A Study on
Theoretical and Practical Aspects of
Weil-Restrictions of Varieties

Claus Diem

Dissertation

A Study on Theoretical and Practical Aspects of Weil-Restrictions of Varieties

Dissertation zur Erlangung des Grades
eines Doktors der Naturwissenschaften

Dem Fachbereich 6
(Mathematik und Informatik) der
Universität-Gesamthochschule Essen
vorgelegt von

Claus Diem
aus Frankfurt am Main

Februar 2001

Die Disputation fand am 31.5.2001 statt.

Die Gutachter waren:
Prof. Dr. Dr. hc Gerhard Frey, Universität-Gesamthochschule Essen
Prof. Dr. Barry Green, Universiteit Stellenbosch, Süd-Afrika
Prof. Dr. Eckart Viehweg, Universität-Gesamthochschule Essen

Zusammenfassung

Für eine feste endliche, separable Körpererweiterung $K|k$ kann man jeder quasi-projektiven K-Varietät auf funktorielle Weise eine quasi-projektive k-Varietät höherer Dimension, die sogenannte Weil-Restriktion, zuordnen.

Diese Arbeit ist dem Studium verschiedener Aspekte dieser Varietäten gewidmet. Der Schwerpunkt liegt zuerst auf Resultaten rein theoretischer Natur. Später werden diese Resultate angewandt, um potentielle Angriffe auf das diskrete Logarithmus-Problem in Klassengruppen von Kurven über endlichen Nicht-Primkörpern darzulegen.

Ich habe diese Arbeit selbstständig verfasst und dabei keine anderen als die in der Literaturliste aufgeführten Hilfsmittel benutzt.

Claus Diem
Essen, Februar 2001

Contents

Foreword

For a fixed finite, separable extension of fields $K|k$, one can attach in a functorial way to every quasi-projective K-variety a higher-dimensional quasi-projective k-variety, the so-called Weil-restriction.

This work is devoted to the study of various aspects of these varieties. At first, the emphasis is on purely theoretical results. Later these results are applied to outline potential attacks on the discrete-logarithm problem in class groups of curves over finite non-prime fields.

Historical background and motivation

Let $K|k$ be a finite Galois extension of fields, X' a quasi-projective K-variety. [1] Then there exists a quasi-projective k-variety W which has in particular the properties that $X'(K) \simeq W(k)$ and $W_K = W \otimes_k K$ is a product of Galois-conjugates of X'. Within the framework of arithmetic algebraic geometry, W is defined by the property that for all k-schemes Z, there exists a functorial bijection $W(Z) \cong X'(Z \otimes_k K)$.

To prove the existence of W one can for example define a certain 1-cocycle datum for a product of Galois-conjugates of X' and then apply "descent" as in A.Weil's paper "The field of definition of a variety"; see [We-F]. Although Weil does not state it explicitly, his paper even contains a construction of W as a subvariety of some concrete projective space; see proof of [We-F, Proposition 1]. In honor of him, W is often called the *Weil-restriction* of X' (with respect to $K|k$). (Here, the word "restriction" refers to the fact that the base-field is "restricted" from K to k.) We follow this terminology.

Weil-restrictions of abelian varieties were studied to solve various problems of arithmetic algebraic geometry and thus also number theory. Prominent examples

[1] Throughout this work, if we are given an extension of fields $K|k$, we will denote varieties over k by X, Y, etc., and varieties over K by X', Y', etc.

are Milne's proof that the conjectures of Birch and Swinnerton-Dyer for abelian varieties over the rationals imply the conjectures for abelian varieties over all number fields and Honda's theorem about the classification of isogeny classes of abelian varieties over finite fields; see [Mi-AA] and [Ho] respectively.

With the rise of arithmetic algebraic geometry, Weil-restrictions were shown to exist in a much a more general context. A construction of the Weil-restriction in a very general setting can be found in the book "Néron Models" by Bosch, Lütkebohmert and Raynaud; see [BLR, 7.6].

After Weil-restrictions where successfully studied to solve problems of "pure mathematics" for decades, a new direction of research was shown by Frey in a talk in 1998; see [Fr]. He suggested to use Weil-restrictions of elliptic curves both as a tool to construct as well as to break discrete-logarithm problems.

The general idea for the use of Weil-restrictions as a means to construct attacks on the discrete-logarithm problem in the group of rational points of an elliptic curve over a finite non-prime field is that as an abelian variety of dimension greater than 1, a Weil-restriction has "more structure" than the original elliptic curve.

In particular, Frey noted that for a fixed elliptic curve and a fixed constant field extension, it should be possible to transform the DL-problem in the group of rational points into DL-problems in class groups of curves on the Weil-restriction. Thus it should in principle be possible to transform the original DL-problem into DL-problems in class-groups of curves of higher genera over a smaller field. If one finds a suitable curve on the Weil-restriction whose genus is not too high, it should be more efficient to solve the DL-problem in this curve than in the original elliptic curve. This is suggested by the results of Gaudry and Enge; see [En], [EG], [Gau].

As discrete-logarithm problems are one of the bases of public-key cryptography (another one being the factorization problem), this shows that Weil-restriction may be relevant from an applied point of view as well.

The first results in this direction were obtained by Galbraith and Smart, and the first major paper in this new direction was written by Gaudry, Hess and Smart; see [GHS].

Introduction

In this work we study Weil-restrictions of varieties both from a pure as well as from an applied point of view. In particular, we show how questions on Weil-restrictions of abelian varieties motivated by the cryptoanalytical applications outlined above can often be proven directly from the defining functorial properties.

Conversely, the problem of finding curves of low genus on Weil-restrictions of a (non-singular, projective, geometrically integral) curve X' is by the defining functorial property equivalent to finding certain coverings of X'. Most of the time it is probably easier to find these coverings of X' (where one can use Galois theory) than to find curves on the Weil-restriction using hyperplane-sections.

Thus when trying to transform the DL-problem in the class group of curve X' over a non-prime finite field into a potentially easier DL-problem in a class group of a curve defined over a smaller field, we emphasis on a Galois-theoretic approach. We would like to regard the Weil-restriction as being only a tool providing the necessary background to motivate that we indeed transform the original DL-problem into an equivalent problem.

The work consists of three chapters and an appendix. Each chapter has its own introduction. The main results are mostly stated in or around a “theorem”. [2] Whenever stating a theorem, we have tried to include all necessary conditions to understand the context properly.

In the chapter one, we first give basic definitions related to Weil-restrictions of varieties and schemes. After having given two constructions of the Weil-restriction in rather abstract settings, we study its first properties. Then we restrict ourselves to a projective variety X'/K with a rational point and study the Weil-restriction of X' with respect to a Galois field extension $K|k$. We analyze the Picard functor of the Weil-restriction W and relate it to the restriction of the Picard functor of X'. In the third section we first give an introduction to Weil-restrictions of abelian varieties. Then we derive the structure of the endomorphism ring of Weil-restrictions of an abelian variety over finite fields.

For the second chapter, let $K|k$ be a Galois field extension of perfect fields and let A be an abelian k-variety, [3] W the Weil-restriction of A_K with respect to $K|k$. In the first section, we give a description of $\mathrm{End}_k(W)$ as a skew-group-ring over $\mathrm{End}_K(A_K)$. We then restrict ourselves to the case that A is an elliptic curve E. Then W is isogenous to the product of E and an abelian variety N called its *trace-zero-hypersurface*. We study the Néron-Severi group of N and in particular the polarizations of N. As a first step towards the determination of the Néron-Severi group of N we include a study of the Néron-Severi group of a product of elliptic curves. In the last section of this chapter, we study an affine open part of N with explicit equations for the particular case that the extension degree $[K:k]$ equals 3.

The third chapter is entirely devoted to cryptoanalytical applications. Let k be a finite field, $K|k$ a field extension of prime degree n. Let X' be a non-singular, geometrically irreducible curve over K. Assume that X' has “cryptographically good” properties. In particular, the group $\mathrm{Cl}^0(X')$ of classes of divisors of degree 0 should have a large prime factor. Let C be a non-singular, geometrically irreducible curve over k with a covering $C \otimes_k K \longrightarrow X'$. Using this covering, we have

[2] A Less important result is called “proposition”, a smaller or more technical result is called “lemma”. The reader should keep in mind however that when we cite a result and call it “proposition” or “lemma” it may in fact be a theorem deeper and more important than the “theorems” in this work.

[3] In our terminology, A_K is an *old* abelian variety. Thus the title of the chapter.

an explicit morphism from $\mathrm{Cl}^0(X')$ to $\mathrm{Cl}^0(C)$. The hope is that if the genus of C is not "too large", perhaps the discrete-logarithm problem in the group $\mathrm{Cl}^0(C)$ is "easier" than the discrete-logarithm problem in the original group $\mathrm{Cl}^0(X')$. Applying results of the previous two chapters, we will give theoretical results predicting when the large prime factor to be preserved under the morphism to $\mathrm{Cl}^0(C)$. Then we use Galois theory to construct rather explicitly some examples.

Acknowledgments

First and foremost, I thank my supervisor, Prof. Dr. Dr. h.c. G. Frey, for suggesting the initial direction for this work, his enthusiasm and the ideas he gave me in numerous discussions.

With great pleasure, I thank my wife, Marianne, for her understanding and support.

I thank Prof. Dr. B. Green for his great hospitality during my stay at the Universiteit van Stellenbosch in South Africa and N. Naumann for the fruitful cooperation.

Additionally, I thank (in alphabetical order): Dr. S. Galbraith, Prof. Dr. R. Göbel, Dr. F. Hess, Prof. Dr. U. Jansen, Prof. Dr. E. Kani, Prof. Dr. K. Künnemann, Prof. Dr. W. Lütkebohmert, Prof. Dr. G. Michler, Dr. S. Müller-Stach, Prof. Dr. F. Pop, Prof. Dr. H. Stichtenoth, Prof. Dr. E. Viehweg.

I would like to express my gratitude for financial support by the Friedrich-Naumann-Stiftung, the Deutsche Forschungsgemeinschaft DFG and the Volkswagen Stiftung. The funds of the first two bodies were made available by the Bundesrepublik Deutschland and the Land Nordrhein-Westfalen.

The Institut für Experimentelle Mathematik in Essen provided excellent working conditions.

Needless to say, it is often impossible to try to give credit to specific persons if an idea or a method has been "in the public domain" for a certain time. However, we try to state to whom rather concrete and recent results which we have included in our work or on which our results are built are due.

- The content of Section 1.1 is mostly standard and well-known.
- Subsection 1.3.5 is joint work with N. Naumann.
- Over finite fields, the dimensions of the simple isogeny-factors of W in Corollary 2.8 were first established by N. Naumann.
- Equations (2.20) in Section 2.4 are due to a variety of people, including G. Frey, N. Naumann and the author.

- Morphism (3.1) is due to F. Hess; see [GHS].
- The example in Subsection 3.2.2 is due to S. Galbraith, F. Hess and N. Smart for characteristic 2; see [GHS].
- The idea to use Lemma 3.11 in the proof of Proposition 3.12 was pointed out to the author by H. Stichtenoth.

Notations

Isomorphisms

We use three different signs to denote isomorphisms: If we merely want to indicate that two objects X and Y are isomorphic with some isomorphism we write $X \approx Y$. Most of the time, the isomorphism will be in a certain (obvious) sense "canonical". If this is the case, we write $X \simeq Y$. If we want to stress that an isomorphism is in a certain sense functorial, we write "$\cong$". – Thus if we are given two categories $\mathcal{C}, \mathcal{D}$, two functors $\mathcal{F}, \mathcal{G} : \mathcal{C} \longrightarrow \mathcal{D}$, an isomorphism of functors $\mathcal{F} \approx \mathcal{G}$ and X a $\mathcal{C}$-object, we write $\mathcal{F}(X) \cong \mathcal{G}(X)$.

Let $\mathcal{C}$ be a category, $\mathcal{E}ns$ the category of sets, $\mathcal{F} : \mathcal{C} \longrightarrow \mathcal{E}ns$ a contravariant functor. Let $\mathbf{F}$ be a $\mathcal{C}$-object, $u \in \mathcal{F}(\mathbf{F})$. Then by

$$\varphi : \mathrm{Hom}(-, \mathbf{F}) \longrightarrow \mathcal{F},\ \varphi(\alpha) := \mathcal{F}(\alpha)(u)$$

a natural transformation is defined. Recall that if φ is an isomorphism, one says that $\mathbf{F}$ with the universal element u *represents* $\mathcal{F}$.

Now assume that we know that $\mathcal{F}$ is representable. Then the representing object $\mathbf{F}$ with u is unique up to a unique isomorphism. [4] We think of $\mathbf{F}$ and u as being *fixed*. Thus, if $\mathbf{F}'$ with u' is some object representing $\mathcal{F}$, we write $\mathbf{F} \simeq \mathbf{F}'$.

Rings and Schemes

All rings and schemes considered in this work are assumed to be contained in some fixed universe.

If k is a field, we fix an algebraic closure and denote it by $\overline{k}$. The separable closure of k inside $\overline{k}$ will be denoted by k^{sep}.

All schemes will assumed to be locally Noetherian, i.e. we will work entirely in the category of locally Noetherian schemes which are contained in some fixed universe.

Fix some scheme S and let X be an S-scheme. Then for any S-scheme T, we call the S-morphisms from T to X *T-valued points* of X. Let Y be another

[4] One speaks of "the" representing object. Note however that if one speaks of "the" or "a" representing object one always means an object with a fixed universal element.

S-scheme. Any S-morphism $X \longrightarrow Y$ induces by "push-forward" a functorial morphism (in T) from the T-valued points of X to the T-valued points of Y. Conversely, any such functorial morphism determines an S-morphism from X to Y. [5] We will often use this fact to construct morphisms from X to Y. When we do so we speak of *.-valued points* for T-valued points for some T.

If X and Y are S-schemes, then the T-valued points of product $X \times_S Y$ will be be denoted by (P, Q), where $P \in X(T)$, $Q \in Y(Q)$ (analogous notation for products consisting of more factors).

If X and Z are S-schemes, we denote the product $X \times_S Z$ also by X_Z. If we use this notation, we think of X as being fixed and Z as being variable.

In the context of schemes, all rings will automatically assumed to be commutative. Let A be a (commutative) ring. Let X be an A-scheme, by which we mean a scheme over $\mathrm{Spec}(A)$. Let B be an A-algebra. Then we denote $\mathrm{Spec}(X) \times_{\mathrm{Spec}(A)} \mathrm{Spec}(B)$ by $X \otimes_A B$ or simply by X_B.

Let $\iota : X \hookrightarrow Y$ be a closed immersion, $\alpha : Z \longrightarrow Y$ some morphism. Then by $\alpha^{-1}(X)$ we always mean the *scheme-theoretic* preimage, i.e. $\alpha^{-1}(X) := X \times_Y Z$ where the product is taken relative to ι and α. If α is also a closed immersion, we denote $X \times_Y Z$ also by $X \cap Z$.

Following [Ha, II,4,p.103], a *quasi-projective* morphism $X \longrightarrow Y$ is a morphism which factors into an open immersion followed by a projective morphism. Likewise, an *immersion* is a morphism which factors into an open immersion followed by a closed immersion.

Let k be a field. A *k-variety* X is a separated and reduced scheme of finite type over k. Note that we do not assume X to be irreducible or geometrically reduced. Similarly, a *k-curve* is a separated and reduced scheme of finite type over k which is equidimensional and of dimension 1.

If X is an irreducible K-variety, we denote its function field by $k(X)$. Note that X is geometrically integral (i.e. geometrically reduced, geometrically irreducible) iff $k(X)|k$ is regular.

Galois coverings

Let $h : S' \longrightarrow S$ be a Galois covering of schemes with Galois group G (in the sense of [SGA I, V]). This means by definition (in particular) that there is a fixed injective *anti-homomorphism* $G \hookrightarrow \mathrm{Aut}_S(S')$.

This anti-homomorphism induces a homomorphism $G^{\mathrm{opp}} \hookrightarrow \mathrm{Aut}_S(S')$. We identify G^{opp} with its image.

We denote the elements of G by bold letters. The corresponding operators of h are usually denoted by the same symbol in "usual" letters, i.e. we have an injective *anti-homomorphism* $\boldsymbol{\sigma} \mapsto \sigma$.

[5] This is a trivial fact from category theory: For any category $\mathcal{C}$, the functor $X \mapsto \mathrm{Hom}(-, X)$ is a full and faithful. A less trivial fact is that it suffices to define a morphism of schemes on ring-valued points.

If G is commutative, we identify G with G^{opp} and denote the elements of G also by "usual" letters.

Now let $S' = \mathrm{Spec}(K)$ and $S = \mathrm{Spec}(k)$ be spectra of fields. Then h is determined by the field homomorphism $h^{\#} : k \hookrightarrow K$.

The extension $K|k$ given by $h^{\#}$ is finite and Galois with Galois group G, the galois group of h. (In particular, we denote the automorphisms of the extension $K|k$ also by bold letters.) The anti-homomorphism $G \longrightarrow \mathrm{Aut}_S(S')$ is given by $\boldsymbol{\sigma} \mapsto \sigma$ where σ is given by $\boldsymbol{\sigma} = \sigma^{\#} \in G = \mathrm{Aut}(K|k)$.

The Picard group

Let X be a scheme. Sheaves on X are denoted by $\mathcal{L}, \mathcal{M}$, etc.

The Picard group is the group of isomorphism classes of invertible sheaves on X, denoted $\mathrm{Pic}(X)$. Its elements are denoted by $\overline{\mathcal{L}}, \overline{\mathcal{M}}$, etc.

A morphism $\psi : X \longrightarrow Y$ induces a group-homomorphism $\psi^* : \mathrm{Pic}(Y) \longrightarrow \mathrm{Pic}(X)$.

Let k be a field and let X be a non-singular, geometrically reduced, geometrically irreducible, projective k-variety with a k-rational point. Let $\mathcal{P}\mathrm{ic}(X)$ be the Picard functor $Z \mapsto \mathrm{Pic}(X \times_k Z)/p_Z^* \mathrm{Pic}(Z)$, where $p_Z : X \times_k Z \longrightarrow Z$ is the projection. We denote the elements of $\mathcal{P}\mathrm{ic}(X)(Z)$ by $\overline{\overline{\mathcal{L}}}, \overline{\overline{\mathcal{M}}}$, etc. Under our assumptions on X, the Picard-functor is representable, and we denote a representing object of $\mathcal{P}\mathrm{ic}(X)$ by $\mathbf{Pic}(X)$ and the universal element by $\overline{\overline{\mathcal{P}}}$. The *Picard-scheme*, $\mathbf{Pic}^0(X)$, is the connected component of the zero of $\mathbf{Pic}(X)$. We still denote the universal element by $\overline{\overline{\mathcal{P}}}$. Under the isomorphism $\mathrm{Hom}(-, \mathbf{Pic}(X)) \simeq \mathcal{P}\mathrm{ic}(X)$, $\mathrm{Hom}(-, \mathbf{Pic}^0(X))$ corresponds to a functor which we denote by $\mathcal{P}\mathrm{ic}^0(X)$.

Let X, Y be k-varieties as above, $\psi : X \longrightarrow Y$ a morphism. Then the "pull-back" $\mathcal{P}\mathrm{ic}(Y) \longrightarrow \mathcal{P}\mathrm{ic}(X)$ induced by ψ is denoted by ψ^* and so is the corresponding morphism between the Picard schemes. [6]

Abelian varieties

Let k be a field. An *abelian k-variety* is a geometrically integral, projective k-group-variety. The addition on A is denoted by "+".

Let A be an abelian k-variety.

If we speak of the *endomorphism ring* of A we mean the ring of endomorphisms of A over k, i.e. the endomorphisms of $A_{\overline{k}}$ defined over k. It is denoted by $\mathrm{End}_k(A)$. Likewise, the *endomorphism algebra* of A is the ring $\mathrm{End}_k^0(A) := \mathrm{End}_k^0(A) \otimes_{\mathbb{Z}} \mathbb{Q}$.

If we say that two abelian k-varieties are isogenous or isomorphic, we mean isogenous or isomorphic as abelian k-varieties. We denote isogeny by $\sim$.

The same applies also to complex multiplication: By saying that an elliptic k-curve has *complex multiplication*, we mean that $E_{\overline{k}}$ has complex multiplication

[6] A brief exposé of the Picard functor and the Picard scheme can be found in subsection 1.2.2.

and the complex multiplication is defined over k.

Let Z be some k-scheme, P a Z-valued point of A. Then the *translation* by P is the morphism $T_P = \mathrm{id}_{A_Z} + P \circ p_Z : A_Z \longrightarrow A_Z$, where $p_Z : A_Z \longrightarrow Z$ is the projection.

A dual abelian variety is denoted by $\widehat{A}$, the universal divisional correspondence by $\mathcal{P}$. By definition, $\mathcal{P}\mathrm{ic}^0(A)(Z) \cong \widehat{A}(Z)$ where Z is a k-scheme.

If $\alpha : A \longrightarrow B$ is a morphism, the dual morphism is denoted by $\widehat{\alpha}$. With other words, $\widehat{\alpha} : \widehat{B} \longrightarrow \widehat{A}$ is just another notation for $\alpha^* : \mathbf{Pic}^0(B) \longrightarrow \mathbf{Pic}^0(A)$.

Let $\mathcal{M}$ be an invertible sheaf on A. Then $\phi_{\mathcal{M}} : A \longrightarrow \widehat{A}$ is the morphism associated to the natural transformation $\mathrm{Hom}_k(-, A) \longrightarrow \mathcal{P}\mathrm{ic}^0(A)$ with is given on Z-valued points by $P \mapsto T_P^* p_Z^*(\overline{\mathcal{M}}) \otimes q_Z^*(\overline{\mathcal{M}})^{-1}$, where $q_Z : A_Z \longrightarrow A$ is the projection.

Following [Mi-A], a *polarization* of A is a morphism φ from A to its dual $\widehat{A}$ such that $\varphi \otimes_k \mathrm{id}_{\overline{k}} = \phi_{\mathcal{M}} : A_{\overline{k}} \longrightarrow \widehat{A}_{\overline{k}}$ for some ample sheaf $\mathcal{M}$ on $A_{\overline{k}}$.

The group $\mathrm{NS}(A) := \mathrm{Pic}(A)/\mathrm{Pic}^0(A)$ is called *Néron-Severi group.*

For any natural number n, we denote the (scheme-theoretic) kernel of $\cdot n : A \longrightarrow A$ by $A[n]$.

Let $K|k$ be a finite field extension, A' an abelian K-variety. Then, if A' is defined over k, i.e. if there exists an abelian k-variety A such that $A' \approx A \otimes_k K$, we say that A is an *old* abelian variety (relative to $K|k$). If A' is not isogenous to an abelian variety defined over k or some proper intermediate field λ of $K|k$, then we call A' a *new* abelian variety (relative to $K|k$).

Note that if the extension degree $[K : k]$ is prime, every abelian K-variety is either a new abelian variety or it is isogenous (not necessarily isomorphic) to an old abelian variety.

Chapter 1

Basic properties of Weil-restrictions

Introduction and results

Let k be a field, $K|k$ a finite separable field extension and X'/K a quasi-projective variety. The *base-restriction* of X' with respect to $K|k$ is the functor $\mathcal{R}\mathrm{es}_k^K(X')$ defined by $\mathcal{R}\mathrm{es}_k^K(X')(Z) := X'(Z \otimes_k K)$ for any k-scheme Z. It can be shown that the functor $\mathcal{R}\mathrm{es}_k^K(X')$ is represented by a k-variety $\mathbf{Res}_k^K(X')$, the so-called *Weil-restriction* of X'; see Proposition 1.4.

In the first section of this chapter we give two constructions of the Weil-restriction in a more general situation and show basic properties of it.

In the second section we "pull-back" the invertible sheaves on X' to invertible sheaves on the Weil-restriction. It follows in particular that the Weil-restriction of a quasi-projective variety with a fixed immersion into some projective space is in a canonical way immersed in some higher dimensional projective space; see Proposition 1.13.

Let $K|k$ be a finite Galois extension, let X' be a non-singular, projective K-variety with a K-rational point. We show that under certain conditions on X', the Weil-restriction of the Picard scheme of X' is an abelian variety which is canonically isomorphic to the Picard scheme of the Weil-restriction of X'. This is rather obvious for abelian varieties where the Picard scheme is nothing but the dual abelian variety; see Proposition 1.20. It is also true if $\mathrm{char}(k) = 0$ or $X'_{\overline{K}}$ has a "smooth, proper global lifting"; see Theorem 1, p. 25. (This assumption is always fulfilled if X' is a curve.) The proof relies on the fact that the Picard scheme of a product of varieties over an algebraically closed field is – under our assumptions – reduced and isomorphic to the product of the Picard schemes of the factors.

In the third section, we begin with the study of the Weil-restriction of abelian varieties. Using the results of the previous section, we show how the Weil-restriction of X' inherits the polarizations of X'. In particular, if X' is principally polarized, so is the Weil-restriction.

We then derive the structure of the endomorphism algebra of the Weil-restriction of an abelian variety with respect to an extension of finite fields (see Theorem 2, p. 29) and show that for prime extension degree $[K : k]$, the Weil-restriction of an abelian K-variety which is not isogenous to an abelian variety defined over k is simple (see Theorem 3, p. 31).

The study of the Weil-restriction of abelian varieties will be continued in the next chapter where we consider the Weil-restriction of an abelian variety which is defined over k. (Such abelian varieties will be called *old abelian varieties.*)

1.1 Definition and construction of Weil-restrictions

In this section, we give the definition of "base-restriction" of a functor. Then we show how to construct the Weil-restriction of a quasi-projective scheme with respect to a finite and locally free morphism via "restriction of scalars". Here, we follow [BLR, 7.6]. In the case that the base-morphism is étale, we show how to construct the Weil-restriction via a "geometrical approach". We then restrict ourselves to the case that the base-morphism is Galois and show how the "geometric construction" is related to the construction via "restriction of scalars". Finally we show how the arithmetic operation of the Galois group induces a geometric operation on the Weil-restriction.

We start more abstractly with an abstract category instead of a subcategory of the category of locally Noetherian schemes. This abstract setting is in no way more difficult.

In order to define base-restriction properly, we first define the functor "base-change". This is done in the first subsection.

1.1.1 Base-extension and base-change

We fix some universe $\mathcal{U}$ and denote the category of sets which are contained in this universe by $\mathcal{E}ns$.

Let $\mathcal{C}$ be a category whose objects are contained in $\mathcal{U}$.

Let $\mathcal{D}$ be another category whose objects are contained in $\mathcal{U}$. Then for some functors $\mathcal{F}, \mathcal{G} : \mathcal{C} \longrightarrow \mathcal{E}ns$, the natural transformations between $\mathcal{F}$ and $\mathcal{G}$ form a set. Thus the covariant functors from $\mathcal{C}$ to $\mathcal{D}$ form a category, denoted $\mathrm{Hom}(\mathcal{C}, \mathcal{D})$. Analogously, the contravariant functors form a category, denoted $\mathrm{Hom}^{\mathrm{opp}}(\mathcal{C}, \mathcal{D})$.

