On the Structure of Weil Restrictions of Abelian Varieties

Claus Diem Niko Naumann

June 10, 2003

Abstract

We give a description of endomorphism rings of Weil restrictions of abelian varieties with respect to finite Galois extensions of fields. The results are applied to study the isogeny decompositions of Weil restrictions.

2000 Mathematics Subject Classification Primary: 14K15, Secondary: 11G10.

Introduction

For the use of Weil restrictions of abelian varieties in various fields of mathematics but also because of genuine interest in Weil restrictions themselves, it is important to determine the endomorphism rings and the isogeny decompositions. This is what this article provides – at least in two important special cases.

After giving a brief exposé of general facts about Weil restrictions of abelian varieties in the first section, we study Weil restrictions with respect to extensions of finite fields in the second section. Here we determine the endomorphism algebra of a Weil restriction (see Theorem 1) and then show that under rather general assumptions, the Weil restriction is simple over the base-field (see Theorem 2).

In the third section, we deal with the following situation: $K|k$ is an arbitrary finite Galois extension of fields, A an abelian variety over k, W the Weil restriction of A_K with respect to $K|k$. We describe the endomorphism ring of W as a skew group ring over $\mathrm{End}(A_K)$ (see Theorem 3) and apply this result to study the isogeny decomposition of W over k. In the last subsection the results are applied to give an explicit description of the isogeny decomposition of W in the case of a cyclic field extension; see Theorem 4.

Notation

General

By a *ring* we mean a ring with unity, and by a ring-homomorphism a homomorphism of rings with unity. If R is a ring and Σ a finite set, then by $\mathrm{M}_\Sigma(R)$ we mean the matrix ring over R on the set Σ. For any abelian group G, G° denotes $G \otimes \mathbb{Q}$. If D is a skew field, we denote its center by $Z(D)$. If k is a field, $\overline{k}$ denotes an algebraic closure. If k is some field and X and Z are k-schemes, we denote the k-morphisms from Z to X by $X(Z)$.

Let k be a field. By a *homomorphism* between abelian k-varieties we mean a morphism of k-schemes which preserves the group structure (other authors might call this a k-homomorphism or a k-morphism of abelian varieties). Analogous definitions apply to isogenies and endomorphisms. The group of homomorphisms between two abelian k-varieties A and B is denoted by $\mathrm{Hom}(A,B)$ and the ring of endomorphisms of an abelian k-variety A by $\mathrm{End}(A)$. Following this terminology, we use the notion of a *simple* abelian k-variety where other authors might speak of a k-simple abelian k-variety. If two abelian k-varieties A and B are isogenous, we write $A \sim B$.

If we are given an extension of fields $K|k$, we denote k-schemes by X, Y etc. and K-schemes by X', Y' etc. (or by X_K, Y_K etc. if they are induced by base-change $K|k$).

We denote the dual abelian variety of an abelian k-variety A by $\widehat{A}$. For an invertible sheaf $\mathfrak{L}$ on A, $\phi_{\mathfrak{L}} : A \longrightarrow \widehat{A}$ denotes the corresponding homomorphism; c.f. [7, §6]. Following [6], a polarization φ of A is a homomorphism $A \longrightarrow \widehat{A}$ such that $\varphi \otimes_k \mathrm{id}_{\overline{k}} = \phi_{\mathfrak{L}} : A_{\overline{k}} \longrightarrow \widehat{A}_{\overline{k}}$ for some ample invertible sheaf on $A_{\overline{k}}$.

Galois twists

Let $K|k$ be a Galois extension of fields with Galois group G. Then the elements of G induce automorphisms of the $\mathrm{Spec}(k)$-scheme $\mathrm{Spec}(K)$ – we obtain in this way an anti-isomorphism $G \longrightarrow \mathrm{Aut}_{\mathrm{Spec}(k)}(\mathrm{Spec}(K))$.

We identify the opposite group G^{opp} with $\mathrm{Aut}_{\mathrm{Spec}(k)}(\mathrm{Spec}(K))$. We will always work with G^{opp} instead of G.

Let X' be a K-scheme.

For $\sigma \in G^{\mathrm{opp}}$, let $\sigma^{-1}(X')$ be the pull-back of X' via $\sigma : \mathrm{Spec}(K) \longrightarrow \mathrm{Spec}(K)$, i.e. if $p_K : X' \longrightarrow \mathrm{Spec}(K)$ is the structure morphism, $\sigma^{-1}(X')$ is X' considered as K-scheme via $\sigma^{-1} \circ p_K$. We denote the canonical isomorphism of k-schemes from $\sigma^{-1}(X')$ to X' also by σ. If Y' is another K-scheme and $\alpha : X' \longrightarrow Y'$ is a morphism of K-schemes, we obtain by base-change a morphism of K-schemes $\sigma^{-1}(\alpha) = \sigma^{-1}\alpha\sigma : \sigma^{-1}(X') \longrightarrow \sigma^{-1}(Y')$.

If X' is an abelian K-variety, by pull-back $\sigma^{-1}(X')$ also has the structure of an abelian K-variety.

Frobenius morphisms

Let q be a power of a prime number, k the finite field with q elements, let A be an abelian k-variety. The *Frobenius endomorphism* π_k of A is defined by the identity on the underlying topological space and by $f \mapsto f^q$ on the structure-sheaf $\mathcal{O}_A$. As the name indicates, π_k is an endomorphism of the abelian k-variety A.

Now let $K|k$ be an algebraic extension of fields. We identify the Galois group $\mathrm{Gal}(K|k)$ with its dual. The Frobenius automorphism of $K|k$ (or of $\mathrm{Spec}(K) \longrightarrow \mathrm{Spec}(k)$) is denoted by $\sigma_{K|k}$. If $K = \overline{k}$, we write σ_k instead of $\sigma_{\overline{k}|k}$.

Let A' be an abelian K-variety. As stated above, we have a canonical isomorphism of k-schemes $\sigma_{K|k} : \sigma_{K|k}^{-1}(A') \longrightarrow A'$. The *relative Frobenius homomorphism* (with respect to k) $\pi_k : A' \longrightarrow \sigma_{K|k}^{-1}(A')$ is a homomorphism of abelian K-varieties which is defined as follows: Let F_k be the morphism of the k-scheme A' to itself which is the identity on the underlying topological space and it is given by $f \mapsto f^q$ on the structure-sheaf $\mathcal{O}_{A'}$. Then $\pi_k := \sigma_{K|k}^{-1} \circ F_k : A' \longrightarrow \sigma_{K|k}^{-1}(A')$.

1 Definitions and first results

1.1 Definition of the Weil restriction

Let $K|k$ be a finite Galois extension. Let A' an abelian K-variety. It is well-known that the functor

$$Z \mapsto A'(Z \otimes_k K)$$

from the category of k-schemes to the category of abelian groups is representable by an abelian k-variety; for a construction via Galois theory see Subsection 1.2, for a construction via "restriction of scalars" see [1, 7.6]. (The representatility of the functor by an abelian variety holds more generally for a finite separable extension of fields, but we restrict ourselves to the Galois-case is this article.) A representing object will be denoted $\mathrm{Res}_k^K(A')$ and will be called the *Weil restriction* of A' with respect to $K|k$. The universal element $u \in A'(\mathrm{Res}_k^K(A') \otimes_k K)$ maps the zero of $\mathrm{Res}_k^K(A') \otimes_k K$ to the zero of A' and thus is a homomorphism of abelian K-varieties.

Now, $\mathrm{Res}_k^K(A')$ with u is also a representing object for the functor $B \mapsto \mathrm{Hom}(B_K, A')$ from the category of abelian k-varieties to the category of abelian groups as well as for the functor $B \mapsto \mathrm{Hom}^\circ(B_K, A')$ from the category of abelian k-varieties up to isogeny to the category of $\mathbb{Q}$-vector spaces.

1.2 Construction of the Weil restriction

Let us recall the construction of $\mathrm{Res}_k^K(A')$ via Galois theory.

Let W' be the following product of Galois-conjugates of A':

$$W' := \prod_{\sigma \in G^{\mathrm{opp}}} \sigma^{-1}(A') \tag{1}$$

Let $p_\sigma : W' \longrightarrow \sigma^{-1}(A')$ be the projections, let $\mathrm{Aut}_k(W')$ be the group of automorphisms of the k-scheme W'.

We define a Galois operation on W' by $G^{\mathrm{opp}} \longrightarrow \mathrm{Aut}_k(W')$, $\tau \mapsto \widetilde{\tau}$ where $\widetilde{\tau} = (\tau\, p_{\sigma\tau})_{\sigma \in G^{\mathrm{opp}}}$. Since W' is projective, the quotient $W := W'/G$ under this operation exists and is projective. We have $W' \simeq W_K$.

Fix some k-scheme Z. We have a Galois operation on $W'(Z \otimes_k K)$. If $\tau \in G^{\mathrm{opp}}$ and $P = (P_\sigma)_{\sigma \in G^{\mathrm{opp}}} \in W'(Z \otimes_k K)$, then $\tau((P_\sigma)_{\sigma \in G^{\mathrm{opp}}}) = (\tau(P_{\sigma\tau}))_{\sigma \in G^{\mathrm{opp}}}$. It follows that $P \mapsto (\sigma^{-1}(P))_{\sigma \in G^{\mathrm{opp}}}$ is a bijection between the $Z \otimes_k K$-valued points of A' and the Galois-invariant $Z \otimes_k K$-valued points of W'. On the other hand, by Galois theory, the Galois-invariant $Z \otimes_k K$-valued points of W' are in bijection with the Z-valued points of W. Both bijections are natural in Z.

