelian Varieties.* Oxford University Press, Oxford, 1970.

[Oo1] F. Oort, Subvarieties of moduli spaces. *Invent. math.* **24** (1974), 95–119.

[Oo2] F. Oort, Moduli of abelian varieties and Newton polygons. *C.R. Acad. Sci. Paris* **312** (1991), 385–389.

[Ro] M. Rosen, The Hilbert class field in function fields. *Expo. Math.* **5** (1987), 365–378.

[Sch] N. Schappacher, Tate's Conjecture on the endomorphisms of abelian varieties. In: *Rational Points* (G. Faltings, G. Wüstholz) Vieweg, Braunschweig, 1984, pp. 114–153.

[Se1] J.-P. Serre, *Abelian ℓ-adic Representations and Elliptic Curves.* Benjamin, New York, 1968.

[Se2] J.-P. Serre, Resumé des cours de 1984-1985. *Annuaire du Collège de France* (1985), 85–91 = J.-P. Serre, Œuvres/Collected Papers IV, pp. 27–32.

[ST] J.-P. Serre, J. Tate, Good reduction of abelian varieties. *Ann. Math.* **88** (1968), 492–517 = J.-P. Serre, Œuvres/Collected Papers II, pp. 472–517.