If X and Y are two objects of $\mathcal{C}$, we denote the set of morphisms between X and Y by $\mathrm{Hom}(X, Y)$. An *S-object* is a morphism $\alpha : X \longrightarrow S$, and a morphism between S-objects $\alpha : X \longrightarrow S$ and $\beta : Y \longrightarrow S$ is a morphism $\varphi : X \longrightarrow Y$ such that $\beta \circ \varphi = \alpha$.

As usual, we write X for $X \longrightarrow S$ and $\mathrm{Hom}_S(X,Y)$ for the set of morphisms of S-objects X and Y. For any $S \in \mathcal{C}$ let $\mathcal{C}/S$ be the category of S-objects.

Definition Let $\mathcal{F}, \mathcal{G} : \mathcal{C} \longrightarrow \mathcal{E}ns$ be contravariant functors, $\alpha : \mathcal{F} \longrightarrow \mathcal{G}$ a natural transformation, T some object of $\mathcal{C}$ and $t \in \mathcal{G}(T)$. Then $\mathrm{id}_T \mapsto t$ defines a natural transformation $\beta : \mathrm{Hom}(-,T) \longrightarrow \mathcal{G}$, $\gamma \in \mathrm{Hom}(Z,T) \mapsto \mathcal{G}(\gamma)(t) \in \mathcal{G}(Z)$.

$$\begin{tikzcd} & \mathcal{F} \arrow[d, "\alpha"'] \\ \mathrm{Hom}(-,T) \arrow[r, "\beta", "\mathrm{id} \mapsto t"'] & \mathcal{G} \end{tikzcd}$$

Now let $\mathcal{F} \times_{\mathcal{G}} T : \mathcal{C}/T \longrightarrow \mathcal{E}ns$ be defined as follows:

$$\mathcal{F} \times_{\mathcal{G}} T(Z) = \mathcal{F} \times_{\mathcal{G}} T(\gamma) := \{f \in \mathcal{F}(Z) | \alpha_Z(f) = \beta_Z(\gamma)\}, \ \gamma : Z \longrightarrow T \text{ a } T\text{-object}$$

and for a morphism $f : Y \longrightarrow Z$ of T-objects by

$$\mathcal{F} \times_{\mathcal{G}} T(f) := \mathcal{F}(f)|_{\mathcal{F} \times_{\mathcal{G}} T(Y)}$$

Assume that in $\mathcal{C}$ fiber products exist, i.e. for all $S \in \mathcal{C}$, products exist in the category $\mathcal{C}/S$. Let $\mathcal{F}$ be represented by $(\mathbf{F}, u)$ with $u \in \mathcal{F}(\mathbf{F})$, $\mathcal{G}$ by $(\mathbf{G}, v)$ with $v \in \mathcal{G}(\mathbf{G})$. Let $\mathbf{F} \times_{\mathbf{G}} T$ be the fiber product of the morphism $\mathbf{F} \longrightarrow \mathbf{G}$ which is associated to $\alpha : \mathcal{F} \longrightarrow \mathcal{G}$ and the morphism $T \longrightarrow \mathbf{G}$ which is associated to $\beta : \mathrm{Hom}(-,T) \longrightarrow \mathbf{G}$, let $x : \mathbf{F} \times_{\mathbf{G}} T \longrightarrow \mathbf{F}$, $y : \mathbf{F} \times_{\mathbf{G}} T \longrightarrow T$ be the structural morphisms. Then $\mathcal{F} \times_{\mathcal{G}} T$ is represented by $(\mathbf{F} \times_{\mathbf{G}} T, \mathcal{F}(x)(u))$, where we regard $\mathbf{F} \times_{\mathbf{G}} T$ as a T-scheme via y.

Definition Let $\mathcal{F} : \mathcal{C}/S \longrightarrow \mathcal{E}ns$ be a contravariant functor. The *base-extension* of $\mathcal{F}$ with respect to a morphism $T \longrightarrow S$ is the functor $\mathcal{F} \times_S T = \mathcal{F}_T : \mathcal{C}/T \longrightarrow \mathcal{E}ns$ defined by

$$\mathcal{F}_T(Z) := \mathcal{F}(Z), \ Z \text{ a } T\text{-object}$$

and for a morphism $f : Y \longrightarrow Z$ of T-objects by

$$\mathcal{F}_T(f) := \mathcal{F}(f) : \mathcal{F}(Y) \longrightarrow \mathcal{F}(Z)$$

Note that this definition can be regarded as a special case of the preceding definition with $\mathcal{C}/S$ instead of $\mathcal{C}$ and with $\mathcal{G}$ the trivial functor which assigns to every object the set of one element.

$(-)_T$ is a covariant functor from the category $\mathrm{Hom}^{\mathrm{opp}}(\mathcal{C}/S, \mathcal{E}ns)$ to the category $\mathrm{Hom}^{\mathrm{opp}}(\mathcal{C}/T, \mathcal{E}ns)$. The images of group-objects are group-objects.

Again assume that in $\mathcal{C}$ fiber products exist. Let $T \longrightarrow S$ be a morphism and let X be an S-object. If Z is a T object, then $\mathrm{Hom}_S(Z,X)_T = \mathrm{Hom}_S(Z,X) \simeq \mathrm{Hom}_T(Z, X \times_S T)$, i.e. $\mathrm{Hom}_S(-,X)_T$ is represented by some product $X \times_S T$ (regarded as T-object) with the structural morphism $X \times_S T \longrightarrow X$.

Since by assumption the objects of $\mathcal{C}$ form a set, we can apply the axiom of choice. For every X, we choice products $X \times_S T$ (together with the structural morphisms).

Now let $f : X \longrightarrow Y$ be an S-morphism. Then we define $f \times_S T$ to be the unique morphism such that the diagram

$$\begin{tikzcd}
\mathrm{Hom}(-, X \times_S T) \arrow[r, "\sim"] \arrow[d, "\mathrm{Hom}_T(-, f \times_S T)"] & \mathrm{Hom}(-, X)_T \arrow[d, "\mathrm{Hom}_S(-, f)_T"] \\
\mathrm{Hom}(-, Y \times_S T) \arrow[r, "\sim"] & \mathrm{Hom}(-, Y)_T
\end{tikzcd}$$

is commutative.

We obtain the functor *base-change* $- \times_S T : \mathcal{C}/S \longrightarrow \mathcal{C}/T$, and by construction, we have a natural isomorphism

$$\mathrm{Hom}_T(-, X \times_S T) \cong \mathrm{Hom}_S(-, X)_T.$$

By considering the image of $\mathrm{id}_{X \times_S T}$, we see that the diagram

$$\begin{tikzcd}
X \times_S T \arrow[r] \arrow[d, "f \times_S T"] & X \arrow[d, "f"] \\
Y \times_S T \arrow[r] & Y
\end{tikzcd}$$

is commutative. Since by definition $f \times_S T$ is also a T-morphism,

$$f \times_S T = f \times_S \mathrm{id}_T.$$

1.1.2 Base-restriction

Let $\mathcal{C}$ be again a category whose objects are contained in the universe $\mathcal{U}$ and in which fiber products exist. Let $h : S' \longrightarrow S$ be a morphism in $\mathcal{C}$. Let $\mathcal{F}' : \mathcal{C}/S' \longrightarrow \mathcal{E}ns$ be a contravariant functor.

Definition The *base-restriction* of $\mathcal{F}'$ with respect to h is the following contravariant functor $\mathcal{R}\mathrm{es}_S^{S'}(\mathcal{F}') = \mathcal{R}\mathrm{es}^h(\mathcal{F}') : \mathcal{C}/S \longrightarrow \mathcal{E}ns$:

$$\mathcal{R}\mathrm{es}^h(\mathcal{F}')(Z) := \mathcal{F}'(Z \times_S S'),\ Z \text{ an } S\text{-object}$$
and for a morphism $f : Y \longrightarrow Z$ of S-objects by
$$\mathcal{R}\mathrm{es}^h(X')(f) := \mathcal{F}'(f \times_S \mathrm{id}_{S'}) : \mathcal{F}'(Z \times_S S') \longrightarrow \mathcal{F}'(Y \times_S S').$$

In particular $\mathcal{R}\mathrm{es}^h(\mathcal{F}')(S) = \mathcal{F}'(S')$. $\mathcal{R}\mathrm{es}^h$ is a covariant functor from the category $\mathrm{Hom}^{\mathrm{opp}}(\mathcal{C}/S', \mathcal{E}ns)$ to the category $\mathrm{Hom}^{\mathrm{opp}}(\mathcal{C}/S, \mathcal{E}ns)$.

The images of group-objects are group-objects and $\mathcal{R}\mathrm{es}^h$ restricts to a covariant functor from the category $\mathrm{Hom}^{\mathrm{opp}}(\mathcal{C}/S', \mathcal{E}ns)$ to the category $\mathrm{Hom}^{\mathrm{opp}}(\mathcal{C}/S, \mathcal{E}ns)$.

Note In [BLR] base-restriction is called "direct image" and is denoted by $h_*\mathcal{F}$.

Let $X' \in \mathcal{C}/S'$. Then X' induces the functor $\mathrm{Hom}_{S'}(-, X') : \mathcal{C}/S' \longrightarrow \mathcal{E}ns$. We denote $\mathcal{R}\mathrm{es}^h(\mathrm{Hom}_{S'}(-, X'))$ by $\mathcal{R}\mathrm{es}^h(X') = \mathcal{R}\mathrm{es}_S^{S'}(X')$. So $\mathcal{R}\mathrm{es}^h(X')(Z) = \mathrm{Hom}_{S'}(Z \times_S S', X') = X'(Z \times_S S')$

With this definition, $\mathcal{R}\mathrm{es}^h$ is a covariant functor form the category $\mathcal{C}/S'$ to the category $\mathrm{Hom}^{\mathrm{opp}}(\mathcal{C}/S, \mathcal{E}ns)$.

"Base-extension" commutes with "base-restriction":

Lemma 1.1 *Let $T \longrightarrow S$ be a morphism, $T' := T \times_S S'$. Then*

$$(\mathcal{R}\mathrm{es}_S^{S'}(\mathcal{F}'))_T \cong \mathcal{R}\mathrm{es}_T^{T'}(\mathcal{F}'_{T'}).$$

(Functorially in $\mathcal{F}'$.)

Proof Let Z be a T-scheme. Then

$$\begin{gathered}\mathcal{R}\mathrm{es}_T^{T'}(\mathcal{F}'_{T'})(Z) \overset{\mathrm{Def}}{=} \mathcal{F}'_{T'}(Z \times_T T') = \mathcal{F}'(Z \times_T T') \cong \\ \mathcal{F}'(Z \times_S S') = \mathcal{R}\mathrm{es}_S^{S'}(\mathcal{F}')(Z) = (\mathcal{R}\mathrm{es}_S^{S'}(\mathcal{F}'))_T(Z).\end{gathered}$$

□

Lemma 1.2 *Let $T \longrightarrow S$, $T' := T \times_S S'$. Let $\alpha : X' \longrightarrow T'$. Then*

$$\mathcal{R}\mathrm{es}_T^{T'}(X') = \mathcal{R}\mathrm{es}_S^{S'}(X') \times_{\mathcal{R}\mathrm{es}_S^{S'}(T')} T.$$

Here the right-hand side is defined by $\mathcal{R}\mathrm{es}(\alpha)$ *and* $\mathrm{id} \in \mathcal{R}\mathrm{es}_S^{S'}(T')(T)$ *(which defines the natural transformation* $\mathrm{Hom}_S(-, T) \longrightarrow \mathcal{R}\mathrm{es}_S^{S'}(T')$*).*

Proof Let $\gamma : Z \longrightarrow T'$ be some T'-scheme. Then

$$\begin{gathered}\mathcal{R}\mathrm{es}_T^{T'}(Z) = \mathrm{Hom}_{T'}(Z \times_T T', X') = \\ \{\beta \in \mathrm{Hom}_{S'}(Z \times_T T', X')|\ \alpha \circ \beta = \gamma \times_T T',\ \text{i.e. } \mathcal{R}\mathrm{es}_S^{S'}(\alpha)(\beta) = \gamma \times_T T'\} = \\ \mathcal{R}\mathrm{es}_S^{S'}(X') \times_{\mathcal{R}\mathrm{es}_S^{S'}(T')} T(Z).\end{gathered}$$

□

Let $\mathcal{F} : \mathcal{C}/S \longrightarrow \mathcal{E}ns$ be a functor. Then the morphisms $\mathcal{F}(Z) \longrightarrow \mathcal{F}(Z \times_S S') = \mathcal{F}_{S'}(Z \times_S S')$ induce a natural transformation

$$\mathcal{F} \longrightarrow \mathcal{R}\mathrm{es}_S^{S'}(\mathcal{F}_{S'}).$$

This is natural in $\mathcal{F}$. Thus we get a natural transformation

$$\mathrm{id} \longrightarrow \mathcal{R}\mathrm{es}_S^{S'}((.)_{S'}),$$

where id is the identity functor on the category $\mathrm{Hom}^{\mathrm{opp}}(\mathcal{C}/S, \mathcal{E}ns)$.

Let X be an S-scheme. Then by this construction we get a natural transformation

$$\mathrm{Hom}_S(-, X) \longrightarrow \mathcal{R}\mathrm{es}_S^{S'}(X \times_S S').$$

given by $\alpha \mapsto \alpha \times_S \mathrm{id}_{S'}$. It is defined by mapping the identity on X to the identity on $X \times_S S'$, and it is natural in X.

Lemma 1.3 *If the morphism $S' \longrightarrow S$ is faithful (i.e. if the functor $- \times S' : \mathcal{C}/S \longrightarrow \mathcal{C}/S'$ is faithful), then the natural transformation* $\mathrm{Hom}(-, X) \longrightarrow \mathcal{R}\mathrm{es}_S^{S'}(X \times_S S')$ *is injective.*

□

1.1.3 Weil-restrictions of schemes

In the following and in the rest of the paper we will use the above definitions only for the category $\mathcal{S}ch$ of locally Noetherian schemes which are contained in the fixed universe $\mathcal{U}$.

We will see that within this category for special h and quite general X', the base-restriction $\mathcal{R}\mathrm{es}^h(X')$ is representable. We call a representing object the *Weil-restriction* of X' with respect to $h : S' \longrightarrow S$ and denote it by $\mathbf{Res}_S^{S'}(X')$.

Idea of the construction by restriction of scalars

Assume that S =Spec(A), S' =Spec(B), where $B = A\alpha_1 \oplus \cdots \oplus A\alpha_n$ is a finite and free n-dimensional A-module. Let X' =Spec$(B[X_1, \ldots, X_m]/(f_1, \ldots, f_l))$ be affine and of finite type. The coordinates X_i define a closed immersion $X' \longrightarrow \mathbb{A}_B^m = \mathrm{Spec}(B[X_1, \ldots, X_m])$. We use this immersion to define a scheme W which represents $\mathcal{R}\mathrm{es}_S^{S'}(X')$, the *Weil-restriction* of X' with respect to $S' \longrightarrow S$. It can be constructed by "restriction of scalars":

Fix some A-algebra C. The idea is to express the m coordinates of some $C \otimes_A B$-valued point P of $\mathbb{A}_A^m$ in the basis $(\alpha_1, \ldots, \alpha_n)$ of the A-algebra B. This gives a point p in $\mathbb{A}_A^{nm}$, and expanding out the "equations" f_i in the new variables gives equations $f_{i,j}$, $i = 1, \ldots, l$, $j = 1, \ldots, n$. Now P satisfies the f_i iff p satisfies the $f_{i,j}$. One then proves that the scheme constructed in this way has the correct property not only for every A-algebra C but for any S-scheme Z.

An example

We give a small example to present the idea:

Let $K|k$ be a quadratic field extension with $K = k(\alpha)$ where $\alpha^2 = a \in k$. Let V' be the affine variety in $\mathbb{A}_K^2$ given by $XY = 1$. We are interested in the $C \otimes_k K$-valued points of this variety (for any k-algebra C). Let P be an arbitrary $C \otimes_k K$-valued point of $\mathbb{A}_K^2$ with coordinates $X = X(P)$, $Y = Y(P)$,

$X = x_1 \otimes_k 1 + x_2 \otimes_k \alpha$, $Y = y_1 \otimes_k 1 + y_2 \otimes_k \alpha$. (With $x_i, y_i \in k$.) Then the defining equation $XY = 1$ becomes

$$(x_1y_1 + ax_2y_2 - 1) \otimes_k 1 + (x_1y_2 + x_2y_1) \otimes_k \alpha = 0.$$

This equation is satisfied iff (x_1, x_2, y_1, y_2) satisfies

$$x_1y_1 + ax_2y_2 = 1,\ x_1y_2 + x_2y_1 = 0$$

Let W be the k-scheme defined by these equations. From the construction, $W(C) \cong V'(C \otimes_k K)$ for all k-algebras C. From a general argument (which we will formalize below), it follows that one can generalize this functorial isomorphism from affine k-schemes to arbitrary schemes. It follows that W is the Weil-restriction of X' with respect to $K|k$.

We will now formalize these ideas and prove that the variety W constructed in this way has indeed the correct properties for any S-scheme Z.

Formal construction

Let S =Spec(A), S' =Spec(B) where the ring B is a free A module on the bases $\alpha_1, \dots, \alpha_n$ as above. Let also X' be as above. For each $i = 1, \dots, l$, let $f_{i,j} \in A[x_{1,1}, \dots, x_{m,n}]$ be defined by

$$\begin{aligned} f_{i,1}\alpha_1 + \cdots + f_{i,n}\alpha_n = f_i(x_{1,1}\alpha_1 + \cdots + x_{1,n}\alpha_n, \dots, x_{m,1}\alpha_1 + \cdots + x_{m,n}\alpha_n) \\ \in B[x_{1,1}, \dots, x_{m,n}], \end{aligned}$$

where the right-hand side is the image of f_i under the map

$$B[X_1, \dots, X_m] \longrightarrow B[x_{1,1}, \dots, x_{m,n}],\ X_i \mapsto x_{i,1}\alpha_1 + \cdots + x_{i,n}\alpha_n.$$

Let W :=Spec($A[x_{1,1}, \dots, x_{n,m}]/(f_{i,j})_{i=1,\dots,l,\ j=1,\dots,l}$).

Now, if C is any A-algebra, then $C \otimes_A B = C \otimes_A \alpha_1 \oplus \cdots \oplus C \otimes_A \alpha_n$, and it is immediate that a $C \otimes_A B$-valued point of X' (i.e. a solution of f_i, $i = 1, \dots, n$ in $C \otimes_A B$) corresponds under "restriction of scalars" to exactly one C-valued point of W (i.e. to a solution of the $f_{i,j}$, $i = 1, \dots k$, $j = 1, \dots, n$ in C). This correspondence is functorial in C. Thus W (with the natural transformation "restriction of scalars") represents $\mathcal{R}\mathrm{es}_S^{S'}(X')$ in the category of affine schemes.

Now let Z be an arbitrary S-scheme and let $Z \times_S S' \longrightarrow X'$ be an S'-morphism. Then any open affine part Z^a of Z induces a morphism $Z^a \times_S S' \longrightarrow X'$ and thus a morphism $Z^a \longrightarrow W$. If Z^b is another open affine part of Z, then we also get a morphism $Z^b \longrightarrow W$ and from the functoriality of the construction, it follows that both morphisms agree on the intersection $Z^a \cap Z^b$ (because they agree on all open, affine subsets of the intersection). Thus by glueing we get a morphism $Z \longrightarrow W$. This construction is again functorial in Z. Moreover, any morphism $Z \longrightarrow W$ determines again by functoriality and by glueing a unique morphism $Z \longrightarrow X'$. So, W is indeed a representing object for the functor $\mathcal{R}\mathrm{es}_S^{S'}(X')$.

[The last step follows from fact that $\mathcal{R}\mathrm{es}_S^{S'}(X')$ has the "sheaf property with respect to the Zariski topology" i.e. one can glue morphisms (see [BLR, p.194]) and the general fact that if an affine scheme represents a functor in the category of affine schemes and the functor has the sheaf property with respect to the Zariski topology than the scheme represents the functor in the full category of schemes.]

With this construction, the Weil-restriction of an affine scheme regarded as closed subscheme of m-dimensional affine space is canonically a closed subscheme of $m \cdot n$-dimensional affine space.

Proposition 1.4 *([BLR, 7.6, Theorem 4]) Let S, S' be schemes, $h : S' \longrightarrow S$ a morphism which is finite and locally free. Let X' be an S'-scheme (locally) of finite type. Assume that for each $s \in S$ and each finite set of points $M \subset X' \times_S \operatorname{Spec}(\kappa(s))$ (where $\kappa(s)$ is the residue class field at s), there is an affine open subscheme U' of X' containing M. (E.g. X' is a quasi-projective S'-scheme.) Then the base-restriction is representable by an S-scheme (locally) of finite type, i.e. the Weil-restriction of X' with respect to h exists and is (locally) of finite type.* [1]

proof (outline) We can assume that S and S' are affine and that $S' \longrightarrow S$ is finite and free. For affine X', one can construct the Weil-restriction by "restriction of scalars". For general X', one glues the representing objects of the open affine parts of X' to get a scheme W. This can be done since the Weil restriction of an open inclusion is an open inclusion. Then one constructs a natural transformation $\mathrm{Hom}(-, W) \longrightarrow \mathcal{R}\mathrm{es}_S^{S'}(X')$ using the fact that W has the "sheaf-property with respect to the Zariski-topology". Now one uses the assumption to show that this natural transformation is a bijection. □

For the rest of this subsection, let $S' \longrightarrow S$ be finite and locally free and let X' be an S'-scheme which fulfills the assumptions of the proposition.

We denote an S-scheme which represents $\mathcal{R}\mathrm{es}^h(X')$ by $\mathbf{Res}_S^{S'}(X')$. We will often abbreviate it by W. By definition as a representing object of $\mathcal{R}\mathrm{es}_S^{S'}(X')$, there is a universal morphism $u = u_{X'} : \mathbf{Res}_S^{S'}(X') \times_S S' \longrightarrow X'$ such that if Y is any S-scheme and $c : Y \times_S S' \longrightarrow X'$ is a morphism, there is a unique morphism $b : Y \longrightarrow W$ such that $c = u \circ (b \times_S \mathrm{id}_{S'}) : Y \times_S S' \longrightarrow X'$. As usual,

[1] In [BLR], the proposition is stated without the assumption "locally of finite type". That the Weil-restriction is locally of finite type if X' is follows easily from the construction. That the Weil-restriction is of finite type if X' is, is a more difficult result. – It follows from [BLR, 7.6, Proposition 5 (e)] and our general assumption that all schemes considered be locally Noetherian. Further properties of the Weil-restriction depending on properties of X' and the base-morphism $S' \longrightarrow S$ are given in [BLR, 7.6, Proposition 5]. In the subsequent parts of this work, we will restrict ourself to the case that S is connected, X' is quasi-projective over S' and the base-morphism is étale. Under these assumptions, we will proof all properties of the Weil-restriction we need.

$(\mathbf{Res}_S^{S'}(X'), u)$ is unique up to unique isomorphism.

$$\begin{tikzcd}
Y \times_S S' \arrow[r, "b \times_S \mathrm{id}_{S'}"'] \arrow[d] \arrow[rr, bend left, "c"] & \mathbf{Res}_S^{S'}(X') \times_S S' \arrow[r, "u"] \arrow[d] & X' \\
Y \arrow[r, "\exists!\, b"] & \mathbf{Res}_S^{S'}(X') &
\end{tikzcd} \tag{1.1}$$

If S, S' and X' are affine (with notations as above) and $\mathbf{Res}_S^{S'}(X')$ is constructed by "restriction of scalars" as above, then u is given by

$$\begin{gathered}
B[X_1, \dots, X_m]/(f_i)_{i=1,\dots,l} \longrightarrow B[x_{1,1}, \dots, x_{m,n}]/(f_{i,j})_{i=1,\dots,l, j=1,\dots,n}, \\
X_i \mapsto \alpha_1 x_{i,1} + \dots + \alpha_n x_{i,n}.
\end{gathered} \tag{1.2}$$

Let Y' be another S'-scheme which fulfills the assumptions of the proposition. As said above, every S'-morphism $\gamma : X' \longrightarrow Y'$ induces a natural transformation $\mathcal{R}\mathrm{es}_S^{S'}(\gamma) : \mathcal{R}\mathrm{es}_S^{S'}(X') \longrightarrow \mathcal{R}\mathrm{es}_S^{S'}(Y')$ which is given by "push-forward". This natural transformation corresponds to a morphism $\mathbf{Res}_S^{S'}(\gamma) : \mathbf{Res}_S^{S'}(X') \longrightarrow \mathbf{Res}_S^{S'}(Y')$. By the universal property of $\mathbf{Res}_S^{S'}(Y')$, the morphism in the lowest line of the following commutative diagram exists, is unique and equal to $\mathbf{Res}_S^{S'}(\gamma)$.

$$\begin{tikzcd}
 & X' \arrow[rr, "\gamma"] & & Y' \\
\mathbf{Res}_S^{S'}(X') \times_S S' \arrow[ur, "u_{X'}"'] \arrow[rr] \arrow[d] & & \mathbf{Res}_S^{S'}(Y') \times_S S' \arrow[ur, "u_{Y'}"'] \arrow[d] & \\
\mathbf{Res}_S^{S'}(X') \arrow[rr, "\mathbf{Res}_S^{S'}(\gamma)"] & & \mathbf{Res}_S^{S'}(Y') &
\end{tikzcd} \tag{1.3}$$

Let $S = \mathrm{Spec}(A)$, $S' = \mathrm{Spec}(B)$ be affine, where B is a free A-module on the generators $\alpha_1, \dots, \alpha_n$. Let $X' = \mathrm{Spec}(B[X_1, \dots, X_m]/(f_1, \dots, f_l))$, $Y' = \mathrm{Spec}$ $(B[Y_1, \dots, Y_{\tilde{m}}]/(g_1, \dots, g_{\tilde{l}}))$. Let $\gamma : X' \longrightarrow Y'$ be given by $Y_i \mapsto h_i(X_1, \dots, X_m)$. Then $\gamma\, u_{X'}$ is given by $Y_i \mapsto h_i(\alpha_1 x_{1,1} + \dots + \alpha_n x_{1,n}, \dots, \alpha_1 x_{m,1} + \dots + \alpha_n x_{m,n})$. Let $h_{i,j}$ be defined by $h_i(\alpha_1 x_{1,1} + \dots + \alpha_n x_{1,n}, \dots, \alpha_1 x_{m,1} + \dots + \alpha_n x_{m,n}) = h_{i,1}\alpha_1 + \ldots + h_{i,n}\alpha_n$. Then $\mathbf{Res}_S^{S'}(\gamma)$ is given by $y_{i,j} \mapsto h_{i,j}$.

Let S be connected. Let X be an S-scheme and let $X' := X \times_S S'$. (Again assume that $X' \longrightarrow S'$ fulfills the assumptions of the proposition.) By assumption, the morphism $S' \longrightarrow S$ is flat and surjective, thus it is faithfully flat. In particular, it is faithful, i.e. the functor $- \times_S T$ is faithful. By Lemma 1.3 the natural transformation $\mathrm{Hom}(-, X) \hookrightarrow \mathcal{R}\mathrm{es}_S^{S'}(X)$ is injective. We get a morphism $\iota : X \longrightarrow \mathbf{Res}_S^{S'}(X')$ which is uniquely defined by

$$\mathrm{id}_{X'} = u \circ (\iota \times_S \mathrm{id}_{S'}) \tag{1.4}$$

and which is injective on .-valued points.