It follows that $W = W'/G$ with universal element $u := p_{\mathrm{id}}$ represents the functor $Z \mapsto A'(Z \otimes_k K)$ from the category of k-schemes to the category of sets. Via the group laws on these sets, one defines a group law on W, and with this group law, W is an abelian variety. By construction, the neutral element and the addition law of W coincide after base-change with the neutral element and the addition law of the product of Galois-conjugates in (1). Moreover, the universal element $u = p_{\mathrm{id}}$ is a homomorphism of abelian K-varieties.

From the Galois-operation of W', we obtain

$$\tau^{-1}(p_\sigma) = p_{\sigma\tau}, \text{ especially } \tau^{-1}(u) = p_\tau. \tag{2}$$

1.3 The functor "restriction of scalars"

The assignment $A' \mapsto \mathrm{Res}_k^K(A')$ defines a covariant additive functor Res_k^K from the category of abelian K-varieties (up to isogeny) to the category of abelian k-varieties (up to isogeny). This functor is called "restriction of the field of definition" or "restriction of scalars" or "norm functor"; cf. [5].

For any abelian K-variety A', Res_k^K gives a ring-homomorphism from $\mathrm{End}(A')$ to $\mathrm{End}(\mathrm{Res}_k^K(A'))$ and from $\mathrm{End}^\circ(A')$ to $\mathrm{End}^\circ(\mathrm{Res}_k^K(A'))$.

Let A', B' be abelian K-varieties. Then

$$\mathrm{Hom}(\mathrm{Res}_k^K(A')_K, \mathrm{Res}_k^K(B')_K) \simeq \bigoplus_{\sigma,\nu \in G^{\mathrm{opp}}} \mathrm{Hom}(\nu^{-1}(A'), \sigma^{-1}(B')); \qquad (3)$$

see equations (1) and (5).

Let $\alpha : A' \longrightarrow B'$ be a homomorphism. Then under (3), $\mathrm{Res}_k^K(\alpha) \otimes_k \mathrm{id}_K$ is given by the diagonal "matrix"

$$(\sigma^{-1}(\alpha)\delta_{\sigma,\nu})_{\sigma,\nu \in G^{\mathrm{opp}}} \in \bigoplus_{\sigma,\nu \in G^{\mathrm{opp}}} \mathrm{Hom}(\nu^{-1}(A'), \sigma^{-1}(B')),$$

where $\delta_{\sigma,\nu}$ is the "Kronecker delta". If $\alpha : A' \longrightarrow B'$ is an isogeny, then $\mathrm{Res}_k^K(\alpha) : \mathrm{Res}_k^K(A') \longrightarrow \mathrm{Res}_k^K(B')$ is an isogeny of degree $(\deg(\alpha))^{[K:k]}$.

1.4 The Weil restriction of the dual abelian variety

The Weil restriction of the dual abelian variety is functorially isomorphic to the dual abelian variety of the Weil restriction. This can be seen as follows.

Let $W := \mathrm{Res}_k^K(A')$.

Let Z be some k-scheme, $\mathcal{L}$ some invertible sheaf on $A' \times_K Z_K$, algebraically equivalent to zero. Now consider the invertible sheaf

$$\mathcal{L}_{W_K} := \bigotimes_{\sigma} p_\sigma^* \sigma^*(\mathcal{L}) = \bigotimes_{\sigma} \tilde{\sigma}^* u^*(\mathcal{L})$$

on W_K. The isomorphism class in $\mathrm{Pic}(W_K \times_K Z_K)/\mathrm{Pic}(Z_K)$ of this invertible sheaf corresponds to an element in $\widehat{W_K}(Z_K)$ which is invariant under the Galois-operation and thus defines an element in $\widehat{W}(Z)$.

We obtain in this way a homomorphism $\widehat{A'}(Z_K) \longrightarrow \widehat{\mathrm{Res}_k^K(A')}(Z)$ which is functorial in Z. We thus have a homomorphism $\mathrm{Res}(\widehat{A'}) \longrightarrow \widehat{\mathrm{Res}_k^K(A')}$.

After base-change $K|k$, this homomorphism becomes the canonical isomorphism

$$\prod_{\sigma \in G^{\mathrm{opp}}} \sigma^{-1}(\widehat{A'}) \longrightarrow \prod_{\sigma \in G^{\mathrm{opp}}} \widehat{\sigma^{-1}(A')},$$

thus it is an isomorphism. This isomorphism $\mathrm{Res}(\widehat{A'}) \longrightarrow \widehat{\mathrm{Res}_k^K(A')}$ is functorial in A' as can for example easily be seen after base-change $K|k$. We thus have:

Proposition 1 *For abelian K-varieties A', $\mathrm{Res}_k^K(\widehat{A'})$ is functorially isomorphic to $\widehat{\mathrm{Res}_k^K(A')}$.*

1.5 Weil restrictions of polarized abelian varieties

Let $K|k$ be a finite Galois field extension, A' an abelian K-variety, $\widehat{A'}$ the dual abelian variety.

Let $\varphi : A' \longrightarrow \widehat{A'}$ be a polarization of A', defined by an ample invertible sheaf $\mathfrak{L}$ on $A'_{\overline{K}}$, i.e. $\varphi \otimes_K \mathrm{id}_{\overline{K}} = \phi_{\mathfrak{L}} : A'_{\overline{K}} \longrightarrow \widehat{A'}_{\overline{K}}$. As stated in Subsection 1.3, this induces an isogeny

$$\mathrm{Res}_k^K(\varphi) : \mathrm{Res}_k^K(A') \longrightarrow \mathrm{Res}_k^K(\widehat{A'}) \simeq \widehat{\mathrm{Res}_k^K(A')}.$$

We show now that this homomorphism is again a polarization.

Let $\sigma \in G^{\mathrm{opp}}$. We regard $\sigma^{-1}(\widehat{A'})$ as the dual abelian variety of $\sigma^{-1}(A')$.

Let σ' be a $\mathrm{Spec}(\overline{K})$-automorphism with $\pi \circ \sigma' = \sigma$ for the natural map $\pi : \mathrm{Spec}(\overline{K}) \to \mathrm{Spec}(K)$. Then

$$\sigma^{-1}(\varphi) \otimes_K \mathrm{id}_{\overline{K}} = \sigma'^{-1}(\phi_{\mathfrak{L}}) = \phi_{\sigma'^*(\mathfrak{L})}.$$

Here, the first equation is obvious by the definition of σ' and the second equation is a general fact for all polarizations on abelian varieties. It can be checked rather easily on $\overline{K}$-valued points.

After base-change, we get

$$\mathrm{Res}_k^K(\varphi) \otimes_k \mathrm{id}_K = (\sigma^{-1}(\varphi) \circ p_\sigma)_{\sigma \in G^{\mathrm{opp}}} : \prod_{\sigma \in G^{\mathrm{opp}}} \sigma^{-1}(A') \longrightarrow \prod_{\sigma \in G^{\mathrm{opp}}} \sigma^{-1}(\widehat{A'}).$$

This is a product polarization defined by the ample invertible sheaf

$$\mathfrak{L}_{W_{\overline{k}}} := \bigotimes_{\sigma} (p_\sigma \otimes_K \mathrm{id}_{\overline{K}})^* \sigma'^*(\mathfrak{L}) \tag{4}$$

on $W_{\overline{k}}$.

If one starts with an ample invertible sheaf $\mathfrak{L}$ on A', then analogously to (4), one defines an ample invertible sheaf $\mathfrak{L}_{W_K}$ on W_K. The class of this sheaf in the Picard group is invariant under the operation of $\mathrm{Gal}(K|k)$ and thus defines an ample invertible sheaf on W (because the Picard functor of an abelian variety is representable) – alternatively, one can also define explicitely a descent-datum on $\mathfrak{L}_{W_K}$.

Proposition 2 *Let $K|k$ be a finite Galois field extension, A' an abelian K-variety. If φ is a polarization on A' (defined by a sheaf on A'), then $\mathrm{Res}_k^K(\varphi)$ is a polarization on $\mathrm{Res}_k^K(A')$ (defined by a sheaf on $\mathrm{Res}_k^K(A')$). Furthermore $\deg(\mathrm{Res}_k^K(\varphi)) = (\deg(\varphi))^{[K:k]}$.*

Thus "restriction of scalars" is a functor from the category of polarized abelian K-varieties (with polarizations defined by sheaves on A') to the category of polarized abelian k-varieties (with polarizations defined by sheaves on $\mathrm{Res}_k^K(A')$) which preserves principal polarizations.

1.6 Appendix to Section 1: Products and the Rosati involution

Let k be a field, let B_i for $i = 1, \ldots, m$ and A_j for $j = 1, \ldots, n$ be abelian k-varieties. Let $A := \prod_{j=1,\ldots,n} A_j$, $B := \prod_{i=1,\ldots,m} B_i$. Let $\iota_j^A : A_j \longrightarrow A$ be the inclusions and let $p_j^A : A \longrightarrow A_j$ be the projections. (Similar definitions for B as well as the corresponding dual abelian varieties $\widehat{A}$ and $\widehat{B}$.) Then

$$\begin{array}{ccc} \mathrm{Hom}(A, B) & \longrightarrow & \bigoplus_{i,j} \mathrm{Hom}(A_j, B_i) \\ \psi & \mapsto & (p_i^B \psi \iota_j^A)_{i=1,\ldots,m,\, j=1,\ldots,n} \end{array} \tag{5}$$

is an isomorphism. (The same is true for the corresponding groups $\mathrm{Hom}^\circ(\ldots,\ldots)$ of both sides.)

Thus every homomorphism from A to B is uniquely determined by its "matrix", and conversely, every "matrix" determines a homomorphism. Furthermore, the composition of homomorphisms corresponds to the usual multiplication of matrices.

In particular, under (5), $\mathrm{End}(A)$ is isomorphic to the "matrix ring" $\bigoplus_{i,j} \mathrm{Hom}(A_j, A_i)$.

