THE (p, t, a)-INERTIAL GROUPS AS FINITE MONODROMY GROUPS

VERSION OF September 12, 2025

SÉVERIN PHILIP

ABSTRACT. Silverberg and Zarhin introduced the notion of a (p, t, a)-inertial group in the hope of having a group theoretic characterization of the finite groups that appear as finite monodromy groups – the groups that represent the local obstruction to semi-stable reduction – of abelian varieties in fixed dimension $t + a$. In this text, we provide a positive answer to their question, that is, every (p, t, a)-inertial group is the finite monodromy group of an abelian variety in dimension $t + a$. To prove this, we show a structure theorem on the rational group algebra $\mathbf{Q}[G]$ of ramification groups, refining a theorem of Serre and generalizing results on p-groups of Roquette and Ford.

CONTENTS

1. INTRODUCTION

1.1.1. The finite monodromy groups of abelian varieties have been introduced by Grothendieck in [SGA7.1] exposé IX. They represent the local obstruction to semi-stable reduction. Silverberg

2020 *Mathematics Subject Classification.* 11G25, 14K15, 20C05.

The author is grateful to J. Bergström, G. Rémond and A. Tamagawa for the fruitful discussions about this project.

and Zarhin studied these groups in [SZ98; SZ05], and the author, in order to give an effective version of Grothendieck's semi-stable reduction theorem, in [Phi22a; Phi22b; Phi24].

For a fixed natural integer $g \geq 1$, the list of finite groups which can be realized as finite monodromy groups of some abelian variety of dimension g is not known. An attempt to provide this list is made by the notion of (p, t, a)-inertial groups introduced in [SZ05].

Definition 1.1 ([SZ05])**.** Let p be a prime number or $p = 0$ and t, a positive integers. A finite group G is said to be (p, t, a)-inertial if it satisfies the two following conditions :

(*i*) If $p = 0$ then G is cyclic otherwise G is a semi-product $\Gamma_p \rtimes \mathbf{Z}/n\mathbf{Z}$ with Γ_p a p-group and n an integer prime to p.

(*ii*) For all primes $\ell \neq p$ there is an injection

$$\iota_\ell \colon G \hookrightarrow \mathrm{GL}_t(\mathbf{Z}) \times \mathrm{Sp}_{2a}(\mathbf{Q}_\ell)$$

such that the projection map onto the first factor is independent of ℓ and the characteristic polynomial of the projection of any element onto the second factor has integer coefficients independent of ℓ.

It follows from the definition that the character χ_ℓ of the $\mathbf{Q}_\ell$ representation given by the projection on the second factor has integer values and is independent of ℓ. Note that from the main theorem of [Mau68], condition (i) is equivalent to the fact that G is a quotient of the absolute inertia group of some local fields of equal and mixed characteristic – a ramification group at p.

It is known – see part (i) of Theorem 5.2 of [SZ98] – that finite monodromy groups are (p, t, a)-inertial. The question is now whether the converse is true, that is, does Definition 1.1 characterize the finite groups that appear as finite monodromy groups in dimension $t + a$ over number fields with conditions on the toric and abelian ranks of the reduction with respect to t and a. A precise statement is given by question 1.13 of *loc. cit.* Specifically, the question is to realize a (p, t, a)-inertial group G as the finite monodromy group of an abelian variety A of dimension $g = t + a$ at a place of residue characteristic p. In the same paper they show that the set of (p, t, a)-inertial groups with $t + a = 2$ are realized as finite monodromy groups of abelian surfaces over local fields of equal characteristic p. Further, Chrétien and Matignon in [CM13] have shown that this list is also realized with abelian surfaces over number fields by an ad hoc construction for the last unrealized $(2, 0, 2)$-inertial group.

1.1.2. In this text we give a positive answer to their question.

Theorem 1.2 (Corollary 4.9)**.** *Let G be a finite group. Then G is (p, t, a)-inertial if and only if G is the finite monodromy group of an abelian variety A of dimension $t + a$ over a number field K at a place v of residue characteristic p and A is such that, for all extension L/K for which A_L has semi-stable reduction at the places of L above v, the reduction of A_L at the places above v has toric rank t and abelian rank a.*

We actually show more in Theorem 4.8. Indeed, we show that for G a ramification group and every family of maps as in (ii) of Definition 1.1 there is a realization of G as a finite monodromy group of an abelian variety of dimension $t + a$ over a p-adic field such that we recover that family of maps, up to isomorphism, by taking the ℓ-adic representation of the semi-stable reduction of A. In order to prove this result we deal with the rational group algebra $\mathbf{Q}[G]$ of such groups and give precision to a structure theorem of Serre, Théorème 3 of [Ser60].

We end the last section by a series of example, showcasing how the results in this paper are used to compute the values for which a ramification group is (p,t,a)-inertial in a simple and efficient way.

Theorem 1.3 (Theorem 3.10)**.** *Let G be a ramification group at p. The rational group algebra $\mathbf{Q}[G]$ has the following properties.*

(*i*) *The algebra $\mathbf{Q}[G]$ is quasi-split outside p.*
(*ii*) *If $E \subset \mathbf{Q}[G]$ is a simple factor of $\mathbf{Q}[G]$ then the center $Z(E)$ of E is a CM field or a subfield of $\mathbf{Q}(\mu_{p^\infty})$.*

Furthermore, if $\operatorname{Card} G$ *is odd then no simple factor E of $\mathbf{Q}[G]$ is such that $E \otimes_{\mathbf{Q}} \mathbf{R}$ is a matrix algebra over the quaternions.*

Part (*i*) is the statement of Théorème 3 of [Ser60]. We deal with the possible centers of the simple factors of $\mathbf{Q}[G]$. The main novelty obtained from (*ii*) is that in the event of a simple factor E of $\mathbf{Q}[G]$ being a type III algebra in Albert's classification, then there is a totally real subfield F of $\mathbf{Q}(\mu_p^\infty)$ such that we have $E \simeq \mathrm{M}_n(F \otimes \mathbf{H}_{p,\infty})$ for some integer n where $\mathbf{H}_{p,\infty}$ is the quaternion algebra over $\mathbf{Q}$ ramified only at p and ∞. One notes that this is the endomorphism ring of a supersingular elliptic curve in characteristic p.

1.1.3. The first section is devoted to the study of $\mathbf{C}$-representations of simple finite dimensional $\mathbf{Q}$-algebras that are rational – the characteristic polynomials of the elements have coefficients in $\mathbf{Q}$ – and that admit an invariant symplectic form, we say polarized. We are interested in such representations as both the representation of the endomorphism algebra of an abelian variety given by its Tate module and the representations of $\mathbf{Q}[G]$ coming from the second projection of the map ι_ℓ in Definition 1.1 have these properties. Our main goal in this section is to show a characterization of such algebras that can be embedded in a nice way into the endomorphism algebras of abelian varieties – see Definition 2.15 and Theorem 2.22. In order to do this, we first show in Section 2.1 that rational and polarized representations are multiple of a minimal such representation denoted $V_{rp}(E)$. The dimension of this representation depends on the invariants of E and its type in the classification of Albert.

The second section is independent from the first. In the first part of the second section we work on twisted algebras, that is $\mathbf{Q}$-algebras that are obtained by the action of a group on some $\mathbf{Q}$-algebra E. Our main interest is to give some restrictions on their centers in the case of the acting group G being cyclic of order $m \geq 1$. Such an algebra is of the form

$$\bigoplus_{i=0}^{m-1} E.u^i$$

with, for all $x \in E$, $ux = f(x)u$ for some finite order automorphism f of E. When E is simple the center of the twisted algebra is then a product of field extensions of a subfield of $Z(E)$ obtained by extracting roots. A precise statement is given by Proposition 3.2. We then deal with the case of E not being simple. The second part is dedicated to the proof of Theorem 1.3 which is done by applying the previous results to the case of the rational group algebra of a ramification group $G \simeq \Gamma_p \rtimes \mathbf{Z}/n\mathbf{Z}$.

In the last section we gather together our results and show our main theorem. First we relate the definition of (p,t,a)-inertial groups to rational and polarized representations of group algebras. We show that all families of maps $(p_\ell \colon G \to \mathrm{Sp}_{2a}(\mathbf{Q}_\ell))_{\ell \neq p}$ satisfying the rationality condition of

Definition 1.1 (*ii*) can be recovered from an embedding into the endomorphism algebra of an abelian variety A_0 of dimension a over a finite field. We then show that A_0 can furthermore be chosen so that the map $G \to \mathrm{End}\, A_0 \otimes \mathbf{Q}$ has values in $\mathrm{Aut}\, A_0$. We can thus apply Théorème 1.1 of [Phi24] which provides A over a p-adic field whose semi-stable reduction $\overline{A}$ is isogenous to A_0 and verify that the representation from its ℓ-adic Tate module recovers p_ℓ again. We can add the toric part by simply considering $A_0 \times \mathbf{G}_m^t$.

2. Rational representations of simple algebras

In this section we start by gathering results about representations of finite dimensional simple algebras which are rational and admit a symplectic structure. In the second part of this section we relate these results to algebras coming from the endomorphisms of abelian varieties over finite fields, which we call geometric, and introduce the notion of a good embedding to be used in section 4. The main result is a characterization of the algebras that admits a good embedding.

2.1. Rational and polarizable representations of algebras

2.1.1. For the rest of this section let us fix E, a simple finite dimensional –since all algebras we are dealing with will be finite dimensional it will be sometimes omitted for clarity – $\mathbf{Q}$-algebra and denote by F its center. We start by studying the $\mathbf{C}$-representations of such an algebra E and whether those admit invariant bilinear forms.

Definition 2.1. A $\mathbf{C}$-representation of E is a $\mathbf{C}$-vector space V equipped with a linear action of E, that is a map of $\mathbf{Q}$-algebras

$$E \longrightarrow \mathrm{End}_{\mathbf{C}}\, V.$$

For a $\mathbf{C}$-representation V of E, let tr_V denote the central trace of V, that is the composition

$$F \to E \to \mathrm{End}_{\mathbf{C}}\, V \to \mathbf{C}$$

where the last arrow is the trace map.

We will also consider $\mathbf{R}$-representations of E in this section, which are defined in the same way.

Lemma 2.2. *The simple $\mathbf{C}$-representations of E are classified by their central trace.*

Proof. The simple $\mathbf{C}$-representations of E correspond to simple $E \otimes_{\mathbf{Q}} \mathbf{C}$-modules. For f the degree of F over $\mathbf{Q}$ there is an integer n such that we have an isomorphism

$$E \otimes_{\mathbf{Q}} \mathbf{C} \simeq \prod_{i=1}^{f} M_n(\mathbf{C}).$$

This isomorphism is such that $F \otimes_{\mathbf{Q}} \mathbf{C}$ is embedded diagonally and by the projection on each factor we recover the embeddings $\sigma\colon F \to \mathbf{C}$ up to multiplication by n by taking the trace.

As the simple $\mathbf{C}$-representations of E correspond to a choice of such a projection, we see that their central traces are given by the embeddings $F \to \mathbf{C}$ up to multiplication by n and thus they are classified in this way. □

Let $\{\sigma_1, \dots, \sigma_f\}$ be the set of embeddings $F \to \mathbf{C}$. Then, for $i \in \{1, \dots, f\}$ we will denote by V_i the simple $\mathbf{C}$-representation of E which has a multiple of σ_i for its central trace. The $\mathbf{C}$-representation $V_r(E) = \oplus_{i=}^{f} V_i$ is the minimal non trivial one with rational central trace.

Definition 2.3. A positive involution on E is a $\mathbf{Q}$-linear map $^*\colon E \to E$ which satisfies, for all $x, y \in E$,

$$(x^*)^* = x,\ (xy)^* = y^*x^*$$

and $\mathrm{Tr}_E(xx^*) > 0$ for $x \neq 0$. Here, for $x \in E$, the value $\mathrm{Tr}_E(x)$ is the trace of the map given by left multiplication by x in E as a $\mathbf{Q}$-vector space.

If E admits a positive involution we say it is polarizable.

We give some basic results on positive involutions and the trace map on E, which are standard. The fact that an involution is positive can be checked on $E \otimes_{\mathbf{Q}} \mathbf{R}$ considered with the $\mathbf{R}$-linear extension of the involution. For standard results on positive involutions we refer to chapter 8 of [Sch85]. We start with some known facts that are translated in our setting.

Lemma 2.4. *Let E be a simple $\mathbf{Q}$-algebra with center F of degree f over $\mathbf{Q}$. Let L/F be an extension splitting E, that is $E \otimes_F L \simeq \mathrm{M}_n(L)$. Let tr_L be the trace map on $\mathrm{M}_n(L)$ and note that $E \subset \mathrm{M}_n(L)$. Then for all $x \in E$ we have*

$$\mathrm{Tr}_E(x) = \mathrm{tr}(x).$$

Furthermore, considering the embedding $E \subset E \otimes_{\mathbf{Q}} \mathbf{C}$ with $E \otimes_{\mathbf{Q}} \mathbf{C} \simeq \prod_{i=1}^{f} \mathrm{M}_n(\mathbf{C})$ with $\mathrm{tr}_{\mathbf{C}}$ the sum of the trace on each factor, then for $x \in E$ we have $\mathrm{tr}_{\mathbf{C}}(x) = f \cdot \mathrm{Tr}_E(x)$.