Lemma 1.5 *Let S be connected and let $X \longrightarrow S$ be separated such that $X \times_S S' \longrightarrow S'$ fulfills the assumptions of the proposition. Then $\iota : X \longrightarrow \mathbf{Res}_S^{S'}(X \times_S S')$ is a closed immersion.*

Proof Since $X \longrightarrow S$ is separated, so is $\mathbf{Res}_S^{S'}(X') \longrightarrow S'$; see [BLR, 7.6, Proposition 5], under the assumption that X' is quasi-projective over S' and $S' \longrightarrow S$ is étale, this follows also from the construction of W in the next subsection.

Now (1.4) implies that $\iota \times_S \mathrm{id}_{S'}$ is a closed immersion:

The morphism (of topological spaces) $\iota \times_S \mathrm{id}_{S'}$ is injective. Since $\mathbf{Res}_S^{S'}(X') \longrightarrow S'$ is separated, the subset $U' := \{x \in \mathbf{Res}_S^{S'}(X') | \ (\iota \times_S \mathrm{id}_{S'}) \circ u(x) = x\}$ of $\mathbf{Res}_S^{S'}(X')$ is closed. If C' is a closed subset of X', then $\iota \times_S \mathrm{id}_{S'}(C') = U' \cap u^{-1}(C')$, and since U' is closed, this is also closed in $\mathbf{Res}_S^{S'}(X') \times_S S'$. Thus $\iota \times_S \mathrm{id}_{S'}$ is an injective, closed morphism of topological spaces.

For all $x' \in X'$, (1.4) induces an isomorphism of local rings

$$\begin{tikzcd} \mathcal{O}_{X',x'} \arrow[r, "u^{\#}"] & \mathcal{O}_{X',(\iota \times_S \mathrm{id}_{S'})(x')} \arrow[r, "(\iota \times_S \mathrm{id}_{S'})"] & \mathcal{O}_{X',x'}. \end{tikzcd}$$

Thus $\iota^{\#} : \mathcal{O}_{\mathcal{R}\mathrm{es}_S^{S'}(X') \times_S S'} \longrightarrow \iota^*(\mathcal{O}_{X'})$ is surjective.

This means that $\iota \times_S \mathrm{id}_{S'}$ is a closed immersion. Since the morphism $S' \longrightarrow S$ is faithfully flat, we obtain that $\iota : X \longrightarrow \mathbf{Res}_S^{S'}(X')$ is a closed immersion; see [SGA I, VIII, Corollaire 5.5.]. □

1.1.4 The étale case

Now let S be connected and let $S' \longrightarrow S$ be an étale covering, i.e. a finite, flat and unramified morphism; see [SGA I, I] for details. (For example, S' and S could be spectra of fields, and $S' \longrightarrow S$ could be induced by a finite separable field extension.)

Let X' be a quasi-projective S'-scheme. We will give an alternative construction of the Weil-restriction in this case. In this construction we will define a T'-scheme W' for some Galois covering $T' \longrightarrow S$ and a Galois-operation on W'. By [SGA I, V], the quotient scheme of W' under the Galois-operation exists. This quotient scheme will be the Weil-restriction.

Note that under our assumption that all schemes considered be locally Noetherian, "finite and flat" is equivalent to "finite and locally free"; see [Ha, III, Proposition 9.2. (e)]. Thus we will consider a special case of the situation in Proposition 1.4.

Base-change by étale coverings

Before we come to the construction of the Weil-restriction via Galois-operation, we first fix some notation.

Let T' be an S-scheme and let $\sigma : T' \longrightarrow S'$ be an étale covering of S-schemes. [2] Then let $\sigma^{-1}(X')$ be the T'-scheme defined by the following Cartesian diagram [3]

$$\begin{tikzcd}
\sigma^{-1}(X') \arrow[r] \arrow[d] & X' \arrow[d] \\
T' \arrow[r, "\sigma"] & S'.
\end{tikzcd} \tag{1.5}$$

We denote the morphism $\sigma^{-1}(X') \longrightarrow X'$ in the first row of (1.5) by σ.

Let $\sigma : T' \longrightarrow S'$, $\tau : T' \longrightarrow T'$ be S-morphisms. Then $(\sigma\tau)^{-1}(X')$ and $\tau^{-1}(\sigma^{-1}(X'))$ are naturally isomorphic as S'-schemes. We denote the composition $(\sigma\tau)^{-1}(X') \simeq \tau^{-1}(\sigma^{-1}(X')) \xrightarrow{\tau} \sigma^{-1}(X')$ also by τ.

If σ is an isomorphism, we denote $(\sigma^{-1})^{-1}(X)$ also by $\sigma(X)$.

By base-change, an S'-morphism $\alpha : X' \longrightarrow Y'$ induces an S'-morphism $\alpha^\sigma : \sigma^{-1}(X') \longrightarrow \sigma^{-1}(Y')$. If σ is an isomorphism, then $\alpha^\sigma = \sigma^{-1}\alpha\sigma$. In this case, we denote $\alpha^{\sigma^{-1}}$ also by $\sigma(\alpha)$.

With this definition, $p^\sigma : \ \sigma^{-1}(X') \longrightarrow S'$ is the left hand side morphism in (1.5).

Let $S = \operatorname{Spec}(A)$, $S' = \operatorname{Spec}(B)$ and $T' = \operatorname{Spec}(C)$ be affine. Let $X' = \operatorname{Spec}(B[x_1, \dots, x_m]/(f_1, \dots, f_l))$ be affine and of finite type. Then $\sigma : T' \longrightarrow S'$ is given by an A-morphism $\sigma^\# : B \longrightarrow C$.

Let $\sigma : \ T' \longrightarrow S'$ be as above and extend the morphism $\sigma^\# : B \longrightarrow C$ to an "arithmetic" A-morphism $\sigma^\# : B[x_1, \dots, x_m] \longrightarrow C[x_1, \dots, x_m]$ given by $B \ni b \mapsto \sigma^\#(b)$, $x_i \mapsto x_i$. Then the diagram

$$\begin{tikzcd}
C[x_1, \dots, x_m]/(\sigma^\#(f_1), \dots, \sigma^\#(f_l)) & B[x_1, \dots, x_m]/(f_1, \dots, f_l) \arrow[l, "\sigma^\#"'] \\
C \arrow[u] & B \arrow[l, "\sigma^\#"] \arrow[u]
\end{tikzcd}$$

is co-Cartesian and thus defines the underlying ring of $\sigma^{-1}(X')$. If S, S', T' or X' are not affine, $\sigma^{-1}(X')$ and the morphisms of diagram (1.5) can be defined like this locally.

[2] The morphism $\sigma : T' \longrightarrow S'$ might also be a pro-étale covering, i.e. a projective limit of étale coverings (provided T' is still locally Noetherian). For example, $S' \longrightarrow S$ might be defined by a finite separable extension of fields $K|k$, and $\sigma : T' \longrightarrow S'$ might correspond to an inclusion of K into k^{sep}.

[3] The S'-scheme $\sigma^{-1}(X')$ with the morphisms as in the diagram is unique up to a unique S'-isomorphism. In the following we will assume that for all S-schemes S' and T', S'-schemes X' and S-morphisms $\sigma : T' \longrightarrow S'$ we have chosen such a $\sigma^{-1}(X')$.

Note that in the case that $\sigma : T' \longrightarrow S'$ is an isomorphism, the following diagram is Cartesian.

$$\begin{tikzcd}
X' \arrow[r, equal] \arrow[d] & X' \arrow[dd] \\
S' \arrow[d, "\sigma^{-1}"] & \\
T' \arrow[r, "\sigma"] & S'.
\end{tikzcd} \tag{1.6}$$

Thus $\sigma^{-1}(X')$ is (canonically isomorphic to) X' regarded as T'-scheme via the structure morphism $X' \longrightarrow S' \xrightarrow{\sigma^{-1}} T'$.

Construction

We now construct the Weil-restriction of X' with respect to $S' \longrightarrow S$ via Galois-operation. If $S' \longrightarrow S$ is itself Galois, the construction is relatively easy and will be described in the next subsection. Here we continue with the general case.

We first need the following lemma which is a generalization of the fact that for every finite separable field extension $K|k$ there exists a splitting field. This means that there exists a finite Galois field extension $L|k$, included in $\overline{k}$, such that the image of all inclusions of $K|k$ into $\overline{k}$ is contained in L.

Lemma 1.6 *There exists a connected Galois covering $f : T' \longrightarrow S$ such that:*

Fixing a geometric point P_0 of S and a geometric point Q_0 of T' over P_0, every geometric point P' of S' over P_0 defines by $Q_0 \mapsto P'$ a unique morphism $T' \longrightarrow S'$ over S.

Proof This follows from the construction of the étale fundamental group $\pi_1(S, P_0)$; see [SGA I, V,4,g)]. [If S' is connected, in the terms of the étale fundamental group, $S' \longrightarrow S$ corresponds to a conjugacy class in $\pi_1(S, P_0)$ of subgroups of finite index. T' corresponds to the intersection of all subgroups in the conjugacy class. This is a normal subgroup of $\pi_1(S, P_0)$ of finite index.] □

Fix such a T' with Galois group G. This means by definition that there is a fixed injective *anti-homomorphism* $G \hookrightarrow \mathrm{Aut}_S(T')$. [Since T' is connected, this is an isomorphism.] [4]

This anti-homomorphism induces a homomorphism $G^{\mathrm{opp}} \hookrightarrow \mathrm{Aut}_S(T')$, where G^{opp} is the opposite group of G (i.e. there is an anti-isomorphism $G \xrightarrow{\sim} G^{\mathrm{opp}}$). We identify G^{opp} with its image.

We denote the elements of G by bold letters and the corresponding elements of the opposite group G^{opp} by usual letters, i.e. we have an injective *anti-homomorphism $\boldsymbol{\sigma} \mapsto \sigma$.*

[4] In [SGA I, V], the Galois group operates from the right. Writing all homomorphisms from the left, we obtain an anti-homomorphism $G \hookrightarrow \mathrm{Aut}_S(T')$.

Let

$$W' := \prod_{\sigma:T\longrightarrow S'} \sigma^{-1}(X').$$ [5]

For future application, we fix the notation that $p_\sigma : W' \longrightarrow \sigma^{-1}(X')$ is the projection to the "σ-th" factor.

Now define a Galois-operation of W' which is compatible with the operation of G on $f : T' \longrightarrow S$ as follows:

For $\boldsymbol{\tau} \in G$, let $\widetilde{\tau} : \prod_{\sigma:T'\longrightarrow S'} \sigma^{-1}(X') \longrightarrow \prod_{\sigma:T'\longrightarrow S'} \sigma^{-1}(X')$ be defined on .-valued points by $(P_\sigma)_\sigma \mapsto (\tau \circ P_{\sigma\tau})_\sigma$, i.e.

$$p_\sigma \circ \widetilde{\tau} = \tau \circ p_{\sigma\tau}. \tag{1.7}$$

Lemma 1.7 *The map $G^{\mathrm{opp}} \longrightarrow \mathrm{Aut}_S(W')$, $\tau \mapsto \widetilde{\tau}$ is a group-homomorphism.*

Proof

$$\widetilde{\tau_1} \circ (\widetilde{\tau_2} \circ (P_\sigma)_\sigma) = \widetilde{\tau_1} \circ (\tau_2 \circ P_{\sigma\tau_2})_\sigma = \\ (\tau_1\tau_2 \circ P_{\sigma\tau_1\tau_2})_\sigma = \widetilde{\tau_1\tau_2} \circ (P_\sigma)_\sigma$$

□

Since we assumed that X' is quasi-projective, so is W' and the quotient scheme $W := W'/G$ under this operation exists; see [SGA I, V, Proposition 1.8]. Moreover, since the operation is compatible with the Galois-operation on $f : T' \longrightarrow S$, the quotient scheme is an S-scheme with $W \times_S T' \simeq W'$.

We now show that W is the Weil-restriction of X' with respect to $S' \longrightarrow S$.

Let Z be some S-scheme. We will establish a functorial bijection between the $Z \times_S S'$-valued points of the S'-scheme X' and the Galois invariant $Z \times_S T'$-valued points of the T'-scheme W'. (These points are functorially in bijection with the Z-valued points of W.)

We start with the $Z \times_S S'$-valued points of X'. If P is such a point, then $(P^\sigma)_\sigma$ is Galois-invariant. (In fact, for $\boldsymbol{\tau} \in G$, $\widetilde{\tau} \circ (P^\sigma)_\sigma \circ \tau^{-1} = (\tau P^{\sigma\tau} \tau^{-1})_\sigma = (P^{\sigma\tau\tau^{-1}})_\sigma = (P^\sigma)_\sigma$.)

Lemma 1.8 *The map $P \mapsto (P^\sigma)_\sigma$ is an bijection between the $Z \times_S S'$-valued points of X' and the Galois-invariant $Z \times_S T'$-valued points of W'.*

Proof The map is obviously injective. We now show that all Galois-invariant $Z \times_S T'$-valued points of W' have this form.

Let $(P_\sigma)_\sigma$ be a $Z \times_S T'$-valued point of W'. Then this point is Galois invariant iff $(\tau P_{\sigma\tau} \tau^{-1})_\sigma = (P_\sigma)_\sigma$ for all $\boldsymbol{\tau} \in G$, i.e. $P_{\sigma\tau} = P_\sigma^\tau$ for all $\boldsymbol{\tau} \in G$. Assume that this is the case.

[5] Here and for the rest of the subsection, morphisms are always assumed to be S-morphisms.

Let S'_i, $i = 1, \dots$ be the connected components of S', $\iota_i : S'_i \hookrightarrow S'$ the immersions. Let $\sigma_i^{(0)}, \sigma_i^{(1)}, \dots$ be the S-morphisms $T \longrightarrow S'_i$. The sets $\{\iota_i \sigma_i^{(j)} \mid j = 0, \dots\}$ are the orbits of the operation of G on the set of $\sigma : T' \longrightarrow S'$.

Fix some i. We will show that there is some $Z \times_S S'_i$-valued point P_i of $X'_i := \iota_i^{-1}(X')$ with $P_{\iota_i \sigma_i^{(j)}} = P_i^{\sigma_i^{(j)}}$ for all j. By the universal property of the disjoint union, the $\iota_i P_i$ define a morphism $P : Z \times_S S'_i \longrightarrow X'$ with $P^\sigma = P_\sigma$ for all $\sigma : T' \longrightarrow S'$.

Now, $\sigma_i^{(0)} : T' \longrightarrow S'_i$ is a connected Galois covering, let $H_i \leq G$ be its Galois group. Then $\sigma_i^{(0)^{-1}}(X_i) \longrightarrow X'_i$ and $Z \times_S T' \longrightarrow Z \times_S S'_i$ are also Galois with the same Galois group.

For all $\boldsymbol{\tau} \in H_i$, $P^\tau_{\iota_i \sigma_i^{(0)}} = P_{\iota_i \sigma_i^{(0)} \tau} = P_{\iota_i \sigma_i^{(0)}}$. Thus $P_{\iota_i \sigma_i^{(0)}} = P_i^{\sigma_i^{(0)}}$ for some $Z \times_S S_i$-valued point P_i of X'_i. Because G operates transitively on the $\sigma_i^{(j)}$, we also have $P_{\iota_i \sigma_i^{(j)}} = P_i^{\sigma_i^{(j)}}$ for all j. □

We have thus seen that W is the Weil-restriction of X' with respect to $S' \longrightarrow S$. The Weil-restriction is again quasi-projective, and if X' is projective, it is also projective. In Subsection 1.2.1, we will show that if we fix some immersion of X' into a projective space, W is immersed in some concrete higher-dimensional projective space, the immersion being canonical up to an isomorphism of the surrounding projective space.

After we have constructed W, equation (1.7) can be reinterpreted by

$$p_\sigma^\tau = p_{\sigma\tau} \tag{1.8}$$

or – what is the same –

$$\tau(p_\sigma) = p_{\sigma\tau^{-1}}. \tag{1.9}$$

Let $u : W \longrightarrow X'$ be the universal morphism. Then by definition, u corresponds to the identity on W, which is of course given by $(p_\sigma)_\sigma : W' \longrightarrow W'$. It follows that

$$u^\tau = p_\tau. \tag{1.10}$$

By construction, W is quasi-projective and in particular separated. Many other properties of X' carry over to W' and then to W:

Lemma 1.9 *Let S be connected and let $h : S' \longrightarrow S$ be étale. Let X' be a quasi-projective S'-scheme and let W be the Weil-restriction of X' with respect to h. Then*

- *If X' is projective, so is W.*
- *If X' is of finite type, so is W.*

- *If X' is reduced, so is W.*
- *If X' is flat, so is W.*
- *If X' is smooth, so is W.*

Lemma 1.10 *Let $h : S' \longrightarrow S$ be given by a separable finite extension of fields. Then*

- *If X' is geometrically irreducible, so is W.*
- *If X' is geometrically reduced, so is W.*

□

We now review the Weil-restriction as a functor. Let $\gamma : X' \longrightarrow Y'$ be an S'-morphism. By diagram (1.3), $\mathbf{Res}_S^{S'}(\gamma) : \mathbf{Res}_S^{S'}(X') \longrightarrow \mathbf{Res}_S^{S'}(Y')$ is the morphism which corresponds to the $\mathbf{Res}_S^{S'}(X') \times_S S'$-valued point γu of X'.

By the above construction, especially (1.10), this is given by

$$\mathbf{Res}_S^{S'}(\gamma) \times_S T' = ((\gamma u)^\sigma)_\sigma = (\gamma^\sigma p_\sigma)_\sigma : \prod_\sigma \sigma^{-1}(X') \longrightarrow \prod_\sigma \sigma^{-1}(Y'). \qquad (1.11)$$

Let $h : S' \longrightarrow S$ still be étale. Let n be the degree of h (i.e. the number of geometric points over some geometric point of S).

Let X be a quasi-projective S-scheme, $X' := X \times_S S'$.

The quasi-projective S-scheme X is in particular separated, and by Lemma 1.5, the injective natural transformation $\mathrm{Hom}_S(-, X) \hookrightarrow \mathfrak{Res}_S^{S'}(X')$ corresponds to a closed immersion $\iota : X \longrightarrow \mathbf{Res}_S^{S'}(X')$. After a base change $T' \longrightarrow S$ as above, $\mathbf{Res}_S^{S'}(X')$ is isomorphic to $X_{T'}^n$, and $\iota \times_S \mathrm{id}_{T'} = (\mathrm{id})_{i=1}^n : X_{T'} \longrightarrow X_{T'}^n$. This shows again that $\iota \times_S \mathrm{id}_{T'}$ is a closed immersion, and as $S' \longrightarrow S$ is faithfully flat, so is $\iota : X \longrightarrow \mathbf{Res}_S^{S'}(X')$.

1.1.5 The Galois case

We now restrict ourselves to the case that the base-morphism $S' \longrightarrow S$ is Galois.

Let $h : S' \longrightarrow S$ be Galois with Galois group G. Again let X' be a quasi-projective S'-scheme. Then the "geometric construction" of the Weil-restriction becomes much easier:

Let $W' := \prod_{\sigma \in G^{\mathrm{opp}}} \sigma^{-1}(X')$. As above, define a Galois-operation on W' by $\boldsymbol{\tau} \mapsto \widetilde{\tau}$ where $\widetilde{\tau} : (P_\sigma)_{\sigma \in G^{\mathrm{opp}}} \mapsto (\tau \circ P_{\sigma\tau})_{\sigma \in G^{\mathrm{opp}}}$.

Since by assumption X' and thus also W' is quasi-projective, the quotient scheme $W := W'/G$ exists; see [SGA I, V, Proposition 1.8]. We will now show that W which universal element $u := o_{\mathrm{id}}$ is the Weil-restriction of W' with respect to $S' \longrightarrow S$.

Fix some S-scheme Z. Then the $Z \times_S S'$-valued points of W' which are Galois-invariant are exactly the points of the form $(P_\sigma)_{\sigma \in G^{\mathrm{opp}}} = (P^\sigma)_{\sigma \in G^{\mathrm{opp}}} = (\sigma^{-1}(P))_{\sigma \in G^{\mathrm{opp}}}$, where P is a $Z \times_S S'$-valued point of X'.

Thus $P \mapsto (\sigma^{-1}(P))_{\sigma \in G^{\mathrm{opp}}}$ is a bijection between the $Z \times_S S'$-valued points of X' and the Galois-invariant $Z \times_S S'$-valued points of W'. On the other hand, by Galois theory the Galois-invariant $Z \times_S S'$-valued points of W' are in bijection with the Z-valued points of W.

The bijection between the $Z \times_S S'$-valued points of X' and the Z-valued points of W is natural in Z. Moreover, the identity of W corresponds to the projection p_{id} from W' to X'.

So, $W = W'/G$ with universal element $u = p_{\mathrm{id}}$ is the Weil-restriction for X' with respect to $S' \longrightarrow S$.

Remark This construction is of course closely related to the construction in the étale case. For example, equations (1.7) to (1.11) still hold. However, the two constructions are only equal if S' is connected.

Comparison

Again let $S' \longrightarrow S$ be Galois with Galois group G and let X' be a quasi-projective S'-scheme. We show how the first construction arises in a natural way if one tries to find W starting from W' and the Galois action.

Since a Galois covering is by definition étale and finite, it is also locally free (finite and flat is equivalent to finite and locally free [Ha, III, Proposition 9.2.]).

Assume that $S = \mathrm{Spec}(A)$, $S' = \mathrm{Spec}(B)$ and X' are affine and that B is free over A, $B = \alpha_1 A \oplus \cdots \oplus \alpha_n A$ and $X' =$Spec$(B[X_1, \ldots, X_m]/(f_1, \ldots, f_l))$ as in the "Formal construction" of Subsection 1.1.3. This presentation of X' defines a closed immersion $X' \hookrightarrow \mathbb{A}^m_B$, and if we fix this immersion, $\sigma^{-1}(X)$ is also immersed in $\mathbb{A}^m_B$, and $W' = \prod_{\sigma \in G^{\mathrm{opp}}} \sigma^{-1}(X')$ is a closed immersion of ${\mathbb{A}^m_B}^{G^{\mathrm{opp}}} = \mathrm{Spec}(B[\{x_{i,\sigma}\}_{i=1,\ldots,m,\, \sigma \in G^{\mathrm{opp}}}])$. The closed immersion of W' is defined by the presentation $B[\{x_{i,\sigma}\}_{i=1,\ldots,m,\, \sigma \in G^{\mathrm{opp}}}]/((\sigma^{\#}(f_i))(x_{1,\sigma}, \ldots, x_{m,\sigma})_{i=1,\ldots,l,\, \sigma \in G^{\mathrm{opp}}})$ of $\mathrm{Spec}(W')$.

We try to find an affine A-scheme W and a B-isomorphism $\rho : W \otimes_A B \approx W'$ where under the isomorphism ρ, the Galois-operation on W' corresponds to the natural operation of $W \otimes_A B$ induced by the operation G on B. If we have such an isomorphism, W with $p_{\mathrm{id}} \circ \rho$ as universal element is the Weil-restriction of X' with respect to $S' \longrightarrow S$. (Unique up to a unique isomorphism.)

We think of W' with its concrete representation as immersed in ${\mathbb{A}_{\mathbb{B}}}^{mG^{\mathrm{opp}}}$. We are searching for a closed subscheme W^* of some affine B-space which is as closed subscheme defined over A and an isomorphism between W^* and W' which is Galois-invariant. (Where the Galois-operation on W^* is the one induced by the canonical one of the affine space.)

We know already that $\mathbf{Res}^B_A(X') \otimes_A B$ as constructed in Subsection 1.1.3 is such an affine scheme. It is embedded in $\mathbb{A}_B^{mn}$. The coordinate ring of $\mathbb{A}_B^{m\,G^{\text{opp}}}$ is the free B-algebra on $x_{i,\sigma}$, $i = 1, \dots, m, \sigma \in G^{\text{opp}}$ and the coordinate ring of $\mathbb{A}_B^{mn}$ is the free B-algebra on $x_{1,1}, \dots, x_{m,n}$.

The invertible matrix

$$\begin{pmatrix} \sigma^{\#}(\alpha_1) \\ \vdots \\ \sigma^{\#}(\alpha_n) \end{pmatrix}_{\sigma \in G^{\text{opp}}}$$

defines an isomorphism

$$\begin{aligned} \rho^{\#} : B[\{x_{i,\sigma}\}_{i=1,\dots,m,\, \sigma \in G^{\text{opp}}}] &\longrightarrow B[\{x_{i,j}\}_{i=1,\dots,m,\, j=1,\dots,n}] \\ x_{i,\sigma} &\mapsto \sigma^{\#}(\alpha_1)x_{i,1} + \cdots + \sigma^{\#}(\alpha_n)x_{i,n}. \end{aligned}$$

And this induces an isomorphism

$$\rho : \mathbb{A}_B^{mn} \longrightarrow \mathbb{A}_B^{m\,G^{\text{opp}}}.$$

Let $i = 1, \dots, l$. Then under $\rho^{\#}$, $\sigma^{\#}(f_i)(x_{1,\sigma}, \dots, x_{m,\sigma})$ is mapped to $\sigma^{\#}(\alpha_1)f_{i,1} + \cdots + \sigma^{\#}(\alpha_n)f_{i,n}$, where the $f_{i,j}$ are defined as in Subsection 1.1.3. As the matrix $(\alpha_{i,\sigma})_{i,\sigma}$ is invertible, the ideal generated by these elements for all $\sigma \in G^{\text{opp}}$ equals the ideal generated by $f_{i,1}, \dots, f_{i,n}$. Therefore, the ideal generated by $(\sigma^{\#}(f_i))(x_{1,\sigma}, \dots, x_{m,\sigma})$ for $i = 1, \dots, l$, $\sigma \in G^{\text{opp}}$ is mapped to the ideal generated by $f_{i,j}$ for $i = 1, \dots, l$, $j = 1, \dots, n$.

Thus ρ identifies the Weil-restriction W' with $\mathbf{Res}_A^B(X') \otimes_A B$ as constructed in Subsection 1.1.3. It is also Galois invariant, as can be seen as follows:

$$\rho^{\#}\widetilde{\tau}^{\#}(x_{i,\sigma}) = \rho^{\#}(x_{i,\sigma\tau}) = \tau^{\#}\sigma^{\#}(\alpha_1)x_{i,1} + \cdots + \tau^{\#}\sigma^{\#}(\alpha_n)x_{i,n} = \tau^{\#}\rho^{\#}(x_{i,\sigma})$$

Arithmetic becomes geometric operation

Let $S' \longrightarrow S$ be Galois with Galois group G. [6]

Let X be a quasi-projective S-scheme, $X' := X \times_S S'$. For $\tau \in G^{\text{opp}}$, let

$$s_\tau : W' = X'^{G^{\text{opp}}} \longrightarrow W' = X'^{G^{\text{opp}}}$$

be given on .-valued points by

$$(P_\sigma)_{\sigma \in G^{\text{opp}}} \mapsto (P_{\sigma\tau})_{\sigma \in G^{\text{opp}}}.$$

Then the Galois-operation on $W_{S'} = W' = X'^{G^{\text{opp}}}$ is given by $\boldsymbol{\tau} \mapsto \widetilde{\tau} = \tau s_\tau = s_\tau \tau$. where $\tau : X'^{G^{\text{opp}}} \longrightarrow X'^{G^{\text{opp}}}$ is the "canonical" arithmetical operation induced by base-change from $S' \longrightarrow S$.