For later use we want to study how the Rosati involution with respect to a product polarization operates on the "matrices". It is convenient to generalize the concept of a "Rosati involution" first.

Let X and Y be abelian k-varieties with fixed polarizations $\varphi_X : X \longrightarrow \widehat{X}$, $\varphi_Y : Y \longrightarrow \widehat{Y}$. Then for every $\psi \in \mathrm{Hom}^\circ(X, Y)$, we denote $\varphi_X^{-1}\, \widehat{\psi}\, \varphi_Y \in \mathrm{Hom}^\circ(Y, X)$ by ψ' and call it the *Rosati involution* of ψ with respect to φ_X and φ_Y.

Now for $i = 1, \ldots, m$, $j = 1, \ldots, n$, let $\varphi_{B_i} : B_i \longrightarrow \widehat{B_i}$ and $\varphi_{A_j} : A_i \longrightarrow \widehat{A_j}$ be polarizations. Let φ_A and φ_B be the corresponding product polarizations.

Lemma 3 *Let $\psi \in \mathrm{Hom}^\circ(A, B)$ be given by the "matrix" $(\psi_{i,j})_{i=1,\ldots,m,\, j=1,\ldots,n}$, $\psi_{i,j} \in \mathrm{Hom}^\circ(A_j, B_i)$. Then with respect to φ_A and φ_B, the Rosati involution of ψ is given by the "matrix" $(\psi'_{j,i})_{i=1,\ldots,n,\, j=1,\ldots,m}$ with $\psi'_{j,i} \in \mathrm{Hom}^\circ(B_j, A_i)$.*

Proof Straightforward calculation. □

2 Results for finite fields

Let $K|k$ be a finite extension of *finite* fields of degree n. Let A' be an abelian variety over K, W the Weil restriction of A' with respect to $K|k$.

2.1 The endomorphism algebra

We now study the endomorphism algebra and the isogeny decomposition of W over k.

Let $\pi_k : A' \longrightarrow \sigma_{K|k}^{-1}(A')$ be the relative Frobenius homomorphism with respect to k and let $\pi_k : W \longrightarrow W$ be the Frobenius endomorphism; cf. "Notation".

Let π_K be the Frobenius endomorphism of A'. Then the image of π_K under the ring-homomorphism Res_k^K equals the endomorphism π_k^n of W. (In fact, after base-change $K|k$, $\mathrm{Res}_k^K(\pi_K)$ as well as π_k^n become equal to the Frobenius endomorphism of W_K.) Thus the ring-homomorphism $\mathrm{Res}_k^K : \mathrm{End}(A') \longrightarrow \mathrm{End}(W)$ restricts to an inclusion $\mathbb{Z}[\pi_K] \longrightarrow \mathrm{End}(W)$, given by $\pi_K \mapsto \pi_k^n$. This ring-homomorphism extends to a ring-homomorphism $\mathbb{Z}[\pi_K][X]/(X^n - \pi_k) \longrightarrow \mathrm{End}(W)$, given by $X \longrightarrow \pi_k$.

The Frobenius endomorphism π_k of W commutes with all endomorphisms of W. Thus by the universal property of the tensor product, the ring-homomorphisms $\mathrm{End}(A') \longrightarrow \mathrm{End}(W)$, $\lambda \mapsto \mathrm{Res}_k^K(\lambda)$ and $\mathbb{Z}[\pi_K][X]/(X^n - \pi_K) \longrightarrow \mathrm{End}(W)$, $X \mapsto \pi_k$ induce a ring-homomorphism

$$\mathrm{End}(A') \otimes_{\mathbb{Z}[\pi_K]} \mathbb{Z}[\pi_K][X]/(X^n - \pi_K) \longrightarrow \mathrm{End}(W),\ \lambda \mapsto \mathrm{Res}_k^K(\lambda),\ X \mapsto \pi_k.$$

Theorem 1 *Let $K|k$ be an extension of degree n of finite fields. Let A' be an abelian K-variety, W the Weil restriction of A' with respect to $K|k$. Then*

$$\mathrm{End}^\circ(A') \otimes_{\mathbb{Q}[\pi_K]} \mathbb{Q}[\pi_K][X]/(X^n - \pi_K) \longrightarrow \mathrm{End}^\circ(W),\ \lambda \mapsto \mathrm{Res}_k^K(\lambda),\ X \mapsto \pi_k$$

is an isomorphism.

Proof By the defining property of the Weil restriction, as abelian groups,

$$\mathrm{Hom}^\circ(W, W) \simeq \mathrm{Hom}^\circ(\prod_{i=0}^{n-1} \sigma_{K|k}^{-i}(A'), A') \text{ via } a \mapsto p_{\mathrm{id}} \circ (a \otimes_k \mathrm{id}_K). \quad (6)$$

We show that the homomorphism of abelian groups

$$\begin{gathered}\mathrm{Hom}^\circ(A', A') \otimes_{\mathbb{Q}[\pi_K]} \mathbb{Q}[\pi_K][X]/(X^n - \pi_K) \longrightarrow \mathrm{Hom}^\circ(W, W) \simeq \\ \mathrm{Hom}^\circ(\textstyle\prod_{i=0}^{n-1} \sigma_{K|k}^{-i}(A'), A') \simeq \bigoplus_{i=0}^{n-1} \mathrm{Hom}^\circ(\sigma_{K|k}^{-i}(A'), A')\end{gathered} \quad (7)$$

is an isomorphism. Since we already know the homomorphism in the theorem to be a ring-homomorphism, this will conclude the proof.

Let $\sigma_k \in \mathrm{Gal}(\overline{k}|k)$ be the Frobenius automorphism. By base-change, this induces an automorphism σ_k of the k-scheme $W_{\overline{k}}$.

The endomorphism $\pi_k : W \longrightarrow W$ is uniquely determined by the fact that it operates on $\overline{k}$-valued points P of $W_{\overline{k}}$ as the inverse of the "arithmetic Frobenius operation": $(\pi_k \otimes_k \mathrm{id}_{\overline{k}}) \circ P = \sigma_k^{-1}(P)$.

Let $P = (P_i)_{i=0}^{n-1}$ be a $\overline{k}$-valued point of $W_{\overline{k}} \simeq \prod_{i=0}^{n-1} \sigma_{K|k}^{-i}(A')_{\overline{K}}$. Then $\sigma_k^{-1}(P) = (\sigma_k^{-1}(P_{i-1}))_{i=0}^{n-1}$ (where $P_{-1} := P_{n-1}$); see Subsection 1.2. Thus $(\pi_k \otimes_k \mathrm{id}_{\overline{k}}) \circ P = \sigma_k^{-1}(P) = (\sigma_k^{-1}(P_{i-1}))_{i=0}^{n-1} = ((\pi_k \otimes_k \mathrm{id}_{\overline{k}}) \circ P_{i-1})_{i=0}^{n-1}$.

It follows that under the isomorphism $W_K \simeq \prod_{i=0}^{n-1} \sigma_{K|k}^{-i}(A')$, the endomorphism $\pi_k \otimes_k \mathrm{id}_K$ of W_K is given by the "matrix"

$$\begin{pmatrix} 0 & \cdots & \cdots & \pi_k \\ \pi_k & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ 0 & \ddots & \pi_k & 0 \end{pmatrix}.$$

For $\lambda \in \mathrm{End}^\circ(A')$, $\mathrm{Res}_k^K(\lambda) \otimes_k \mathrm{id}_K$ is given by the diagonal "matrix"

$$\begin{pmatrix} \lambda & & & \\ & \sigma_{K|k}^{-1}(\lambda) & & \\ & & \ddots & \\ & & & \sigma_{K|k}^{-(n-1)}(\lambda) \end{pmatrix};$$

see Subsection 1.3. Let x denote the image of X in $\mathbb{Q}[\pi_K][X]/(X^n - \pi_K)$. Let $\lambda_1 x + \lambda_2 x^2 + \cdots + \lambda_n x^n \in \mathrm{Hom}^\circ(A', A') \otimes_{\mathbb{Q}[\pi_K]} \mathbb{Q}[\pi_K][X]/(X^n - \pi_K)$ where $\lambda_i \in \mathrm{End}^\circ(A')$. Such an element is mapped under the homomorphism of the theorem to an endomorphism of W which is represented by the "matrix"

$$\begin{pmatrix} \lambda_n\, \pi_k^n & \lambda_{n-1}\, \pi_k^{n-1} & \cdots & \lambda_2\, \pi_k^2 & \lambda_1\, \pi_k \\ \sigma_{K|k}^{-1}(\lambda_1)\, \pi_k & \sigma_{K|k}^{-1}(\lambda_n)\, \pi_k^n & & \sigma_{K|k}^{-1}(\lambda_3)\, \pi_k^3 & \sigma_{K|k}^{-1}(\lambda_2)\, \pi_k^2 \\ \vdots & & \ddots & & \vdots \\ \sigma_{K|k}^{2-n}(\lambda_{n-2})\, \pi_k^{n-2} & \sigma_{K|k}^{2-n}(\lambda_{n-3})\, \pi_k^{n-3} & & \sigma_{K|k}^{2-n}(\lambda_n)\, \pi_k^n & \sigma_{K|k}^{2-n}(\lambda_{n-1})\, \pi_k^{n-1} \\ \sigma_{K|k}^{1-n}(\lambda_{n-1})\, \pi_k^{n-1} & \sigma_{K|k}^{1-n}(\lambda_{n-2})\, \pi_k^{n-2} & \cdots & \sigma_{K|k}^{1-n}(\lambda_1)\, \pi_k & \sigma_{K|k}^{1-n}(\lambda_n)\, \pi_k^n \end{pmatrix}.$$