Proof. The first part is just [Sch85] Lemma 8.5.11. The second part follows as the embedding $E \subset E \otimes_{\mathbf{Q}} \mathbf{C}$ is the diagonal embedding which recovers the embedding $E \subset E \otimes_F \mathbf{C}$ on each factor. □

For a simple $\mathbf{R}$-algebra $\mathrm{M}_n(D)$ let us denote by $\dagger$ the positive involution given by the conjugate-transpose. For a product of simple $\mathbf{R}$-algebra we denote by $\dagger$ again the positive involution given by the conjugate-transpose on each factor.

Lemma 2.5. *Let E be a simple $\mathbf{Q}$-algebra with a positive involution $*$. Then, there is an isomorphism*

$$(E \otimes_{\mathbf{Q}} \mathbf{R}, *) \simeq (\prod_{i=1}^{r} \mathrm{M}_n(D), \dagger).$$

Furthermore, there is an isomorphism $E \otimes_{\mathbf{Q}} \mathbf{C} \simeq \prod_{i=1}^{f} \mathrm{M}_n(\mathbf{C})$ such that $*$ is given by the conjugate-transpose through the corresponding embedding $E \subset \prod_{i=1}^{f} \mathrm{M}_n(\mathbf{C})$.

Proof. The proof of the first part is identical to the proof of [Sch85] Theorem 8.13.3. The second part follows from Remark 8.13.4 of *loc. cit.* in the case that $D = \mathbf{R}$ or $D = \mathbf{H}$. If $D = \mathbf{C}$, the extension of scalars to $\mathbf{C}$ gives a diagonal embedding $\mathrm{M}_n(D) \subset \mathrm{M}_n(\mathbf{C}) \times \mathrm{M}_n(\mathbf{C})$. It is a simple computation that $*$ is recovered again by the conjugate-transpose on each factor. □

We can now characterize polarizable $\mathbf{Q}$-algebras by the use of hermitian forms.

Proposition 2.6. *The following statements are equivalent.*

(*i*) *The algebra E is polarizable.*
(*ii*) *All $\mathbf{C}$-representation V of E admits a positive definite hermitian form H such that the adjunction on $\mathrm{End}_{\mathbf{C}} V$ induced by H leaves the image of E invariant.*
(*iii*) *The representation $V_r(E)$ admit a positive definite hermitian form H such that the adjunction on $\mathrm{End}_{\mathbf{C}} V$ induced by H leave E invariant.*

Proof. For $(i) \Rightarrow (ii)$, let V be a $\mathbf{C}$-representation of E and consider its decomposition $V = \oplus_{i=1}^{f} V_i^{n_i}$. The image of $E \otimes_{\mathbf{Q}} \mathbf{C}$ in $\mathrm{End}_{\mathbf{C}} V$ is a diagonal embedding of the simple factors such that $n_i \neq 0$ repeated n_i times. By the choice of a basis of V, and thus an isomorphism $\mathrm{M}_n(\mathbf{C}) \simeq \mathrm{End}_{\mathbf{C}} V$ and by Lemma 2.5 the adjunction to the standard positive definite hermitian form, which is the conjugate-transpose, restricts to the image of $E \otimes_{\mathbf{Q}} \mathbf{C}$ in $\mathrm{M}_n(\mathbf{C})$ by stabilizing the image of E.

The implication $(ii) \Rightarrow (iii)$ is trivial. So consider the $\mathbf{C}$-representation $V_r(E)$ and assume it admits a positive definite hermitian form H such that the image of E in $\mathrm{End}_{\mathbf{C}} V_r(E)$ – note that the sequence of maps $E \to E \otimes_{\mathbf{Q}} \mathbf{R} \to \mathrm{End}_{\mathbf{C}} V_r(E)$ is injective – is stable by the adjunction induced by H. By Lemma 2.4 this adjunction restricts to a positive involution on $E \otimes_{\mathbf{Q}} \mathbf{R}$ which stabilizes E and thus it induces a positive involution on E. □

For the rest of the section we will furthermore assume that E is polarizable with positive involution *. We can now define the dual representation of a $\mathbf{C}$-representation of E.

Definition 2.7. Let V be a $\mathbf{C}$-representation of E given by the action $\rho\colon E \to \mathrm{End}_{\mathbf{C}} V$. Then the dual representation $V^\vee$ of E is the dual vector space $V^\vee$ with the action of $x \in E$ given by $\rho(x^*)^t$.

We say that a non degenerate bilinear form B on V is invariant if it induces an isomorphism of $\mathbf{C}$-representations $V \simeq V^\vee$.

We say that V is polarized if there is a non degenerate symplectic form on V which is invariant.

Note that for $x \in E$ and $v \in V^\vee$, the action of x on v is given, in matrix form with a basis B of V and the corresponding dual basis of $V^\vee$ by

$$\rho(x^*)^t \cdot v = (v^t \cdot \rho(x^*))^t.$$

Lemma 2.8. *Let V be a $\mathbf{C}$-representation of E. There is a positive definite hermitian form on V which induces a $\mathbf{C}$-anti-isomorphism $V \simeq V^\vee$. In particular, the central trace $\mathrm{tr}_{V^\vee}$ of $V^\vee$ is given by $\overline{\mathrm{tr}_V}$.*

Proof. As before we consider an hermitian form H on V such that the adjunction coincides with * on the image of E and choose a basis for which it is the conjugate transpose. Let $h\colon V \to V^\vee$ be the anti-isomorphism induced by H. Then for $x \in E$ and $v \in V$, we have that

$$h(\rho(x) \cdot v) = \overline{v}^t \cdot \overline{\rho(x)}^t.$$

Now, since $\rho(x)^t = \rho(x^*)$ we get both claims by writing the product $\overline{v}^t \cdot \overline{\rho(x^*)}$ in the dual basis in a standard way, which corresponds to transposing again. □

Lemma 2.9. *Let V be a simple $\mathbf{C}$-representation of E. Then tr_V has values in $\mathbf{R}$ if and only if $V \simeq V^\vee$ and there is an $\mathbf{R}$-representation V_0 of E such that $V \simeq V_0 \otimes_{\mathbf{R}} \mathbf{C}$ if and only if there is a non-degenerate bilinear symmetric form on V which is invariant.*

Proof. The first part of the statement follows directly from Lemma 2.2. For the second part, if $V \simeq V_0 \otimes_{\mathbf{R}} \mathbf{C}$ note that V_0 corresponds to a simple factor of $E \otimes_{\mathbf{Q}} \mathbf{R}$ of the form $M_n(\mathbf{R})$ and not $\mathrm{M}_n(\mathbf{H})$ as V would not be simple in that last case. In that case, the positive involution can just be given by the transposition on $\mathrm{End}_{\mathbf{R}} V_0$ and we thus recover a symmetric bilinear form on V_0 which induces an isomorphism $V \simeq V^\vee$ after base change. For the converse, let B be the invariant bilinear symmetric form on V. We follow the proof of [Ser77] of the corresponding statement for group representations on p.107–108. Let H be an hermitian positive definite form such that the

adjunction recovers the involution on E and $h\colon V \to V^\vee$ the induced map. For all $x \in V$ there is a unique element $\varphi(x)$ such that for all $y \in Y$

$$B(x,y) = \overline{H(\varphi(x),y)}.$$

The map φ obtained in this way is antilinear and bijective. Its square φ^2 is an automorphism of V. Since B is symmetric we have for all $x, y \in V$

$$H(\varphi^2(x),y) = \overline{B(\varphi(x),y)} = \overline{B(y,\varphi(x))} = H(\varphi(y),\varphi(x)).$$

It follows that φ^2 is hermitian as $H(\varphi(y),\varphi(x)) = \overline{H(\varphi(x),\varphi(y)}$ and thus from the previous equality we get

$$H(\varphi^2(x),y) = \overline{H(\varphi^2(y),x)} = H(x,\varphi^2(y)).$$

From the equality, for all $x \in V$,

$$H(\varphi(x),\varphi(x)) = H(\varphi^2(x),x)$$

we see that φ^2 is positive definite. We thus get a unique hermitian positive definite $v \in \mathrm{End}_{\mathbf{C}} V$ such that $v^2 = \varphi^2$ and v commutes with φ. Set $\sigma = \varphi \circ v^{-1}$, it is an antilinear endomorphism of V. We get $\sigma^2 = \mathrm{id}$. Let V_0 and V_1 be the eigenspaces of σ for the values 1 and -1 respectively. Since σ is antilinear we have $V_1 = iV_0$ and

$$V = V_0 \oplus iV_0.$$

But since B and H are invariant for the action of E we get that V_0 and $V_1 = iV_0$ are stable and $V = V_0 \otimes_{\mathbf{R}} \mathbf{C}$ as desired. □

Proposition 2.10. *Let V be a simple $\mathbf{C}$-representation of E and $n \in \mathbf{N}$. Then exactly one of the three following possibilities holds.*

- *(i) The representation V is not isomorphic to its dual $V^\vee$.*
- *(ii) There is a non degenerate symmetric form on V which is invariant.*
- *(iii) There is a non degenerate bilinear symplectic form on V which is invariant.*

In the first case, the smallest $\mathbf{C}$-representation of E containing V^n which is polarized is $V^n \oplus (V^\vee)^n$. In the second case if V^n is polarized then n is even.

Proof. The distinction between the first case and the two others is just whether $V \simeq V^\vee$, or whether tr_V has values in $\mathbf{R}$. If it does, then there is a non-degenerate bilinear form on V coming from the isomorphism $V \simeq V^\vee$. Let B be this form and $B = B_0 + B_1$ its decomposition in symmetric and alternate parts. Both induce maps of $\mathbf{C}$-representation between V and $V^\vee$ so that by Schur's lemma only one is non zero.

In the first two cases we see that $V \oplus V^\vee$ is polarized by considering the standard symplectic form on a basis adapted to the direct sum decomposition. Now let W be a representation containing V^n which is polarized. Since $W \simeq W^\vee$, in the case that V is not isomorphic to its dual we must have $(V^\vee)^n \subset W^\vee$ but also V^n by the isomorphism $W \simeq W^\vee$.

In the second case, let $\lambda\colon V^n \simeq (V^\vee)^n$ be the isomorphism induced from an invariant symplectic form on V^n. For a simple sub-representation $W \subset V^n$, $W \simeq V$, we have $\lambda(W) \subset W^\perp$ as the symplectic form restricts to the zero form on W. It follows that $W \oplus \lambda^{-1}(W^\vee)$ form a symplectic subspace of V^n. By induction we thus get that n is even. □

2.1.2. The skew-fields over $\mathbf{Q}$ of finite dimension which are polarizable have been classified by Albert. We will recall this classification here, see [Mum08] p.186 (202) for more details. First, we need some results on the classification of simple algebras. By class field theory, skew-fields E over $\mathbf{Q}$ are classified by local invariants $\mathrm{inv}_v E$ at the places v of the center F. By the Brauer-Hasse-Noether theorem these local invariants are given by an element of $\mathbf{Q}/\mathbf{Z}$ which is moreover in $\mathbf{Z}/2\mathbf{Z}$ if v is an infinite real place and 0 if it is a complex place, only finitely many of them are non zero and they sum to zero in $\mathbf{Q}/\mathbf{Z}$. In general we extend this classification by Wedderburn's theorem. That is if E is a simple $\mathbf{Q}$-algebra isomorphic to $\mathrm{M}_n(D)$ for some skew-field D with center F, we set $\mathrm{inv}_v(E) = \mathrm{inv}_v(D)$ for a place v of F. These invariants classify such algebras E – see [Sch85] chapter 8 for an introduction to Brauer groups and Brauer equivalence and [Har17] for the computation of Brauer groups of local fields and the Brauer-Hasse-Noether theorem. Now, the Albert classification has four types.

- Type I : The skew-field D is a totally real number field.
- Type II : The skew-field D is a quaternion algebra over its center F. The number field F is totally real and for every embedding $\sigma\colon F \to \mathbf{R}$ there is an isomorphism
$$\mathbf{R} \otimes_F D \simeq M_2(\mathbf{R}).$$
- Type III : The skew-field D is a quaternion algebra over its center F. The number field F is totally real and for every embedding $\sigma\colon F \to \mathbf{R}$ there is an isomorphism
$$\mathbf{R} \otimes_F D \simeq \mathbf{H}$$
where $\mathbf{H}$ is the standard quaternion algebra over $\mathbf{R}$.
- Type IV : The center F of D is a totally imaginary quadratic extension of a totally real field F_0 with conjugation $\bar{\cdot}$ over F_0. The local invariants are such that for any finite place v such that $\overline{v} = v$ then $\mathrm{inv}_v(D) = 0$ and otherwise $\mathrm{inv}_v(D) + \mathrm{inv}_{\overline{v}}(D) = 0$.

By the theorem of Wedderburn again we extend this classification to simple and polarizable $\mathbf{Q}$-algebras of finite dimension. That is if $E \simeq \mathrm{M}_n(D)$ for some skew-field D is polarizable then D is polarizable and the type of E is that of D.

We can now restate Proposition 2.10 in this context.