For any S-scheme Z, G operates on $\mathfrak{R}\mathrm{es}_S^{S'}(X')(Z) = \mathrm{Hom}_{S'}(Z \times_S S', X \times_S S')$ by

$$\tau(P) = \tau P \tau^{-1}.$$

[6] For the moment and the next Lemma, $S' \longrightarrow S$ might also be a pro-Galois covering.

These operations define an automorphism of the functor $\mathcal{R}\mathrm{es}_S^{S'}(X')$ which we denote again by τ, and $G^{\mathrm{opp}} \longrightarrow \mathrm{Aut}(\mathcal{R}\mathrm{es}_S^{S'}(X'))$ is a group-homomorphism. Let $\mathcal{R}\mathrm{es}_S^{S'}(X')(Z)^G$ be the set of Galois-invariant elements, and let $\mathcal{R}\mathrm{es}_S^{S'}(.)^G$ be the functor defined by $\mathcal{R}\mathrm{es}_S^{S'}(X')^G(Z) := \mathcal{R}\mathrm{es}_S^{S'}(X')(Z)^G$.

Lemma 1.11 *The inclusion* $\mathrm{Hom}_S(-,X) \hookrightarrow \mathcal{R}\mathrm{es}_S^{S'}(X')$ *induces a bijection*

$$\mathrm{Hom}_S(-,X) \cong \mathcal{R}\mathrm{es}_S^{S'}(X')^G,$$

natural in X.

□

The automorphism τ of the functor $\mathcal{R}\mathrm{es}_S^{S'}(X')$ defines an S-automorphism of the representing object $\mathbf{Res}_S^{S'}(X')$ which we denote by a_τ.

We want to calculate how a_τ operates on $\mathbf{Res}_S^{S'}(X_{S'}) \times_S S' \cong \prod_{\sigma \in G^{\mathrm{opp}}} X_{S'} = X_{S'}^{G^{\mathrm{opp}}}$.

We have $\tau(u) = \tau(p_{\mathrm{id}}) = p_{\tau^{-1}}$ by (1.8). The S-morphism a_τ of $\mathbf{Res}_S^{S'}(X')$ is the $\mathbf{Res}_S^{S'}(X')$-valued point of $\mathbf{Res}_S^{S'}(X')$ which corresponds to $\tau(u)$. So $a_\tau = (\tau(u)^\sigma)_{\sigma \in G^{\mathrm{opp}}} = ((p_{\tau^{-1}})^\sigma)_{\sigma \in G^{\mathrm{opp}}} = (p_{\tau^{-1}\sigma})_{\sigma \in G^{\mathrm{opp}}}$ (The last equation is again (1.8).)

Lemma 1.12 a_τ *operates on .-valued points by* $(P_\sigma)_{\sigma \in G^{\mathrm{opp}}} \mapsto (P_{\tau^{-1}\sigma})_{\sigma \in G^{\mathrm{opp}}}$. *In particular, the group-homomorphism* $G \longrightarrow \mathrm{Aut}(\mathcal{R}\mathrm{es}_S^{S'}(X')) \simeq \mathrm{Aut}_S(\mathbf{Res}_S^{S'}(X'))$ *is injective.*

Compare this operation with the operation of s_τ!

Let X be a group-scheme. Then the map $P \mapsto \sum_{\sigma \in G^{\mathrm{opp}}} \sigma(P)$ defines a natural transformation $\mathcal{R}\mathrm{es}_S^{S'}(X') \longrightarrow \mathcal{R}\mathrm{es}_S^{S'}(X')(.)^G$ and thus by Lemma 1.11 a morphism

$$\mathcal{R}\mathrm{es}_S^{S'}(X') \longrightarrow \mathrm{Hom}_S(-,X), \tag{1.12}$$

which is natural in X. The composition $\mathrm{Hom}_S(-,X) \hookrightarrow \mathcal{R}\mathrm{es}_S^{S'}(X') \longrightarrow \mathrm{Hom}_S(-,X)$ is given by multiplication with $|G|$.

1.2 Pull-back of sheaves to the Weil-restriction

1.2.1 Pull-back of modules

Let S be connected and $S' \longrightarrow S$ étale, X' a quasi-projective S'-scheme, $W = \mathbf{Res}_S^{S'}(X')$. Let T' be as in Lemma 1.6 so that $W_{T'} \simeq \prod_\sigma \sigma^{-1}(X')$.

Let $\mathcal{L}$ be an quasi-coherent $\mathcal{O}_{X'}$-module on X'. Then $\mathcal{L}_{W_{T'}} := \bigotimes_\sigma p_\sigma^* \sigma^*(\mathcal{L})$ is an $\mathcal{O}_{W_{T'}}$-module with

$$\tilde{\tau}^{-1*} \bigotimes_\sigma p_\sigma^* \sigma^*(\mathcal{L}) \simeq \bigotimes_\sigma \tilde{\tau}^{-1*} p_\sigma^* \sigma^*(\mathcal{L}) \overset{(1.7)}{\simeq} \bigotimes_\sigma p^*_{\sigma\tau^{-1}} \tau^{-1*} \sigma^*(\mathcal{L}) \simeq$$
$$\bigotimes_\sigma p^*_{\sigma\tau^{-1}} (\sigma\tau^{-1})^*(\mathcal{L}) \simeq \bigotimes_\sigma p_\sigma^* \sigma^*(\mathcal{L}).$$

Let w_τ be the isomorphism from right to left. Then $\tau \mapsto w_\tau$ defines a 1-cocycle-datum for the $\mathcal{O}_{W_{S'}}$-module $\mathcal{L}_{W_{S'}}$. Thus $\mathcal{L}_{W_{S'}}$ is a G-sheaf. Now, by Proposition A.30, it “descends” to an $\mathcal{O}_{X'}$-module $\mathcal{L}_W$ on W.

This module is (up to unique isomorphism) independent of the choice of T'. For, assume the construction was performed with two different $f_1 : T_1' \longrightarrow S$, $f_2 : T_2' \longrightarrow S$. Call the resulting sheaves $\mathcal{L}_W^{(1)}$ and $\mathcal{L}_W^{(2)}$. Then there exists a $f_3 : T_3' \longrightarrow S$ (again Galois and connected) such that f_3 factors through f_1 and f_2. Now the pull-backs of $\mathcal{L}_W^{(1)}$ and $\mathcal{L}_W^{(2)}$ to $W \times_S T_3'$ are naturally isomorphic and thus so are $\mathcal{L}_W^{(1)}$ and $\mathcal{L}_W^{(2)}$.

Let S and thus S' be affine. By construction, if $\mathcal{L}$ is a very ample invertible sheaf, then $\mathcal{L}_{W_{T'}} = \bigotimes_\sigma p_\sigma^* \sigma^*(\mathcal{L})$ is very ample and so is $\mathcal{L}_W$. Since a sheaf is ample, if some power is very ample, $\mathcal{L}_W$ is ample, if $\mathcal{L}$ is ample.

The canonical embedding

Now let $S' \longrightarrow S$ be defined by a finite, separable extension of fields $K|k$ of degree n, let $L|K$ be a splitting field of $K|k$, and denote the Galois group of $L|k$ by G. Let X' be a separated quasi-projective K-scheme with a fixed immersion $X' \longrightarrow \mathbb{P}_K^m$.

Then for $\sigma : \mathrm{Spec}(L) \longrightarrow \mathrm{Spec}(K)$ (over $\mathrm{Spec}(k)$), $\sigma^{-1}(X)$ is immersed in $\mathbb{P}_L^m$, and via the Segre-embedding, W_L is immersed in $\mathbb{P}_L^{(m+1)^n-1}$. – We want to show that W is also immersed in $(m+1)^n - 1$-dimensional projective space. [7]

The immersion $X' \longrightarrow \mathbb{P}_K^m$ corresponds to a very ample sheaf $\mathcal{L}$ with global sections $M_0, \ldots, M_m$ which generate $\mathcal{L}$. The ring $\Gamma(X, \mathcal{L})$ is included in $\Gamma(\sigma^{-1}(X), \sigma^*(\mathcal{L}))$. If we identify $\Gamma(X, \mathcal{L})$ with its image, the M_i are again global sections which generate $\sigma^*(\mathcal{L})$.

Let i run through all maps

$$(\mathrm{Spec}(L) \longrightarrow \mathrm{Spec}(K) \text{ (over } \mathrm{Spec}(k)) \longrightarrow \{0, \ldots, m\}, \ \sigma \mapsto i_\sigma.$$

Then the M_i are global sections of $\sigma^*(\mathcal{L})$ which generate the sheaf. The Segre-embedding is defined by the $(m+1)^n$ global sections $\otimes_\sigma M_{i_\sigma}$ of $\mathcal{L}_{W_L} = \bigotimes_\sigma \sigma^*(\mathcal{L})$, which generate the sheaf.

[7] The following argumentation is inspired by A.Weil's original use of the Weil-restriction in [We-F].

Now, $\Gamma(W,\mathcal{L}_W)$ is included in $\Gamma(W_L,\mathcal{L}_{W_L})$, and we want to find $(m+1)^n$ global sections of $\mathcal{L}_W$ such that all $\otimes_\sigma M_{i_\sigma}$ are linear combinations of these (and vice versa).

The L-module $\mathcal{L}_{W_L}$ is isomorphic to the pull-back of $\mathcal{L}_W$ to W_L. For the following argumentation we will identify these two sheaves on W_L. There is a Galois-operation on $\Gamma(W_L,\mathcal{L}_{W_L})$ and

$$\Gamma(W_L,\mathcal{L}_{W_L})^G = \Gamma(W,\mathcal{L}_W).$$

(See the remark following Proposition A.30 for details.) Conversely,

$$\Gamma(W_L,\mathcal{L}_{W_L}) \simeq \Gamma(W,\mathcal{L}_W)\otimes_k L$$

Here we use that "taking global sections commutes with flat base-change", i.e cohomology commutes with flat base-change" for the special case of 0-dimensional cohomology groups; see [Ha, III, Proposition 9.3].

More generally, if H is any subgroup of G and L^H the corresponding fixed field,

$$\Gamma(W_L,\mathcal{L}_{W_L})^H \simeq \Gamma(W,\mathcal{L}_W)\otimes_k L^H. \tag{1.13}$$

Call the $(m+1)^n$ global sections $\otimes_\sigma(M_{i_\sigma})$ of $\mathcal{L}_{W_L}$ P_l, $l=1,\dots,(m+1)^n$. The Galois group G operates on the set of P_l.

For some l, let G_l be the stabilizer of P_l in G, k_l the fixed field of G_l in L, let $[k_l:k]=d$. Choose a basis $\beta_1,\dots,\beta_d$ of $k_l|k$. Then by (1.13), there exist $Q_1^{(l)},\dots,Q_d^{(l)}\in\Gamma(W,\mathcal{L}_W)$ with

$$P_l=\sum_{j=1}^d \beta_j\, Q_j^{(l)}.$$

For $\boldsymbol{\sigma}\in G$, let $\sigma^\#$ denote the corresponding operation on $\mathcal{L}_{W_L}$. The orbit of P_l under G has exactly d elements and $\tau^\#(P_l)=\sum_{j=1}^d \tau^\#(\beta_j)\,Q_j^{(l)}$ for all $\boldsymbol{\tau}\in G$.

Choose from every orbit of the operation of G on the set of L_l one representative. Call this set $P_{l_1},P_{l_2},\dots$. Then the $Q_j^{(l_i)}$ are $(m+1)^n$ global section of $\mathcal{L}_W$ which span the same linear space in $\Gamma(W_L,\mathcal{L}_{W_L})$ as the P_l do.

We obtain an immersion $W\longrightarrow\mathbb{P}_k^{(m+1)^n-1}$ which is canonical up to an isomorphism of $\mathbb{P}_k^{(m+1)^n-1}$. Moreover, after base-change and identification of W_L with $\prod_{\sigma\in G}\sigma^{-1}(X)$, this immersion is up to an isomorphism of $\mathbb{P}_k^{(m+1)^n-1}$ the Segre embedding.

Proposition 1.13 *Let $K|k$ be a finite separable extension of fields. Let X' be a separated quasi-projective K-scheme with a fixed immersion $X'\longrightarrow\mathbb{P}_K^m$. Then the Weil-restriction of X' with respect to $K|k$ is immersed in $\mathbb{P}_k^{(m+1)^n-1}$. This immersion is canonical up to an isomorphism of $\mathbb{P}_k^{(m+1)^n-1}$.*

Pull-back of Weil-divisors

Let $K|k$ be a separable field extension, let $L|k$ be a splitting field. Let X' be a nonsingular k-variety. Then Weil-divisor classes correspond to classes of invertible sheaves. Let the invertible sheaf $\mathcal{L}$ by defined by the effective Weil divisor B which we regard as (not necessarily reduced) closed subscheme of X'. Then by Proposition A.29, the sheaf $\mathcal{L}_{W_L}$ is defined by the closed subscheme $D := \sum_\sigma p_\sigma^{-1}\sigma^{-1}(B)$. The operation of $\widetilde{\sigma}$ on W_L' induces an operation on D. The immersion $D \longrightarrow W_L$ is now invariant under this operation, and D descends. It defines the sheaf $\mathcal{L}(B)_W$ on W.

1.2.2 The Picard functor and the Picard scheme

We include the following subsection mainly for notational reasons.

Let k be a field, let X be a geometrically integral non-singular projective k-variety with a k-rational point P_0.

Definitions We denote the isomorphism class of an invertible sheaf $\mathcal{L}$ on some k-scheme by $\overline{\mathcal{L}}$. For any scheme Y, the isomorphism classes of invertible sheaves on Y form a set, and with the operation of the tensor product, this set is an abelian group, the so-called *Picard group* of Y, denoted $\mathrm{Pic}(Y)$.

Let $\mathcal{P}\mathrm{ic}(X)$ be the contravariant group-functor which is defined as follows:

For any k-scheme Z, let $p_Z : X \times_k Z \longrightarrow Z$ be the projection. Let $\mathcal{P}\mathrm{ic}(X)(Z) := \mathrm{Pic}(X \times_k Z)/p_Z^*\mathrm{Pic}(Z)$. We will denote this quotient by $\mathrm{Pic}(X \times_k Z)/\mathrm{Pic}(Z)$ and its elements by $\overline{\overline{\mathcal{L}}}, \overline{\overline{\mathcal{M}}}$, etc.

For any morphism $\alpha : Y \longrightarrow Z$, $\mathcal{P}\mathrm{ic}(X)(\alpha)$ is defined by $(\mathrm{id}_X \times_k \alpha)^* : \mathrm{Pic}(X \times_k Z)/\mathrm{Pic}(Z) \longrightarrow \mathrm{Pic}(X \times_k Y)/\mathrm{Pic}(Y)$. (Consistently, we would have to write $\overline{(\mathrm{id}_X \times_k \alpha)^*}$ or even more accurately $\overline{\overline{(\mathrm{id}_X \times_k \alpha)^*}}$ but we omit the bar.)

Note that $p_Z \circ (P_0 \times_k \mathrm{id}_Z) = \mathrm{id}_Z$ implies that $(P_0 \times_k \mathrm{id}_Z)^* \circ p_Z^* = \mathrm{id}_{\mathrm{Pic}(Z)}$. Thus $\mathrm{Pic}(X \times_k Z)/p_Z^*\mathrm{Pic}(Z)$ is functorially isomorphic to the subgroup of $\overline{\mathcal{M}} \in \mathrm{Pic}(X \times_k Z)$ such that $(P_0 \times_K \mathrm{id}_Z)^*(\overline{\mathcal{M}}) = 0$.

The association $X \mapsto \mathcal{P}\mathrm{ic}(X)$ defines a contravariant functor from the category of punctured geometrically integral projective k-varieties to the category of contravariant functors from the category of k-schemes to the category of abelian groups. If $\alpha : X \longrightarrow Y$ is a morphism, we denote $\mathcal{P}\mathrm{ic}(\alpha) : \mathcal{P}\mathrm{ic}(Y) \longrightarrow \mathcal{P}\mathrm{ic}(X)$ by α^*.

Proposition 1.14 *Under the above conditions on X, $\mathcal{P}\mathrm{ic}(X)$ is represented by a k-group-scheme* $\mathbf{Pic}(X)$ *which is locally of finite type.*

Proof First see [BLR, 8.1, Proposition 4] and then [BLR, 8.2, Theorem 3]. □

Let $\overline{\mathcal{P}} \in \mathrm{Pic}(X \times_k \mathbf{Pic}(X))$ be a representative of the universal element $\overline{\overline{\mathcal{P}}} \in \mathrm{Pic}(X \times_k \mathbf{Pic}(X))/\mathrm{Pic}(\mathbf{Pic}(X))$.

Let $\mathcal{P}\mathrm{ic}^0(X)$ be defined by: For any k-scheme Z, let $\mathcal{P}\mathrm{ic}^0(X)(Z)$ be the subgroup of $\overline{\overline{\mathcal{M}}} \in \mathcal{P}\mathrm{ic}(X)(Z)$ for which there exists a *connected* k-scheme T with two Z-rational points $\alpha, \beta : Z \longrightarrow T$ and an $\overline{\overline{\mathcal{N}}} \in \mathcal{P}\mathrm{ic}(X)(T)$ such that $(\mathrm{id}_X \times_k \alpha)^*(\overline{\overline{\mathcal{N}}}) = 0$ and $(\mathrm{id}_X \times_k \beta)^*(\overline{\overline{\mathcal{N}}}) = \overline{\overline{\mathcal{M}}}$.

Definition The *Picard scheme* $\mathbf{Pic}^0(X)$ is the identity component of $\mathbf{Pic}(X)$.

It is immediate that $\mathbf{Pic}^0(X)$ with the restriction of $\overline{\overline{\mathcal{P}}}$ represents $\mathcal{P}\mathrm{ic}^0(X)$. We denote the restriction of $\overline{\mathcal{P}}$ still by $\overline{\mathcal{P}}$.

Because $\mathbf{Pic}^0(X)$ has a k-rational point, it is also geometrically connected; see Lemma A.28.

Proposition 1.15 *Again under the above conditions on X, $\mathbf{Pic}^0(X)$ is a* projective *k-group-scheme.*

Proof See [BLR, 8.4, Theorem 3]. □

In the case that X is a curve, the Picard scheme is geometrically reduced, thus it is an abelian variety, called the *Jacobian variety* of X, denoted in this work by $J(X)$; see [Mi-J] for a detailed account about the Jacobian variety.

Base change

Let $k \longrightarrow \lambda$ be a morphism of fields. Then X_λ has a λ-rational point, and for all λ-schemes Z, $\mathrm{Pic}(X_\lambda \times_\lambda Z)/\mathrm{Pic}(Z) \simeq \mathrm{Pic}(X \times_k Z)/\mathrm{Pic}(Z)$, therefore $\mathcal{P}\mathrm{ic}(X_\lambda) \simeq \mathcal{P}\mathrm{ic}(X)_\lambda$.

Let $\overline{\mathcal{P}} \in \mathrm{Pic}(X \times_k \mathbf{Pic}(X))$ be the representative of the universal element defined above, let $\overline{\mathcal{P}_\lambda}$ be the pull-back of $\overline{\mathcal{P}}$ to $\mathrm{Pic}(X \times_k \mathbf{Pic}(X) \otimes_k \lambda) \simeq \mathrm{Pic}(X_\lambda \times_\lambda \mathbf{Pic}(X)_\lambda)$. This represents an element $\overline{\overline{\mathcal{P}_\lambda}} \in \mathrm{Pic}(X_\lambda \times_\lambda \mathbf{Pic}(X)_\lambda)/\mathrm{Pic}(\mathbf{Pic}(X)_\lambda)$. With this element, $\mathcal{P}\mathrm{ic}(X_\lambda)$ is represented by $\mathbf{Pic}(X)_\lambda$.

An important special case of this is the following:

Let $K|k$ be a Galois field extension, $\boldsymbol{\sigma} \in \mathrm{Gal}(K|k)$. Let X' be a non-singular projective K-variety with a K-rational point. Consider X'/K and the corresponding automorphism $\sigma : \mathrm{Spec}(K) \longrightarrow \mathrm{Spec}(K)$ as a special case of the above result. It follows that $\mathcal{P}\mathrm{ic}(\sigma^{-1}(X'))$ is represented by $(\sigma^{-1}(\mathbf{Pic}(X')), \sigma^*(\overline{\overline{\mathcal{P}}}))$, and analogously, $\mathcal{P}\mathrm{ic}^0(\sigma^{-1}(X'))$ is represented by $\sigma^{-1}(\mathbf{Pic}(X')^0)$.

1.2.3 The Picard functor of the Weil-restriction

In this subsection we study the relationship between the Picard-functor and the Weil-restriction.

Let $K|k$ be a finite Galois field extension, X a geometrically integral, non-singular, projective k-variety with a k-rational point.

Since $\mathbf{Pic}(X)$ is the disjoint union of projective schemes, its Weil-restriction exists. By Lemma 1.11, we have a natural transformation

$$\mathrm{Hom}_k(-,\mathbf{Pic}(X)) \simeq \mathcal{R}\mathrm{es}_k^K(\mathbf{Pic}(X)_K)^G \simeq \mathcal{R}\mathrm{es}_k^K(\mathbf{Pic}(X_K))^G, \tag{1.14}$$

and by (1.12) we have a morphism

$$\mathcal{R}\mathrm{es}_k^K(\mathbf{Pic}(X_K)) \longrightarrow \mathrm{Hom}_k(-,\mathbf{Pic}(X)) \tag{1.15}$$

We define a Galois-operation on the functor $\mathcal{R}\mathrm{es}_k^K(\mathcal{P}\mathrm{ic}(X_K))$: For $\boldsymbol{\sigma} \in G$, let $\sigma : X \times_k Z \otimes_k K \simeq (X \otimes_K \times_K Z_K)$ be the "natural" operation induced by base-change, i.e. $\sigma = \mathrm{id}_X \times_k \mathrm{id}_Z \times_k \sigma$ or – what is the same – $\sigma = (\mathrm{id}_X \times_k \sigma) \times_K (\mathrm{id}_Z \times_k \sigma)$. Now let $\boldsymbol{\sigma} \in G$ operate on $\mathrm{Pic}(X \times_k Z \otimes_k K))/\mathrm{Pic}(Z \otimes_k K) \simeq \mathrm{Pic}((X \otimes_k K) \times_K (Z \otimes_k K))/\mathrm{Pic}(Z \otimes_k K)$ by σ^{-1^*}.

Lemma 1.16 *The Galois-operation on $\mathcal{R}\mathrm{es}_k^K(\mathbf{Pic}(X_K))$ corresponds to the Galois-operation on the functor $\mathcal{R}\mathrm{es}_k^K(\mathcal{P}\mathrm{ic}(X_K))$.*

Proof Let $\overline{\mathcal{P}_K} \in \mathrm{Pic}(X_K \times_K \mathbf{Pic}(X)_K)$ be the representative of the universal element of $\mathcal{P}\mathrm{ic}(X_K)$ constructed above. Then $\overline{\mathcal{P}_K}$ by construction is invariant under the Galois-operation.

Let $\alpha : Z \otimes_k K \longrightarrow \mathbf{Pic}(X_K)$ be a K-morphism, $\boldsymbol{\sigma} \in G$. Then by definition, $\mathrm{id}_{X_K} \times_K \sigma(\alpha) = \sigma \circ (\mathrm{id}_{X_K} \times_K \alpha) \circ \sigma^{-1}$. Thus

$$\begin{gathered}(\mathrm{id}_{X_K} \times_K \sigma(\alpha)\,)^*\,(\overline{\overline{\mathcal{P}_K}}) = \sigma^{-1^*}\,(\mathrm{id}_{X_K} \times_K \alpha)^*\,\sigma^*\,(\overline{\overline{\mathcal{P}_K}}) = \\ \sigma^{-1^*}\,(\mathrm{id}_{X_K} \times_K \alpha)^*\,(\overline{\overline{\mathcal{P}_K}})\end{gathered}$$

□

Let $q_K : X_K \longrightarrow X$ be the projection. Then it follows from (1.14) that q_K^* induces an isomorphism

$$q_K^* : \mathcal{P}\mathrm{ic}(X) \xrightarrow{\sim} \mathcal{R}\mathrm{es}_k^K(\mathcal{P}\mathrm{ic}(X_K))^G. \tag{1.16}$$

Note that this means in particular that every sheaf on X_K whose *isomorphism class* is invariant under G descends to a sheaf on X. This is a stronger statement than Galois-descent of quasi-coherent modules.

Let $\overline{\overline{\mathcal{M}'}} \in \mathcal{R}\mathrm{es}_k^K(\mathcal{P}\mathrm{ic}(X_K))(Z) = \mathcal{P}\mathrm{ic}(X_K)(Z \times_k K)$. Then $\sum_{\sigma \in G^{\mathrm{opp}}} \sigma^*(\overline{\overline{\mathcal{M}'}}) \in \mathcal{R}\mathrm{es}_k^K(\mathcal{P}\mathrm{ic}(X_K))^G$, thus there exists an $\overline{\overline{\mathcal{M}}} \in \mathcal{P}\mathrm{ic}(X)(Z)$ with $(q_K \times_k \mathrm{id}_Z)^*(\overline{\overline{\mathcal{M}}}) = \overline{\overline{\mathcal{M}'}}$.

Definition We call the element $\overline{\overline{\mathcal{M}}}$ just defined the *norm* of $\overline{\overline{\mathcal{M}'}}$ and denote it by $\mathrm{N}(\overline{\overline{\mathcal{M}'}})$. [8]

We get a natural transformation

$$\mathcal{N} : \mathcal{R}\mathrm{es}_k^K(\mathcal{P}\mathrm{ic}(X_K)) \longrightarrow \mathcal{P}\mathrm{ic}(X),$$

which we also call *norm*.

Via the representing objects, this natural transformation corresponds to (1.15).

[8] In [EGA II, 6.5], the *norm* of an invertible sheaf is defined in a more general situation. Note however that our definition applies for *classes* of sheaves.

Now let X' be any geometrically integral, non-singular, projective K-variety with a K-rational point P_0, let $W = \mathbf{Res}_k^K(X')$ be the Weil-restriction of X' with respect to $K|k$. By definition of W, it has a k-rational point.