The elements of $\mathrm{Hom}^\circ(A', A') \otimes_{\mathbb{Q}[\pi_K]} \mathbb{Q}[\pi_K][X]/(X^n - \pi_K)$ have a unique representation as $\lambda_1 x + \lambda_2 x^2 + \cdots + \lambda_n x^n$ with $\lambda_i \in \mathrm{End}^\circ(A')$. Under (7), this element corresponds to the first row in the above matrix, i.e. to the row vector

$$\begin{pmatrix} \lambda_n \pi_k^n & \lambda_{n-1} \pi^{n-1} & \cdots & \lambda_1 \pi_k \end{pmatrix}.$$

Now, every element of $\bigoplus_{i=0}^{n-1} \mathrm{Hom}^\circ(\sigma_{K|k}^{-i}(A'), A')$ has this form with unique λ_i. Thus (7) is an isomorphism. □

Remark 4 Since the Frobenius endomorphism has degree a power of $p = \mathrm{char}(k)$, we obtain in fact an isomorphism

$$(\mathrm{End}(A') \otimes_{\mathbb{Z}[\pi_K]} \mathbb{Z}[\pi_K][X]/(X^n - \pi_K)) \otimes \mathbb{Z}[1/p] \longrightarrow \mathrm{End}(W) \otimes \mathbb{Z}[1/p].$$

Corollary 5 $\mathrm{End}^\circ(W)$ *is commutative if and only if* $\mathrm{End}^\circ(A')$ *is commutative.*

The isomorphism of Theorem 1 implies that the corresponding centers are isomorphic. Recalling from [10] that $Z(\mathrm{End}^\circ(A')) = \mathbb{Q}[\pi_K]$, we thus get:

Corollary 6 *We have an isomorphism* $\mathbb{Q}[\pi_K][X]/(X^n - \pi_K) \simeq Z(\mathrm{End}^\circ(W))$.

2.2 Simplicity of the Weil restriction

We are interested in the question whether the Weil restriction W is simple.

In order that W be simple, it is obviously necessary that A' is simple. Furthermore, it is necessary that A' is not isogenous to any abelian K-variety which can be defined over any proper intermediate field λ of $K|k$ (i.e. any field λ with $k \subseteq \lambda \subsetneq K$). (This holds for arbitrary finite separable field extensions $K|k$.)

For assume that this is the case. Since the scalar restriction of an isogeny is an isogeny, we can assume that A' itself can be defined over such a λ; $A' = A_\lambda$ for some λ as above and an abelian λ-variety A. By the defining functorial property of $W = \mathrm{Res}_k^K(A')$, we have a canonical homomorphism $\mathrm{Res}_k^\lambda(A) \longrightarrow W$ which is easily seen to be an immersion. Since the dimension of the immersed abelian variety is strictly smaller, W is not simple.

We thus make the following assumption:

A' is a simple abelian K-variety which is not isogenous to any abelian K-variety which can be defined over some proper intermediate field λ of $K|k$.

Lemma 7 *Under our assumption on A', there does not exist a divisor q of n ($q \neq 1$) such that $\pi_K \in \mathbb{Q}[\pi_K]^q$.*

Proof Assume that such a q exists and let $\beta \in \mathbb{Q}[\pi_K]$ be such that $\beta^q = \pi_K$. (In particular $\mathbb{Q}[\pi_K] = \mathbb{Q}[\beta]$.)

Let λ be the subfield of $K|k$ of index q, let V be the Weil restriction of A' with respect to $K|\lambda$. Denoting by χ characteristic polynomials of Frobenius-actions on Tate-modules we have $\chi_V(T) = \chi_{A'}(T^q)$, and β is a root of χ_V. This follows from the well-known fact that the operation of the absolute Galois group of λ on $V(\overline{K})$ is induced by the operation of the absolute Galois group of K on $A'(\overline{K})$; see [5, §1,a)].

It is easy to see that V contains a simple abelian λ-variety A such that the characteristic polynomial of the Frobenius of A has β as a root.

The structure of the endomorphism algebra $\mathrm{End}^\circ(A)$ can be calculated from $\mathbb{Q}[\beta]$ as abstract field with generator β; see Subsection 2.3. Inserting β and π_K into formula (8), one sees that the central-simple $\mathbb{Q}[\pi_K]$-algebras

$\mathrm{End}^{\circ}(A)$ and $\mathrm{End}^{\circ}(A')$ have the same local invariants, thus they are isomorphic. Since by formula (9), the dimension of abelian varieties can be calculated from their endomorphism algebras, it follows that $\dim(A) = \dim(A')$.

The immersion $A \longrightarrow V = \mathrm{Res}_{\lambda}^{K}(A')$ induces by the defining functorial property of the Weil restriction a non-trivial homomorphism $A_K \longrightarrow A'$. Since the dimensions agree and A' is simple, this is an isogeny. A contradiction. □

We now make use of the following well-known fact from field theory; see [4, VI, §9, especially Theorem 9.1]:

Lemma 8 *Let F be a field, $\alpha \in F, \alpha \neq 0$ and $n \in \mathbb{N}$. Assume that $\alpha \notin F^q$ for all prime divisors q of n. Then either $X^n - \alpha$ is irreducible over F or $4|n$ and $\alpha \in -4F^4$.*

Together with Corollary 6, this implies:

Proposition 9 *Under our assumption on A',*

- *either $\mathrm{Res}_k^K(A')$ has exactly one isotypic component, i.e. all simple abelian subvarieties are isogenous*
- *or $4|n$ and $\pi_K \in -4\mathbb{Q}[\pi_K]^4$.*

Proof By the previous two lemmata, under our assumption on A', either $X^n - \pi_K$ is irreducible over $\mathbb{Q}[\pi_K]$ or $4|n$ and $\pi_K \in -4\mathbb{Q}[\pi_K]^4$. Corollary 6 implies: $X^n - \pi_K$ is irreducible over $\mathbb{Q}[\pi_K]$ if and only if $Z(\mathrm{End}^{\circ}(\mathrm{Res}_k^K(A')))$ is a field. This in turn is equivalent to the fact that $\mathrm{Res}_k^K(A')$ has exactly one isotypic component. □

Remark 10 By Honda's Theorem (see Proposition 12), it is obviously possible that additionally to our general assumption on A' the second condition is satisfied. It is interesting to note that there even exist ordinary elliptic curves E' over fields of the form $\mathbb{F}_{p^4}$ (p prime) which are non-isogenous to any elliptic $\mathbb{F}_{p^4}$-curve which can be defined over $\mathbb{F}_{p^2}$ and which satisfy $\pi_K \in -4\mathbb{Q}[\pi_K]^4$. Then $\mathrm{Res}_{\mathbb{F}_p}^{\mathbb{F}_{p^4}}(E')$ has more than one isotypic component. Since on the other hand it cannot contain an elliptic curve by our first assumption on E', $\mathrm{Res}_{\mathbb{F}_p}^{\mathbb{F}_{p^4}}(E')$ has exactly two isotypic components both of which are simple.

For example, let p be a prime such that $\left(\frac{-2}{p}\right) = 1$, let $K := \mathbb{F}_{p^4}, k := \mathbb{F}_p$.

By assumption, p splits in the field $\mathbb{Q}[\sqrt{-2}]$; see [8, Satz 8.5.]. Since this field has class number 1, there is a prime element $\nu \in \mathcal{O}_{\mathbb{Q}[\sqrt{-2}]}$ such that $(\nu)(\overline{\nu}) = (p)$. (Where $-$ denotes conjugation.) Since the norm of an element is always positive, this implies $\nu\overline{\nu} = p$. If $i \in \mathbb{N}$, then $\nu^i \neq \overline{\nu}^i$, thus $\nu^i \notin \mathbb{Q}$.

Let $\alpha := -\nu^4$. Then $\alpha^i \notin \mathbb{Q}$ for all $i \in \mathbb{N}$. In particular, $\mathbb{Q}[\alpha] = \mathbb{Q}[\sqrt{-2}]$. Let E' be a simple abelian K-variety which corresponds to $(\mathbb{Q}[\alpha], \alpha)$ by Honda's Theorem (see Proposition 12). By formula (8), all local invariants of $\mathrm{End}^\circ(E')$ are congruent to 0, thus $\mathrm{End}^\circ(E') \simeq \mathbb{Q}[\alpha]$, and E' is an elliptic K-curve. Since $\alpha^i \notin \mathbb{Q}$ for all $i \in \mathbb{N}$, E' is ordinary.

The algebraic integer $\alpha = -\nu^4 = -4(\frac{\nu}{\sqrt{-2}})^4$ lies in $-4\mathbb{Q}[\alpha]^4$. It remains to check that E' is not isogenous to any elliptic K-curve which can be defined over $\mathbb{F}_{p^2}$.

Assume this was the case. Then there is a $\beta \in \mathrm{End}^\circ(E') = \mathbb{Q}[\alpha] = \mathbb{Q}[\sqrt{-2}]$ with $\beta^2 = \alpha = -\nu^4$. This implies $i = \sqrt{-1} = \frac{\beta}{\nu^2} \in \mathbb{Q}[\sqrt{-2}]$, a contradiction.

Our aim is now to give conditions under which the Weil restriction of A' is even simple.

Theorem 2 *Let $K|k$ be an extension of finite fields of degree n and A' a simple abelian K-variety. Assume that A' is not isogenous to any abelian K-variety which can be defined over a proper intermediate field of $K|k$. Assume in addition that one of the following holds:*

- $\mathrm{End}(A')$ *is commutative and further, if* $4|n$, *then* $\pi_K \notin -4\mathbb{Q}[\pi_K]^4$.
- *The extension degree n is prime.*

Then $\mathrm{Res}_k^K(A')$ *is simple.*

Proof Assume as in the theorem that A' is not isogenous to any abelian variety which can be defined over a proper intermediate field of $K|k$.