Proposition 2.11. *Let $n \in \mathbf{N}$. If E is of type III then every simple representation is polarized. If it is of type IV, for every simple representation V of E, the smallest representation containing V^n which is polarized is $V^n \oplus (V^\vee)^n$. If it is of type I or II, for every simple representation V, the representation V^n is polarized if and only if n is divisible by 2.*

Proof. First we see that if E is of type I, II or III if and only if for every simple representation V the central trace has values in $\mathbf{R}$. This settles the case of type IV with Proposition 2.10, as in this case a simple representation V is not isomorphic to its dual.

For type I and II we see that every simple representation V is of the form $V_0 \otimes_{\mathbf{R}} \mathbf{C}$ and thus the result follows from Lemma 2.9 and Proposition 2.10.

If E is of type III we see that the simple modules V can not be written in the form $V \otimes_{\mathbf{R}} V_0$ as we have $\dim_{\mathbf{C}} V = 2$ while simple $\mathbf{R}$-representation are of dimension 4. It follows from Lemma 2.9 together with Proposition 2.10 that all such V are polarized. □

2.1.3. We move to consider representations that are rational and classify them. We also classify those that are rational and polarized by the type of the polarizable algebra E.

Definition 2.12. A $\mathbf{C}$-representation V of E is rational if the characteristic polynomials of the image of the elements of E as endomorphisms of V have coefficients in $\mathbf{Q}$.

From Wedderburn's theorem we have that $E \simeq \mathrm{M}_n(D)$ for some skew-field $D/\mathbf{Q}$ of finite dimension and center F. Let us set $d^2 = [D : F]$ and $f = [F : \mathbf{Q}]$ as well as $\deg(E) = ndf$.

The following is roughly Lemma 1 of chapter II of [ST61]. We record it here for completeness.

Lemma 2.13. *Let V be a rational $\mathbf{C}$-representation of E. Then V is a free $F \otimes_{\mathbf{Q}} \mathbf{C}$-module.*

Proof. Let again $\{\sigma_1, \dots, \sigma_f\}$ denote the embeddings of F in $\mathbf{C}$. The representation V is given by the direct sum of $V_i^{n_i}$ and for $x \in F$ we have

$$\mathrm{tr}_V(x) = nd \sum_{i=1}^{f} n_i \sigma_i(x).$$

We thus see that $\mathrm{tr}_V(x)$ is rational for all $x \in F$ if and only if n_i is independent of i. That is, we have

$$V \simeq (\bigoplus_{i=1}^{f} V_i)^m \simeq (\bigoplus_{i=1}^{f} \mathbf{C}^{nd})^m$$

as a $F \otimes_{\mathbf{Q}} \mathbf{C}$-module. □

Theorem 2.14. *All the rational (resp. and polarized) $\mathbf{C}$-representations of E are multiples of the representation $V_r(E)$ (resp. a unique such representation denoted $V_{rp}(E)$). Furthermore we have that $\dim_{\mathbf{C}} V_r(E) = \deg E$, $V_{rp}(E) \simeq V(E)$ if E is of type III and IV, and $V_{rp}(E) \simeq V_r(E)^2$ if E is of type I and II.*

Proof. Let V be a rational $\mathbf{C}$-representation of E. By Lemma 2.13 we have that V is a free $F \otimes_{\mathbf{Q}} \mathbf{C}$-module, that is

$$V \simeq (\prod_{i=1}^{f} \mathbf{C})^m$$

for some $m \in \mathbf{N}$. It follows that $mf = \dim_{\mathbf{C}} V$.

On the other hand, we have an isomorphism $E \otimes_{\mathbf{Q}} \mathbf{C} \simeq \prod_{i=1}^{f} E_i$ with $E_i \simeq \mathrm{M}_{nd}(\mathbf{C})$ a simple algebra whose simple module is $V_i = \mathbf{C}^{nd}$. Hence a decomposition

$$V \simeq \bigoplus_{i=1}^{f} V_i^{n_i}.$$

It follows that $V_i^{n_i}$ is isomorphic to $\mathbf{C}^m$ as a vector space and thus

$$ndn_i = m.$$

Finally, we get that $V \simeq V_r(E)^{\frac{m}{nd}}$ as a $\mathbf{C}$-representation of E. Note that since $V_r(E) = \bigoplus_{i=1}^{f} V_i$ and $\dim_{\mathbf{C}} V_i = nd$ the equality $\dim_{\mathbf{C}} V_r(E) = \deg(E)$ holds.

For the last part of the statement, first note that from the first part if V is rational and polarized it is a multiple of $V_r(E)$. Now, by Proposition 2.11 if E is of type III the equality $V_r(E) = V_{rp}(E)$ holds. If E is of type IV, we have that $f = 2f^+$ for some $f^+ \in \mathbf{N}$ and that for $i \in \{1, \dots, f\}$ the

simple representation V_i is not isomorphic to its dual $V_i^\vee$. As we also have that $V_i^\vee = V_j$ for some $j \in \{1, \dots, f\}$, up to some renumbering we get

$$V_r(E) = \bigoplus_{i=1}^{f^+} V_i \oplus V_i^\vee.$$

Again Proposition 2.11 gives that $V_r(E) = V_{rp}(E)$ in this case.

For the remaining cases, where E is of type I and II, let $V \simeq V_r(E)^m$ be a rational and polarized $\mathbf{C}$-representation of E. As the isomorphism $V \simeq V^\vee$ from the symplectic form on V respects the action of E it induces an isomorphism between corresponding isotypic components of V and $V^\vee$. Since in those cases, every isotypic component is isomorphic to its dual, this gives that the symplectic form on V induces a non degenerate invariant symplectic form on each of its isotypic components V_i^m. Proposition 2.11 gives that m is divisible by 2. We thus have that $V \simeq V_r(E)^{2k}$ and $V_{rp}(E) = V_r(E)^2$. □

For the rest of the text we will keep the notation $V_r(E)$ and $V_{rp}(E)$ for the unique rational or rational and polarized $\mathbf{C}$-representations of a simple polarizable $\mathbf{Q}$-algebra E which generates the others.

2.2. Geometric Albert algebras and good embeddings

2.2.1. Let us fix a prime number p. We will say that a simple $\mathbf{Q}$-algebra E of finite dimension is quasi-split outside p if $E \otimes_{\mathbf{Q}} \mathbf{Q}_\ell$ is quasi-split for all primes $\ell \neq p$ – an algebra is quasi-split if its a matrix algebra over a field. This is equivalent to the fact that the local invariants of E at all finite places not above p are 0.

Definition 2.15. Let E and E' be polarizable simple $\mathbf{Q}$-algebras. A good embedding is an injective morphism $E \hookrightarrow E'$ such that $V_{rp}(E) = V_{rp}(E')$.

Note that when there is an embedding $E \hookrightarrow E'$ we have that $\deg(E) \mid \deg(E')$. In the case of a good embedding, from Theorem 2.14 it follows that either $\deg(E) = \deg(E')$ or $2\deg(E) = \deg(E')$.

Lemma 2.16. *A polarizable simple algebra E quasi-split outside p admits a good embedding in a polarizable algebra E' quasi-split outside p of type IV if and only if it is not of type III.*

Proof. Consider a good embedding $E \hookrightarrow E'$ and denote by F and F' the centers of E and E' respectively. Let $F_0 = F \cap F'$. We get an embedding

$$E \otimes_{F_0} F' \hookrightarrow E'.$$

It follows that $\dim_{\mathbf{C}} V_r(E \otimes_{F_0} F') \leq \dim_{\mathbf{C}} V_{rp}(E') = \deg(E')$. As the embedding $E \hookrightarrow E'$ is good we also have that

$$\epsilon \deg E = \deg E'$$

where ϵ is 1 if E is of type III or IV and 2 if it is of type I or II. Now, if E is of type III, then as F' is a CM field we have an inequality

$$\dim_{\mathbf{C}} V_r(E \otimes_{F_0} F') = \deg(E \otimes_{F_0} F') \geq 2\deg(E)$$

and we get a contradiction

$$\deg E = \deg E' \geq 2 \deg E.$$

For the converse, if E is of type I or II we consider the embedding

$$E \hookrightarrow E \otimes_F K$$

for a CM field extension K/F of degree 2. Note that $E\otimes_F K$ is a type IV simple algebra quasi-split outside p. This embedding is good as

$$V_{rp}(E) = V_r(E)^2 = V_r(E\otimes_F K) = V_{rp}(E\otimes_F K).$$

□

2.2.2. For a simple abelian variety A over $\overline{\mathbf{F}_p}$ the endomorphism algebra $\operatorname{End} A\otimes\mathbf{Q}$ is a polarizable simple $\mathbf{Q}$-algebra quasi-split outside p. By the works of Tate, if $E\simeq \operatorname{End} A\otimes\mathbf{Q}$ for some abelian variety A over $\mathbf{F}_{p^n}$ there is a description of $\operatorname{inv}_v E$ in terms of the valuation at v of the Frobenius of A if $p\mid v$. A precise statement is given by [Tat71] Théorème 1. The algebra $D=\operatorname{End} A\otimes_{\mathbf{Z}}\mathbf{Q}$ is central over $\mathbf{Q}(\pi)$ where π is the Frobenius of A, it is quasi-split outside p and we have

$$\begin{cases}\operatorname{inv}_v(D) = \frac{v(\pi)}{v(p^n)}\cdot[\mathbf{Q}(\pi)_v\colon \mathbf{Q}_p] \text{ for all places } v\mid p\\ \operatorname{inv}_v(D)=0 \text{ for all places } v \text{ above a prime } \ell\neq p\\ \operatorname{inv}_v(D)=\frac{1}{2} \text{ for all real places } v\end{cases}$$

Furthermore, the equality $2\dim A=\deg D$ holds.

Definition 2.17. A polarizable simple $\mathbf{Q}$-algebra E quasi-split outside p is said to be geometric if there is an abelian variety A over $\overline{\mathbf{F}_p}$ such that

$$E\simeq \operatorname{End} A\otimes\mathbf{Q}.$$

For simplicity, we will say that an algebra E is geometric if it is a polarizable simple $\mathbf{Q}$-algebra quasi-split outside p and it is geometric.
Let us denote by $\mathbf{H}_{p,\infty}$ the quaternion algebra over $\mathbf{Q}$ quasi-split outside p such that $\operatorname{inv}_p(\mathbf{H}_{p,\infty}) = \operatorname{inv}_\infty(\mathbf{H}_{p,\infty}) = 1/2$. The following fact is direct from [Tat71] Exemple (a) p.97.

Lemma 2.18. *Let E be a geometric $\mathbf{Q}$-algebra of type III. Then E is the endomorphism algebra of a power of a supersingular elliptic curve over $\overline{\mathbf{F}_p}$ and we have*

$$E\simeq \mathrm{M}_n(\mathbf{H}_{p,\infty}).$$

Lemma 2.19. *If E is of type III, quasi-split outside p and there is a good embedding $E\hookrightarrow E'$ with E' polarizable, geometric and quasi-split outside p then $E\simeq \mathrm{M}_n(F\otimes\mathbf{H}_{p,\infty})$ for some totally real number field F.*

Proof. By Lemma 2.16 we have that E' is of type III. Since E' is geometric, the previous lemma gives an isomorphism

$$E'\simeq \mathrm{M}_{n'}(\mathbf{H}_{p,\infty}).$$

Let $E\simeq \mathrm{M}_n(D)$ so that $\deg(E)=2nf$ where $f=[F:\mathbf{Q}]$ with $F=Z(E)$ the center of E. Since the embedding is good we have $\deg(E)=\deg(E')$ which is

$$2nf = 2n'$$

so that $n'=nf$. The centralizer $Z_{E'}(E)$ of E in E' is a simple algebra that contains F and from the centralizer theorem, see [Sch85] chapter 8, Theorem 5.4 we have that

$$\dim Z_{E'}(E)\cdot\dim E = d^2f\cdot 4n^2f = \dim E' = 4n^2f^2.$$

It follows that $d=1$ and $Z_{E'}(E)=F$. It also follows from [Sch85] chapter 8, Theorem 4.5 that

$$E'\otimes_{\mathbf{Q}} F\sim Z_{E'}(F)=E$$

where $\sim$ denotes the Brauer equivalence – that the algebras have the same local invariants. This is equivalent to the fact that there is an isomorphism

$$E \simeq \mathrm{M}_n(F \otimes \mathbf{H}_{p,\infty}).$$

□

2.2.3. In order to prove the main theorem of this section we need to recall some facts about Weil numbers and Honda-Tate theory – see [Tat71].

Definition 2.20. Let $q = p^n$. A Weil q-number (sometimes q-Weil number) is an algebraic integer π such that for all embedding $\sigma\colon \mathbf{Q}(\pi) \hookrightarrow \mathbf{C}$ we have

$$|\sigma(\pi)| = q^{\frac{1}{2}}.$$

The theorem of Honda-Tate states that there is a one-to-one correspondence between conjugacy classes of Weil q-numbers and simple abelian varieties over $\mathbf{F}_q$ up to isogeny. In particular, to construct abelian varieties over finite fields it is enough to construct such algebraic integers.