Consider the natural transformation

$$\begin{tikzcd}
\mathcal{T} : \mathcal{R}\mathrm{es}_k^K(\mathcal{P}\mathrm{ic}(X')) \arrow[r, "\mathcal{R}\mathrm{es}_k^K(u^*)"] & \mathcal{R}\mathrm{es}_k^K(\mathcal{P}\mathrm{ic}(W_K)) \arrow[d, "\overline{\overline{\mathcal{M}'}} \mapsto \bigotimes_{\sigma \in G^{\mathrm{opp}}} \sigma^*(\overline{\overline{\mathcal{M}'}})"] \arrow[dd, bend right=60, "\mathcal{N}"'] \\
 & \mathcal{R}\mathrm{es}_k^K(\mathcal{P}\mathrm{ic}(W_K))^G \arrow[d, "\sim"', "{q_K^*}^{-1}"] \\
 & \mathcal{P}\mathrm{ic}(W).
\end{tikzcd} \tag{1.17}$$

Lemma 1.17 *$\mathcal{T}$ is injective.*

Proof Let Z be a k-scheme. Then $\boldsymbol{\tau} \in G$ operates on $\mathrm{Pic}(W_K \times_K Z_K) \simeq \mathrm{Pic}(W \times_k Z \otimes_k K)$ by τ^{-1*}. (Where τ is the "natural" operation on $W \times_k Z \otimes_k K$.)

Now $(W \times_k Z)_K \simeq \prod_\sigma \sigma^{-1}(X' \times_K Z_K)$. Under this isomorphism, τ operates on $\mathrm{Pic}(\prod_\sigma \sigma^{-1}(X' \times_K Z_K))$ by $\widetilde{\tau}^{-1*}$, where $\widetilde{\tau}$ is the "twisted" operation as in the construction of the Weil-restriction in the Galois case.

Under the identification of $(W \times_k Z)_K$ with $\prod_\sigma \sigma^{-1}(X' \times_K Z_K)$, $\sum_{\sigma \in G^{\mathrm{opp}}} \sigma^*(.) \circ \mathcal{R}\mathrm{es}_k^K(u^*) : \mathcal{R}\mathrm{es}_k^K(\mathcal{P}\mathrm{ic}(X'))(Z) \longrightarrow \mathcal{R}\mathrm{es}_k^K(\mathcal{P}\mathrm{ic}(W_K))^G(Z)$ is given by

$$\mathrm{Pic}(X' \times_K Z_K)/\mathrm{Pic}(Z_K) \longrightarrow (\mathrm{Pic}(\prod_{\sigma \in G^{\mathrm{opp}}} \sigma^{-1}(X' \times_K Z_K))/\mathrm{Pic}(Z_K))^G$$
$$\overline{\overline{\mathcal{M}}} \mapsto \sum_{\sigma \in G^{\mathrm{opp}}} \widetilde{\sigma}^*(p_{\mathrm{id}}^*(\overline{\overline{\mathcal{M}}})) = \sum_{\sigma \in G^{\mathrm{opp}}} p_\sigma^*(\sigma^*(\overline{\overline{\mathcal{M}}})).$$

By assumption X' has a K-rational point P_0, and $\sigma^{-1}(P_0)$ is a k-rational point of $\sigma^{-1}(X')$. These rational points define a closed immersion $\iota = (\iota_\sigma)_\sigma : X' \longrightarrow \prod_\sigma \sigma^{-1}(X')$, given by $\iota_{\mathrm{id}} = \mathrm{id}_{X'}$, $\iota_\sigma = \sigma^{-1}(P)$ for $\sigma \neq \mathrm{id}$. Now $(\iota \times_k \mathrm{id}_Z)^* \circ \sum_{\sigma \in G^{\mathrm{opp}}} \sigma^*(.) \circ (u \times_k \mathrm{id}_Z)^*$ is the identity on $\mathcal{R}\mathrm{es}_k^K(\mathcal{P}\mathrm{ic}(X'))(Z)$. □

The functor $\mathcal{T}$ restricts to a natural transformation $\mathcal{T} : \mathcal{R}\mathrm{es}_k^K(\mathcal{P}\mathrm{ic}^0(X')) \longrightarrow \mathcal{P}\mathrm{ic}^0(\mathcal{R}\mathrm{es}_k^K(X'))$, and this induces a morphism between the corresponding representing objects.

$$\mathbf{T} : \mathbf{Res}_k^K(\mathbf{Pic}^0(X')) \longrightarrow \mathbf{Pic}^0(\mathbf{Res}_k^K(X'))$$

After the base change $K|k$, $\mathbf{T}$ becomes the canonical morphism

$$\mathbf{U} : (\prod_{\sigma \in G^{\mathrm{opp}}} \sigma^{-1}(\mathbf{Pic}^0(X')) \longrightarrow \mathbf{Pic}^0(\prod_{\sigma \in G^{\mathrm{opp}}} \sigma^{-1}(X'))),$$

induced by $p_\sigma^* : \sigma^{-1}(\mathbf{Pic}^0(X')) \longrightarrow \mathbf{Pic}^0(\prod_\sigma \sigma^{-1}(X'))$.

We are interested whether $\mathcal{T}$ or – what is the same – $\mathbf{T}$ is an isomorphism. We only have to check this for $\mathbf{U}$ or $\mathbf{U} \otimes_K \mathrm{id}_{\overline{K}}$.

The phrase "smooth proper global lifting" used in the following theorem is defined in Subsection A.1.1. Under this condition, $\mathbf{U} \otimes_K \mathrm{id}_{\overline{K}}$ is an isomorphism of abelian varieties; see Proposition A.4. It thus follows the following theorem.

Theorem 1 *Let $K|k$ be a finite Galois field extension, let X' be an integral non-singular projective K-variety with a K-rational point. Assume that* $\mathrm{char}(k) = 0$ *or that $X'_{\overline{K}}$ has a smooth proper global lifting. Then $\mathbf{T} : \mathbf{Res}_k^K(\mathbf{Pic}^0(X')) \longrightarrow \mathbf{Pic}^0(\mathbf{Res}_k^K(X'))$ is an isomorphism of abelian varieties.*

Corollary 1.18 *Let X' be a geometrically integral non-singular projective K-curve with a K-rational point. Then $\mathbf{T}$ is an isomorphism of abelian varieties.*

Proof If $\mathrm{char}(k) > 0$, every such curve has a smooth, proper global lifting; see [Po, Satz 10.1]. □

Corollary 1.19 *Let X' be a curve as above. Then* $\mathrm{N} \circ u^* : \mathrm{Pic}^0(X') \longrightarrow \mathrm{Pic}^0(\mathbf{Res}_k^K(X'))$ *is an isomorphism.*

1.3 Weil-restrictions of abelian varieties

In this section, we study first properties of the Weil-restriction of abelian varieties with respect to a finite separable field extension. In the next chapter, we will study the Weil-restriction of old abelian varieties – i.e. abelian varieties which are defined over k – more in depth.

Let $K|k$ be a separable extension of fields, A' an abelian K-variety. Let W be the Weil-restriction of A' with respect to $K|k$. Then

$$W_{k^{\mathrm{sep}}} \simeq \prod_{\substack{\sigma : \mathrm{Spec}(k^{\mathrm{sep}}) \longrightarrow \mathrm{Spec}(K) \\ (\text{over } \mathrm{Spec}(k))}} \sigma^{-1}(A'),$$

thus W is also an abelian variety.

1.3.1 Weil-Restrictions and dual abelian varieties

Let $K|k$ be Galois, A' an abelian K-variety.

Since the product of a dual abelian variety of a product of abelian varieties is the product of the duals, the morphism $\mathbf{U}$ on the previous page is an isomorphism. Thus the morphism $\mathbf{T}$ defined in the last subsection is an isomorphism.

Proposition 1.20 *Let $K|k$ be a finite Galois field extension, let A' be an abelian variety. Then $\mathbf{T} : \mathbf{Res}_k^K(\widehat{A'}) \longrightarrow \widehat{\mathbf{Res}_k^K}(A')$ is an isomorphism of abelian varieties.*

□

1.3.2 The Galois-operation on geometric points

The following Proposition is well known; see for example [Mi-AA, par. 1].

Proposition 1.21 *Let k be perfect. The Galois-operation on $\mathbf{Res}_k^K(A')(\overline{K})$ is the induced representation of the one of $A'(\overline{K})$*

$$\mathbf{Res}_k^K(A')(\overline{K}) \simeq \mathbf{Ind}_{\mathbb{Z}[\mathrm{Gal}(\overline{K}|K)]}^{\mathbb{Z}[\mathrm{Gal}(\overline{K}|k)]}(A'(\overline{K}))$$

and the same is true for the Tate-module

$$T_l(\mathbf{Res}_k^K(A')(\overline{K})) \simeq \mathbf{Ind}_{\mathbb{Z}_l[\mathrm{Gal}(\overline{K}|K)]}^{\mathbb{Z}_l[\mathrm{Gal}(\overline{K}|k)]}(T_l(A'_{\overline{K}}))$$

for every prime l.

In particular, if $K|k$ is an extension of finite fields, the characteristic polynomials of the relative Frobenius morphisms are related by

$$\chi_{\mathbf{Res}_k^K(A')/k}(X) = \chi_{A'/K}(X^n).$$

Proof We only show the first isomorphism, the proof of the second is analogous.

The Galois-operation of $\mathrm{Gal}(\overline{K}|k)$ on $\mathbf{Res}_k^K(A')(\overline{K}) \simeq \prod_\sigma \sigma^{-1}(A')(\overline{K})$ is given by $\boldsymbol{\tau} \mapsto ((P_\sigma)_\sigma \mapsto (\tau(P_{\sigma\tau}))_\sigma)$.

Let $\iota^\# : K \hookrightarrow \overline{K}$ be the inclusion, corresponding to $\iota : \mathrm{Spec}(\overline{K}) \longrightarrow \mathrm{Spec}(K)$. The immersion $\iota^{-1}(A') \hookrightarrow \prod_\sigma \sigma^{-1}(A') \simeq W_K$ to the factor "ι" induces an injection $A'(\overline{K}) \hookrightarrow \prod_\sigma \sigma^{-1}(A')(\overline{K}) \simeq W_K(\overline{K})$ which is compatible with the operation of $\mathbb{Z}[\mathrm{Gal}(\overline{K}|K)]$. By the universal property of the induced representation, we have a $\mathbb{Z}[\mathrm{Gal}(\overline{K}|k)]$-module-homomorphism

$$\mathbf{Ind}_{\mathbb{Z}[\mathrm{Gal}(\overline{K}|K)]}^{\mathbb{Z}[\mathrm{Gal}(\overline{K}|k)]}(A'(\overline{K})) \longrightarrow \mathbf{Res}_k^K(A')(\overline{K}). \ (*)$$

Now for every inclusion $\sigma^\# : K \hookrightarrow \overline{K}$ (over k), let $\boldsymbol{\sigma'}$ be a continuation to a $\overline{K}$-automorphism (i.e. $\sigma^\# = \boldsymbol{\sigma'}\iota^\# : K \longrightarrow \overline{K}$ or – what is the same – $\sigma = \iota\sigma' : \mathrm{Spec}(\overline{K}) \longrightarrow \mathrm{Spec}(K)$).

On the left-hand side of (*), every element has a unique representation in the form $\sum_\sigma \sigma'(P_\sigma)$ with $P_\sigma \in A'(\overline{K})$. Such an element is mapped to the element $(\sigma'(P_\sigma))_\sigma$. Also every element of the left-hand side has this form for unique P_σ.

We thus have an isomorphism. □

1.3.3 The functor "Weil-restriction"

We have already seen that $\mathcal{R}\mathrm{es}_k^K$ is a functor and so is $\mathbf{Res}_k^K$. It restricts to a functor from the category of abelian K-varieties to the category of abelian k-varieties which respects the addition.

For abelian K-varieties A', B', the homomorphism of abelian groups $\mathbf{Res}_k^K$: $\mathrm{Hom}_K(A', B') \longrightarrow \mathrm{Hom}_k(\mathbf{Res}_k^K(A'), \mathbf{Res}_k^K(B'))$ extends canonically to a homomorphism $\mathbf{Res}_k^K : \mathrm{Hom}_K^0(A', B') \longrightarrow \mathrm{Hom}_k^0(\mathbf{Res}_k^K(A'), \mathbf{Res}_k^K(B'))$. Thus the functor $\mathbf{Res}_k^K$ extends to a functor from the "category of abelian K-varieties up to isogeny" to the category of abelian "category of abelian k-varieties up to isogeny". [9]

In particular, $\mathbf{Res}_k^K$ is a ring-homomorphism from $\mathrm{End}_K(A')$ to $\mathrm{End}_k(\mathbf{Res}_k^K(A'))$ and from $\mathrm{End}_K^0(A')$ to $\mathrm{End}_k^0(\mathbf{Res}_k^K(A'))$.

Let $K|k$ be Galois. Let A', B' be abelian K-varieties. Then

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

see equation (A.3) in Subsection A.2.3.

Let $\alpha : A' \longrightarrow B'$ be a morphism. Then by (1.11), $\mathbf{Res}_k^K(\alpha)\otimes_k \mathrm{id}_K$ is given by the diagonal "matrix" $(\sigma^{-1}(\alpha)\delta_{\sigma,\nu})_{\sigma,\nu\in G^{\mathrm{opp}}} \in \bigoplus_{\sigma,\nu\in G^{\mathrm{opp}}} \mathrm{Hom}_K(\nu^{-1}(A'), \sigma^{-1}(B'))$.

Now let $\alpha : A' \longrightarrow B'$ be an isogeny. Then $\mathbf{Res}_k^K(\alpha) : \mathbf{Res}_k^K(A') \longrightarrow \mathbf{Res}_k^K(B')$ is also an isogeny.

For every k-scheme Z, we have the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \ker(\alpha)(Z\otimes_k K) \arrow[r] \arrow[d, no head, "\sim"] & A'(Z\otimes_k K) \arrow[r] \arrow[d, no head, "\sim"] & B'(Z\otimes_k K) \arrow[d, no head, "\sim"] \\
0 \arrow[r] & \mathbf{Res}_k^K(\ker(\alpha))(Z) \arrow[r] & \mathbf{Res}_k^K(A')(Z) \arrow[r] & \mathbf{Res}_k^K(B')(Z).
\end{tikzcd}$$

Since the first row is exact (in the category of abelian groups), so is the last. Thus the kernel of the isogeny $\mathbf{Res}_k^K(\alpha)$ is $\mathbf{Res}_k^K(\ker(\alpha))$.

1.3.4 Weil-restrictions of a polarized abelian varieties

Let $K|k$ be a Galois field extension, A' an abelian K-variety, $\widehat{A'}$ the dual abelian variety. By Proposition 1.20, $\mathbf{Res}_k^K(\widehat{A'})$ is (canonically isomorphic to) the dual abelian variety of $\mathbf{Res}_k^K(A')$.

Let $\varphi : A' \longrightarrow \widehat{A'}$ be a polarization of A', defined by an ample sheaf $\mathfrak{L}$ on $A'_{\overline{K}}$, i.e. $\varphi\otimes_K \mathrm{id}_{\overline{K}} = \phi_{\mathfrak{L}} : A'_{\overline{K}} \longrightarrow \widehat{A'}_{\overline{K}}$. [10] As above, this induces an isogeny

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

which has by the above remarks kernel $\mathbf{Res}_k^K(\ker(\varphi))$. We show now that this morphism is again a polarization.

[9] The *category of abelian k-varieties up to isogeny* consists of all abelian k-varieties, where for two abelian k- varieties A and B, the set of morphisms is $\mathrm{Hom}_k^0(A,B)$; cf. [Mu, par. 19], see also Subsection A.2.1.

[10] For a polarization φ of A', we do not require that there exists a sheaf defined over K which defines φ; see Subsection A.2.2 for details.

Let $\sigma \in G^{\mathrm{opp}}$. As at the end of Subsection 1.2.2, 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 $\sigma'^{\#}|_K = \sigma^{\#}$. Then by Lemma A.9, $\varphi^\sigma \otimes_K \mathrm{id}_{\overline{K}} = \phi_{\mathfrak{L}}^{\sigma'} = \phi_{\sigma'^*(\mathfrak{L})}$. (In particular, the class of $\sigma'^*(\mathfrak{L})$ in the Néron-Severi group is independent of the choice of σ'.)

After base-change, we get

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

This is a "product polarization" defined by the ample sheaf

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

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

If one starts with an ample sheaf $\mathfrak{L}$ on A', then the polarization $\mathbf{Res}_k^K(\varphi)$ is defined by the ample sheaf $\mathfrak{L}_{W_K} := \bigotimes_\sigma \widetilde{\sigma}^* p_{\mathrm{id}}^*(\mathfrak{L})$ on W_K. The class of $\mathfrak{L}_{W_K}$ in the Picard group is invariant under the Galois-operation and thus this construction defines an ample sheaf on W. (This follows also directly from the results in Subsection 1.2.1.)

Proposition 1.22 *Let $K|k$ be a finite Galois field extension, A' an abelian variety over K. If φ is a (principal) polarization on A' (defined by a sheaf over K), then $\mathbf{Res}_k^K(\varphi)$ is a (principal) polarization on $\mathbf{Res}_k^K(A')$ (defined by a sheaf over k).*

Thus "Weil-restriction" is a functor from the category of polarized abelian K-varieties (with polarizations defined by a sheaf over K) [11] to the category of polarized abelian k-varieties (with polarizations defined by a sheaf over k). The images of principally polarized abelian K-varieties are principally polarized.

1.3.5 Weil-restrictions of abelian varieties over finite fields [12]

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

We now study the endomorphism algebra [13] and the isogeny decomposition of W.

In the next chapter, we will study the same question for Weil-restrictions of abelian varieties with respect to an arbitrary Galois extension $K|k$ under the assumption that the abelian K-variety A' is defined over k.

[11] For definition of the category of polarized abelian varieties see Subsection A.2.2 in the appendix.

[12] This subsection is joint work with N.Naumann.

[13] Recall the following definitions: The *endomorphism ring* of an abelian variety A over a field k is the ring of endomorphisms of A over k, i.e. the endomorphisms of $A_{\overline{k}}$ defined over k. It is denoted by $\mathrm{End}_k(A)$. The *endomorphism algebra* of A is the ring $\mathrm{End}_k^0(A) := \mathrm{End}_k(A) \otimes_{\mathbb{Z}} \mathbb{Q}$.

In the following, we make use of various concepts of "Frobenius morphisms"; see Subsection A.3.4 for details.

Identify $\mathrm{Gal}(K|k)$ with its dual and denote by $\sigma_k^K \in \mathrm{Gal}(K|k)$ the Frobenius automorphism, defining a $\mathrm{Spec}(k)$-automorphism σ_k^K of $\mathrm{Spec}(K)$. By base-change, this induces the *arithmetic Frobenius isomorphism* $\sigma_k^K : {\sigma_k^K}^{-1}(A') \longrightarrow A'$.

We also have the *geometric Frobenius endomorphism* $\pi_k : A' \longrightarrow {\sigma_k^K}^{-1}(A')$ which is an isogeny of p-power degree whose kernel is connected. Just as for every isogeny, there exists a $\pi_k^{-1} \in \mathrm{Hom}^0_{\overline{k}}(\sigma_k^{-1}(A'_{\overline{k}}), A'_{\overline{k}})$ which is a left- and right-inverse for π_k; see Lemma A.7.

Analogously, we have a geometric Frobenius endomorphism $\pi_k : W \longrightarrow W$.

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

The geometric Frobenius endomorphism π_k of W commutes with all endomorphisms of W. Thus by the universal property of the tensor product (see [FD, proposition 3.2]), the ring-homomorphisms $\mathrm{End}_K(A') \longrightarrow \mathrm{End}_k(W)$, $\lambda \mapsto \mathbf{Res}_k^K(\lambda)$ and $\mathbb{Z}[\pi_K][X]/(X^n - \pi_K) \longrightarrow \mathrm{End}_k(W)$, $X \mapsto \pi_k$ induce a ring-homomorphism

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

Theorem 2 *Let $K|k$ be an extension of finite fields of degree n. Let A' be an abelian K-variety, W the Weil-Restriction of A' with respect to $K|k$. Then*

$$\mathrm{End}^0_K(A') \otimes_{\mathbb{Q}[\pi_K]} \mathbb{Q}[\pi_K][X]/(X^n - \pi_K) \longrightarrow \mathrm{End}^0_k(W),\ \lambda \mapsto \mathbf{Res}_k^K(\lambda),\ X \mapsto \pi_k$$

is an isomorphism.

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

$$\mathrm{Hom}^0_k(W,W) \simeq \mathrm{Hom}^0_K\Big(\prod_{i=0}^{n-1} {\sigma_k^K}^{-i}(A'), A'\Big) \text{ via } a \mapsto p_{\mathrm{id}} \circ (a \otimes_k \mathrm{id}_K). \tag{1.18}$$

We show that the homomorphism of abelian groups

$$\begin{gathered}\mathrm{Hom}^0_K(A', A') \otimes_{\mathbb{Q}[\pi_K]} \mathbb{Q}[\pi_K][X]/(X^n - \pi_K) \longrightarrow \mathrm{Hom}_k(W,W) \simeq \\ \mathrm{Hom}^0_K\big(\textstyle\prod_{i=0}^{n-1} {\sigma_k^K}^{-i}(A'), A'\big) \simeq \bigoplus_{i=0}^{n-1} \mathrm{Hom}^0_K({\sigma_k^K}^{-i}(A'), A')\end{gathered} \tag{1.19}$$

¿from left to right is an isomorphism.

Let $\sigma_k \in \mathrm{Gal}(\overline{k}|k)$ again be the Frobenius automorphism. Again by base-change, this induces the arithmetic Frobenius automorphism $\sigma_k : W_{\overline{k}} \longrightarrow W_{\overline{k}}$.

The morphism $\pi_k : W \longrightarrow W$ 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 isomorphism: $\pi_k \circ P = \sigma_k^{-1}(P) = P^{\sigma_k}$; see Lemma A.32.

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 by definition of the Galois-operation on $W_{\overline{k}}$, $\sigma_k(P) = (\sigma(P_{i+1}))_{i=0}^{n-1}$ (where $P_n = P_0$). Thus $\pi_k \circ P = \sigma_k^{-1}(P) = (\sigma_k^{-1}(P_{i-1}))_{i=0}^{n-1} = (\pi_k \circ P_{i-1})_{i=0}^{n-1}$.

Thus under the isomorphism $W_K \simeq \prod_{i=0}^{n-1} \sigma_k^{K^{-i}}(A')$, the geometric Frobenius endomorphism π_k of W 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 some $\lambda \in \mathrm{End}_K^0(A')$, $\mathbf{Res}_k^K(\lambda)$ is given by the diagonal "matrix"

$$\begin{pmatrix} \lambda & & & \\ & \sigma_k^{K^{-1}}(\lambda) & & \\ & & \ddots & \\ & & & \sigma_k^{K^{1-n}}(\lambda) \end{pmatrix}.$$

Let x be the image of X in $\mathbb{Q}[\pi_K][X]/(X^n - \pi_K)$. Let $\lambda_1 x + \lambda_2 x^2 + \cdots + \lambda_n x^n \in \mathrm{Hom}_K^0(A', A') \otimes_{\mathbb{Q}[\pi_K]} \mathbb{Q}[\pi_K][X]/(X^n - \pi_K)$ where $\lambda_i \in \mathrm{End}_K^0(A')$. Such an element is mapped under the homomorphism of in 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 $\mathrm{Hom}_K^0(A', A') \otimes_{\mathbb{Q}[\pi_K]} \mathbb{Q}[\pi_K][X]/(X^n - \pi_K)$ have a unique representation as $\lambda_1 x + \lambda_2 x^2 + \cdots + \lambda_n x^n$ where $\lambda_i \in \mathrm{End}_K^0(A')$. Under homomorphism (1.19), this element corresponds to the first row in the above matrix, i.e. to the row vector $(\ \lambda_n \pi_k^n \ \ \lambda_{n-1} \pi^{n-1} \ \ \cdots \ \ \lambda_1 \pi_k \ )$. Now, every element of $\bigoplus_{i=0}^{n-1} \mathrm{Hom}_K^0(\sigma_k^{K^{-i}}(A'), A')$ has this form with unique λ_i. Thus (1.19) is an isomorphism. □

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

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

Corollary 1.23 $\mathrm{End}_k^0(W)$ *is commutative iff* $\mathrm{End}_K^0(A')$ *is commutative.*

□

Now assume that A' is a simple new abelian variety [14] *with commutative endomorphism ring.*

We are interested in the question whether W is simple. This is the case iff $\mathrm{End}(W) \simeq \mathrm{End}_K^0(A'/K)[X]/(X^n - \pi_K) \simeq \mathbb{Q}[\pi_K]/(X^n - \pi_K)$ is a field, i.e. iff $X^n - \pi_K$ is irreducible over $\mathrm{End}_K^0(A') \simeq \mathbb{Q}[\pi_K]$.

So, W is *not* simple iff $X^n - \pi_K$ is reducible over $\mathrm{End}_K^0(A') \simeq \mathbb{Q}[\pi_K]$. Under the condition $4 \nmid n$, this is equivalent to the existence of a $\beta \in \mathbb{Q}[\pi_K]$ and a prime divisor q of n with $\beta^q = \pi_K$; see [Lo, par. 14, Satz 2].

We claim that under the assumptions on A' and the additional assumption $4 \nmid n$, W is simple. [15]

Assume that $4 \nmid n$ and W is not simple so that $\beta^q = \pi_K$ for some prime $q|n$ and $\beta \in \mathbb{Q}[\pi_K]$ (so that $\mathbb{Q}[\pi_K] = \mathbb{Q}[\beta]$). Let $\lambda|k$ be the intermediate field of $K|k$ with $[K : \lambda] = q$. We claim that A' is isogenous to an abelian variety defined over λ.

Let V be the Weil-restriction of A' with respect to $K|\lambda$. Then $\chi_{V/\lambda}(X) = \chi_{A'/K}(X^q)$, and β is a root of $\chi_{V/\lambda}$, the characteristic polynomial of the Frobenius of V; see Proposition 1.21. So V contains a simple abelian variety A such that the characteristic polynomial of the Frobenius of A has β as a root. The endomorphism ring of A is commutative (since the endomorphism ring of V is) and thus isomorphic to $\mathbb{Q}[\beta] = \mathbb{Q}[\pi_K]$. This is a number field of degree $2d$ over $\mathbb{Q}$, thus A has dimension d. So $A \otimes_\lambda K$ is a d-dimensional abelian subvariety of $V \otimes_\lambda K \simeq \prod_{i=0}^{n-1} \sigma_\lambda^{K^{-i}}(A')$, thus $A \otimes_\lambda K \approx \sigma_\lambda^{K^{-i}}(A')$ for some i. Now, $\sigma_\lambda^{K^{-i}}(A') \sim A'$ via the i-power of the (geometric) Frobenius endomorphism relative to λ. Thus $A \otimes_\lambda K \sim A'$.

We proved:

Theorem 3 *Let $K|k$ be an extension of finite fields of degree n and assume $4 \nmid n$. If A' is a simple new abelian variety over K with commutative endomorphism ring (i.e. A' might be a non-super-singular elliptic curve), then the Weil-restriction of A' with respect to $K|k$ is simple.*

[14] We fixed the following definition: If A' is defined over k, i.e. if there exists an abelian k-variety A such that $A' \approx A \otimes_k K$, then we say that A is an *old* abelian variety (relative to $K|k$). If A' is not isogenous to an abelian variety defined over k or some proper intermediate field λ of $K|k$, then we call A' a *new* abelian variety (relative to $K|k$).