We first treat the case that $\mathrm{End}(A')$ is commutative and further, if $4|n$, then $\pi_K \notin -4\mathbb{Q}[\pi_K]^4$. Under these conditions, $\mathrm{End}^\circ(\mathrm{Res}_k^K(A'))$ is also commutative (see Corollary 5), and by the above Proposition, $\mathrm{Res}_k^K(A')$ has exactly one isotypic component. This implies that $\mathrm{Res}_k^K(A')$ is simple.

We now come to the case that the extension degree n is a prime. Let $B \subseteq \mathrm{Res}_k^K(A')$ be a simple abelian subvariety. Applying base-change, we get $B_K \subseteq \prod_{i=0}^{n-1} \sigma_{K|k}^{-i}(A')$. This implies $\dim(A') \,|\, \dim(B)$. Additionally, the dimensions cannot be equal since otherwise by the defining functorial property of the Weil restriction, we would have an isogeny $B_K \longrightarrow A'$ which is impossible by assumption. On the other hand, since by Proposition 9 $\mathrm{Res}_k^K(A')$ has exactly one isotypic component, $\dim(B) \,|\, \dim(\mathrm{Res}_k^K(A')) = n \dim(A')$. Since n is a prime, this implies $\dim(B) = \dim(\mathrm{Res}_k^K(A'))$ thus $B = \mathrm{Res}_k^K(A')$. □

Remark 11 Let $K := \mathbb{F}_{p^4}, k := \mathbb{F}_p$ where p is a prime with $p \equiv 1 \pmod 4$. We will now give an elliptic K-curve E' with *non-commutative* endomorphism ring such that $\mathrm{Res}_k^K(E')$ is *non-simple* even though E' is not isogenous to any abelian $\mathbb{F}_{p^4}$-variety which can be defined over $\mathbb{F}_{p^2}$ and the condition $\pi_K \notin -4\mathbb{Q}[\pi_K]^4$ is satisfied.

Let E' be a simple abelian K-variety which corresponds to the integer $-p^2$ by Honda's Theorem; see Proposition 12. By formula (8), the local invariants of $\mathrm{End}^{\circ}(E')$ at p and ∞ are congruent to $\frac{1}{2}$, thus E' is a supersingular elliptic curve such that all endomorphisms of $E'_{\overline{\mathbb{F}}_p}$ can be defined over $\mathbb{F}_{p^4}$.

Assume there is an elliptic $\lambda := \mathbb{F}_{p^2}$-curve E such that $E_K \sim E'$. Let π_λ be its Frobenius endomorphism. Then we have $\mathbb{Q}[\pi_\lambda] \simeq \mathbb{Q}[i]$ ($i := \sqrt{-1}$), and under this isomorphism, π_λ corresponds to ip. Now by assumption, p splits in $\mathbb{Q}[i]$, and from formula (8), it follows that the local invariants of $\mathrm{End}^{\circ}(E)$ over p are congruent to $\frac{1}{2}$, thus by (9), E is 2-dimensional, a contradiction.

Let W be the Weil restriction of E' with respect to $K|k$. Then by Corollary 6, the center of $\mathrm{End}^{\circ}(W)$ is isomorphic to $\mathbb{Q}[X]/(X^4 + p^2) = \mathbb{Q}[\sqrt[4]{-p^2}]$, and under this isomorphism π_k corresponds to $\sqrt[4]{-p^2}$. In this field, p is ramified of degree 2 and splits into 2 prime ideals (because it already splits in the subfield $\mathbb{Q}[i]$). Again by formula (8), the endomorphism algebras of the simple components of W are fields, thus isomorphic to $\mathbb{Q}[\sqrt[4]{-p^2}]$. It follows with (9) that the simple components of W are 2-dimensional, thus W is not simple.

2.3 Appendix to Section 2: Some results by Honda and Tate

For the convenience of the reader, we recall Honda's Theorem on the classification of simple abelian varieties over finite fields and Tate's results how to compute the structure of the endomorphism ring of an abelian variety over a finite field; c.f. [3, 10, 11].

Fix a finite field $k = \mathbb{F}_q$, where $q = p^a$ with p a prime and $a \in \mathbb{N}$. Then, if A is a simple abelian k-variety and π_k is its Frobenius endomorphism, for every inclusion φ of $\mathbb{Q}[\pi_k]$ into $\overline{\mathbb{Q}}$, we have $|\varphi(\pi_k)| = q^{\frac{1}{2}}$.

Now Honda's Theorem states:

Proposition 12 (Honda) *The assignment $A \mapsto (\mathbb{Q}[\pi_k], \pi_k)$ induces a bijection between the set of isogeny classes of simple abelian k-varieties and the set of isomorphism classes of fields $\mathbb{Q}[\alpha]$ with fixed generator α such that α is an algebraic integer and under all inclusions into $\overline{\mathbb{Q}}$, α has absolute value $q^{\frac{1}{2}}$.*

By Honda's Theorem, for every simple abelian k-variety A, the structure of the endomorphism algebra $\mathrm{End}^{\circ}(A)$ only depends on $\mathbb{Q}[\pi_k]$ as abstract field with generator π_k. Since $\mathrm{End}^0(A)$ is central-simple over $\mathbb{Q}[\pi_k]$, to determine its structure, we only have to give its local invariants at all finite and real valuations.

The formula for this is as follows: Let v be a normalized valuation of $\mathbb{Q}[\pi_k]$. Then, if v is finite, the local invariant of $\mathrm{End}^\circ(A)$ at v is given by

$$\mathrm{inv}_v \equiv \frac{v(\pi_k)}{a} f_v \pmod 1, \tag{8}$$

where f_v denotes the absolute residue degree of $\mathbb{Q}[\pi_k]$ at v. In particular, if v is a finite valuation which does not lie over the valuation of p, the local invariant is congruent to 0.

If v is real, then the local invariant is congruent to $\frac{1}{2}$.

Let m be the least common denominator of the local invariants. Then the order of $\mathrm{End}^\circ(A)$ in the Brauer group of $\mathbb{Q}[\pi_k]$ is m, $m^2 = [\mathrm{End}^\circ(A) : \mathbb{Q}[\pi_k]]$, and the dimension of A in given by

$$\dim(A) = \frac{1}{2}\, m\, [\mathbb{Q}[\pi_k] : \mathbb{Q}]. \tag{9}$$

3 Results for abelian varieties which can be defined over the base-field

Throughout this section, let $K|k$ be a finite Galois extension of degree n with Galois group G, and let A be an abelian k-variety of dimension d. Let W be the Weil restriction of A_K with respect to $K|k$.

We want to determine the structure of the endomorphism ring of W, and the isogeny decomposition of W over k.

3.1 Arithmetic becomes geometric operation

For any k-scheme Z, G operates on $A_K(Z_K)$ by $\tau(P) = \tau P \tau^{-1}$. These operations define an automorphism of the functor $Z \mapsto A_K(Z_K)$ from the category of k-schemes to the category of abelian groups. We obtain automorphisms of the representing object $W = \mathrm{Res}_k^K(A_K)$ which we denote by a_τ for $\tau \in G^{\mathrm{opp}}$. We thus have a group-homomorphism $a : G^{\mathrm{opp}} \longrightarrow \mathrm{Aut}(W)$, $\tau \longrightarrow a_\tau$, where $\mathrm{Aut}(W)$ denotes the group of automorphisms of the abelian k-variety W.

We want to calculate how $a_\tau \otimes_k \mathrm{id}_K$ operates on $W_K \simeq A_K^{G^{\mathrm{opp}}}$.

We have $\tau(u) = \tau(p_{\mathrm{id}}) = p_{\tau^{-1}} : W_K \longrightarrow A_K$ by (2). The homomorphism a_τ of the abelian k-variety W is the W-valued point of W which corresponds to $\tau(u)$. So by Subsection 1.2, $a_\tau \otimes_k \mathrm{id}_K = (\sigma^{-1}(\tau(u)))_{\sigma \in G^{\mathrm{opp}}} = (\sigma^{-1}(p_{\tau^{-1}}))_{\sigma \in G^{\mathrm{opp}}} = (p_{\tau^{-1}\sigma})_{\sigma \in G^{\mathrm{opp}}}$. (The last equation follows from (2).) We have established:

Lemma 13 $a_\tau \otimes_k \mathrm{id}_K : A_K^{G^{\mathrm{opp}}} \longrightarrow A_K^{G^{\mathrm{opp}}}$ *operates on Z-valued points (any Z) by $(P_\sigma)_{\sigma \in G^{\mathrm{opp}}} \mapsto (P_{\tau^{-1}\sigma})_{\sigma \in G^{\mathrm{opp}}}$.*

3.2 The endomorphism ring as skew group ring

Lemma 14 *Let $\tau \in G^{\mathrm{opp}}, \lambda \in \mathrm{End}(A_K)$. Then $a_\tau \circ \mathrm{Res}_k^K(\lambda) = \mathrm{Res}_k^K(\tau(\lambda)) \circ a_\tau \in \mathrm{End}(W)$.*

Proof Easy calculation on Z-valued points. □

To formulate the result about the structure of the endomorphism ring of W, we need a generalization of the concept of a group ring first.

Definition Let Λ be a ring, G a group, $t : G \longrightarrow \mathrm{Aut}(\Lambda)$ a group-homomorphism. The application of $t(\sigma)$ to some $\lambda \in \Lambda$ will by denoted by $\sigma(\lambda)$. Following [9], we define the *skew group ring* $\Lambda^t[G]$ to be the following ring:[1] The underlying abelian group is Λ^G with the usual "componentwise" addition. As usual, for $\tau \in G$, let τ also denote $(\delta_{\sigma,\tau})_{\sigma \in G} \in \Lambda^G$.The multiplication is defined by $\sum_{\sigma \in G} \lambda_\sigma \, \sigma \cdot \sum_{\nu \in G} \mu_\nu \, \nu = \sum_{\sigma,\nu \in G} \lambda_\sigma \, \sigma(\mu_\nu) \, \sigma\nu$.