Proposition 2.21. *A simple polarizable* $\mathbf{Q}$*-algebra of type IV quasi-split outside* p *admits a good embedding in a geometric* $\mathbf{Q}$*-algebra.*

Proof. Let E be a simple polarizable $\mathbf{Q}$-algebra of type IV quasi-split outside p. As before, let $E \simeq \mathrm{M}_n(D)$ for some skew-field D over $\mathbf{Q}$ with center F. The skew-field D is itself a simple polarizable $\mathbf{Q}$-algebra of type IV with center F and if it admits a good embedding in a geometric polarizable $\mathbf{Q}$-algebra E' of type IV quasi-split outside p then $E \hookrightarrow \mathrm{M}_n(E')$ is a good embedding. So we will assume $E = D$.

From the definition the fact that D is of type IV we have that $\mathrm{inv}_v(D) + \mathrm{inv}_{\overline{v}}(D) = 0$ in $\mathbf{Q}/\mathbf{Z}$ for all finite places v of F. For all those places v above p, let us choose a non-negative representative in $\mathbf{Q}$ of $\mathrm{inv}_v(D)$ such that $\mathrm{inv}_v(D) + \mathrm{inv}_{\overline{v}}(D) = [F_v : \mathbf{Q}_p]$. Note that if $v = \overline{v}$ we have that $[F_v : \mathbf{Q}_p]$ is even by the characterization of type IV so that we can avoid choosing $\mathrm{inv}_v(D) = 1/2$. For a place v of F let e_v be the ramification index at v. Let $n \in \mathbf{N} \setminus \{0\}$ be such that for all places v above p

$$n \cdot \frac{\mathrm{inv}_v(D)}{[F_v : \mathbf{Q}_p]} \in \mathbf{N}$$

and for a place v above p let

$$n_v = ne_v \cdot \frac{\mathrm{inv}_v(D)}{[F_v : \mathbf{Q}_p]}.$$

Note that we have $n_v + n_{\overline{v}} = ne_v$ by construction.

Consider the ideal $\prod_{v|p} \mathfrak{p}_v^{n_v}$ where $\mathfrak{p}_v$ is the prime of $\mathcal{O}_F$ associated to the place $v \mid p$. Then, up to multiplying n by an integer big enough we can assume this ideal is principal, given by (π). We have

$$(\pi\overline{\pi}) = \prod_{v|p} \mathfrak{p}_v^{n_v + n_{\overline{v}}} = \prod_{v|p} (\mathfrak{p}_v^{e_v})^n = (p^n).$$

Thus we have $\pi\overline{\pi} = p^n u_0$ with $u_0 \in \mathcal{O}_{F^+}^\times$. Let $m \in \mathbf{N}$ be such that $u_0^m = u\overline{u}$ with $u \in \mathcal{O}_F^\times$, this is possible as the norm map has finite index.

Now consider $\pi_1 = \pi^m u^{-1}$. We have

$$\pi_1\overline{\pi_1} = p^{nm} u_0^m u_0^{-m} = p^{mn}.$$

In particular, π_1 is a Weil p^{mn}-integer and the associated abelian variety by Honda-Tate theory A_0 is such that $D_0 = \operatorname{End} A_0 \otimes \mathbf{Q}$ has center $F_0 = \mathbf{Q}(\pi_1)$ and invariants

$$\operatorname{inv}_{v_0}(D_0) = \frac{v_0(\pi_1)}{v_0(p^{mn})} \cdot [F_{0v_0} : \mathbf{Q}_p] = \frac{mn_v}{mne_v} \cdot [F_{0v_0} : \mathbf{Q}_p] = \frac{\operatorname{inv}_v(D)}{[F_v : F_{0v_0}]}$$

for all places $p \mid v_0 \mid v$ of $\mathbf{Q}(\pi_1)$ above p and below v.

It follows that $D = D_0 \otimes_{\mathbf{Q}(\pi_1)} F$ and that $D \subset \operatorname{End} A_0^{[F:\mathbf{Q}(\pi_1)]} \otimes \mathbf{Q} = \mathrm{M}_{[F:\mathbf{Q}(\pi_1)]}(D_0)$. The simple algebra D_0 has degree $\deg(D_0) = d \cdot [\mathbf{Q}(\pi_1) : \mathbf{Q}]$ so that

$$\deg(D) = df = d \cdot [F : \mathbf{Q}(\pi_1)] \cdot [\mathbf{Q}(\pi_1) : \mathbf{Q}] = \deg(\mathrm{M}_{[F:\mathbf{Q}(\pi_1)]}(D_0))$$

and the embedding is good. □

We can now state the main theorem of this section.

Theorem 2.22. *A simple and polarizable $\mathbf{Q}$-algebra E quasi-split outside p admits a good embedding into a geometric $\mathbf{Q}$-algebra E' if and only if it is either not of type III or of the form $\mathrm{M}_n(F \otimes \mathbf{H}_{p,\infty})$ for some totally real number field F.*

Proof. Assume first that E is of type III. Then by Lemma 2.19 if E admits a good embedding it is of the required form. So assume furthermore that $E \simeq \mathrm{M}_n(F \otimes \mathbf{H}_{p,\infty})$ for some totally real number field F. Then the embedding

$$E \hookrightarrow \mathrm{M}_{fn}(\mathbf{H}_{p,\infty})$$

is good where $f = [F : \mathbf{Q}]$.

In all other cases, combine Lemma 2.16 with Proposition 2.21 to get the result. □

3. The rational group algebra of ramification groups

We start by developing some technical points on $\mathbf{Q}$-algebras that are twisted by cyclic groups. The main results is given in the second part of the section and applies the results of the first part to give a description of the rational group algebra $\mathbf{Q}[G]$ of ramification groups, giving precisions to a theorem of Serre and generalizing results of Roquette and Ford.

3.1. Twisted Q-algebras

3.1.1. Let G be a finite group. For a finite dimensional $\mathbf{Q}$-algebra E and a morphism $\varphi\colon G \to \operatorname{Aut} E$ we denote by $E[G,\varphi]$ the $\mathbf{Q}$-algebra defined by $\bigoplus_{g\in G} E.g$ where the multiplication is given, for all $x, y \in E$ and all $g, h \in G$, by

$$xg \cdot yh = x\varphi(g)(y) \cdot gh.$$

When E has a positive involution $*$ and φ verifies $\varphi(g)(x)^* = \varphi(g)(x^*)$ for all $g \in G$ and $x \in E$, that is $\varphi(G) \subset \operatorname{Aut}(E,*)$, then there is an induced involution on $E[G,\varphi]$ given by

$$(xg)^* = g^{-1}x^* = \varphi(g^{-1})(x^*)g^{-1}.$$

Lemma 3.1. *The involution induced by $*$ on $E[G,\varphi]$ is positive if and only if $*$ is.*

Proof. For all $x \in E$ and $g \in G$ we have

$$\begin{aligned}(xg)(xg)^* &= xg\varphi(g^{-1})(x^*)g^{-1}\\ &= x\varphi(g)\big(\varphi(g^{-1})(x^*)\big)gg^{-1}\\ &= xx^*.\end{aligned}$$

The statement now follows as the multiplication by xx^* on $E[G,\varphi]$ stabilizes the direct sum decomposition we have $\mathrm{Tr}_{E[G,\varphi]}(xx^*) = \mathrm{Card}\, G \cdot \mathrm{Tr}_E(xx^*)$. □

Note that for a finite group H the rational group algebra $\mathbf{Q}[H]$ is equipped with a natural positive involution – see the last section of [Lew06] for example – given for $h \in H$ by

$$h \mapsto h^{-1}.$$

Thus from Proposition 8.1 of [Rém17] each of the simple factor $E \subset \mathbf{Q}[G]$ that appear in the decomposition of $\mathbf{Q}[G]$ is a polarizable $\mathbf{Q}$-algebra. This is a particular case of the construction presented here with $\varphi\colon G \to \mathrm{Aut}\,\mathbf{Q}$ the trivial map and $*$ the identity on $\mathbf{Q}$.

Assume now that H is carrying a G action by a map $G \to \mathrm{Aut}\, H$. The action extends to a map $\varphi\colon G \to \mathrm{Aut}\,\mathbf{Q}[H]$ and we have

$$\mathbf{Q}[H][G,\varphi] = \mathbf{Q}[H \rtimes G].$$

One can check that the action of G is compatible with the natural involution on $\mathbf{Q}[H]$ and the induced involution on $\mathbf{Q}[H \rtimes G]$ is again the natural one.

3.1.2. We will now only consider the case when the acting group G is cyclic. Let $m \in \mathbf{N}$ be such that $G \simeq \mathbf{Z}/m\mathbf{Z}$ and let $\sigma = \varphi(1) \in \mathrm{Aut}\, E$. In this situation we will write $E[m,\sigma]$ in place of $E[G,\varphi]$. We also write

$$E[m,\sigma] = \bigoplus_{i=0}^{m-1} E.u^i$$

with $ux = \sigma(x)u$ for $x \in E$ and $u^m = 1$.

We are interested in the center of such algebras. Let us start by a special case. The algebra E is simple and let $\tau = \sigma_{|Z(E)} \in \mathrm{Aut}\, Z(E)$. The order n of τ divides m and we have that σ^n is an automorphism of the simple algebra E central over $F = Z(E)$. By Skolem-Noether's theorem we get that there is an element $y \in E^\times$ such that for all $x \in E$ we have

$$\sigma^n(x) = y^{-1}xy.$$

We show that we can further choose y to be fixed by σ and have further properties.

Proposition 3.2. *Let E be a simple algebra with an automorphism σ of order m. Let $\tau = \sigma_{|Z(E)}$ and n its order. Then we can choose $y \in E^\times$, such that for all $x \in E$*

$$\sigma^n(x) = y^{-1}xy,$$

to be fixed by σ. In this case, $y^{\frac{m}{n}}$ is an element of F^τ and there is an isomorphism

$$\psi\colon Z(E[m,\sigma]) \simeq F^\tau[X]/(X^{\frac{m}{n}} - y^{\frac{m}{n}}).$$

Moreover, if E has a positive involution $*$ stable by σ which induces an involution noted $*$ again on $E[m,\sigma]$ we can choose ψ such that $X^* = yy^*X^{-1}$ in the quotient. In particular, we have $yy^* \in F^\tau$.

Proof. Let us start by showing we can choose such a y to be fixed by σ. Start with $y \in E^\times$ given by Skolem-Noether's theorem applied to σ^n. As the automorphisms σ and σ^n of E commute, we have for all $x \in E$

$$\sigma(\sigma^n(x)) = \sigma(y)^{-1}\sigma(x)\sigma(y) = \sigma^n(\sigma(x)) = y^{-1}\sigma(x)y$$

so that $\sigma(x)\sigma(y)y^{-1} = \sigma(y)y^{-1}\sigma(x)$ and thus $t = \sigma(y)y^{-1}$ is an element of F.
In the cyclic extension F/F^τ the norm of t is

$$N_{F/F^\tau}(t) = \prod_{i=0}^{n-1} \tau^i(t) = \prod_{i=0}^{n-1} \sigma^i(\sigma(y)y^{-1}) = \sigma^n(y)y^{-1} = 1.$$

By the Hilbert's theorem 90 we get an element $s \in F^\times$ such that $t = \tau(s)s^{-1}$. Let us set $y' = ys^{-1}$. For all $x \in E$ we have

$$\sigma^n(x) = {y'}^{-1}xy'$$

as s commutes with x. The element y' verifies further

$$\sigma(y') = \sigma(y)\sigma(s^{-1}) = \sigma(y)\sigma(t)\sigma^2(s)^{-1} = \sigma^2(y)\sigma^2(s)^{-1} = \sigma^2(y')$$

which is just $y' = \sigma(y')$ as desired. For all $x \in E$ we also have

$$y'^{-\frac{m}{n}}xy'^{\frac{m}{n}} = \sigma^{n\cdot\frac{m}{n}}(x) = x.$$

In particular, $y'^{\frac{m}{n}}$ is central and fixed by τ.

We will now assume that y was chosen such that it has the properties proven in the first part and we show that there is an isomorphism $\psi\colon E[m,\sigma] \simeq F^\tau[X]/X^{\frac{m}{n}} - y^{\frac{m}{n}}$. By definition we have

$$E[m,\sigma] = \bigoplus_{i=0}^{m-1} Eu^i.$$

Let us consider an element $z \in Z(E[m,\sigma])$ given by

$$z = \sum_{i=0}^{m-1} a_i u^i.$$

Since $zu = uz$ we get $\sigma(a_i) = a_i$ for all $i \in \{0,\dots,m-1\}$ and the equality $zx = xz$ for all $x \in E$ gives $a_i\sigma^i(x) = xa_i$. For $i \in \{0,\dots,m-1\}$ such that n does not divide i there is an $x \in F$ such that $\sigma^i(x) \neq x$ and thus $a_i = 0$. Let us set $b_i = a_{ni}y^{-i}$ for $0 \leq i \leq \frac{m}{n} - 1$. For all $x \in E$ we have

$$xb_i = xa_{ni}y^{-i} = a_{ni}\sigma^{ni}(x)y^{-i} = a_{ni}y^{-i}x = b_ix$$

so that $b_i \in F$ and $\sigma(b_i) = b_i$ gives furthermore that $b_i \in F^\tau$. Going back to the element z we have

$$z = \sum_{i=0}^{\frac{m}{n}-1} b_i y^i u^{ni}$$

with $b_i \in F^\tau$. Conversely let us show that all elements z of this form are in the center of $E[m,\sigma]$. It is enough to check that it is the case for yu^n. Let $x \in E$, we have

$$yu^n x = y\sigma^n(x)u^n = xyu^n$$

and we also have

$$uyu^n = \sigma(y)u^{n+1} = yu^n \cdot u.$$

Thus we have $Z(E[m,\sigma]) = F^\tau[yu^n]$ with $(yu^n)^{\frac{m}{n}} = y^{\frac{m}{n}}$.