[15] The following proof is inspired by the proof of the "arithmetical part" of Honda's Theorem; cf. [Ho]. As stated by Honda, the argument goes back to Tate.

Chapter 2

Weil-restrictions of old abelian varieties

Introduction and results

In this chapter, we continue with the study of Weil-restrictions of abelian varieties. We restrict ourselves to the following situation:

Let $K|k$ be a finite Galois field extension, A an abelian k-variety. [1] Let W be the Weil-restriction of A_K with respect to $K|k$.

We begin with the determination of the ring of endomorphisms of W over k. The result is that this ring is canonically isomorphic to the so-called *skew-group-ring* of $\mathrm{End}_K(A_K)$ with the group $\mathrm{Gal}(K|k)$ and the natural operation of $\mathrm{Gal}(K|k)$ on $\mathrm{End}_K(A_K)$; see Theorem 4, p. 35.

We then restrict ourselves even further to the case that A is an elliptic curve E and $K|k$ is a cyclic field extension of odd degree of perfect fields. In this case, W is isogenous to a product of the elliptic curve E itself and the so-called *trace-zero-hypersurface* N. If E has no complex multiplication, than N is simple; see Theorem 5, p. 42. [2]

Our goal is then to study polarizations of N. In particular, we want to know if there exist principal polarizations on N.

In order to do so we study in an excursus first the Néron-Severi group of a product of elliptic curves. For each element of the Néron-Severi group we give an explicit divisor which defines the given element; see Theorem 6, p. 48.

There exists a canonical polarization on N, and this polarization has kernel $E[n] = E \cap N$. It follows in particular, that after a choice of a generator of $\mathrm{Gal}(K|k)$, N is canonically isomorphic to its dual; see Proposition 2.17.

However, the existence of this isomorphism does not mean that N is always

[1] According to our terminology, A_K is then an *old* abelian K-variety. Thus the title of this chapter.

[2] By saying that all elliptic k-curve has *complex multiplication*, we mean that $E_{\overline{k}}$ has complex multiplication and the complex multiplication is defined over k.

principally polarized as one sees from the following result:

If E has no complex multiplication then N is not principally polarized. If n is prime, it is isogenous to a principally polarized abelian variety iff the group scheme $E[n]$ contains a non-trivial sub-group scheme over k; see Corollary 2.26, p. 58 to Theorem 7, p. 57.

If E has complex multiplication, the situation is more complicated. For $n = 3$, we give an explicit criterion whether the abelian surface N is principally polarized; see Theorem 8, p. 59.

In the last section of this chapter, we specialize to the case $n = 3$ so that N is an abelian surface. We give explicit equations for an affine, open part of N and try to find curves of genus 2 on N whose existence was predicted by the previous results. The curves constructed will also serve as examples in the next chapter.

2.1 The endomorphism ring

Throughout this section, let $K|k$ be a finite Galois extension of fields 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 $A_K := A \otimes_k K$ with respect to $K|k$.

We want to determine the structure of the endomorphism ring of W, and determine in which isogeny factors W splits.

2.1.1 The endomorphism ring as skwe-group-ring

Recall that in Subsection 1.1.5, we have seen that the arithmetic operation of G on A_K induces a geometric operation on W. If $\boldsymbol{\tau} \in G$, the corresponding k-automorphism of W is denoted by a_τ.

Lemma 2.1 *Let $\boldsymbol{\tau} \in G, \lambda \in \mathrm{End}_K(A_K)$. Then $a_\tau \circ \mathbf{Res}_k^K(\lambda) = \mathbf{Res}_k^K(\tau(\lambda)) \circ a_\tau \in \mathrm{Aut}_k(W)$.*

Proof We check the relation for the corresponding automorphisms of the functor $\mathfrak{Res}_k^K(A_K)$. Let Z be a k-scheme, $P \in \mathfrak{Res}_k^K(A_K)(Z)$. Then

$$\begin{aligned}(a_\tau\, \lambda)(P) &= \tau \circ \lambda \circ P \circ \tau^{-1} = \tau \circ \lambda \circ \tau^{-1} \circ \tau \circ P \circ \tau^{-1} \\ &= \tau(\lambda) \circ \tau \circ P \circ \tau^{-1} = (\tau(\lambda)\, a_\tau)(P)\end{aligned}$$

□

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 [3] Let Λ be a ring, G a group, $t : G \longrightarrow \mathrm{Aut}(\Lambda)$ a group-homomorphism. The image of $\sigma \in G$ under t will again be denoted by σ. Following [Kar], we define the *skew-group-ring* $\Lambda^t[G]$ to be the following ring: [4] The underlying set is Λ^G, i.e. the set of functions $(\lambda_\sigma)_{\sigma\in G} : G \longrightarrow \Lambda$. The addition is defined pointwise, just as for the "usual" group ring. Also as usually, for $\tau \in G$, let $\tau \in \Lambda^t[G]$ also denote the function $\sigma \mapsto \delta_{\sigma,\tau} \in \Lambda^t[G]$. Here, $\delta_{\sigma,\tau}$ is the "Kronecker delta", $\delta_{\tau,\tau} = 1$ and $\delta_{\sigma,\tau} = 0$ if $\sigma \neq \tau$. The multiplication is defined by $\sum_{\sigma\in G} \lambda_\sigma \, \sigma \cdot \sum_{\nu\in G} \mu_\nu \, \nu = \sum_{\sigma,\nu\in G} \lambda_\sigma \, \sigma(\mu_\nu) \, \sigma\nu$.

Lemma 2.2 *$\Lambda^t[G]$ is a ring.*

Proof We only have to check the associativity of the multiplication. Using the fact that t is a group-homomorphism, one calculates on generating elements (of the abelian group $\Lambda^t[G]$)

$$\begin{gathered}(\lambda\,\sigma \cdot \beta\,\tau) \cdot \gamma\,v = \lambda\,\sigma(\beta)\,\sigma\tau \cdot \gamma\,v = \\ \lambda\,\sigma(\beta)\,\sigma\tau(\gamma)\,\sigma\tau v = \lambda\,\sigma \cdot \beta\,\tau(\gamma)\,\tau v = \lambda\,\sigma \cdot (\beta\,\tau \cdot \gamma\,v)\end{gathered}$$

□

$\Lambda^t[G]$ has the following universal property:

Lemma 2.3 *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, $t : G^{\mathrm{opp}} \longrightarrow \mathrm{Aut}(\mathrm{End}_K(A_K))$ the natural operation given by $\sigma \mapsto (\lambda \mapsto \sigma(\lambda) = \sigma\lambda\sigma^{-1})$. From Lemmata 2.1 and 2.3 it follows that $\sum_{\sigma\in G^{\mathrm{opp}}} \lambda_\sigma \, \sigma \mapsto \sum_{\sigma\in G^{\mathrm{opp}}} \mathbf{Res}_k^K(\lambda_\sigma)\, a_\sigma$ defines a ring-homomorphism

$$\mathrm{End}_K(A_K)^t[G^{\mathrm{opp}}] \longrightarrow \mathrm{End}_k(W). \tag{2.1}$$

Theorem 4 *Let $K|k$ be a finite Galois extension of fields with Galois group G, A an abelian variety over k, W the Weil-restriction of A_K with respect to $K|k$, $t : G^{\mathrm{opp}} \longrightarrow \mathrm{Aut}(\mathrm{End}_K(A_K))$ the natural operation. Then $\mathrm{End}_K(A_K)^t[G^{\mathrm{opp}}] \longrightarrow \mathrm{End}_k(W)$ is an isomorphism.*

Proof Analogously to the proof of Theorem 2, we make use of the isomorphism $\mathrm{Hom}_k(W,W) \simeq \mathrm{Hom}_K(A_K^{G^{\mathrm{opp}}}, A_K) \simeq \bigoplus_{\sigma\in G^{\mathrm{opp}}} \mathrm{Hom}_K(A_K, A_K)$ on the right-hand side.

[3] This definition is a special case of the more general definition of a *crossed product* (with respect to some operation); cf. [Kar, Chapter 10, 2].

[4] In [CR], the same ring is called *twisted group ring*. However, in [Kar], this word is reserved for the special case of a crossed product with respect to a trivial Galois-operation.

By (1.9), the image of some $\sigma \in G^{\mathrm{opp}}$ in $\mathrm{Hom}_K(A_K^{G^{\mathrm{opp}}}, A_K)$ 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 $\lambda_\sigma \in \mathrm{End}_K(A_K)$) 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. □

By tensoring the above isomorphism over $\mathbb{Z}$ with $\mathbb{Q}$, we get

Corollary 2.4 $\mathrm{End}_K^0(A_K)^t[G^{\mathrm{opp}}] \longrightarrow \mathrm{End}_k^0(W)$ *is an isomorphism.*

We know that the ring $\mathrm{End}_k^0(W)$ is semi-simple. Thus the skew-group-ring $\mathrm{End}_K^0(A_K)^t[G^{\mathrm{opp}}]$ is semi-simple.

It can be proven more generally that every skew-group-ring of a semisimple ring in which the group order is (finite and) invertible is semisimple or even more generally that every crossed product of a semisimple ring is semisimple; see [Kar, Volume I, Chapter 10, Corollary 2.5].

We now want to study the ring-homomorphism [5]

$$\begin{gathered}\mathrm{End}_K(A_K)^t[G^{\mathrm{opp}}] \xrightarrow{\sim} \mathrm{End}_k(W) \hookrightarrow \\ \mathrm{End}_K(W_K) \simeq \mathrm{End}_K(A_K^{G^{\mathrm{opp}}}) \simeq \mathrm{M}_{G^{\mathrm{opp}}}(\mathrm{End}_K(A_K)).\end{gathered} \tag{2.2}$$

For $\sigma \in G^{\mathrm{opp}}$, let $\iota_\sigma : A_K \longrightarrow A_K^{G^{\mathrm{opp}}}$ be the immersion to the "σ-th" factor, and let $p_\sigma : \prod_{\sigma \in G^{\mathrm{opp}}} A_K \longrightarrow A_K$ be the projection to the "σ-th" factor. Now, $\mathrm{End}_K(A_K^{G^{\mathrm{opp}}}) \longrightarrow \mathrm{M}_{G^{\mathrm{opp}}}(\mathrm{End}_K(A_K))$, $\psi \mapsto (p_\sigma \psi \iota_\nu)_{\sigma,\nu \in G^{\mathrm{opp}}}$ is a ring-homomorphism; see Subsection A.2.3.

We denote the matrix corresponding to a_τ by A_τ and the matrix corresponding to $\mathbf{Res}_k^K(\lambda)$ by $J(\lambda)$.

We have already established in Subsection 1.3.3 that $J(\lambda)$ is the diagonal matrix $(\sigma^{-1}(\lambda)\delta_{\sigma,\nu})_{\sigma,\nu \in G^{\mathrm{opp}}}$.

We want to determine to which matrix 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* $(\delta_{\sigma,\nu})_{\nu \in G}$. Recall that $a_\tau = (p_{\tau^{-1}\sigma})_{\sigma \in G}$; see Lemma 1.12. Thus

$$A_\tau = (\delta_{\tau^{-1}\sigma,\nu})_{\sigma,\nu \in G} = (\delta_{\sigma,\tau\nu})_{\sigma,\nu \in G}. \tag{2.3}$$

Before continuing we want to clarify the definition of the left regular (matrix) representation.

[5] Let Λ be a ring and Σ a finite set. Then by $\mathrm{M}_\Sigma(\Lambda)$ we mean the ring consisting of: The set of functions $a = (a_{\sigma,\tau})_{\sigma,\tau \in \Sigma} : \Sigma \times \Sigma \longrightarrow \Lambda$ with pointwise addition and multiplication defined by $(a \cdot b)_{\sigma,\tau} := \sum_{\gamma \in \Sigma} a_{\sigma,\gamma} b_{\gamma,\tau}$. After the choice of a bijection of Σ with the numbers $1, \ldots, |\Sigma|$, $\mathrm{M}_\Sigma(\Lambda)$ is canonically isomorphic to $\mathrm{M}_{|\Sigma|}(\Lambda)$, the matrix ring in $|\Sigma|$ variables.

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 as Λ-right module free on a finite set of generators Σ, i.e. $\Xi \simeq \Lambda^\Sigma$ as Λ-right modules. Multiplication of elements of Ξ from the left on itself induces a ring-homomorphism

$$L : \Xi \longrightarrow \mathrm{End}^r_\Lambda(\Xi) \simeq \mathrm{End}^r_\Lambda(\Lambda^\Sigma), \tag{2.4}$$

the *left regular representation.*

For a fixed basis Σ, the right-hand side of (2.4) is canonically isomorphic to the matrix ring $\mathrm{M}_\Sigma(\Lambda)$. The isomorphism $\mathrm{M}_\Sigma(\Lambda) \xrightarrow{\sim} \mathrm{End}^r_\Lambda(\Lambda^\Sigma)$ is given as follows: To every matrix $(a_{\sigma,\nu})_{\sigma,\nu\in\Sigma}$ associate the endomorphism $(x_\sigma)_{\sigma\in\Sigma} \mapsto (\sum_{\nu\in\Sigma} a_{\sigma,\nu}x_\nu)_{\sigma\in\Sigma}$. (This is given on the basis elements $\nu = (\delta_{\sigma,\nu})_{\sigma\in\Sigma}$ by $\nu \mapsto \sum_{\sigma\in\Sigma} \sigma\, a_{\sigma,\nu}$.) The inverse is

$$\begin{gathered}\mathrm{End}^r_\Lambda(\Lambda^\Sigma) \longrightarrow \mathrm{M}_\Sigma(\Lambda),\ a \mapsto (\alpha_{\sigma,\nu})_{\sigma,\nu\in\Sigma} \text{ with } \alpha_{\sigma,\nu} \in \Lambda \\ \text{and } a(\nu) = \textstyle\sum_{\sigma\in\Sigma} \sigma\, \alpha_{\sigma,\nu}\end{gathered} \tag{2.5}$$

By composition of (2.4) with (2.5), we get the *left regular matrix representation* (with respect to the basis Σ).

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

(In particular, for $\Lambda = \Xi$ and $\Sigma = \{1\}$, the left regular matrix representation is the identity on Λ.)

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

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

So

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

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

Proposition 2.5 *Homomorphism (2.2) is the left regular matrix representation of the skew-group-ring* $\mathrm{End}_K(A_K)^t[G^{\mathrm{opp}}]$ *with respect to the basis* G^{opp}.

2.1.2 The Rosati involution, isotypic components and orthogonality

The Rosati involution

Let $\varphi : A_K \longrightarrow \widehat{A}_K$ be a polarization. Then $\mathbf{Res}_k^K(\varphi) : W \longrightarrow \widehat{W}$ is also a polarization; see Subsection 1.3.4.

We want to calculate how the Rosati involution of W with respect to $\mathbf{Res}_k^K(\varphi)$ is given under the isomorphism of Corollary 2.4.

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

First of all, the (defining) equation $\lambda' = \varphi^{-1}\widehat{\lambda}\varphi$ where $\lambda \in \mathrm{End}_K^0(A_K)$ implies

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

To calculate the Rosati involution of a_τ, we use the inclusion of $\mathrm{End}_k^0(W)$ into the matrix ring $\mathrm{M}_{G^{\mathrm{opp}}}(\mathrm{End}_K^0(A))$ and the fact that $\mathbf{Res}_k^K(\varphi) \otimes_k \mathrm{id}_K$ is a product polarization, and calculate the Rosati involution with the help of Lemma A.16.

Since a_τ corresponds to the matrix $A_\tau = (\delta_{\sigma,\tau\nu})_{\sigma,\nu\in G^{\mathrm{opp}}}$ (see (2.3)), 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 2.6 *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 2.4, the Rosati involution associated to the polarization* $\mathbf{Res}_k^K(\varphi) : W \longrightarrow \widehat{W}$ *is given by* $\sum_{\sigma\in G^{\mathrm{opp}}} \lambda_\sigma \sigma \mapsto \sum_{\sigma\in G^{\mathrm{opp}}} \sigma^{-1}\lambda'_\sigma = \sum_{\sigma\in G^{\mathrm{opp}}} \sigma^{-1}(\lambda'_\sigma)\,\sigma^{-1}$.

Dimensions of components

From now on, let k be perfect.

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 $K|k$, let $t : G^{\mathrm{opp}} \longrightarrow \mathrm{End}_K(A_K)$ be the natural operation.

Let $D \subseteq \mathrm{End}^0_K(A_K)$ be a subring which is a division ring and which is invariant under the operation t.

Let $\bigoplus_{i=1}^s \Lambda_i \simeq D^t[G^{\mathrm{opp}}]$ be a decomposition of the $D^t[G^{\mathrm{opp}}]$-right module $D^t[G^{\mathrm{opp}}]$, where we regard the Λ_i as submodules of $D^t[G^{\mathrm{opp}}]$. This defines partition of unity $1 = \sum_i e_i$ where the e_i are pairwise orthogonal and idempotent and $e_i \in \Lambda_i$. Now, $\Lambda_i = e_i\, D^t[G^{\mathrm{opp}}]$, and conversely, if we are given a decomposition of the unity $1 = \sum_i e_i$ with pairwise orthogonal idempotents e_i, $\Lambda_i := e_i\, D^t[G^{\mathrm{opp}}]$ defines a decomposition of the $D^t[G^{\mathrm{opp}}]$-right module $D^t[G^{\mathrm{opp}}]$.

Via the inclusion $D^t[G^{\mathrm{opp}}] \hookrightarrow \mathrm{End}^0_K(A_K)^t[G^{\mathrm{opp}}] \simeq \mathrm{End}^0_k(W)$, we can regard the e_i to be elements of $\mathrm{End}^0_k(W)$. For each i, let $c_i \in \mathbb{N}$ such that $c_i e_i \in \mathrm{End}_k(W)$.

Now let $W_i := c_i e_i(W)$. Then $\bigoplus_{i=1}^s W_i \sim W$. (Conversely, such an isogeny decomposition where the W_i are abelian subvarieties of W defines a partition of unity and thus a decomposition of $\mathrm{End}^0_K(A_K)$ as right-$\mathrm{End}^0_K(A_K)$ module; see A.2.5 for details.)

Proposition 2.7 *Let $D \subseteq \mathrm{End}^0_K(A_K)$ be a subring which is a division ring which is invariant under the operation t on $\mathrm{End}^0_K(A_K)$. Let $\bigoplus_{i=1}^s \Lambda_i \simeq D^t[G^{\mathrm{opp}}]$ be a decomposition of the $D^t[G^{\mathrm{opp}}]$-right module $D^t[G^{\mathrm{opp}}]$. This corresponds to the partition of unity $1 = \sum_i e_i$. Let $W_i := c_i e_i(W)$ as above. Then $W_{iK} \approx A_K^{n_i}$ where*

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

Proof Choose a bijection of G^{opp} with 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 $\mathrm{End}^0_K(A_K)^t[G^{\mathrm{opp}}]$, 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 $\iota_{\mathrm{M}} : \mathrm{M}_{G^{\mathrm{opp}}}(D) \longrightarrow \mathrm{M}_{G^{\mathrm{opp}}}(\mathrm{End}^0_K(A_K))$ 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 such that $BL_D(e_i)B^{-1}$ is zero outside a block of size n_i where it is the identity matrix. By multiplying B with a constant in $\mathbb{N}$, we can assume that all entries of B lie in $D \cap \mathrm{End}_K(A_K)$.

Let b be the endomorphism of $A_K^{G^{\mathrm{opp}}} \simeq A_K^n$ which is associated to $\iota_{\mathrm{M}}(B)$. By our notational conventions, the endomorphism associated to the matrix $L(e_i) = \iota_{\mathrm{M}} L_D(e_i)$ is $e_i \otimes_k \mathrm{id}_K$. We see that $b^{-1}(e_i \otimes_k \mathrm{id}_K)b$ is the projection of $A_K^{G^{\mathrm{opp}}} \simeq A_K^n$

to $A_K^{n_i}$. Thus the image of $b^{-1}c_i(e_i \otimes_k \mathrm{id}_K)b$ is $A_K^{n_i}$, and the image of $c_i\, e_i \otimes_k \mathrm{id}_K$ is isomorphic to $A_K^{n_i}$. □

Remark Let A be simple, $D = \mathrm{End}_K^0(A_K)$. Assume that all e_i in the above proposition are central. Then all Λ_i as above are rings and $\bigoplus_{i=1}^s \Lambda_i \simeq D^t[G^{\mathrm{opp}}]$ is an isomorphism of rings. Further, the $W_i = c_i e_i(W)$ are generated by the isotypic components of W and $\Lambda_i \simeq \mathrm{End}_k^0(W_i)$. So in particular, the number n_i in the above proposition satisfies $n_i = \dim_D(\mathrm{End}_k^0(W_i))$.

The Rosati involution and representation theory

In Subsection A.2.5, the following is shown:

A decomposition of an abelian variety into isotypic components corresponds to the partition of unity $1 = \sum_i e_i$ into central simple pairwise orthogonal idempotents. (The decomposition of the abelian variety as well as the partition of unity are unique up to a permutation.)

Further, the isotypic components are orthogonal with respect to any polarization. This corresponds to the fact that for any Rosati involution $e_i = e_i'$.

We now want to show how for the Weil-restriction W the orthogonality of the isotypic components is closely related to a well-known result from representation theory.

To use this result, we make the assumption, that *A is simple, the endomorphism ring of A_K is commutative and all endomorphisms of A_K are defined over k.* Fix a polarization φ on A.

Under our assumptions, $\mathrm{End}_k^0(W)$ is isomorphic to the “ordinary” group ring $\mathrm{End}_K^0(A_K)[G^{\mathrm{opp}}]$.

We fix an inclusion of $\mathrm{End}_K^0(A_K)$ into $\overline{\mathbb{Q}}$. Then the Rosati involution operates on $\mathrm{End}_K^0(A_K)$ by conjugation.

Let $(\ldots)'$ be the involution of $\overline{\mathbb{Q}}[G^{\mathrm{opp}}]$ given by $\sum_{\sigma\in G^{\mathrm{opp}}}\lambda_\sigma\sigma \mapsto \sum_{\sigma\in G^{\mathrm{opp}}}\overline{\lambda_\sigma}\sigma^{-1}$. Note that by Proposition 2.6, this involution restricts to the Rosati involution on $\mathrm{End}_K^0(A_K)[G^{\mathrm{opp}}]$.

Let χ_j, $j = 1, \ldots$ be the character maps of G^{opp}. And let $1 = \sum_j e^{(j)}$ be the decomposition of the unity in the ring $\overline{\mathbb{Q}}[G^{\mathrm{opp}}]$. Then by representation theory, $e^{(j)} = \sum_{\sigma\in G^{\mathrm{opp}}} \frac{1}{n}\chi_j(1)\chi_j(\sigma^{-1})\,\sigma$; see [La, XVIII, Proposition 4.4.].

This implies $e^{(j)\prime} = \sum_{\sigma\in G^{\mathrm{opp}}} \frac{1}{n}\sigma^{-1}\overline{\chi_j(1)\chi_j(\sigma^{-1})} = \sum_{\sigma\in G^{\mathrm{opp}}} \frac{1}{n}\chi_j(1)\chi_j(\sigma)\,\sigma^{-1} = e^{(j)}$.

The central idempotents e_i of the group ring $\mathrm{End}_K(A_K)[G^{\mathrm{opp}}]$ have the form $\sum_\gamma e^{(i_\gamma)}$, where all i_γ are distinct. Thus $e_i = e_i'$ for the Rosati involution with respect to $\mathbf{Res}_k^K(\varphi)$, which is consistent with the result $e_i = e_i'$ for general abelian varieties and any polarization.

2.1.3 The cyclic case

Let k still be a perfect field. We now apply the above results to the case that G is cyclic.

We identify G with G^{opp} and fix some generator $\sigma \in G$. Let $a = a_\sigma \in \mathrm{End}_k(W)$ be the automorphism corresponding to σ. (Since G is commutative, $a_\sigma = s_\sigma^{-1}$; see p. 17)

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

$$\mathbb{Q}[X]/(X^n-1) \longrightarrow \mathrm{End}_K^0(A_K)^t[G],\ x \mapsto \sigma.$$

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

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

Here, Φ_d is the d-th cyclotomic polynomial, a normalized and irreducible polynomial of degree $\varphi(d)$ whose roots are the primitive d-th roots of unity. So $\mathbb{Q}[X]/\Phi_d = \mathbb{Q}(\zeta_d)$.

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 pairwise orthogonal idempotents and define a partition of unity. The decomposition corresponding to this partition 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 2.7, 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 $c_d(\mathrm{id} - E_d(a)) = c_d \sum_{f|n, f\neq d} \Psi_f(a)\Phi'_f(a) = (c_d \sum_{f|n,\, f\neq d} \Psi_f(a) \prod_{g|n,\, g\neq d, f} \Phi_g(a))\, \Phi_d(a)$. 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.

Let W'_d be the abelian subvariety which is generated by the W_f, $f|n$, $f \neq d$. Then $W'_d = (\mathrm{id} - E_d(a))(W) = (\sum_{f\neq d} E_f)(W)$. Analogously to the above arguments one shows that $W'_d = \Phi_d(a)(W)$ and that W'_d is the reduced identity component of the kernel of $\Phi'_d(a)$.

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 variety whose endomorphism are all defined over k and whose endomorphism ring is commutative.

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

Also if A is a non-super-singular elliptic curve over any field and n is odd, then all endomorphism of A_K are 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 $\mathrm{End}_K(A_K)$ has order 2, and consequently the kernel of the representation $\mathrm{Gal}(K|k) \longrightarrow \mathrm{Aut}(\mathrm{End}_K(A_K))$ is trivial.

Under the assumptions, we have the isomorphisms

$$\begin{array}{ccccc} \mathrm{End}_k^0(A_k)[X]/(X^n-1) & \simeq & \mathrm{End}_K^0(A_K)[G] & \simeq & \mathrm{End}_k^0(W) \\ x & \mapsto & \sigma & \mapsto & a \end{array} .$$

Let Φ_d split into the product of the non-trivial irreducible polynomials $\Phi_d^{(1)}, \Phi_d^{(2)}, \ldots, \Phi_d^{(r_d)}$ over $\mathrm{End}_k^0(A)$. Let $\Phi_d^{(i)} := (X^n-1)/\Phi_d^{(i)}$. Since X^n-1 is in characteristic 0 a separable polynomial, the $\Phi_d^{(i)}$ are all different for all 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 $E_d^{(i)} := \Psi_d^{(i)}{\Phi'}_d^{(i)}$.

Then again by Proposition 2.7, $W_d^{(i)} := E_d^{(i)}(a)(W)$ is an abelian variety with $W_{d\,K}^{(i)} \approx A_K^{\deg(\Phi_d(i))}$. The abelian subvariety $W_d^{(i)}$ is simple and its endomorphism ring is isomorphic to the integral commutative ring $\mathrm{End}_k(A)[X]/\Phi_d^{(i)}$. Since $\mathrm{End}_k(W)$ is communtative, the $W_d^{(i)}$ are pairwise non-isogenous and they are thus 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 iff Φ_d is irreducible over $\mathrm{End}_k^0(A)$, i.e. iff $\mathrm{End}_k^0(A)$ and $\mathbb{Q}(\zeta_d)$ are linearly disjoint. [6] If we fix an inclusion of $\mathrm{End}_k^0(A)$ into $\overline{\mathbb{Q}}$, this is the case iff $\mathrm{End}_k^0(A) \cap \mathbb{Q}(\zeta_d) = \mathbb{Q}$.