The ring Λ is naturally immersed in $\Lambda^t[G]$. For fixed Λ, G and $t : G \longrightarrow \mathrm{Aut}(\Lambda)$, the ring $\Lambda^t[G]$ has the following universal property:

Lemma 15 *Let B be a ring, $f : \Lambda \longrightarrow B$ be a ring-homomorphism, and let $g : G \longrightarrow B^*$ be a group-homomorphism. Assume that for $\lambda \in \Lambda, \tau \in G$, $g(\tau)\, f(\lambda) = f(\tau(\lambda))\, g(\tau)$. Then there is a unique ring-homomorphism $\Lambda^t[G] \longrightarrow B$ with $\lambda \mapsto f(\lambda)$ and $\tau \mapsto g(\tau)$.*

Now let G be the Galois group as above, $t : G^{\mathrm{opp}} \longrightarrow \mathrm{Aut}(\mathrm{End}(A_K))$ the natural operation given by $\sigma \mapsto (\lambda \mapsto \sigma(\lambda) = \sigma\lambda\sigma^{-1})$. From Lemmata 14 and 15 it follows that $\sum_{\sigma \in G^{\mathrm{opp}}} \lambda_\sigma \, \sigma \mapsto \sum_{\sigma \in G^{\mathrm{opp}}} \mathrm{Res}_k^K(\lambda_\sigma)\, a_\sigma$ defines a ring-homomorphism

$$\mathrm{End}(A_K)^t[G^{\mathrm{opp}}] \longrightarrow \mathrm{End}(W). \tag{10}$$

Theorem 3 *Let $K|k$ be a finite Galois extension with Galois group G, A an abelian k-variety, W the Weil restriction of A_K with respect to $K|k$, $t : G^{\mathrm{opp}} \longrightarrow \mathrm{Aut}(\mathrm{End}(A_K))$ the natural operation. Then*

$$\mathrm{End}(A_K)^t[G^{\mathrm{opp}}] \longrightarrow \mathrm{End}(W), \ \sum_{\sigma \in G^{\mathrm{opp}}} \lambda_\sigma \, \sigma \mapsto \sum_{\sigma \in G^{\mathrm{opp}}} \mathrm{Res}_k^K(\lambda_\sigma)\, a_\sigma$$

is an isomorphism.

[1] This ring is a special case of a *crossed product* (with respect to some operation); cf. [9]. In [2], the same ring is called *twisted group ring*. However, in [9], this word is reserved for the special case of a crossed product with respect to a trivial group operation.

Proof Analogously to the proof of Theorem 1, we make use of the isomorphism $\mathrm{Hom}(W,W) \simeq \mathrm{Hom}(A_K^{G^{\mathrm{opp}}}, A_K) \simeq \bigoplus_{\sigma \in G^{\mathrm{opp}}} \mathrm{Hom}(A_K, A_K)$ of the right-hand side.

By (2), the image of some $\sigma \in G^{\mathrm{opp}}$ in $\mathrm{Hom}(A_K^{G^{\mathrm{opp}}}, A_K)$ is $p_{\sigma^{-1}}$, corresponding to the row vector which is zero except at the "σ-th" entry where it is 1.

Thus the image of $\sum_{\sigma \in G^{\mathrm{opp}}} \lambda_\sigma \sigma$ (where $\lambda_\sigma \in \mathrm{End}(A_K)$) is $\sum_{\sigma \in G^{\mathrm{opp}}} \lambda_{\sigma^{-1}} \, p_\sigma$, corresponding to the row vector $(\lambda_{\sigma^{-1}})_{\sigma \in G^{\mathrm{opp}}}$.

It is thus immediate that we have an isomorphism. □

Corollary 16 *The isomorphism in the theorem induces an isomorphism* $\mathrm{End}^\circ(A_K)^t[G^{\mathrm{opp}}] \longrightarrow \mathrm{End}^\circ(W)$.

By the Complete Reducibility Theorem (see [6, Proposition 12.1]) we know that the ring $\mathrm{End}^\circ(W)$ is semi-simple. Thus the skew group ring $\mathrm{End}^\circ(A_K)^t[G^{\mathrm{opp}}]$ is semi-simple.

It can be proven more generally that every crossed product over a semi-simple ring with a finite group in which the group order is invertible is semi-simple; see [9, Theorem 4.1.].

We now want to study the ring-homomorphism

$$\begin{gathered} \mathrm{End}(A_K)^t[G^{\mathrm{opp}}] \xrightarrow{\sim} \mathrm{End}(W) \hookrightarrow \\ \mathrm{End}(W_K) \simeq \mathrm{End}(A_K^{G^{\mathrm{opp}}}) \simeq \mathrm{M}_{G^{\mathrm{opp}}}(\mathrm{End}(A_K)). \end{gathered} \tag{11}$$

We denote the matrix corresponding to a_τ by A_τ and the matrix corresponding to $\mathrm{Res}_k^K(\lambda)$ by $J(\lambda)$ (for a_τ as above and $\lambda \in \mathrm{End}(A_K)$).

We have already shown in Subsection 1.3 that $J(\lambda)$ is the diagonal matrix $(\sigma^{-1}(\lambda)\delta_{\sigma,\nu})_{\sigma,\nu \in G^{\mathrm{opp}}}$.

Let us determine to which matrix $A_\tau \in \mathrm{M}_{G^{\mathrm{opp}}}(\mathrm{End}(A_K))$ the endomorphism a_τ corresponds. First of all, $p_\sigma : W_K \simeq A_K^{G^{\mathrm{opp}}} \longrightarrow A_K$ corresponds to the row vector $(\delta_{\sigma,\nu})_{\nu \in G^{\mathrm{opp}}}$. As $a_\tau = (p_{\tau^{-1}\sigma})_{\sigma \in G^{\mathrm{opp}}}$ (see Lemma 13), we get

$$A_\tau = (\delta_{\tau^{-1}\sigma,\nu})_{\sigma,\nu \in G^{\mathrm{opp}}} = (\delta_{\sigma,\tau\nu})_{\sigma,\nu \in G^{\mathrm{opp}}}. \tag{12}$$

Before continuing let us recall the definition of the left regular (matrix) representation.

The left regular (matrix) representation

Let Λ be a ring. If $\Lambda \longrightarrow \Xi$ is a homomorphism of rings, we can regard Ξ as Λ-right module, and if we do so, we write $\mathrm{End}^r_\Lambda(\Xi)$ for the ring of endomorphisms.

Now let $\Lambda \longrightarrow \Xi$ be a homomorphism of rings and assume additionally that Ξ is free as Λ-right module on a finite set of generators Σ, i.e. $\Xi \simeq \Lambda^\Sigma$ as Λ-right modules. Multiplication by elements of Ξ from the left induces a ring-homomorphism

$$l : \Xi \longrightarrow \mathrm{End}^r_\Lambda(\Xi) \simeq \mathrm{End}^r_\Lambda(\Lambda^\Sigma), \tag{13}$$

the *left regular representation.*

For a fixed basis Σ, the right-hand side of (13) is canonically isomorphic to the matrix ring $\mathrm{M}_\Sigma(\Lambda)$. The isomorphism is given as follows:

$$\begin{array}{c} \mathrm{End}^r_\Lambda(\Lambda^\Sigma) \longrightarrow \mathrm{M}_\Sigma(\Lambda),\ a \mapsto (\alpha_{\sigma,\nu})_{\sigma,\nu\in\Sigma} \text{ with } \alpha_{\sigma,\nu} \in \Lambda \\ \text{and } a(\nu) = \sum_{\sigma\in\Sigma} \sigma\, \alpha_{\sigma,\nu}. \end{array} \tag{14}$$

By composition of (13) with (14), we get the *left regular matrix representation* (with respect to the basis Σ).

$$L : \Xi \longrightarrow \mathrm{M}_\Sigma(\Lambda).$$

We now apply these concepts in the context of the skew group ring. Let G be a finite group, $t : G \longrightarrow \mathrm{Aut}(\Lambda)$ be a homomorphism, $\Lambda^t[G]$ the corresponding skew group ring.

We calculate explicitly the left regular representation $l : \Lambda^t[G] \longrightarrow \mathrm{End}^r_\Lambda(\Lambda^t[G])$ and the left regular matrix representation $L : \Lambda^t[G] \longrightarrow \mathrm{M}_G(\Lambda)$ with respect to the basis G.

Let $\tau \in G$. Then $l(\tau) : \nu \mapsto \tau\nu = \sum_{\sigma\in G} \sigma\delta_{\sigma,\tau\nu}$ and thus

$$L(\tau) = (\delta_{\sigma,\tau\nu})_{\sigma,\nu\in G}.$$

Let $\lambda \in \Lambda$. Then $l(\lambda) : \nu \mapsto \lambda\,\nu = \nu\,\nu^{-1}(\lambda)$ and thus

$$L(\lambda) = (\sigma^{-1}(\lambda)\,\delta_{\sigma,\nu})_{\sigma,\nu\in G}.$$

We are now going to relate these definitions and calculations with our situation. So let $\Lambda := \mathrm{End}(A_K)$, G the Galois group and $t : G^{\mathrm{opp}} \longrightarrow \mathrm{End}(A_K)$ the natural operation. Let L be the left regular matrix representation of Λ with respect to the basis G^{opp}. Then $L(\tau) = A_\tau$ and $L(\lambda) = J(\lambda)$. Thus:

Proposition 17 *Homomorphism (11) is the left regular matrix representation of the skew group ring* $\mathrm{End}(A_K)^t[G^{\mathrm{opp}}]$ *with respect to the basis* G^{opp}.