For the last part, note first that for all $x \in E$

$$(yy^*)^{-1}xyy^* = y^{*-1}y^{-1}xyy^* = y^{*-1}\sigma^n(x)y^* = (y\sigma^n(x^*)y^{-1})^* = x$$

and thus $yy^* \in F^\tau$. We now compute

$$yu^n(yu^n)^* = yu^n u^{-n}y^* = yy^*.$$

□

Specifying the context again we get a more precise statement.

Proposition 3.3. *Assume that $E \simeq \mathrm{M}_d(K)$ where K is a CM field and $*$ is a positive involution on E stable by σ. Let us assume furthermore that τ is the complex conjugation on K and that we have chosen y as in Proposition 3.2. Then $yy^* \in F^\tau$ is the square of an element of K.*

Proof. Let us denote by $\bar{\cdot}$ the complex conjugation and its extension to E acting on the coefficients on the matrices. By conjugation by an element $w \in E^\times$ we have $*$ given for all $x \in E$ by $x^* = w^{-1}\overline{x}^t w$. By Skolem-Noether's theorem we also have that $\sigma(x) = z^{-1}\overline{x}z$ for an element $z \in E^\times$ and all $x \in E$.

As for $x \in E$ we have

(*i*) $(x^*)^* = x$, which is $(w^{-1}\overline{x}^t w)^* = w^{-1}\overline{w}^t x(w^{-1}\overline{w}^t)^{-1} = x$

(*ii*) $\sigma(x)^* = \sigma(x^*)$ which is $w^{-1}\overline{\sigma(x)}^t w = w^{-1}\overline{z}^t x\overline{z^{-1}}^t w = z^{-1}\overline{w^{-1}}x^t\overline{w}z$

(*iii*) $\sigma^2(x) = y^{-1}xy$ which is $\sigma(z^{-1}\overline{x}z) = z^{-1}\overline{z^{-1}}x\overline{z}z = y^{-1}xy$

the elements $w^{-1}\overline{w}^t$, $\overline{w}zw^{-1}\overline{z^{-1}}$ and $\overline{z}zy^{-1}$ are central. By $\sigma(y) = y$ we even have that $y^{-1}z\overline{z}$, which is an element of K, is fixed by the complex conjugation and thus by $*$. We now have

$$\begin{aligned}
yy^* &= (\overline{z}zy^{-1})^{-1}\cdot\overline{z}z\cdot(\overline{z}z\cdot\overline{z}zy^{-1})^{-1})^* = (\overline{z}zy^{-1})^{-2}\cdot\overline{z}z\cdot(\overline{z}z)^* \\
&= (\overline{z}zy^{-1})^{-2}\cdot\overline{z}z\cdot w^{-1}\overline{z}^t w\cdot w^{-1}z^t w = (y^{-1}z\overline{z})^{-2}\cdot\overline{z}z\cdot w^{-1}\overline{z}^t z^t w \\
&= (\overline{z}zy^{-1})^{-2}\cdot\overline{z}\overline{w^{-1}}\overline{w}zw^{-1}\overline{z}^t z^t w = (\overline{z}zy^{-1})^{-2}\cdot\overline{w}zw^{-1}\overline{z}^t\cdot\overline{z}\overline{w^{-1}}z^t w \\
&= (\overline{z}zy^{-1})^{-2}\cdot\overline{w}zw^{-1}\overline{z}^t\cdot\overline{z}\overline{w^{-1}}w^t{w^{-1}}^t z^t\overline{w}^t\overline{w^{-1}}^t w.
\end{aligned}$$

Notice now that since $w^{-1}\overline{w}^t$ is central we have $w^{-1}\overline{w}^t = \overline{w}{w^{-1}}^t$ and thus

$$\begin{aligned}
yy^* &= (\overline{z}zy^{-1})^{-2}\cdot\overline{w}zw^{-1}\overline{z}^t\cdot\overline{z}{w^{-1}}^t z^t\overline{w}^t\cdot(w^{-1}\overline{w}^t)^{-2} \\
&= (\overline{z}zy^{-1})^{-2}\cdot(\overline{w}zw^{-1}\overline{z}^t)^2\cdot{\overline{w}^t}^{-2}.
\end{aligned}$$

The last equality is again from the fact that $\overline{w}zw^{-1}\overline{z}^t$ is central and thus fixed by the transposition. We finally have obtained that yy^* is a square of an element of K. □

3.1.3. In order to deal with the general case, where E is not assumed simple, we will need a few lemmas that might be well known.

Lemma 3.4. *Let E be a simple $\mathbf{Q}$-algebra, $k, m \geq 1$ and $f \in \operatorname{Aut} E^k$ such that $f^m = 1$. Then we can choose a basis $(x_1, \ldots, x_k)$ and a partition $I_1, \ldots, I_r$ of $\{1, \ldots, k\}$ such that for every $j \in \{1, \ldots, r\}$ the action of f stabilizes $\bigoplus_{i\in I_j} Ex_i$ and acts on such a factor by*

$$f(x_1, \ldots, x_{\operatorname{Card} I_j}) = (\sigma_j(x_{\operatorname{Card} I_j}), x_1, \ldots, x_{\operatorname{Card} I_j - 1})$$

where $\sigma_j \in \operatorname{Aut} E$ and we have chosen a renumbering of the x_i's such that $i \in I_j$.

Proof. First note that f acts on $\mathbf{Q}^k \subset E^k$ by permutation. We consider the partition $I_1, \dots, I_r$ of $\{1, \dots, k\}$ obtained from the decomposition of the permutation action of f on $\mathbf{Q}^k$ as disjoint cycles. For $j \in \{1, \dots, r\}$ we can now consider the algebra – which is a subset of E^k – which corresponds to the subset I_j, is isomorphic to $E^{\operatorname{Card} I_j}$ and which is stable by f. In this subalgebra the images of $E \times 0 \cdots \times 0$ are all isomorphic to E and we have an isomorphism

$$E^{\operatorname{Card} I_j} \simeq E \times f(E) \times \cdots \times f^{\operatorname{Card} I_j - 1}(E).$$

In a basis adapted to this isomorphism we get the result. As this holds for all $j \in \{1, \dots, r\}$, we are done.

□

Lemma 3.5. *Let E be a $\mathbf{Q}$-algebra, $m, k \geq 1$ and $\sigma \in \operatorname{Aut} E$ of order dividing m. Then we have an isomorphism*

$$E[m, \sigma]^k = E^k[m, \sigma^{\times k}]$$

where $\sigma^{\times k} \in \operatorname{Aut} E^k$ is the product.

Proof. By definition we have

$$E[m, \sigma]^k = \bigoplus_{j=1}^{k} \bigoplus_{i=0}^{m-1} E.u^i = \bigoplus_{i=0}^{m-1} \bigoplus_{j=1}^{k} E.u^i.$$

Now, since $\bigoplus_{j=1}^{k} E.u^i$ is just $E^k(u^{\times k})^i$ where $u^{\times k}$ is the k-tuple with each coordinate being u we thus have

$$E[m, \sigma]^k = E^k[m, \sigma^{\times k}].$$

□

We go back to the situation of Lemma 3.4 to show that we are left with matrix algebras over some algebra of the form $E[m, \sigma]$ for each stable factor.

Lemma 3.6. *Let E be a simple algebra, $m, k \geq 1$ and $f \in \operatorname{Aut} E^k$. Let us assume that f acts on E^k by*

$$f(x_1, \dots, x_k) = (\sigma(x_k), x_1, \dots, x_{k-1})$$

for some $\sigma \in \operatorname{Aut} E$ with $\sigma^m = 1$. Then we have

$$E^k[mk, f] \simeq \mathrm{M}_k(E[m, \sigma]).$$

Proof. Let Δ be the subalgebra of diagonal matrices in $\mathrm{M}_k(E[m, \sigma])$. By definition we have

$$\Delta \simeq E[m, \sigma]^k.$$

Now consider the matrix of $M_k(E[m, \sigma])$ defined as

$$M = \begin{bmatrix} 0 & & & u \\ 1 & \ddots & & \\ & \ddots & \ddots & \\ & & 1 & 0 \end{bmatrix}$$

We have

$$\mathrm{M}_k(E[m,\sigma)] = \bigoplus_{i=0}^{k-1} \Delta M^i = \bigoplus_{i=0}^{k-1} E[m,\sigma]^k M^i.$$

By the previous lemma, we have $E[m,\sigma]^k \simeq E^k[m,\sigma^{\times k}]$. Hence we have

$$\begin{aligned}\mathrm{M}_k(E[m,\sigma)] &= \bigoplus_{i=0}^{k-1} E^k[m,\sigma^{\times k}]M^i \\ &= \bigoplus_{i=0}^{k-1}\bigoplus_{j=0}^{m-1} E^k u^j M^i\end{aligned}$$

where on the last equality u is identified as the diagonal matrix uI. But since $uI = M^k$ we have

$$\mathrm{M}_k(E[m,\sigma)] = \bigoplus_{i=0}^{k-1}\bigoplus_{j=0}^{m-1} E^k M^{kj+i}.$$

Let us now remark that by construction, for $x \in E^k$, we have $Mx = f(x)M$ so that

$$\mathrm{M}_k(E[m,\sigma)] = \bigoplus_{i=0}^{k-1}\bigoplus_{j=0}^{m-1} E^k M^{kj+i} = \bigoplus_{i=0}^{km-1} E^k M^i = E^k[mk, f].$$

□

Our last lemma concerns the general case but with an interior automorphism.

Lemma 3.7. *Let E be a $\mathbf{Q}$-algebra, $m \geq 1$ and $f \in \operatorname{Int} E$ such that $f^m = 1$. Then we have an isomorphism*

$$E[m,f] \simeq E \otimes_{Z(E)} Z(E[m,f]).$$

Proof. Since f is interior, let $y \in E^\times$ be such that for all $x \in E$

$$f(x) = y^{-1}xy.$$

As $f^m = 1$ we have $y^m \in Z(E)$. We further have that in $E[m,f]$ the element yu is central. Indeed, for all $x \in E$ we have

$$xyu = yf(x)u = yf(x)y^{-1}yu = xyu$$

and

$$uyu = f(y)u^2 = yu \cdot u.$$

We thus have

$$E[m,f] = \bigoplus_{i=0}^{m-1} E(yu)^i = E \otimes_{Z(E)} \bigoplus_{i=0}^{m-1} Z(E)(yu)^i.$$

From this we get

$$Z(E[m,f]) = \bigoplus_{i=0}^{k-1} Z(E)(yu)^i$$

and the result follows. □

We can now show that the centers of the $\mathbf{Q}$-algebras we are interested in have a specific form.

Theorem 3.8. *Let E be a simple algebra with positive involution $*$ and $m,k \geq 1$. Let $f \in \mathrm{Aut}(E^k, *^{\times k})$ with $f^m = 1$. Assume that $Z(E) \subset K$ for some CM field K and that one of the following holds*

(1) *m is odd*
(2) *$E \simeq \mathrm{M}_d(K)$*
(3) *$E \simeq \mathrm{M}_d(\mathbf{Q})$.*

Then $Z(E^k[m,f])$ is a product of CM fields and subfields of K or in case (3) a product of such fields and of quadratic extensions of $\mathbf{Q}$. Furthermore, in case (3), these are matrix algebras over their centers.

Proof. From Lemma 3.4 the action breaks into disjoint part over which Lemma 3.6 gives a description in terms of matrix algebras of the form $\mathrm{M}_r(E[m',\sigma])$ for some $m' \mid m$, $r \leq k$ and $\sigma \in \mathrm{Aut}\, E$. The center of such an algebra is given by the center of $E[m',\sigma]$ so we need only to deal with the case $k = 1$.

Let us assume $k = 1$. We are thus in the situation of Proposition 3.2 whose notation we reuse. Each factor of the center is thus an extension L/F^τ generated by an element α such that $\alpha^{\frac{m}{n}} \in F^\tau$ and $\alpha\alpha^* = yy^*$. Since $E[m,\sigma]$ is equipped with a positive involution, each factor of its center, and L in particular, is also equipped with such an involution. By the classification of Albert they are thus CM or totally real.

If L is not CM, it is totally real and so is F^τ. In this case it follows that $\alpha\alpha^* = \alpha^2 \in F^\tau$. Now, if (1) holds, note that m/n is odd so that $\alpha^{\frac{m}{n}} \in F^\tau$ and $\alpha^2 \in F^\tau$ give $\alpha \in F^\tau$ which is just $L = F^\tau$.