It particular, non of the W_d splits if $\mathrm{End}_k^0(A) = \mathbb{Q}$ as is the case if A is an elliptic curve without complex multiplication.

We proved:

Theorem 5 *Let $K|k$ be a finite cylcic field extension of degree n of perfect fields. Let A be an abelian variety over a field k.*

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 $W_{dK} \approx A_K^{\varphi(d)}$, and W is isogenous to the product of the W_d. Here, $W_1 = A$ itself.

Assume in addition that A_K is simple, $End_K^0(A_K)$ is commutative and all endomorphisms of A_K are defined over k. Fix an inclusion of $\mathrm{End}_K^0(A_K)$ *into* $\overline{\mathbb{Q}}$.

[6] For definition of "linear disjoint" see Subsection A.3.1 in the appendix.

Then the isotypic components of W are all simple, and its endomorphism rings are all commutative. For each d, W_d is simple iff $\mathrm{End}^0_k(A) \cap \mathbb{Q}(\zeta_d) = \mathbb{Q}$.

Let A be a non-super-singular elliptic curve with complex multiplication (defined over k). Fix an inclusion of $\mathrm{End}_k(A)$ into $\overline{\mathbb{Q}}$.

Then $\mathrm{End}^0_k(A)$ is a imaginary quadratic extension of $\mathbb{Q}$. Now $\mathrm{End}^0_k(A)$ and $\mathbb{Q}(\zeta_d)$ are not linearly disjoint iff $\mathrm{End}^0_k(A) \subseteq \mathbb{Q}(\zeta_d)$. If this is the case then Φ_d splits into two polynomials of degree $\frac{1}{2}\varphi(d)$.

Let A still be a non-super-singular elliptic curve and let k be finite. Then $\mathrm{End}^0_k(A) = \mathbb{Q}[\alpha]$ where α is a root of the characteristic polynomial of the Frobenius. Thus Φ_d splits iff $\alpha \in \mathbb{Q}(\zeta_d)$.

Corollary 2.8 *Under the assumptions of the theorem, let A be a non-super-singular elliptic curve with* $\mathrm{End}_k(A) = \mathrm{End}_K(A_K)$ *(this condition is automatically satisfied over finite fields or if n is odd).*

Then for each d, W_d is not simple iff A_K has complex multiplication and $\mathrm{End}^0_k(A) \subseteq \mathbb{Q}(\zeta_d)$. *If this is the case, W_d contains canonically two simple non-isogenous abelian subvarieties with dimension $\frac{\varphi(d)}{2}$, and W_d is isogenous to the product of these abelian subvarieties.* [7]

The trace-zero-hypersurface

Let again A be an abelian k-variety.

By the above argumentation, W is isogenous to W_1 which is isomorphic to A itself and W_1', the abelian subvariety of W generated by W_d for $d|n$ and $d \neq 0$. Now $\Phi_1 = X - 1$ and $\Phi_1' = X^{n-1} + \cdots + 1$ and thus $W_1 = (a^{n-1} + \cdots + \mathrm{id})(W)$, $W_1' = (a - \mathrm{id})(W)$, and W_1 is the reduced itentity component of the kernel of $a - \mathrm{id}$ and W_1' is the reduced itentity component of the kernel of $a^{n-1} + \cdots + \mathrm{id}$.

Now both these kernels are in fact itself equal to W_1, W_1' respectively. This is obvious for W_1, since $\ker(a - \mathrm{id})$ is by definition equal to A embedded in W. But it is also true for W_1':

Let $N := \ker(\Phi_1'(a)) = \ker(a^{n-1} + \cdots + \mathrm{id})$. Let $\Sigma_n := \{0, \ldots, n-1\}$ and consider the isomorphism $W_{\overline{k}} \simeq E^G_{\overline{k}} \simeq E^{\Sigma_n}_{\overline{k}}$ where the "σ^i-th" factor corresponds to the i-the factor. Under this isomorphism, $N_{\overline{k}}$ corresponds to $\ker(p_0 + \cdots + p_{n-1})$, where for $i = 0, \ldots, n-1$, the $p_i : E^{\Sigma_n}_{\overline{k}} \longrightarrow E_{\overline{k}}$ are the projections. Now $\ker(p_0 + \cdots + p_{n-1}) \longrightarrow E^{n-1}_{\overline{k}}$, $P = (P_0, \ldots, P_{n-1}) \mapsto (P_1, \ldots, P_{n-1})$ is an isomorphism.

As $W_1' = N = \ker(\Phi_0'(a)) = \ker(a^{n-1} + \cdots + \mathrm{id})$, we call N the *trace-zero-hypersurface* of W (although this term is not completely accurate if $\dim(A) > 1$).

Note that W is isogenous to $A \times_k N$ but not isomorphic to it, for $N \cap A :=$
$N \times_W A = \ker(\overbrace{\mathrm{id}_A + \cdots + \mathrm{id}_A}^{n \text{ times}}) = \ker([n]) = A[n]$.

[7] Over finite fields, the dimensions of the simple isogeny-factors of W in Corollary 2.8 were first established by N. Naumann using the l-adic representation; see [Na].

This fact makes the study of N particularly interesting, and we will concentrate on this object for the rest of the chapter.

The following result gives a flavor of the consequent results about N.

Let $\varphi : A \longrightarrow \widehat{A}$ be a polarization of A, defined by the ample sheaf $\mathfrak{L}$ on $A_{\overline{k}}$. As said above, $\mathbf{Res}_k^K(\varphi) : W \longrightarrow \widehat{W}$ is also a polarization, defined by the sheaf $\mathfrak{L}_{W_{\overline{k}}}$.

We are interested in the kernel of the polarization $\widehat{\iota_N}\,\mathbf{Res}_k^K(\varphi)\,\iota_N$ defined by $\iota_N^*(\mathfrak{L}_{W_{\overline{k}}})$.

Proposition 2.9 $A \cap N = A[n]$ *is immersed in* $\ker(\widehat{\iota_N}\,\mathbf{Res}_k^K(\varphi)\,\iota_N)$. *If* φ *is a principal polarization, they are equal.*

Proof The first statement follows from Lemma A.19, the second from Lemma A.23 with $f = \mathrm{id} - a^{n-1}$. (It is $N = \mathrm{im}(f)$, and further $f = f'$ by proposition 2.6 and $\ker(f') = \ker(f) = A$.) □

Let E be a non-super-singular elliptic curve, N the associated trace-zero-hypersurface. We want to study the Néron-Severi group of N via a "geometric" approach. In order to do so, we now study the Néron-Severi group of the product of isomorphic elliptic curves.

2.2 The Néron-Severi group of a product of isomorphic elliptic curves

Let E be an elliptic curve over a perfect field K, let n be a natural number. In this section, we want to study the various properties of the endomorphism ring and the Néron-Severi group of E^n.

In the first subsection, we put the results of [Mu, p.208-210] into more concrete terms. In the second subsection, we give a basis for the Néron-Severi group of E^n, then in the show the Néron-Severi group on an abelian variety which is a twist of E^n (i.e. which is after a base-change isomorphic to E^n) can (in principle) be calculated. This result will be the basis of the calculations of the next section.

2.2.1 The Néron-Severi group and the endomorphism ring

The canonical product polarization of E^n

Let $p_i : E^n \longrightarrow E$ be the projections and let $\iota_i : E \hookrightarrow E^n$ be the immersions onto the "i-th factor".

Let D_i be the divisor [8] $p_i^{-1}(0) = E \times E \times \cdots \times E \times 0 \times E \cdots E$ (0 in the i-th position), $D := \sum_{i=1}^n D_i$.

[8] Since abelian varieties are non-singular, effective (Weil- or Cartier)-divisors are in bijection

Let $\varphi : E \longrightarrow \widehat{E}$ be the canonical principal polarization defined by the ample divisor (0). The divisor D defines the "canonical" product polarization of E^n, let $\varphi_n : E^n \longrightarrow \widehat{E^n}$ denote this polarization. Since (0) defines a principal polarization of E, φ_n is a principal polarization, i.e. φ_n an isomorphism. (Corresponding to the fact that D has Euler-characteristic $n!$.) [9]

The Galois group $\mathrm{Gal}(\overline{K}|K)$ operates on $\mathrm{NS}(E^n_{\overline{K}})$, and we have an inclusion $\phi : \mathrm{NS}(E^n_{\overline{K}})^{\mathrm{Gal}(\overline{K}|K)} \longrightarrow \mathrm{Hom}_K(E^n, \widehat{E^n})$, $\overline{\mathcal{M}} \mapsto \phi_{\overline{\mathcal{M}}}$. By composition with the homomorphism φ_n^{-1}, $\mathrm{NS}(E^n_{\overline{K}})^{\mathrm{Gal}(\overline{K}|K)}$ becomes a subgroup of $\mathrm{End}_K(E^n) \simeq \mathrm{M}_n(\mathrm{End}_K(E))$. [10] Its image equals the subgroup of elements which are fixed under the Rosati involution; see Lemma A.14. [11]

The Rosati involution

If $\lambda \in \mathrm{End}^0_K(E)$, let $\overline{\lambda}$ denote the corresponding conjugated element. (If E is super-singular, let $\overline{\lambda}$ be the conjugated element in the field extension $\mathbb{Q}(\lambda)$.) Then the Rosati involution of E (with respect to the ample divisor (0)) is given by $\lambda \mapsto \overline{\lambda}$.

The following lemma is a special case of Lemma A.16:

Lemma 2.10 *The Rosati involution of E^n with respect to $\mathcal{L}(D)$ is given by $A \mapsto \overline{A}^\top$ (transposition and conjugation) on $\mathrm{M}_n(\mathrm{End}^0_K(E))$.*

So if E is non-super-singular, $\mathrm{NS}(E^n_{\overline{K}})^{\mathrm{Gal}(\overline{K}|K)}$ is isomorphic to the group of hermitian matrices of $\mathrm{M}_n(\mathrm{End}_K(E^n))$.

The degree and the Euler-characteristic

Let us state how the degree and the Euler-characteristic of a divisor can be calculated if it is given as an element of $\mathrm{M}_n(\mathrm{End}_K(E^n))$. We follow the ideas of [Mu, p.209].

First, we need to know how the degree of an endomorphism given as an element of $\mathrm{M}_n(\mathrm{End}_K(E^n))$ can be calculated. On $\mathrm{End}_K(E)$, the degree of $\lambda \in \mathrm{End}_K(E)$ is given by $\deg(\lambda) = \lambda\overline{\lambda}$.

Lemma 2.11 *Assume that E is non-super-singular. The degree function of E^n is given on $\mathrm{M}_n(\mathrm{End}_K(E))$ by $\deg(A) = \det(A)\,\overline{\det(A)}$.*

with closed subschemes of pure codimension 1. We will also call such subschemes *(effective) divisors.* We will use that for some surjection $a : A \longrightarrow B$ of non-singular, connected varieties A, B and some closed subscheme of pure codimension 1 D of B, the "pull-back" of the Cartier-divisor associated to D corresponds to the scheme-theoretic inverse image $a^{-1}(D)$; see Subsection A.3.2.

[9] This section relies on Subsection A.2.2 in the appendix.

[10] It it important here that D defines a principal polarization.

[11] We will see that $\mathrm{NS}(E^n) \hookrightarrow \mathrm{NS}(E^n_{\overline{K}})^{\mathrm{Gal}(\overline{K}|K)}$ is an isomorphism.

Proof The equation is true for singular matrices (which correspond to endomorphism with non-finite kernel and thus have by definition degree 0).

Further, the equation is true for diagonal matrices (the value on both sides being the product over the squares of the norms of the diagonal elements), for upper/lower triangular matrices with diagonal elements all 1 (the value on both sides being 1) and for permutation matrices (where the value on both sides is again 1).

Let A be non-singular. By the complete Gauß-Algorithm, there exist B_i, $i = 1, \ldots, m$ which are diagonal matrices or upper/lower triangular with diagonal elements 1 or permutation matrices such that $B_m \cdots B_1 A = aI$, where $a \in \mathbb{N}$.

Since the equation is multiplicative on both sides and true for all B_i and for aI, it is also true for A. □

Remark If E is super-singular, a similar result holds: If we chose a quadratic field extension F inside $\mathrm{End}^0_K(E)$, then $\mathrm{M}_n(F)$ is a subgroup of $\mathrm{M}_n(\mathrm{End}^0_K(E))$. On this group, the lemma holds. (To calculate the degree for the whole group $\mathrm{End}^0_K(E^n)$, one has to use the so-called *reduced norm.*)

For any divisor C on E^n, the degree of C (i.e. the degree of $\phi_{\mathfrak{L}(C)}$) is the degree of the endomorphism $\varphi_n^{-1} \circ \phi_{\mathfrak{L}(C)}$ of E^n. If this endomorphism corresponds to the matrix A with entries in a commutative subring of $\mathrm{End}_K(E)$, by the Riemann-Roch-theorem and the above result, $\chi(\mathfrak{L}(C))^2 = \deg(\mathfrak{L}(C)) = \det(A)\overline{\det(A)}$, thus $|\chi(\mathfrak{L}(C))| = |\det(A)|$.

Lemma 2.12 *Again let C be a divisor on E^n. Assume that E is non-super-singular or that C fulfills the conditions of the above remark. Then $\chi(\mathfrak{L}(C)) = \det(A)$.*

This follows from the following lemma.

Lemma 2.13 *Let the notations and the conditions on C be as above. Then $\chi(\mathfrak{L}(D)^z \otimes \mathfrak{L}(C)) = \det(zI + A) = p_{-A}(z)$, where p_{-A} is the characteristic polynomial of the matrix $-A$.*

Proof For any $z \in \mathbb{Z}$, $|\chi(\mathfrak{L}(D)^z \otimes \mathfrak{L}(C))| = |\chi(\mathfrak{L}(zD + C))| = |\det(zI + A)|$ by linearity and the above result. So we only have to check that the sign is correct.

By the Riemann-Roch theorem, $z \mapsto \chi(\mathfrak{L}(D)^z \otimes \mathfrak{L}(C)) = \frac{1}{n!}(zD + C)^n$ is a polynomial function of degree n, and $\frac{1}{n!}(zD + C)^n = \frac{1}{n!}(z^n(D)^n +$(lower order terms))$= z^n+$ (lower order terms). Analogously, $p_{-A}(z) = z^n+$ (lower order terms). Thus for large z, $p_{-A}(z)$ and $\chi(\mathfrak{L}(D)^z \otimes \mathfrak{L}(C))$ are both positive, and thus they are equal for these z. Especially, they are equal for infinitely many z, and being polynomial functions they are equal. □

Lemma 2.14 *Let the notations and the conditions on C be as above, and further assume $\mathcal{L}(C)$ to be non-degenerate. Then $i(\mathcal{L}(C))$, the index of $\mathcal{L}(C)$, is the number of negative eigenvalues of A. In particular, $\mathcal{L}(C)$ is ample iff $\det(A) \neq 0$ and the eigenvalues of A are all positive.*

Proof By Proposition A.25 (cf. [Mu, par. 16, p. 155]) and the above lemma, the index is the number of positive roots of p_{-A}, i.e. the number of positive eigenvalues of $-A$, i.e. the number of negative eigenvalues of A. The second statement is a reformulation of Lemma A.26. □

2.2.2 A basis for the Néron-Severi group

For each $i = 1, ..., n$, let $\lambda_i \in \mathrm{End}_K(E)$. Let not all λ_i be 0. Let $\underline{\lambda} := (\lambda_1, \ldots, \lambda_n)$ and let $\lambda := \lambda_1 p_1 + \cdots + \lambda_n p_n : E^n \longrightarrow E$ be the corresponding morphism.

Now the closed subscheme $C(\underline{\lambda}) := \ker(\lambda)$ is purely $n-1$-dimensional and is thus an effective divisor on E^n. The .-valued points of $C(\underline{\lambda})$ are

$$\{P = (P_1, \ldots, P_n) | \; \lambda_1 \circ P_1 + \lambda_2 \circ P_2 + \cdots + \lambda_n \circ P_n = 0\}.$$

Proposition 2.15 *The class of the sheaf $\mathcal{L}(C(\underline{\lambda}))$ (in $NS(E^n)$) corresponds to the endomorphism with the matrix*

$$\begin{pmatrix} \overline{\lambda_1}\lambda_1 & \overline{\lambda_1}\lambda_2 & \cdots & \overline{\lambda_1}\lambda_n \\ \overline{\lambda_2}\lambda_1 & \overline{\lambda_2}\lambda_2 & \cdots & \overline{\lambda_2}\lambda_n \\ \vdots & \vdots & \ddots & \vdots \\ \overline{\lambda_n}\lambda_1 & \overline{\lambda_n}\lambda_2 & \cdots & \overline{\lambda_n}\lambda_n \end{pmatrix} = \begin{pmatrix} \overline{\lambda_1} \\ \overline{\lambda_2} \\ \vdots \\ \overline{\lambda_n} \end{pmatrix} \begin{pmatrix} \lambda_1 & \lambda_2 & \cdots & \lambda_n \end{pmatrix}.$$

Proof In the notation of Subsection A.2.3, we have to show that $\varphi_n^{-1}\phi_{\mathcal{L}(C(\lambda))} = \lambda'\lambda$.

We may assume that K is algebraically closed. We use that for all K-valued points P of E^n and endomorphisms λ, $\lambda \circ T_P = T_{\lambda \circ P} \circ \lambda$.

Now, for every K-valued point P of E^n, $\phi_{\mathcal{L}(C(\underline{\lambda}))} \circ P$ is defined by $T_P^{-1}(C(\underline{\lambda})) - C(\underline{\lambda}) = T_P^{-1}\lambda^{-1}(0) - \lambda^{-1}(0) = \lambda^{-1}(T_{\lambda \circ P}^{-1}(0) - (0))$. Thus $\phi_{\mathcal{L}(C(\underline{\lambda}))} = \widehat{\lambda}\varphi\lambda = \varphi_n\lambda'\lambda$. □

Notation Let $\lambda \in \mathrm{End}_K(E)$ and $1 \leq i < j \leq n$. Let $C_{i,j}^{\lambda}$ be the divisor associated with the closed subscheme

$$\{P = (P_1, \ldots, P_n) | P_i + \lambda \circ P_j = 0\}.$$

Then the by the above results the matrix of C is zero but at the entries $(i,i), (i,j), (j,i), (j,j)$. Here it looks like

$$\begin{pmatrix} 1 & \lambda \\ \overline{\lambda} & \lambda\overline{\lambda} \end{pmatrix}$$

We see that the group of endomorphisms of E^n invariant under the Rosati involution is generated by the endomorphisms corresponding to D_i and $C^{\lambda}_{i,j}$. So $\mathrm{NS}(E^n) \simeq \mathrm{NS}(E^n_{\overline{K}})^{\mathrm{Gal}(\overline{K}|K)}$. We can give a basis for $\mathrm{NS}(E^n)$ in terms of a basis of $\mathrm{End}_K(E)$.

Theorem 6 *Let K be a perfect field and let E be a non-super-singular elliptic K-curve. Then* $\mathrm{NS}(E^n) \simeq \mathrm{NS}(E^n_{\overline{K}})^{\mathrm{Gal}(\overline{K}|K)}$.

With the above notations,

- *if E has no complex multiplication (over K), then D_i for $i = 1, \dots, n$ and $C^1_{i,j}$ for $i < j$ is a basis for* $\mathrm{NS}(E^n)$.
- *if* $\mathrm{End}_K(E)$ *is an order in a quadratic imaginary field and κ, λ is a basis of* $\mathrm{End}_K(E)$, *then D_i for $i = 1, \dots, n$ and $C^{\kappa}_{i,j}$, $C^{\lambda}_{i,j}$ for $i < j$ is a basis for* $\mathrm{NS}(E^n)$.
- *if* $\mathrm{End}_K(E)$ *is an order in a quaternion algebra and $\kappa, \lambda, \mu, \nu$ is a basis of* $\mathrm{End}_K(E)$, *then D_i for $i = 1, \dots, n$ and $C^{\kappa}_{i,j}$, $C^{\lambda}_{i,j}$, $C^{\mu}_{i,j}$, $C^{\nu}_{i,j}$ for $i < j$ is a basis for* $\mathrm{NS}(E^n)$.

2.2.3 The Néron-Severi group of a twist

Let $K|k$ be a Galois field extension of odd degree and let E be a non-super-singular elliptic curve over k. Let A be an abelian k-variety such that $A_K \approx E^n_K$. We want to calculate the Néron-Severi-group of A as a subgroup of $\mathrm{End}_K(E^n_K) \simeq \mathrm{M}_n(\mathrm{End}_K(E_K))$.

By Lemma A.11, the Néron-Severi-group of A consists of those elements of the Néron-Severi-group of $A_K \approx E^n_K$ which are invariant under the Galois-action. For each $\boldsymbol{\sigma} \in G$, we have an arithmetic operation of A_K/K. Under the isomorphism $A_K \approx E^n_K$ this operation corresponds to an automorphism $\widetilde{\sigma}$ on E^n_K. $\widetilde{\sigma}$ is of the form $s_\sigma \sigma$ with σ the canonical automorphism of E^n_K/K and s_σ a K-automorphism of E^n_K.

Under our assumption that E be non-super-singular and n be odd, all endomorphisms of E_K are defined over k. So also all endomorphisms of E^n_K are defined over k and so all elements of $\mathrm{NS}(E^n_K)$ are invariant under σ and in order to determine the invariant elements under the action of $\widetilde{\sigma}$ we have to calculate which elements are invariant under s_σ for all $\boldsymbol{\sigma} \in G$.

A special case of Proposition A.15 is:

Let $x \in \mathrm{NS}(E^n_K)$, corresponding to a hermitian matrix $X \in \mathrm{M}_n(\mathrm{End}_k(E))$. Then $s^*_\sigma(x)$ corresponds to the matrix $\overline{S_\sigma}^\top X S_\sigma$.

This implies:

Proposition 2.16 *Let $K|k$ be a Galois field extension of with Galois group G of odd degree. Let E be a non-super-singular elliptic curve over k. Let A be an* *abelian k-variety such that $A_K \approx E_K^n$. Assume that all K-endomorphisms of E_K are defined over k. For each $\boldsymbol{\sigma} \in G$, the Galois-operation on A_K/K is defined by $\widetilde{\sigma} = \sigma s_\sigma$ where s_σ is a K-automorphism of E^n corresponding to a matrix $S_\sigma \in \mathrm{M}_n(End_K(E_K))$.*

Let $x \in \mathrm{NS}(E^n)$, corresponding to a hermitian matrix $X \in \mathrm{M}_n(\mathrm{End}_k(E))$. Then $x \in NS(A)$ iff for all $\boldsymbol{\sigma} \in G$,

$$\overline{S_\sigma}^\top X S_\sigma = X.$$

2.3 The Néron-Severi group of the trace-zero-hypersurface

In this section, we study the Néron-Severi group of the trace-zero-hypersurface N of the Weil-restriction of a non-super singular elliptic curve with respect to a cyclic Galois extension of odd degree. In particular, we want to know if N has a principal polarization; see Subsection 1.3.4.

Let $K|k$ be a cyclic Galois extension of degree n with Galois group G. Identify G with G^{opp} and let σ be a generating element of G.

Let E be an elliptic curve, W be the Weil-restriction of $E_K := E \otimes_k K$ with respect to $K|k$. Let N be the trace-zero-hypersurface, $\iota_N : N \hookrightarrow W$ the embedding.

2.3.1 The canonical polarization of the trace-zero-hypersurface

Let φ be the canonical principal polarization of E. Then $\mathbf{Res}_k^K(\varphi)$ is a principal polarization of W.

As in the end of Subsection 2.1.3, let Σ_n denote the set $\{0, \ldots, n-1\}$. Then $W_K \simeq E_K^{\Sigma_n}$, and under this identification $\mathbf{Res}_k^K(\varphi)$ is defined by the divisor $D := \sum_i D_i$ where $D_i := p_i^{-1}(0)$. (This divisor is Galois-invariant under the "twisted operation" and descends to a divisor on W.)

We call the pull-back of the polarization $\mathbf{Res}_k^K(\varphi)$ the *canonical polarization of N*. Since W is not the product of E and N but only isogenous to the product, the pull-back of this polarization is not principal.

Recall that with Proposition 2.9, the kernel of this polarization is

$$K(\iota_N^*(\mathcal{L}(D))) = E \cap N = E[n]. \tag{2.6}$$

This implies:

Proposition 2.17 *After the choice of the generator σ of* $\mathrm{Gal}(K|k)$*, N is canonically isomorphic to its dual.*

Proof Since the polarization $\phi_{\iota_N^*\mathcal{L}(D)}$ has kernel $E[n]$, $\widehat{N}$ is canonically isomorphic to $N/E[n]$.

Now choose a generator σ of $\mathrm{Gal}(K|k)$. The morphism $a_\sigma - \mathrm{id} : N \longrightarrow N$ has kernel $E[n]$. Thus this morphism induces an isomorphism of N with $N/E[n]$. □

We can give a sufficient condition so that N is isogenous to a principally polarized abelian variety.

Proposition 2.18 *Let $K|k$ be an extension of prime degree l. If the group scheme $E[l]$ has a non-trivial subgroup over k - e.g. if k contains an l-torsion-point of E or if* $\mathrm{char}(k) = l$, *then N is isogenous to a principally polarized abelian variety.*

Proof Any non-trivial subgroup of the group $E[l]$ is automatically a maximal isotropic subgroup of $\iota_N^*(\mathcal{L}(D))$; see [Mu, p.233-234]. [12] If E has a k-rational l-torsion point, then this point defines a prime subgroup. If $\mathrm{char}(k) = l$, then the Frobenius endomorphism of E is purely inseparable and has degree l. Its kernel defines a non-trivial (connected) subgroup of $E[l]$. □

To give an idea of the methods employed in this chapter, we give a new proof of equation (2.6).

If we identify $W_K \simeq E_K^G$ with $E_K^{\Sigma_n}$ where the "σ^i-th" factor corresponds to the i-th factor, then for any K-scheme S, the S-valued points of A_K are $P = (P_0, \ldots, P_{n-1})$ where $P_i \in E_K(S)$ and $P_0 + \cdots + P_{n-1} = 0$. So via $P = (P_0, \ldots, P_{n-1}) \mapsto (P_1, \ldots, P_{n-1})$, N_K is identified with E_K^{n-1}.

Under this identification of N_K with E_K^{n-1} the divisor $\iota_N^{-1}(D)$ is given by $\sum_{i=1}^{n-1} D_i + C$ where C is the kernel of $p_0 + \cdots + p_{n-1}$. By Proposition 2.15, the corresponding matrix is

$$\begin{pmatrix} 2 & 1 & \cdots & 1 & 1 \\ 1 & 2 & \ddots & 1 & 1 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 1 & 1 & \ddots & 2 & 1 \\ 1 & 1 & \cdots & 1 & 2 \end{pmatrix}.$$

By subtracting the lines one sees that all .-valued points of the kernel have the from $P = (P_1, \ldots, P_1)$. Then one sees that $P_1 \in E[n]$. □

We identify N_K with E_K^{n-1} as in the above proof. Then σ operates on N_K by $\widetilde{\sigma} = \sigma s$, where σ is the canonical arithmetic automorphism of E_K^{n-1}/K and the automorphism s is given by

$$(P_1, \ldots, P_{n-1}) \mapsto (P_2, P_3, \ldots, P_{n-1}, -P_1 - \cdots - P_{n-1}).$$

[12] In [Mu] it is proven that over an algebraically closed field every abelian variety is isogenous to a principally polarized abelian variety. This is not true over an arbitrary groundfield, the reason being that the kernel of a polarization need not have a non-trivial subgroup.