3.3 The Rosati involution

Let $\varphi : A_K \longrightarrow \widehat{A}_K$ be a polarization. Then $\mathrm{Res}_k^K(\varphi) : W \longrightarrow \widehat{W}$ is also a polarization; see Subsection 1.5.

We want to calculate how the Rosati involution of W with respect to $\mathrm{Res}_k^K(\varphi)$ is given under the isomorphism of Corollary 16.

Let us denote the Rosati involution by $(\ldots)'$.

First of all, the (defining) equation $\lambda' = \varphi^{-1}\widehat{\lambda}\varphi$ where $\lambda \in \mathrm{End}^\circ(A_K)$ implies

$$\mathrm{Res}_k^K(\lambda') = \mathrm{Res}_k^K(\varphi)^{-1} \circ \mathrm{Res}_k^K(\widehat{\lambda}) \circ \mathrm{Res}_k^K(\varphi) = \mathrm{Res}_k^K(\lambda)'.$$

(This holds more generally for any abelian K-variety A' instead of A_K.)

We use the inclusion of $\mathrm{End}^\circ(W)$ into the matrix ring $\mathrm{M}_{G^{\mathrm{opp}}}(\mathrm{End}^\circ(A))$ and the fact that $\mathrm{Res}_k^K(\varphi) \otimes_k \mathrm{id}_K$ is a product polarization to calculate the Rosati involution of a_τ with the help of Lemma 3.

Since a_τ corresponds to the matrix $A_\tau = (\delta_{\sigma,\tau\nu})_{\sigma,\nu\in G^{\mathrm{opp}}}$ (see (12)), a'_τ corresponds to the matrix $(\delta_{\nu,\tau\sigma})_{\sigma,\nu\in G^{\mathrm{opp}}} = (\delta_{\tau^{-1}\nu,\sigma})_{\sigma,\nu\in G^{\mathrm{opp}}} = (\delta_{\sigma,\tau^{-1}\nu})_{\sigma,\nu\in G^{\mathrm{opp}}} = A_{\tau^{-1}}$. Thus

$$a'_\tau = a_{\tau^{-1}}.$$

Since the Rosati involution is an anti-ring-endomorphism, this implies:

Proposition 18 *Let $K|k$ be a finite Galois field extension with Galois group G, A an abelian k-variety, W the Weil restriction of A_K with respect to $K|k$. Let $\varphi : A \longrightarrow \widehat{A}$ be a polarization. Let $\lambda \mapsto \lambda'$ be the Rosati involution associated to φ. Then under the isomorphism of Corollary 16, the Rosati involution associated to the polarization $\mathrm{Res}_k^K(\varphi) : W \longrightarrow \widehat{W}$ is given by $\sum_{\sigma\in G^{\mathrm{opp}}} \lambda_\sigma\, \sigma \mapsto \sum_{\sigma\in G^{\mathrm{opp}}} \sigma^{-1}\lambda'_\sigma = \sum_{\sigma\in G^{\mathrm{opp}}} \sigma^{-1}(\lambda'_\sigma)\, \sigma^{-1}$.*

3.4 Dimensions of components

As in the above proposition, let A be an abelian k-variety, $K|k$ a galois field extension of degree n with galois group G, W the Weil restriction of A_K with respect to $K|k$, and let $t : G^{\mathrm{opp}} \longrightarrow \mathrm{End}(A_K)$ be the natural operation.

Assume $D \subseteq \mathrm{End}^\circ(A_K)$ is a skew field, invariant under the operation t.

Let $\bigoplus_{i=1}^s \Lambda_i = D^t[G^{\mathrm{opp}}]$ be a decomposition of the $D^t[G^{\mathrm{opp}}]$-right module $D^t[G^{\mathrm{opp}}]$. This defines a decomposition $1 = \sum_i e_i$ where the e_i are orthogonal idempotents, $e_i \in \Lambda_i$, such that $\Lambda_i = e_i\, D^t[G^{\mathrm{opp}}]$. Conversely, if we are given a decomposition $1 = \sum_i e_i$ with orthogonal idempotents e_i, then the $\Lambda_i := e_i\, D^t[G^{\mathrm{opp}}]$ define a direct sum decomposition of the $D^t[G^{\mathrm{opp}}]$-right module $D^t[G^{\mathrm{opp}}]$.

Via the inclusion $D^t[G^{\mathrm{opp}}] \hookrightarrow \mathrm{End}^{\circ}(A_K)^t[G^{\mathrm{opp}}] \simeq \mathrm{End}^{\circ}(W)$, we can regard the e_i to be elements of $\mathrm{End}^{\circ}(W)$. For each i, let $c_i \in \mathbb{N}$ such that $c_i e_i \in \mathrm{End}(W)$.

Now put $W_i := (c_i e_i)(W)$. The W_i are abelian subvarieties of W and $\bigoplus_{i=1}^{s} W_i \sim W$. (Conversely, such an isogeny decomposition where the W_i are abelian subvarieties of W determines a decomposition of $\mathrm{End}^{\circ}(W)$ as right-$\mathrm{End}^{\circ}(W)$ module.)

Proposition 19 *Let $D \subseteq \mathrm{End}^{\circ}(A_K)$ be a skew field, invariant under the operation t on $\mathrm{End}^{\circ}(A_K)$. Let $\bigoplus_{i=1}^{s} \Lambda_i = D^t[G^{\mathrm{opp}}]$ be a decomposition of the $D^t[G^{\mathrm{opp}}]$-right module $D^t[G^{\mathrm{opp}}]$. This corresponds to a decomposition $\mathrm{id}_{A_K} = \sum_i e_i$. Let $W_i := (c_i e_i)(W)$ be as above. Then $W_{iK} \approx A_K^{n_i}$ (non-canonical isomorphism) where*

$$n_i = \dim_D(\Lambda_i).$$

Proof Choose a bijection between G^{opp} and the set $\{1, \ldots, n\}$. Then $A_K^{G^{\mathrm{opp}}} \simeq A_K^n$.

Let l and L be the left regular (matrix) representations of $\mathrm{End}^{\circ}(A_K)^t[G^{\mathrm{opp}}]$, l_D and L_D the left regular (matrix) representations of $D^t[G^{\mathrm{opp}}]$ (both regular matrix representations with respect to the basis G^{opp}). Let $\iota_{\mathrm{M}} : \mathrm{M}_{G^{\mathrm{opp}}}(D) \longrightarrow \mathrm{M}_{G^{\mathrm{opp}}}(\mathrm{End}(A_K))$ be the canonical inclusion. Then $L = \iota_{\mathrm{M}} L_D$.

By construction $l_D(e_i)$ is the identity on Λ_i and zero on all Λ_j for $j \neq i$.

Let n_i be the dimension of the D-module Λ_i. For each i, choose a basis $(b_i^{(j)})_{j=1,\ldots,n_i}$ of the D-module Λ_i. Then all n elements $b_i^{(j)}$ define a basis of the D-module $D^t[G^{\mathrm{opp}}]$. With respect to this basis, the matrix associated to $l_D(e_i)$ is zero outside a block of size n_i where it is the identity matrix.

We now have two matrix representations of $l_D(e_i)$ with respect to different bases, and via a base change matrix, we can transform one into the other: There exists an invertible matrix $B \in \mathrm{Gl}_n(D)$ such that $BL_D(e_i)B^{-1}$ is zero outside a block of size n_i where it is the identity matrix.

Let $b \in \mathrm{End}^{\circ}(A_K^{G^{\mathrm{opp}}}) \simeq \mathrm{End}^{\circ}(A_K^n)$ correspond to $\iota_{\mathrm{M}}(B)$. By Proposition 17 and our notational conventions, the endomorphism associated to the matrix $L(e_i) = \iota_{\mathrm{M}} L_D(e_i)$ is $e_i \otimes_k \mathrm{id}_K$. By the above considerations, $b(e_i \otimes_k \mathrm{id}_K)b^{-1}$ is an endomorphism whose image is isomorphic to $A_K^{n_i}$. It follows that the image of $c_i\, e_i \otimes_k \mathrm{id}_K$ is also isomorphic to $A_K^{n_i}$. □

Remark 20 Let A_K be simple, $D = \mathrm{End}^{\circ}(A_K)$. Assume that all e_i in the above proposition are central. Then all Λ_i as above are rings and we have an isomorphism $\prod_{i=1}^{s} \Lambda_i \simeq D^t[G^{\mathrm{opp}}] \simeq \mathrm{End}^{\circ}(W)$ of rings. Furthermore, the $(c_i e_i)(W)$ are generated by isotypic components of W and $\Lambda_i \simeq \mathrm{End}^{\circ}((c_i e_i)(W))$. So in particular, the number n_i in the above proposition satisfies $n_i = \dim_D(\mathrm{End}^{\circ}(W_i))$.

3.5 The cyclic case

We now apply the above results to the case that G is cyclic of order n.

We identify G with G^{opp} and fix some generator $\sigma \in G$. Let $a = a_\sigma \in \mathrm{End}(W)$ be the automorphism corresponding to σ.

Denote the residue class of X in $\mathbb{Q}[X]/(X^n - 1)$ by x. Then we have an inclusion

$$\mathbb{Q}[X]/(X^n - 1) \longrightarrow \mathrm{End}^{\circ}(A_K)^t[G], \ x \mapsto \sigma.$$

The polynomial $X^n - 1 \in \mathbb{Z}[X]$ splits over $\mathbb{Z}$ as

$$X^n - 1 = \prod_{d|n} \Phi_d,$$

where Φ_d is the d-th cyclotomic polynomial.