In the case of (2), we have $F^\tau = K^\tau$ a totally real subfield of K so that $\tau^{\frac{n}{2}}$ is the complex conjugation. Applying Proposition 3.3 with $\sigma = f^{\frac{n}{2}}$ we get $\beta \in K$ such that $\alpha^2 = yy^* = \beta^2$ and $L = K^\tau(\beta) \subset K$.

In the last case, we just note again that if L is not CM it is a totally real field, quadratic over $\mathbf{Q}$. The last statement follows from Lemma 3.7 as in this case the action for $k = 1$ must be interior. □

3.2. The rational group algebra of ramification groups

3.2.1. Let p be a prime number. A ramification group at p is a finite group of the form $\Gamma_p \rtimes \mathbf{Z}/n\mathbf{Z}$ where Γ_p is a p-group and n is prime to p. We will omit to say "at p" when the prime p is clear from context. It is part of the main result of [Mau68] that all such groups can be realized as the inertia group of an extension of p-adic fields. Recall from paragraph 3.1.1 that the group algebra $\mathbf{Q}[G]$ and each of its simple factors are equipped with a natural positive involution.

We start by a lemma in the specific case where $\mathrm{Card}\, G$ is odd and it verifies condition (B_q) of [Ser60] p.409 for an odd prime $q \neq p$.

(B_q) *There exists a normal subgroup C of G such that G/C is a q-group.*

Lemma 3.9. *Let G be a ramification group of odd order and satisfying (B_q) for an odd prime $q \neq p$. Then the algebra $\mathbf{Q}[G]$ has no simple factor of type III.*

Proof. We follow the description given by the second case in the proof of Théorème 3 of [Ser60]. With the fact that G is a ramification group at p, satisfies B_q and is of odd order we have an isomorphism

$$G \simeq \mathbf{Z}/p^e\mathbf{Z} \rtimes (\mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/q^f\mathbf{Z})$$

for some integers $e, f, m \geq 0$ and m prime to p and q. Let T be the kernel of the conjugation action of G on $\mathbf{Z}/p^e\mathbf{Z}$. By definition, $\mathbf{Z}/p^e\mathbf{Z} \subset T$ but also $C \subset T$ since it is a cyclic group containing $\mathbf{Z}/p^e\mathbf{Z}$. We get that G is an extension of $T \simeq \mathbf{Z}/p^e\mathbf{Z} \times \mathbf{Z}/mq^w\mathbf{Z}$, $w \geq 1$ an integer less than f, and $R = G/T \simeq \mathbf{Z}/q^{f-w}\mathbf{Z}$. This extension is given by an element $a \in H^2(R, T)$ with values in $\mathbf{Z}/mq^w\mathbf{Z} \subset T$.

Now, we have $\mathbf{Q}[G] = \mathbf{Q}[T][R, \varphi]$ for the action $\varphi\colon R \to \operatorname{Aut} T$. As $\operatorname{Aut} T$ stabilizes the decomposition of $\mathbf{Q}[T]$ into a product of cyclotomic fields it is also the case of the action of R. We get

$$\mathbf{Q}[G] \simeq \bigoplus_{d|p^e mq^w} A_d$$

where A_d is $\mathbf{Q}(\mu_d)[R, \varphi']$. For $d = \operatorname{Card} T$ we denote A_d by $A[G]$. The algebra $A[G]$ is a cyclic algebra given by $(\mathbf{Q}(\mu_{p^e mq^w})/F, a)$. All other simple factors are described in the same way as $A[G/G']$ for a normal subgroup $G' \subset G$ and thus satisfies the conditions of the lemma.

By construction, the field $F \subset \mathbf{Q}(\mu_{p^e mq^w})$ is the center of $A[G]$ and contains $\mathbf{Q}(\mu_{mq^w})$ as the action of R is trivial on the corresponding subgroup of G. If F is totally real we must have $mq^w \in \{1, 2\}$. Since the order of G is odd this implies $mq^w = 1$ but then a which has values in $\mathbf{Z}/mq^w\mathbf{Z}$ is just trivial, hence $A[G]$ is of type II. As this applies to all simple factors of $\mathbf{Q}[G]$, from the fact they are all of the form $A[G/G']$, we have that $\mathbf{Q}[G]$ has no factor of type III. □

3.2.2. We can now prove our main technical result which is the following structure theorem. It gives precision to Théorème 3 of [Ser60] on the group algebra $\mathbf{Q}[G]$ and generalizes the results of Roquette and Ford on p-groups in [Roq58; For87].

Theorem 3.10. *Let G be a ramification group at p. The rational group algebra $\mathbf{Q}[G]$ has the following properties.*

(*i*) *The algebra $\mathbf{Q}[G]$ is quasi-split outside p.*
(*ii*) *If $E \subset \mathbf{Q}[G]$ is a simple factor of $\mathbf{Q}[G]$ then the center $Z(E)$ of E is a CM field or a subfield of $\mathbf{Q}(\mu_{p^\infty})$.*

Furthermore, if $\operatorname{Card} G$ *is odd then no simple factor of $\mathbf{Q}[G]$ is of type III.*

Proof. The statement (*i*) is exactly Théorème 3 of [Ser60] by the equivalence given in Proposition 1 of *loc. cit.*

Let us prove (*ii*). Since G is a ramification group it is of the form $H \rtimes \mathbf{Z}/m\mathbf{Z}$ with H a p-group and m prime to p. We thus have

$$\mathbf{Q}[G] \simeq \mathbf{Q}[H][m, f]$$

for some $f \in \operatorname{Aut} \mathbf{Q}[H]$ with $f^m = 1$. By Proposition 1.4 of [Yam74] the center of a simple factor of $\mathbf{Q}[H]$ is given by $\mathbf{Q}(\chi)$ for some character χ of H. Now, since H is a p-group, this gives that the centers of the simple factors of $\mathbf{Q}[H]$ are subfields of the CM field $\mathbf{Q}(\mu_{p^n})$ for some $n \in \mathbf{N}$. As $\mathbf{Q}[H]$ is equipped with a positive involution, stable by f – see paragraph 3.1.1 – we are in position to apply Theorem 3.8. If $p = 2$ then m is odd and we are in case (1). If p is odd, by Satz 2 (and the following paragraph) of [Roq58], the simple factors of $\mathbf{Q}[H]$ are matrix algebras over their center and by Theorem 1.(i) of [For87] these centers are of the form $\mathbf{Q}(\mu_{p^e})$ for some $e \geq 0$. More precisely, except for the factor $\mathbf{Q}$ coming from the trivial representation we have $e \geq 1$. Indeed, let $\mathrm{M}_n(\mathbf{Q}(\chi)) = \mathrm{M}_n(\mathbf{Q})$ be one of the factor with $n \geq 1$, for an irreducible non trivial character χ of H. By Ford, there is a linear character λ of a subgroup of H that induces χ.

Since $\mathbf{Q}(\chi) = \mathbf{Q}(\lambda)$ we have that λ is trivial. But then χ can not be irreducible and non trivial as a character induced by the trivial character of a proper subgroup is a permutation character, and contains the trivial character. We are thus either in the case (2) of Theorem 3.8 or considering the trivial action on the factor $\mathbf{Q}$ corresponding to the trivial representation which only yields copies of $\mathbf{Q}$.

To prove the last part of the statement we argue as the proof of Théorème 3 in [Ser60].

Let $G' \subset G$ be a subgroup satisfying (B_q) for some prime number q. If $q = p$ then G' is a p-group with p odd so that the results of Ford and Roquette ensure that no algebra of type III appears as a simple factor of $\mathbf{Q}[G']$. If $q \neq p$, since $\operatorname{Card} G$ is odd we must have $q \neq 2$ and Lemma 3.9 ensures that there are not type III algebra in the decomposition of $\mathbf{Q}[G']$.

Let us remark now that for a $\mathbf{Q}$-algebra E of finite dimension with positive involution we have $E \otimes_{\mathbf{Q}} \mathbf{R}$ is quasi-split if and only if E has no factor of type III. In particular, we see that for all subgroups satisfying (B_q), for some prime q, of G, the algebra $\mathbf{Q}[G']$ is quasi-split over $\mathbf{R}$. By Brauer's induction theorem – see for example Proposition 2 of [Ser60] – the algebra $\mathbf{Q}[G]$ is also quasi-split over $\mathbf{R}$ which is equivalent to the fact that there is no factor of type III in its decomposition. □

4. The (p,t,a)-inertial groups as finite monodromy groups

In this section p is a fixed prime number. The goal is to apply the results of the two previous part to (p,t,a)-inertial groups and show that these groups are realized as finite monodromy groups of abelian varieties of dimension $g = t + a$ over number fields, answering a question of Silverberg and Zarhin.

4.1. Symplectic realization of finite groups and a characterization of (p,t,a)-inertial groups

4.1.1. We start by a lemma on rational representations of simple polarizable algebras over the fields $\mathbf{Q}_\ell$. For any field extension $K/\mathbf{Q}$ and a $\mathbf{Q}$-algebra E we extend the definition of a representation, a rational representation and a polarized representation of E to be a K-vector space with an action of E which is $\mathbf{Q}$-linear and having the corresponding properties. We are only concerned with the fields $\mathbf{Q}_\ell$ for $\ell \neq p$. To that end, let us fix an embedding $\mathbf{Q}_\ell \subset \mathbf{C}$ for every $\ell \neq p$. For a simple algebra E quasi-split outside p, the results of Section 2.1 extend without difficulty.

Lemma 4.1. *Let E be a simple $\mathbf{Q}$-algebra quasi-split outside p and $\ell \neq p$ a prime number. If V is a rational $\mathbf{C}$-representation of E then it is of the form $V_\ell \otimes_{\mathbf{Q}_\ell} \mathbf{C}$ for a unique $\mathbf{Q}_\ell$-representation V_ℓ of E which is rational. In particular, the rational $\mathbf{Q}_\ell$-representation of E are the multiples of $V_r(E)_\ell$ and the rational and polarized $\mathbf{Q}_\ell$-representations of E are the multiples of $V_{rp}(E)_\ell$.*

Proof. By Theorem 2.14 it is enough to show that the $\mathbf{C}$-representation $V_r(E)$ verifies the statement.

Let us write $E \simeq \mathrm{M}_n(D)$ with D a skew-field of center F over $\mathbf{Q}$ and $\deg E = ndf$ by setting $d^2 = [D : F]$ and $f = [F : \mathbf{Q}]$. We have a decomposition

$$F \otimes_{\mathbf{Q}} \mathbf{Q}_\ell = \prod_{i=1}^{r} F_i$$

and since E is quasi-split outside p we have

$$E \otimes_{\mathbf{Q}} \mathbf{Q}_\ell \simeq \prod_{i=1}^{r} \mathrm{M}_{nd}(F_i).$$

For $i \in \{1, \dots, r\}$ let $E_i = F_i^{nd}$ be the unique non trivial simple $\mathrm{M}_{nd}(F_i)$-module. We consider the rational $\mathbf{Q}_\ell$-representation

$$V_r(E)_\ell = \bigoplus_{i=1}^{r} E_i.$$

We have

$$V_r(E)_\ell \otimes_{\mathbf{Q}_\ell} \mathbf{C} = \bigoplus_{i=1}^{r} (\mathbf{C}^{nd})^{[F_i:\mathbf{Q}_\ell]} = \bigoplus_{i=1}^{f} \mathbf{C}^{nd}.$$

Hence $V_r(E)_\ell \otimes_{\mathbf{Q}_\ell} \mathbf{C}$ is a rational $\mathbf{C}$-representation of E of dimension $\deg E$. It is thus isomorphic to $V_r(E)$ which concludes.

The last part of the statement is clear for rational $\mathbf{Q}_\ell$-representations. For a rational and polarized $\mathbf{Q}_\ell$-representation V it is also clear that $V \otimes_{\mathbf{Q}_\ell} \mathbf{C}$ is rational and polarized so that $V = V_{rp}(E)_\ell^n$ for some integer $n \in \mathbf{N}$. It thus suffices to see that $V_{rp}(E)_\ell$ is polarized. If E is of type I, II and IV this follows exactly as in the case of $\mathbf{C}$-representations. For E of type III we thus need to show that $V_r(E)_\ell$ is polarized. From the proof of the first part we know that

$$V_r(E)_\ell = \bigoplus_{i=1}^{r} E_i$$

and the sum runs over all simple $\mathbf{Q}_\ell$-representations of E. In particular, we have $V_r(E)_\ell \simeq V_r(E)_\ell^\vee$. This isomorphism induces an isomorphism $V_r(E) \simeq V_r(E)^\vee$ and the induced non degenerate bilinear form on $V_r(E)$ is invariant. Since there is only one and it is symplectic we are done. □

4.1.2. We will give a characterization of (p, t, a)-inertial groups through representations of algebras but first we introduce and characterize the notion of a symplectic realization of a ramification group. This will add clarity to the fact that we will not only realize the groups themselves but also any choice of a representation that satisfies part (ii) of Definition 1.1.

Definition 4.2. Let G be a ramification group. A symplectic realization of G of dimension $2a$ is the data of a quotient E of $\mathbf{Q}[G]$ and a rational and polarized $\mathbf{C}$-representation V of E of dimension $2a$.

Note that in the definition, we consider E equipped with the positive involution induced by the natural one on $\mathbf{Q}[G]$ and with a map $G \to E$.

Theorem 4.3. *Let G be a ramification group. The symplectic realizations (E, V) of G of dimension $2a$ are in correspondence with family of maps $(p_\ell \colon G \to \mathrm{Sp}_{2a}(\mathbf{Q}_\ell))_{\ell \neq p}$ such that the characteristic polynomials of the elements of G have integer coefficients independent of ℓ. The correspondence is such that, for $\ell \neq p$, the map $p_\ell \colon G \to \mathrm{Sp}_{2a}(\mathbf{Q}_\ell)$ is obtained by composition by the canonical map $G \to E$, that is p_ℓ coincides with*

$$G \to E \to \mathrm{End}_{\mathbf{Q}_\ell} V_\ell.$$

Proof. Let $(p_\ell\colon G \to \mathrm{Sp}_{2a}(\mathbf{Q}_\ell))_{\ell\neq p}$ be a family of maps as in the statement. Let us fix $\ell \neq p$ a prime and consider E the $\mathbf{Q}$-algebra generated by G in $M_{2a}(\mathbf{Q}_\ell)$. The algebra E is a quotient of $\mathbf{Q}[G]$ by construction and one can note that it does not depend on the choice of ℓ. It is also by construction that E acts on $V_\ell = \mathbf{Q}_\ell^{2a}$ and this action has an invariant symplectic form. In other words, V_ℓ is a rational and polarized $\mathbf{Q}_\ell$-representation of E. By Lemma 4.1 the space $V_\ell \otimes_{\mathbf{Q}_\ell} \mathbf{C}$ is a $\mathbf{C}$-rational and polarized representation of E.

Let E be a quotient of $\mathbf{Q}[G]$ and V a rational and polarized $\mathbf{C}$-representation of E. Let $\ell \neq p$ be a prime. Again, by Lemma 4.1, to the representation V corresponds a rational and polarized $\mathbf{Q}_\ell$-representation V_ℓ. Now, since E is a quotient of $\mathbf{Q}[G]$ it is equipped with a map $\rho\colon G \to E$ and the positive involution on E is such that $\rho(g)^* = \rho(g^{-1})$. In particular, since V_ℓ is polarized we see that $\rho(g)$ is an element of the symplectic group. In other words, the restriction to the image of G in E of the map $E \to \mathrm{End}_{\mathbf{Q}_\ell} V_\ell$ has image in $\mathrm{Sp}_{2a}(\mathbf{Q}_\ell)$. We recover this way a family of maps $(p_\ell\colon G \to \mathrm{Sp}_{2a}(\mathbf{Q}_\ell))_{\ell\neq p}$ which satisfy the condition.

It is clear that both constructions are inverse to each other. □

Corollary 4.4. *Let G be a ramification group at p and $t, a \in \mathbf{N}$. Then G is (p,t,a)-inertial if and only if there is a symplectic realization (E,V) of G and a map $G \to \mathrm{GL}_t(\mathbf{Z})$ such that the induced map*

$$G \to \mathrm{GL}_t(\mathbf{Z}) \times E$$

is injective.

Proof. By definition, if G is (p,t,a)-inertial there is a family of injective maps $(\iota_\ell\colon G \to \mathrm{GL}_t(\mathbf{Z}) \times \mathrm{Sp}_{2a}(\mathbf{Q}_\ell))_{\ell\neq p}$ for which the projections p_ℓ on the second factor satisfy the condition of Theorem 4.3. So there is a quotient E of $\mathbf{Q}[G]$ with a polarized V representation of E such that p_ℓ is obtained by the composition

$$G \to E \to \mathrm{End}_{\mathbf{Q}_\ell} V_\ell.$$

Since the second map is injective we have that the induced map

$$G \to \mathrm{GL}_t(\mathbf{Z}) \times E$$

is also injective.

The converse is straightforward from Theorem 4.3. The data of (E,V) gives a family of maps $(p_\ell\colon G \to \mathrm{Sp}_{2a}(\mathbf{Q}_\ell))_{\ell\neq p}$ which gives an injection

$$\iota_\ell\colon G \to \mathrm{GL}_t(\mathbf{Z}) \times \mathrm{Sp}_{2a}(\mathbf{Q}_\ell)$$

for all $\ell \neq p$ by construction. □

4.1.3. We finish this section by relating symplectic realizations to geometric embeddings introduced in Section 2.2. We show that all realizations are geometric in the sense of the following definition, which is the first form of our main result and the main step towards realizing the (p,t,a)-inertial groups as finite monodromy groups. To that end, we recall some results of Tate on abelian varieties and their Tate modules.

Let A be an abelian variety of dimension a over $\overline{\mathbf{F}_p}$. For a prime $\ell \neq p$, the endomorphism ring $\mathrm{End}\, A$ acts on the ℓ-adic Tate module $T_\ell A = \varprojlim_n A[\ell^n]$. Let $V_\ell(A)$ denote the $\mathbf{Q}_\ell$-vector space $T_\ell A \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell$. The representation of the $\mathbf{Q}$-algebra $E(A) = \mathrm{End}\, A \otimes_{\mathbf{Z}} \mathbf{Q}$ given by $V_\ell(A)$ is rational and polarized – see [Mum08] Theorem 4 on p. 167 (181). By Lemma 4.1 the representation $V_\ell(A)$

corresponds to a $\mathbf{C}$-representation $V(A)$ of $E(A)$ and since the characteristic polynomials of the representation $V_\ell(A)$ are independent of ℓ the $\mathbf{C}$-representation $V(A)$ is independent of ℓ. For an abelian variety A over a finite field, we will keep the notation $E(A)$ and $V(A)$ for its endomorphism algebra and the $\mathbf{C}$-representation of $E(A)$ associated to its ℓ-adic Tate module. Note that when $E(A)$ is simple, by the results of Tate on the dimension of $E(A)$ we have in this case that $V(A) = V_{rp}(E(A))$.

Definition 4.5. A symplectic realization (E, V) of a ramification group G is said to be geometric if there is an abelian variety A over $\overline{\mathbf{F}_p}$ and an embedding $E \subset E(A)$ such that the induced $\mathbf{C}$-representation of E given by $V(A)$ is isomorphic to V.

Theorem 4.6. *Let G be a ramification group at p. All symplectic realizations of G are geometric.*

Proof. Let (E, V) be a symplectic realization of G. First note that if E is not simple and we have a decomposition in simple factors $E \simeq \prod_{i=1}^r E_i$ then V splits in a direct sum of representations $V \simeq \bigoplus_{i=1}^r V_{rp}(E_i)^{n_i}$ for some $n_i \in \mathbf{N}$. For each $i \in \{1, \dots, r\}$ we get a symplectic representation $(E_i, V_{rp}(E_i)^{n_i})$ of G and it is clear that (E, V) is geometric if and only if $(E_i, V_{rp}(E_i)^{n_i})$ is geometric for each $i \in \{1, \dots, r\}$. We thus assume E is simple.

We start by showing that $(E, V_{rp}(E))$ is a symplectic realization of G which is geometric. Since G is a ramification group, by (i) of Theorem 3.10 the algebra E is quasi-split outside p. If E is of type I, II or IV then by Theorem 2.22 we have a good embedding $E \to E(A)$ for some abelian variety A over $\overline{\mathbf{F}_p}$. We thus have that $V(A) = V_{rp}(E(A)) = V_{rp}(E)$ and the realization (E, V) is geometric.

Let us now consider the case where E is of type III. By (ii) of Theorem 3.10 the center of E is subfield of $\mathbf{Q}(\mu_{p^n})$ for some $n \in \mathbf{N}$. But this field is totally ramified at p and thus also the center F of E. Hence there is only one Brauer class of type III algebras over F, the algebras of the form $\mathrm{M}_k(F \otimes \mathbf{H}_{p,\infty})$. It follows that E is of that form and by Theorem 2.22 again there is A over $\overline{\mathbf{F}_p}$ with $V(A) = V_{rp}(A) = V_{rp}(E)$.

We go back to the general case, that is of a realization (E, V) of G with E simple. By Theorem 2.14 the representation V is isomorphic to $V_{rp}(E)^n$ for some $n \in \mathbf{N}$. From the previous case, let B be an abelian variety over $\overline{\mathbf{F}_p}$ with $E \hookrightarrow E(B)$ such that $V(B) = V_{rp}(E)$. The abelian variety $A = B^n$ suits our needs. Indeed, we have a diagonal embedding $E \hookrightarrow E(A) \simeq \mathrm{M}_n(E(B))$ for which the induced $\mathbf{C}$-representation $V(A)$ has the desired property $V(A) = V_{rp}(E)^n = V$ as $\mathbf{C}$-representations of E. □

4.2. The realization of (p, t, a)-inertial groups as finite monodromy groups

4.2.1. Let us start by recalling the results of [Phi24] which relate to finite monodromy groups. For an abelian variety A over a p-adic field K, the finite monodromy group $\Phi(A)$ of A is the Galois group of the smallest field extension L_A of the maximal unramified extension K^{un} of K such that A_{L_A} has semi-stable reduction – the fact that L_A/K^{un} is Galois is section 4 of Exposé IX of [SGA7.1].

In [Phi24], based on chapter 2 of [FC90], there is a notion of a polarized semi-abelian variety. We recall it here as it is used in the main theorem.

Definition 4.7. Let A_0 and A_0^t be semi-abelian varieties over a finite field. A polarization $\lambda_0 \colon A_0 \to A_0^t$ is a map of semi-abelian varieties

$$\begin{array}{ccccccccc} 0 & \longrightarrow & T_0 & \longrightarrow & A_0 & \longrightarrow & B_0 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \lambda_{T_0}} & & \downarrow{\scriptstyle \lambda_0} & & \downarrow{\scriptstyle \lambda_{B_0}} & & \\ 0 & \longrightarrow & T_0^t & \longrightarrow & A_0^t & \longrightarrow & B_0^\vee & \longrightarrow & 0 \end{array}$$

such that the induced maps λ_{T_0} is an isogeny and λ_{B_0} is a polarization. A semi-abelian variety A_0 equipped with a polarization λ_0 is said to be polarized.

In the next sections of the text, we will conserve the notations T_0 and B_0 for the maximal torus and abelian quotient of a semi-abelian variety A_0. Note that, for a prime $\ell \neq p$, through the ℓ-adic Tate module of B_0 there is a map

$$\operatorname{Aut} A_0 \longrightarrow \mathrm{GL}_t(\mathbf{Z}) \times \mathrm{Sp}_{2a}(\mathbf{Q}_\ell)$$

where t is the dimension of T_0 and a the dimension of B_0.

The main theorem of [Phi24] now states that a ramification group G is the finite monodromy group of some abelian variety if and only if there is an embedding $G \subset \operatorname{Aut}(A_0, \lambda_0)$ for some polarized semi-abelian variety A_0 over $\overline{\mathbf{F}_p}$ – see Théorème 1.1 of [Phi24].

4.2.2. We can now show that all (p,t,a)-inertial groups are realized as finite monodromy groups in dimension $t+a$. More precisely, we show that for a ramification group G all symplectic realizations are obtained by realizations of G as a finite monodromy group. We first give the context for a precise meaning of this last part. For an abelian variety A over a p-adic field K, its finite monodromy group Φ_A acts on the reduction of A_{L_A}, which is a semi-abelian variety A_0 over $\overline{\mathbf{F}_p}$. This action produces an injection $G \hookrightarrow \operatorname{Aut}(A_0, \lambda_0)$ and a symplectic realization $(E(B_0), V(B_0))$. We show that all symplectic realizations of G are obtained in this way.