Let $\Phi'_d := (X^n - 1)/\Phi_d$. By the Euclidian algorithm, there exist $\Psi_d \in \mathbb{Q}[X]$ with $\sum_{d|n} \Psi_d \Phi'_d = 1$. Let $E_d := \Psi_d \, \Phi'_d$. Then the $E_d(x) \in \mathbb{Q}[X]/(X^n - 1)$ are pair-wise orthogonal idempotents. The corresponding decomposition is

$$\mathbb{Q}[X]/(X^n - 1) \simeq \prod_{d|n} \mathbb{Q}[X]/\Phi_d = \prod_{d|n} \mathbb{Q}(\zeta_d).$$

(This is nothing but the Chinese Remainder Theorem in this particular case.)

Let $W_d := c_d \, E_d(a)(W)$ for suitable $c_d \in \mathbb{N}$. We then have an isogeny decomposition

$$W \sim \prod_{d|n} W_d,$$

and by Proposition 19, the W_d are abelian varieties with $W_{dK} \approx A_K^{\varphi(d)}$.

We also have $W_d = \Phi'_d(a)(W)$. – We only have to show that $c_d \Phi'_d(a)(W) \subseteq W_d$. This follows from $\Phi'_d(x) = (\sum_{f|n} \Psi_f(x) \Phi'_f(x))\Phi'_d(x) = \Psi_d(x){\Phi'_d}^2(x) = E_d(x)\Phi'_d(x)$.

It is clear that W_d is also the reduced identity component of the kernel of

$$\begin{aligned} &c_d(\mathrm{id} - E_d(a)) = c_d \textstyle\sum_{f|n, f\neq d} \Psi_f(a)\Phi'_f(a) = \\ &(c_d \textstyle\sum_{f|n,\, f\neq d} \Psi_f(a) \prod_{g|n,\, g\neq d,f} \Phi_g(a)) \, \Phi_d(a). \end{aligned}$$

It is also the reduced identity component of the kernel of $\Phi_d(a)$. – We only have to show that W_d is contained in this kernel. But since $W_d = \Phi'_d(a)(W)$ and $\Phi'_d(x)\Phi_d(x) = 0$, this is obvious.

We now want to study whether the W_d are simple or split further. We make the following assumptions.

A_K is a simple abelian K-variety whose endomorphisms can be defined over k and whose endomorphism ring is commutative.

Note that if k is finite, all endomorphisms of A_K can automatically be defined over k if we assume $\mathrm{End}(A_K)$ to be commutative.

Also if A is an ordinary elliptic curve over an arbitrary field k and n is odd, then all endomorphisms of A_K can be defined over k. This is because under this condition, $\mathrm{End}(A_K)$ is either $\mathbb{Z}$ or a quadratic order, thus the only possible non-trivial automorphism of $\mathrm{End}(A_K)$ has order 2, and consequently the image of the representation $\mathrm{Gal}(K|k) \longrightarrow \mathrm{Aut}(\mathrm{End}(A_K))$ is trivial.

Under the assumptions, we have the isomorphisms

$$\begin{array}{ccccc} \mathrm{End}^\circ(A)[X]/(X^n-1) & \simeq & \mathrm{End}^\circ(A_K)[G] & \simeq & \mathrm{End}^\circ(W) \\ x & \mapsto & \sigma & \mapsto & a \end{array} .$$

Let Φ_d split into the product of the non-trivial monic irreducible polynomials $\Phi_d^{(1)}, \Phi_d^{(2)}, \ldots, \Phi_d^{(r_d)}$ over $\mathrm{End}^\circ(A)$. Let ${\Phi'}_d^{(i)} := (X^n-1)/\Phi_d^{(i)}$. Since $X^n - 1$ is separable in characteristic zero, the $\Phi_d^{(i)}$ are pair-wise coprime for varying d and i, and there exist $\Psi_d^{(i)}$ with $\sum_{d|n}\sum_{1=i}^{r_d} \Psi_d^{(i)}{\Phi'}_d^{(i)} = 1$. Let $E_d^{(i)} := \Psi_d^{(i)}{\Phi'}_d^{(i)}$.

Let $W_d^{(i)} := c_d^{(i)}E_d^{(i)}(a)(W)$ for suitable $c_d^{(i)} \in \mathbb{N}$. Then again by Proposition 19, $W_d^{(i)}$ is an abelian k-variety with $(W_d^{(i)})_K \approx A_K^{\deg(\Phi_d^{(i)})}$. The abelian k-variety $W_d^{(i)}$ is simple and its endomorphism algebra is isomorphic to the field $\mathrm{End}^\circ(A)[X]/\Phi_d^{(i)}$. The $W_d^{(i)}$ are pair-wise non-isogenous (since $\mathrm{End}^\circ(W)$ is commutative), thus they are the isotypic components of W.

As above, one sees that $W_d^{(i)} = {\Phi'}_d^{(i)}(a)(W)$ and that $W_d^{(i)}$ is the reduced identity component of the kernel of $\Phi_d^{(i)}(a)$.

The component W_d is simple if and only if Φ_d is irreducible over $\mathrm{End}^\circ(A)$, i.e. if and only if $\mathrm{End}^\circ(A) \otimes_{\mathbb{Q}} \mathbb{Q}(\zeta_d)$ is a field. If we fix an inclusion of $\mathrm{End}^\circ(A)$ into $\overline{\mathbb{Q}}$, this is the case if and only if $\mathrm{End}^\circ(A) \cap \mathbb{Q}(\zeta_d) = \mathbb{Q}$.

In particular, none of the W_d splits further if $\mathrm{End}^\circ(A) = \mathbb{Q}$ as is the case if A is an elliptic curve without complex multiplication (over k).

We proved:

Theorem 4 *Let $K|k$ be a cyclic field extension of degree n. Let A be an abelian k-variety.*

Let W be the Weil restriction of A_K with respect to $K|k$. For all $d|n$, W contains canonically an abelian subvariety W_d with $W_{dK} \approx A_K^{\varphi(d)}$ (non-canonically), and W is isogenous to the product of the W_d. Here, $W_1 = A$ itself.

Assume in addition that A_K is simple, $\mathrm{End}^\circ(A_K)$ *is commutative and all endomorphisms of A_K can be defined over k. Then the isotypic components of W are all simple, and its endomorphism rings are all commutative. Fix an inclusion of* $\mathrm{End}^\circ(A_K)$ *into* $\overline{\mathbb{Q}}$*. Then for each d, W_d is simple if and only if* $\mathrm{End}^\circ(A) \cap \mathbb{Q}(\zeta_d) = \mathbb{Q}$.

Let E be an ordinary elliptic k-curve with complex multiplication (over k). Fix an inclusion of $\mathrm{End}^\circ(E)$ into $\overline{\mathbb{Q}}$. As $\mathrm{End}^\circ(E)$ is a quadratic extension of $\mathbb{Q}$, $\mathrm{End}^\circ(E) \cap \mathbb{Q}(\zeta_d) \supsetneq \mathbb{Q}$ if and only if $\mathrm{End}^\circ(E) \subseteq \mathbb{Q}(\zeta_d)$. If this is the case then Φ_d splits into two polynomials of degree $\frac{1}{2}\varphi(d)$ over $\mathrm{End}^\circ(E)$.

Corollary 21 *Under the assumptions of the theorem, let E be an ordinary elliptic k-curve with* $\mathrm{End}(E) = \mathrm{End}(E_K)$ *(this condition is automatically satisfied over finite fields or if n is odd).*

Then for each d, W_d is not simple if and only if E has complex multiplication over k and $\mathrm{End}^\circ(E) \subseteq \mathbb{Q}(\zeta_d)$*. If this is the case, W_d contains two simple non-isogenous abelian subvarieties of dimension $\frac{\varphi(d)}{2}$, and W_d is isogenous to the product of these abelian subvarieties.*

In partular, if n is prime and $n \equiv 1$ mod 4 or $n \equiv 3$ mod 4 and $\sqrt{-n} \notin$ $\mathrm{End}^\circ(E)$*, we have an isogeny decomposition $W \sim E \times N$ where N is simple.*

Acknowledgements

The results are part of the doctoral thesis of the first author. The thesis was supported by the Friedrich-Naumann-Stiftung, the Deutsche Forschungsgemeinschaft DFG and the Volkswagen Stiftung.

Special cases of some of the present results were obtained in the graduate thesis of the second author.

We would like to thank G. Frey for introducing us the the subject and for constant support during the preparation of our theses.

References

[1] S. Bosch, W. Lütkebohmert, and M. Raynaud. *Néron models.* Springer-Verlag, Berlin, 1990.

[2] C.W. Curtis and I. Reiner. *Methods of representation theory. Vol. I,II.* John Wiley & Sons., Ney York, 1981, 1987.

[3] T. Honda. Isogeny classes of abelian varieties over finite fields. *J. Math. Soc. Japan*, 20, 1968.

[4] S. Lang. *Algebra.* Springer-Verlag, New York, third edition, 2002.

[5] J.S. Milne. On the arithmetic of abelian varieties. *Invent. Math.*, 17:177–190, 1972.

[6] J.S. Milne. Abelian varieties. In *Arithmetic geometry*, pages 103–150. Springer-Verlag, New York, 1986.

[7] D. Mumford. *Abelian varieties.* Tata Institute of Fundamental Research, Bombay, 1970.

[8] J. Neukirch. *Algebraische Zahlentheorie.* Springer-Verlag, Berlin, 1991.

[9] D. Passman. *Infinite Crossed Products.* Academic Press, San Diego, 1989.

[10] J. Tate. Endomorphisms of abelian varieties over finite fields. *Invent. Math.*, 2, 1966.

[11] J. Tate. Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda). In *Seminaire Bourbaki 1968/69, No.352, 95-110.* 1971.

Claus Diem: Institut für Experimentelle Mathematik, Universität Duisburg-Essen, Essen, Germany. e-mail: diem@exp-math.uni-essen.de

Niko Naumann: Mathematisches Institut der Universität Münster, Münster, Germany. e-mail: naumannn@uni-muenster.de