Theorem 4.8. *Let G be a ramification group at p. Then for all family of injective maps $(\iota_\ell \colon G \to \mathrm{GL}_t(\mathbf{Z}) \times \mathrm{Sp}_{2a}(\mathbf{Q}_\ell))_{\ell \neq p}$ with second projection corresponding to a symplectic realization (E,V) of dimension $2a$ of G there is an abelian variety A of dimension $t+a$ over a p-adic field K such that G is the finite monodromy group of A. Moreover, the action of G on the reduction A_0 of A_{L_A} recover the first projection $G \to \mathrm{GL}_t(\mathbf{Z})$ of ι_ℓ for any $\ell \neq p$ and the symplectic realization (E,V) up to isomorphism.*

Proof. Let (E,V) be the symplectic realization coming from the second projection of the family of maps $(\iota_\ell)_{\ell \neq p}$. From Theorem 4.6 this realization is geometric so there is an abelian variety B_0 over $\overline{\mathbf{F}_p}$ such that $E \subset E(B_0')$ and $V(B_0') = V$. Consider the image of the order $\mathbf{Z}[G]$ of $\mathbf{Q}[G]$ in $E(B_0')$. It is contained in a maximal order and by Theorem 3.13 of [Wat69] there is an abelian variety B_0 for which $E(B_0) = E(B_0')$ and $V(B_0) = V(B_0')$ but also such that $\operatorname{End} B_0 \subset E(B_0)$ contains the image of G. Since G is finite there is a polarization λ_0 of B_0 which is stable by G and we can consider the semi-abelian variety $A_0 = \mathbf{G}_m^t \times B_0$ over $\overline{\mathbf{F}_p}$. The semi-abelian variety A_0 is polarized by (id, λ_0) and we have an injective map

$$G \longrightarrow \operatorname{Aut} A_0 = \mathrm{GL}_t(\mathbf{Z}) \times \operatorname{Aut} B_0.$$

By Théorème 1.1 of [Phi24] we get an abelian variety A over p-adic field K such that G is the finite monodromy group of A and the reduction of A_{L_A} is isogenous to A_0. By construction, the symplectic realization obtained by (A,G) is isomorphic to (E,V). □

Corollary 4.9. *Let G be a ramification group. Then G is (p,t,a)-inertial if and only if G is the finite monodromy group of an abelian variety A of dimension $t+a$ over a number field K at a place v of residue characteristic p. Furthermore, we can choose A such that, for L/K an extension for which A_L has semi-stable reduction at the places of L above v, the reduction of A_L at the places above v has toric rank t and abelian rank a.*

Proof. By Theorem 4.8 we get that if G is (p,t,a) inertial such an abelian variety A' over a p-adic field exists. By Theorem 4.3 of [Phi22a] we get A over a number field which satisfies all our conditions. The converse is given, for example, by Theorem 5.2 of [SZ98]. □

4.2.3. We finish by giving some examples of computations on specific groups. For a ramification group G, we are able to determine the values for which it is (p,t,a)-inertial in a methodic way with finitely many steps. Note that, from the regular representation of G, it is clear that there are minimal integers $t_G, a_G \geq 1$ such that G is $(p,t_G,0)$ and $(p,0,a_G)$-inertial. It is also clear that if G is (p,t,a)-inertial for some $t,a \geq 0$ then it is trivially $(p,t+n,a+m)$-inertial for any $n,m \geq 0$. We thus see that there is only finitely many couples (t,a) for which G is not (p,t,a)-inertial, inside a box of height t_G-1 and length a_G-1 starting from $(0,0)$ in the lattice $\mathbf{Z}^2$. Lastly, we remark that if G is (p,t,a)-inertial with $t,a \geq 1$ in a non-trivial way, that is for fixed $\ell \neq p$ the map

$$\iota_\ell \colon G \longrightarrow \mathrm{GL}_t(\mathbf{Z}) \times \mathrm{Sp}_{2a}(\mathbf{Q}_\ell)$$

has its images in each factor not G, then G is a subdirect factor of the product of two of its non trivial normal subgroups. In other words, there are normal proper subgroups K and H in G such that $K \cap H = \{1\}$ such that the natural map

$$G \longrightarrow G/K \times G/H$$

is injective. For a group for which no such subgroups exists, the set of exceptional couples (t,a) for which it is not (p,t,a)-inertial will exactly be the box mentioned previously.

Example 4.10. We give three examples.

(*i*) Let $n \geq 1$ and $G = \mathbf{Z}/n\mathbf{Z}$. Cyclic groups are ramification groups at all primes p. We compute the list of exceptional couples (t,a) for G, which does not depend on p. Let D_n be the set of ordered couples (r,s) of factors of n such that r is prime to s and $n = r \cdot s$. Considering the factors $\mathbf{Q}(\mu_r)$ and $\mathbf{Q}(\mu_s)$ of $\mathbf{Q}[G]$ we get a representation $G \to \mathrm{GL}_{\varphi(r)}(\mathbf{Z})$ with image $\mathbf{Z}/r\mathbf{Z}$ on one side and a symplectic realization $(\mathbf{Q}(\mu_s), V_{rp}(\mathbf{Q}(\mu_s)))$ on the other. This symplectic realization gives a family of maps, for all primes ℓ,

$$p_\ell \colon G \to \mathrm{Sp}_{\varphi(s)}(\mathbf{Q}_\ell)$$

with images $\mathbf{Z}/s\mathbf{Z}$. The product maps

$$G \longrightarrow \mathrm{GL}_{\varphi(r)}(\mathbf{Z}) \times \mathrm{Sp}_{\varphi(s)}(\mathbf{Q}_\ell)$$

are injective by construction and make G into a $(p, \varphi(r), \frac{\varphi(s)}{2})$-inertial group. It is an easy check that for any value $t,a \geq 0$ with $t \leq \varphi(r)-1$ or $a \leq \frac{\varphi(s)}{2}-1$ for any couple $(r,s) \in D_n$, G is not (p,t,a)-inertial.

We thus recover and generalize the result of Silverberg and Zarhin for small cyclic groups in [SZ05].

(*ii*) We consider the wreath product $G = Q_8 \wr \mathbf{Z}/2\mathbf{Z}$. This group is shown to be $(2,0,2)$-inertial by Silverberg and Zarhin in [SZ05] and was realized as a finite monodromy group over number fields by Chrétien and Matignon in [CM13]. Note that in this group, all pair of normal subgroups intersect non-trivially so that it can not be a (p,t,a)-inertial group with $t, a \geq 1$ in a non-trivial way. We thus look for the smallest rational and polarized faithful representation coming from a factor of its rational algebra in order to compute t_G and a_G. Let us start by computing the rational group algebra of $Q_8 \times Q_8$. We have

$$\begin{aligned}\mathbf{Q}[Q_8 \times Q_8] &= (\mathbf{Q} \times \mathbf{Q} \times \mathbf{Q} \times \mathbf{Q} \times \mathbf{H}_{2,\infty}) \otimes_{\mathbf{Q}} (\mathbf{Q} \times \mathbf{Q} \times \mathbf{Q} \times \mathbf{Q} \times \mathbf{H}_{2,\infty}) \\ &= \mathbf{Q}^4 \times (\mathbf{Q}^2)^6 \times (\mathbf{H}_{2,\infty}^2)^4 \times \mathrm{M}_4(\mathbf{Q})\end{aligned}$$

where we regrouped the factors that are swapped by the $\mathbf{Z}/2\mathbf{Z}$-action coming from G. The factors that are fixed get doubled in $\mathbf{Q}[G]$ and those that are swapped give 2×2 matrix algebra over the respective division algebra by Lemma 3.7. We thus have

$$\mathbf{Q}[G] = \mathbf{Q}^8 \times \mathrm{M}_2(\mathbf{Q})^6 \times \mathrm{M}_4(\mathbf{Q})^2 \times \mathrm{M}_2(\mathbf{H}_{2,\infty})^4.$$

Now, it is an easy check that we have an embedding $G \hookrightarrow \mathrm{M}_2(\mathbf{H}_{2,\infty})$ so that G is both $(2,0,2)$-inertial since $\deg \mathrm{M}_2(\mathbf{H}_{2,\infty}) = 4$ and it is a type III algebra, and $(2,8,0)$-inertial since the Schur index of $\mathbf{H}_{2,\infty}$ is 2. We thus have $t_G = 8$ and $a_G = 2$ and since G is not a subdirect product it is not $(2,t,a)$-inertial for any (t,a) in the box delimited by $(0,0)$, $(7,0)$, $(7,1)$ and $(0,1)$ except for the values in the top and right edges.

(*iii*) Consider the dihedral group $G = D_{13}$ of order 26. By the table on page 105 of [GB02] we have

$$\mathbf{Q}[G] = \mathbf{Q} \times \mathbf{Q} \times \mathrm{M}_2(\mathbf{Q}(\zeta_{13} + \zeta_{13}^{-1}).$$

We get a faithful representation from the factor $\mathrm{M}_2(\mathbf{Q}(\zeta_{13} + \zeta_{13}^{-1}))$ which yield by a simple computation $t_G = 6$ and $a_G = 3$. Since G is not a subdirect product again, the exceptional values are in the box delimited by $(0,0)$, $(5,0)$, $(5,2)$ and $(0,2)$.

In general, given a ramification group G one can determine the values for which it is (p,t,a)-inertial by computing the rational group algebra $\mathbf{Q}[G]$ and the faithful representations given by the quotients of $\mathbf{Q}[G]$. Then, the values are computed using the dimension of the given representations and the degrees of the polarized representation of the simple algebras in play.

References

[CM13] P. Chrétien and M. Matignon, "Maximal wild monodromy in unequal characteristic," *J. Number Theory*, vol. 133, no. 4, pp. 1389–1408, 2013 (cit. on pp. 2, 27).

[FC90] G. Faltings and C.-L. Chai, *Degeneration of abelian varieties* (Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]). Springer-Verlag, Berlin, 1990, vol. 22, pp. xii+316, With an appendix by David Mumford (cit. on p. 24).

[For87] C. E. Ford, "Characters of p-groups," *Proc. Amer. Math. Soc.*, vol. 101, no. 4, pp. 595–601, 1987 (cit. on p. 20).

[GB02] C. R. Giraldo Vergara and F. E. Brochero Martínez, "Wedderburn decomposition of some special rational group algebras," *Lect. Mat.*, vol. 23, no. 2, pp. 99–106, 2002 (cit. on p. 27).

[SGA7.1] A. Grothendieck, *Modèles de Néron et monodromie.* Sémin. Géom. Algébrique, Bois-Marie 1967–1969, SGA 7 I, Exp. No. 9, Lect. Notes Math. 288, 313-523. Avec un appendice par M. Raynaud, 1972 (cit. on pp. 1, 24).

[Har17] D. Harari, *Cohomologie galoisienne et théorie du corps de classes* (Savoirs Actuels). Les Ulis: EDP Sciences; Paris: CNRS Éditions, 2017 (cit. on p. 8).

[Lew06] D. W. Lewis, "Involutions and anti-automorphisms of algebras," *Bull. London Math. Soc.*, vol. 38, no. 4, pp. 529–545, 2006 (cit. on p. 14).

[Mau68] E. Maus, "Die gruppentheoretische Struktur der Verzweigungsgruppenreihen," *J. Reine Angew. Math.*, vol. 230, pp. 1–28, 1968 (cit. on pp. 2, 19).

[Mum08] D. Mumford, *Abelian varieties* (Tata Institute of Fundamental Research Studies in Mathematics). Tata Institute of Fundamental Research, Bombay; by Hindustan Book Agency, New Delhi, 2008, vol. 5, pp. xii+263, With appendices by C. P. Ramanujam and Yuri Manin, Corrected reprint of the second (1974) edition (cit. on pp. 8, 23).

[Phi22a] S. Philip, "On the semi-stability degree for abelian varieties," *Bull. Lond. Math. Soc.*, vol. 54, no. 6, pp. 2174–2187, 2022 (cit. on pp. 2, 26).

[Phi22b] ——, "Variétés abéliennes CM et grosse monodromie finie sauvage," *J. Number Theory*, vol. 240, pp. 163–195, 2022 (cit. on p. 2).

[Phi24] ——, "Groupes de monodromie finie des variétés abéliennes," *(submitted) arxiv:2412.11900*, p. 33, 2024 (cit. on pp. 2, 4, 24, 25).

[Rém17] G. Rémond, "Variétés abéliennes et ordres maximaux," *Rev. Mat. Iberoam.*, vol. 33, no. 4, pp. 1173–1195, 2017 (cit. on p. 14).

[Roq58] P. Roquette, "Realisierung von Darstellungen endlicher nilpotenter Gruppen.," *Arch. Math.*, vol. 9, pp. 241–250, 1958 (cit. on p. 20).

[Sch85] W. Scharlau, *Quadratic and Hermitian forms* (Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]). Springer-Verlag, Berlin, 1985, vol. 270, pp. x+421 (cit. on pp. 5, 8, 11).

[Ser60] J.-P. Serre, "Sur la rationalité des représentations d'Artin," *Ann. of Math. (2)*, vol. 72, pp. 405–420, 1960 (cit. on pp. 2, 3, 19–21).

[Ser77] ——, *Linear representations of finite groups* (Graduate Texts in Mathematics), French. Springer-Verlag, New York-Heidelberg, 1977, vol. Vol. 42, pp. x+170 (cit. on p. 6).

[ST61] G. Shimura and Y. Taniyama, *Complex multiplication of abelian varieties and its applications to number theory* (Publications of the Mathematical Society of Japan). Mathematical Society of Japan, Tokyo, 1961, vol. 6, pp. xi+159 (cit. on p. 9).

[SZ98] A. Silverberg and Y. G. Zarhin, "Subgroups of inertia groups arising from abelian varieties," *J. Algebra*, vol. 209, no. 1, pp. 94–107, 1998 (cit. on pp. 2, 26).

[SZ05] ——, "Inertia groups and abelian surfaces," *J. Number Theory*, vol. 110, no. 1, pp. 178–198, 2005 (cit. on pp. 2, 26, 27).

[Tat71] J. Tate, "Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda)," in *Séminaire Bourbaki. Vol. 1968/69: Exposés 347–363*, ser. Lecture Notes in Math. Vol. 175, Springer, Berlin, 1971, Exp. No. 352, 95–110 (cit. on pp. 11, 12).

[Wat69] W. C. Waterhouse, "Abelian varieties over finite fields," *Ann. Sci. École Norm. Sup. (4)*, vol. 2, pp. 521–560, 1969 (cit. on p. 25).

[Yam74] T. Yamada, *The Schur subgroup of the Brauer group* (Lecture Notes in Mathematics). Springer-Verlag, Berlin-New York, 1974, vol. Vol. 397, pp. v+159 (cit. on p. 20).

Department of Mathematics, Stockholms universitet SE-106 91 Stockholm, Sweden
Email address: severin.philip@math.su.se