This corresponds to the matrix

$$S = \begin{pmatrix} 0 & 1 & \ddots & 0 \\ \vdots & \ddots & \ddots & 0 \\ 0 & \ddots & 0 & 1 \\ -1 & -1 & \cdots & -1 \end{pmatrix}. \tag{2.7}$$

As a special case of Proposition 2.16 we get:

Proposition 2.19 *Let $K|k$ be a cyclic Galois extension of perfect fields and let E be a non-super-singular elliptic curve. Assume that all K-endomorphism of E_K are defined over k. Let N be the trace-zero-hypersurface of the Weil-restriction with respect to $K|k$. Let S be defined as in equation (2.7). Then the Néron-Severi group of N corresponds to the subgroup of hermitian matrices X with entries in $\mathrm{End}_k(E)$ which satisfy*

$$S^\top X S = X.$$

2.3.2 A basis for the Néron-Severi group

From now on we assume that the degree n is odd and that E is non-super singular.

Recall that under our assumption that n be odd, all K-endomorphism of E_K are defined over k.

Let $n = 2m+1$. Then N is an abelian variety of dimension $2m$, $N_K \simeq E_K^{2m}$. We want to define a basis of $\mathrm{NS}(E^{2m}) = \mathrm{NS}(E_K^{2m})$ which is permuted under the operation of the Galois group of K over k, i.e. if x is an element of the basis, then $s^*(x)$ shall also be an element of the basis. Then the linear invariants of this basis form a basis of $\mathrm{NS}(N_K)^{\mathrm{Gal}(K|k)} \simeq \mathrm{NS}(N)$.

We consider the case that E has no complex multiplication first. In this case $\mathrm{NS}(E^{2m})$ is the group of symmetric $2m \times 2m$-matrices with entries in $\mathbb{Z}$, and so we want to find a basis for this group such that if X is an element of this basis, $S^\top X S$ is also an element of this basis.

Let E_{ij} be the matrix which is zero except at the entry (i,j) where it is 1.

Let $A_{i,j}$ be the matrix which is zero except at (i,j) and (j,i) where it is 1. (If $i = j$ there is only one non-zero entry.) So $A_{i,i} = E_{i,i}$ and $A_{i,j} = E_{i,j} + E_{j,i}$ for $i \neq j$. The $m(2m+1)$ matrices $A_{i,j}$ for $1 \leq i \leq j \leq n$ form a basis of the free abelian group of symmetric matrices with entries in $\mathbb{Z}$. For any symmetric matrix X, let $X = \sum_{i \leq j} X(i,j) A_{i,j}$ where $X(i,j) \in \mathbb{Z}$. We also write $X(j,i)$ for $X(i,j)$ $(i \leq j)$.

Let $B_l := \sum_{i=1,\cdots,2m} -E_{i,l} + \sum_{j=1,\cdots,2m} -E_{l,j} =$

$$\left(\begin{array}{cccccccc}
 & & & & l\text{-th column} & & & \\
 & & & & -1 & & & \\
 & & & & \vdots & & & \\
 & & & & -1 & & & \\
l\text{-th row} & -1 & \cdots & -1 & -2 & 1 & \cdots & 1 \\
 & & & & -1 & & & \\
 & & & & \vdots & & & \\
 & & & & -1 & & &
\end{array}\right).$$

Let $V := \sum_{1 \leq i,j \leq 2m} E_{i,j} = ((1))$ be the matrix whose entries are all 1.

Lemma 2.20 *Let m be a number. Then $A_{i,j}$ for $i \leq j, j-i \neq m, m+1$, B_l for $l \neq m, m+1$ and V form a basis for the free abelian group of symmetric $2m \times 2m$-matrices with entries in $\mathbb{Z}$.*

Proof The set defined in the lemma consists of $m(2m+1) - (2m-1)$ of the form $A_{i,j}$, $2m-2$ elements of the form B_l and V, thus the total number of elements is $m(2m+1)$ – as required for a basis.

We have to check that that the base change matrix from the basis $A_{i,j}$, $i, j = 1, \ldots, n$ to the elements in the lemma is invertible.

For this, we only have to check that the following $2m-1 \times 2m-1$-matrix is invertible:

$$\begin{pmatrix}
B_1(1, m+1) & \cdots & B_{m-1}(1, m+1) & B_{m+2}(1, m+1) & \cdots & B_{2m}(1, m+1) & V(1, m+1) \\
\vdots & & \vdots & \vdots & & \vdots & \vdots \\
B_1(m, 2m) & \cdots & B_{m-1}(m, 2m) & B_{m+2}(m, 2m) & \cdots & B_{2m}(m, 2m) & V(m, 2m) \\
B_1(1, m+2) & \cdots & B_{m-1}(1, m+2) & B_{m+2}(1, m+2) & \cdots & B_{2m}(1, m+2) & V(1, m+2) \\
\vdots & & \vdots & \vdots & & \vdots & \vdots \\
B_1(m-1, 2m) & \cdots & B_{m-1}(m-1, 2m) & B_{m+2}(m-1, 2m) & \cdots & B_{2m}(m-1, 2m) & V(m-1, 2m)
\end{pmatrix}$$

This is

$$\begin{pmatrix}
B_1 & B_2 & \cdots & B_{m-1} & B_{m+2} & \cdots & B_{2m-1} & B_{2m} & V \\
\downarrow & \downarrow & & \downarrow & \downarrow & & \downarrow & \downarrow & \downarrow \\
-1 & & & & 0 & \cdots & \cdots & 0 & 1 \\
 & -1 & & & -1 & & & & 1 \\
 & & \ddots & & & \ddots & & & \vdots \\
 & & & -1 & & & -1 & & 1 \\
0 & \cdots & \cdots & 0 & & & & -1 & 1 \\
-1 & & & & -1 & & & & 1 \\
 & -1 & & & & \ddots & & & 1 \\
 & & \ddots & & & & -1 & & \vdots \\
 & & & -1 & & & & -1 & 1
\end{pmatrix}.$$

Except for the sign this has the same determinant as

$$\begin{pmatrix} 1 & & & & 0 & \cdots & \cdots & 0 & 1 \\ & 1 & & & 1 & & & & 1 \\ & & \ddots & & & \ddots & & & \vdots \\ & & & 1 & & & 1 & & 1 \\ 0 & \cdots & \cdots & 0 & & & & 1 & 1 \\ 0 & & & & 1 & & & & 0 \\ & 0 & & & -1 & \ddots & & & 0 \\ & & \ddots & & & \ddots & 1 & & \vdots \\ & & & 0 & & & -1 & 1 & 0 \end{pmatrix}.$$

And the determinant of this matrix is

$$\det\begin{pmatrix} & & & 1 & 1 \\ 1 & & & & 0 \\ -1 & \ddots & & & 0 \\ & \ddots & 1 & & \vdots \\ & & -1 & 1 & 0 \end{pmatrix} = \det\begin{pmatrix} 1 & & & \\ -1 & \ddots & & \\ & \ddots & 1 & \\ & & -1 & 1 \end{pmatrix} = 1.$$

□

We now check that this basis is permuted under the Galois-operation, i.e. if X is an element of the basis, then $S^\top XS$ is another element of the basis.

We do some calculations first.

Let $j < 2m$. Then $E_{i,j}S = E_{i,j+1}$.

$E_{i,2m}S = \sum_{j=1,\dots,2m} -E_{i,j}$.

Let $i < 2m$. Then $S^\top E_{i,j} = E_{i+1,j}$.

$S^\top E_{2m,j} = \sum_{i=1,\dots,2m} -E_{i,j}$.

It follows

Let $i, j < 2m$. Then $S^\top E_{i,j}S = E_{i+1,j+1}$.

Let $i < 2m$. Then $S^\top E_{i,2m}S = S^\top(\sum_{j=1,\dots,2m} -E_{i,j}) = \sum_{j=1,\dots,2m} -E_{i+1,j}$.

Let $j < 2m$. Then $S^\top E_{2m,j}S = S^\top E_{2m,j+1} = \sum_{i=1,\dots,2m} -E_{i,j+1}$.

$S^\top E_{2m,2m}S = S^\top(\sum_{j=1,\dots,2m} -E_{2m,j}) = \sum_{i,j=1,\dots,2m} E_{i,j}$.

And this implies

Let $i < 2m$. Then $S^\top(\sum_{j=1,\dots,2m} E_{i,j})S = \sum_{j=1,\dots,2m-1} E_{i+1,j+1} + \sum_{j=1,\dots,2m} -E_{i+1,j} = -E_{i+1,1}$.

$S^\top(\sum_{j=1,\dots,2m} E_{2m,j})S = \sum_{i=1,\dots,2m,j=1,\dots,2m-1} -E_{i,j+1} + \sum_{i,j=1,\dots,2m} E_{i,j} = \sum_{i=1,\dots,2m} E_{i,1}$.

Let $j < 2m$. Then $S^\top(\sum_{i=1,\dots,2m} E_{i,j})S =$

$\sum_{i=1,\dots,2m-1} E_{i+1,j+1} + \sum_{i=1,\dots,2m} -E_{i,j+1} = -E_{1,j+1}$.
$S^\top(\sum_{i=1,\dots,2m} E_{i,2m})S = \sum_{i=1,\dots,2m-1\, j=1,\dots,2m} -E_{i+1,j} + \sum_{i,j=1,\dots,2m} E_{i,j} = \sum_{j=1,\dots,2m} E_{1,j}$.
And
$S^\top(\sum_{i,j=1,\dots,2m} E_{i,j})S =$
$(S^\top(\sum_{i=1,\dots,2m-1} \sum_{j=1,\dots,2m} E_{i,j})S + S^\top(\sum_{j=1,\dots,2m} E_{2m,j})S =$
$(\sum_{i=1,\dots,2m-1} -E_{i+1,1}) + (\sum_{i=1,\dots,2m} E_{i,1}) = E_{1,1}$.

It follows:

Lemma 2.21
Let $1 < i \leq j$. Then $S^\top A_{i,j} S = A_{i+1,j+1}$.
$S^\top A_{2m,2m} S = V$.
$S^\top V S = A_{1,1}$.
Let $i < 2m$. Then $S^\top A_{i,2m} S = B_{i+1}$.
$S^\top B_{2m} S = B_1$.
Let $l < 2m$. Then $S^\top B_l S = A_{1,l+1}$.

With this result it is easy to give a basis of $\mathrm{NS}(N)$ as a subgroup of $M_{2m\times 2m}(\mathbb{Z})$. For the convenient notation let for $l = 0, \dots, 2m-1$ $V_l := \sum_{i=1,\dots,2m-l} A_{i,i+l}$.

So if we call the main-diagonal the 0-diagonal and give numbers $1, \dots, 2m-1$ to the upper diagonals and numbers $-1, \dots, -2m+1$ to the lower diagonals, then V_i is zero except at the ith and $-i$th diagonal where all entries are 1.

It follows from the lemma that the following matrices define a basis of $\mathrm{NS}(N)$:
$V_0 + \sum_{i=0,\dots,2m-1} V_i$.
$V_1 + B_1 + B_{2m}$ if $m \geq 2$.
$V_l + V_{2m-l+1} + B_l + B_{2m-l+1}$ for $l = 2, \dots, m-1$ (if $2 \leq l \leq m-1$, then $m+1 < 2m-l+1 \leq 2m-1$).

We now study the case that E has complex multiplication (over k). Since we assumed that E is non-super-singular, $\mathrm{End}_k(E)$ is an order in an imaginary quadratic field. There exists an $\lambda\ \in\!\mathrm{End}_k(E)$ such that $1, \lambda$ is a basis of the free abelian group $\mathrm{End}_k(E)$. (If $(1, \lambda')$ is a basis of the main order and f is the conductor of the order then $(1, f\lambda')$ is a basis of $\mathrm{End}_k(E)$.)

With respect to this λ we want to define a basis of the free abelian group of hermitian $n \times n$-matrices with entries in $\mathbb{Z}[\lambda]\ =\!\mathrm{End}_k(E)$. The basis defined above will be a part of the new basis. Then we will show that the new elements of the basis are also permuted by the Galois action.

Let $i \neq j$. Let $A^\lambda_{i,j}$ be the matrix which is zero except at the places (i,j) and (j,i). At the place (i,j) it has value λ, at place (j,i) is has value $\overline{\lambda}$. So $A_{i,j} := \lambda E_{i,j} + \overline{\lambda} E_{j,i}$.

$A_{i,j}$ $(i \leq j), A^\lambda_{i,j}$ $(i < j)$ is a basis for the group of hermitian $n \times n$-matrices with entries in $\mathbb{Z}[\lambda]$. If X is any such matrix we define $X(i,j,\lambda)$ by $X = \sum_{i \leq j} X(i,j) A_{i,j} + \sum_{i<j} X(i,j,\lambda) A^\lambda_{i,j}$.

Let $B^\lambda_l := \sum_{i=1,\cdots,2m} -\lambda E_{i,l} + \sum_{j=1,\ldots,2m} -\overline{\lambda} E_{l,j} =$

$$\left(\begin{array}{cccccccc}
 & & & & l\text{-th column} & & & \\
 & & & & -\lambda & & & \\
 & & & & \vdots & & & \\
 & & & & -\lambda & & & \\
l\text{-th row} & -\overline{\lambda} & \cdots & -\overline{\lambda} & -\lambda - \overline{\lambda} & -\overline{\lambda} & \cdots & -\overline{\lambda} \\
 & & & & -\lambda & & & \\
 & & & & \vdots & & & \\
 & & & & -\lambda & & &
\end{array}\right).$$

Let $V^\lambda := \sum_{l=1,\ldots,2m} (\lambda + \overline{\lambda}) A_{l,l} + \sum_{1 \leq j < i \leq 2m} A^\lambda_{i,j} =$

$$\begin{pmatrix}
\lambda + \overline{\lambda} & \lambda & \ldots & \lambda \\
\overline{\lambda} & \ddots & \ddots & \vdots \\
\vdots & \ddots & \ddots & \lambda \\
\overline{\lambda} & \ddots & \overline{\lambda} & \lambda + \overline{\lambda}
\end{pmatrix}.$$

Lemma 2.22 *$A_{i,j}$ for $i \leq j, j - i \neq m, m+1$, B_l for $l \neq m, m+1$, $V, A^\lambda_{i,j}$ for $i < j, j - 1 \neq m, m+1$, B^λ_l for $l \neq m, m+1$ and V^λ form a basis for the free abelian group of hermitian $2m \times 2m$-matrices with entries in $\mathbb{Z}[\lambda]$.*

Proof We only have to check that the matrix

$$\begin{pmatrix}
B^\lambda_1(1, m+1, \lambda) & \ldots & B^\lambda_{m-1}(1, m+1, \lambda) & B^\lambda_{m+2}(1, m+1, \lambda) & \ldots & B^\lambda_{2m}(1, m+1, \lambda) & V^\lambda(1, m+1, \lambda) \\
\vdots & & \vdots & \vdots & & \vdots & \vdots \\
B^\lambda_1(m, 2m, \lambda) & \ldots & B^\lambda_{m-1}(m, 2m, \lambda) & B^\lambda_{m+2}(m, 2m, \lambda) & \ldots & B^\lambda_{2m}(m, 2m, \lambda) & V^\lambda(m, 2m, \lambda) \\
B^\lambda_1(1, m+2, \lambda) & \ldots & B^\lambda_{m-1}(1, m+2, \lambda) & B^\lambda_{m+2}(1, m+2, \lambda) & \ldots & B^\lambda_{2m}(1, m+2, \lambda) & V^\lambda(1, m+2, \lambda) \\
\vdots & & \vdots & \vdots & & \vdots & \vdots \\
B^\lambda_1(m-1, 2m, \lambda) & \ldots & B^\lambda_{m-1}(m-1, 2m, \lambda) & B^\lambda_{m+2}(m-1, 2m, \lambda) & \ldots & B^\lambda_{2m}(m-1, 2m, \lambda) & V^\lambda(m-1, 2m, \lambda)
\end{pmatrix}$$

is invertible. But this is the same matrix as the one considered in Lemma 2.20. □

Lemma 2.23
Let $i < j < 2m$. Then $S^\top A^\lambda_{i,j} S = A^\lambda_{i+1,j+1}$.
Let $i < 2m$. Then $S^\top A^\lambda_{i,2m} S = B^\lambda_{i+1}$.
$S^\top B^\lambda_{2m} S = B^\lambda_1$.
Let $l < 2m$. Then $S^\top B^\lambda_l S = A^\lambda_{1,l+1}$.
$S^\top V^\lambda S = V^\lambda$.

Proof Everything is proven by the calculations preceeding Lemma 2.21 but the last equation.
Now, $S^\top(\sum_{1\leq i\leq j\leq 2m} E_{i,j})S = S^\top(\sum_{1\leq i\leq j\leq 2m-1} E_{i,j})S + S^\top(\sum_{i=1,\ldots,2m} E_{i,2m})S = \sum_{2\leq i\leq j\leq 2m} E_{i,j} + \sum_{1\leq j\leq 2m} E_{1,j} = \sum_{1\leq i\leq j\leq 2m} E_{i,j}$
and
$S^\top(\sum_{1\leq j\leq i\leq 2m} E_{i,j})S = S^\top(\sum_{1\leq j\leq i\leq 2m-1} E_{i,j})S + S^\top(\sum_{j=1,\ldots,2m} E_{2m,j})S = \sum_{2\leq j\leq i\leq 2m} E_{i,j} + \sum_{1\leq i\leq 2m} E_{i,1} = \sum_{1\leq j\leq i\leq 2m} E_{i,j}$.
This implies $S^\top V^\lambda S = V^\lambda$. □

Let for $l = 1,\ldots,2m$ $V_l^\lambda := \sum_{l=1,\ldots,2m-l} A^\lambda_{i,i+l}$. Then the following matrices define a basis of $\mathrm{NS}(N)$:
$V_0 + \sum_{i=0,\ldots,2m-1} V_i$
$V_1 + B_1 + B_{2m}$ if $m \geq 2$
$V_l + V_{2m-l+1} + B_l + B_{2m-l+1}$ for $l = 2,\ldots,m-1$ (if $2 \leq l \leq m-1$, then $m+1 < 2m-l+1 \leq 2m-1$)
$V_1^\lambda + B_1^\lambda + B_{2m}^\lambda$ if $m \geq 2$
$V_l^\lambda + V_{2m-l+1}^\lambda + B_l^\lambda + B_{2m-l+1}^\lambda$ for $l = 2,\ldots,m-1$ (if $2 \leq l \leq m-1$, then $m+1 < 2m-l+1 \leq 2m-1$)
$V^\lambda = (\lambda+\overline{\lambda})V_0 + \sum_{l=1,\ldots,2m-1} V_l^\lambda$.

We get the following proposition:

Proposition 2.24 *Let $K|k$ be a cyclic Galois extension of perfect fields of degree $n = 2m+1$. Let E be a non-super-singular elliptic curve over k. Let N be the trace-zero-hypersurface of the Weil-Restriction of E_K with respect to $K|k$. Then* $\mathrm{NS}(N)$*, the Néron-Severi group of N, equals* $\mathrm{NS}(N)^{\mathrm{Gal}(\overline{k}|k)}$ *and is canonically a subgroup of the matrix group* $\mathrm{M}_{2m\times 2m}(\mathrm{End}_k(E))$*. Under this inclusion, the free abelian group* $\mathrm{NS}(N)$ *has the following basis:*

If E has no complex multiplication:
$F_0 := V_0 + \sum_{l=0,\ldots,2m-1} V_l$ *– this defines the canonical polarization of N*
$F_1 := V_1 + B_1 + B_{2m}$ *if* $m \geq 2$
$F_l := V_l + V_{2m-l+1} + B_l + B_{2m-l+1}$ *for* $l = 2,\ldots,m-1$ *(if* $2 \leq l \leq m-1$*, then* $m+1 < 2m-l+1 \leq 2m-1$*).*
In particular, $\mathrm{NS}(N)$ *is m-dimensional.*

If E has complex multiplication and $1,\lambda$ is a basis of $End_k(E)$:
$F_0,\ldots,F_{m-1}$ *and*
$F_0^\lambda := (\lambda+\overline{\lambda})V_0 + \sum_{l=1,\ldots,2m-1} V_l^\lambda$.
$F_1^\lambda := V_1^\lambda + B_1^\lambda + B_{2m}^\lambda$ *if* $m \geq 2$
$F_l^\lambda := V_l^\lambda + V_{2m-l+1}^\lambda + B_l^\lambda + B_{2m-l+1}^\lambda$ *for* $l = 2,\ldots,m-1$
In particular, $\mathrm{NS}(N)$ *is $2m$-dimensional.*

In this proposition, we use the same notations as above, i.e.
$B_l := \sum_{i=1,\cdots,2m} -E_{i,l} + \sum_{j=1,\ldots,2m} -E_{l,j}$

$B_l^\lambda := \sum_{i=1,\cdots,2m} -\lambda E_{i,l} + \sum_{j=1,\dots,2m} -\overline{\lambda} E_{l,j}$
$V_l := \sum_{i=1,\dots,2m-l} E_{i,i+l} + \sum_{j=1,\dots 2m-l} E_{j+l,j}$ for $l \geq 0$
$V_l^\lambda := \sum_{i=1,\dots,2m-l} \lambda E_{i,i+l} + \sum_{j=1,\dots,2m-l} \overline{\lambda} E_{j+l,j}$ for $l \geq 1$.

Definition Let $\mathcal{G}_m$ be the subgroup of $M_{2m\times 2m}(\mathbb{Z})$ which is generated by the matrices $F_0, \dots, F_m$. We have seen that $F_0, \dots, F_m$ is a basis for this group.

Let N be the trace-zero-hypersurface as above. Then $\mathrm{NS}(N)$ is embedded in $\mathrm{M}_n(\mathrm{End}_k(E))$, and the elements of $\mathrm{NS}(N)$ which correspond under this injection to elements of $\mathcal{G}_m$ define a subgroup of $\mathrm{NS}(N)$ which we call the *generic part* of $\mathrm{NS}(N)$. Loosely speaking, the elements of the generic part of $\mathrm{NS}(N)$ are those elements which "do not come from complex multiplication". In particular, if E has no complex multiplication, the generic part of $\mathrm{NS}(N)$ is the full group.

Theorem 7 *Let $K|k$ be a cyclic Galois extension of perfect fields of odd degree n. Let E be a non-super-singular elliptic curve over k. Let N be the trace-zero-hypersurface of the Weil-Restriction of E_K with respect to $K|k$. Then* $\mathrm{NS}(N)$*, the Néron-Severi group of N, equals* $\mathrm{NS}(N_{\overline{k}})^{\mathrm{Gal}(\overline{k}|k)}$.

If E has no complex multiplication (over k), the kernel of any element of $\mathrm{NS}(N)$ *contains the group scheme $E \cap N = E[n]$ of n-torsion points of E.*

If E has complex multiplication, the statement is true for all elements of the generic part of $\mathrm{NS}(N)$ *defined above.*

Proof Let $n = 2m+1$. Under the isomorphism $N_K \simeq E_K^{2m}$, the .-valued points of $E_K[n]$ correspond to the .-valued points of E_K^{2m} which are of the form $(P, \dots, P)$ for $P \in E_K[n]$. We claim that for $l = 0, \dots, m-1$, the sum of all the columns of F_l is a vector of the form $n \begin{pmatrix} a_1 \\ \vdots \\ a_{2m} \end{pmatrix}$ with $a_i \in \mathbb{Z}$. It follows from this claim that all .-valued points of $E[n]$ are mapped to zero under every element of the generic part of $\mathrm{NS}(N)$.

The claim is obviously true for F_0; see Proposition 2.9 with the second proof, p. 50.

We make two *definitions*:
First, for every symmetric $2m \times 2m$-matrix X, we denote $\sum_{j=1,\dots,2m} X(i,j)$ by $X^{(i)}$. The claim is then that for all $l = 1, \dots,\ m, i = 1, \dots, 2m$, $F_l^{(i)}$ is divisible by n.
Second, for $1 \leq i \leq j \leq 2m$ let $\chi_{[i,j]} := \sum_{\gamma=i,\dots,j} \delta_{\gamma,.} : \{1, \dots, 2m\} \longrightarrow \mathbb{Z}$, i.e. $\chi_{[i,j]}(\mu) = 1$ iff $i \leq \mu \leq j$ and 0 otherwise. $(1 \leq \mu \leq 2m)$

Then $V_l^{(.)} = \chi_{[1,2m-l]} + \chi_{[l+1,2m]}$.

In particular, $V_1^{(1)} = 1$, $V_1^{(i)} = 2$ for $2 \leq i \leq 2m-1$, $V_1^{(2m)} = 1$. Thus $V_1^{(i)} = 2 - \delta_{1,i} - \delta_{2m,i}$.

Further, for $l = 2, \leq m-1$, $1 \leq i \leq 2m$, $(V_l + V_{2m-l+1})^{(i)} = (\chi_{[1,2m-l]} + \chi_{[l+1,2m]} + \chi_{[1,l-1]} + \chi_{[2m-l+2,2m]})(i) = 2 - \delta_{l,i} - \delta_{2m-l+1,i}$.

It follows for $l = 1, \dots m-1$:
For $i \neq l, 2m-l+1$ is $F_l^{(i)} = 2 + B_l(i,l) + B_{2m-l+1}(i, 2m-l+1) = 2 - 2 = 0$.
$F_l^{(l)} = 1 + \sum_{j=1,\dots,2m} B_l(l,j) + B_{2m-l+1}(l, 2m-l+1) = 1 - (2m+1) - 1 = -(2m+1) = -n$.
$F_l^{(2m-l+1)} = 1 + \sum_{j=1,\dots,2m} B_{2m-l+1}(2m-l+1, j) + B_l(2m-l+1, l) = 1 - (2m+1) - 1 = -(2m+1) = -n$. □

If follows:

Corollary 2.25 *No element of the generic part of NS(N) defines a principal polarization.*

We already know that the canonical polarization has kernel $E[n]$. So:

Corollary 2.26 *Let E have no complex multiplication (over k). Then N is not principally polarized. If n is a prime, N is isogenous to a principally polarized abelian variety iff $E[n]$ has a non-trivial sub-groupscheme over k.*

2.3.3 Complex multiplication

Let $K|k$ be as above and let E be a non-super-singular elliptic curve with complex multiplication (over k). We want to study whether the trace-zero-hypersurface N is principally polarized. Since $\mathrm{NS}(N) \simeq \mathrm{NS}(N_{\overline{k}})^{\mathrm{Gal}(\overline{k}|k)}$, all polarizations of N are defined by ample sheaves on N itself.

With Proposition 2.24 and the help of Lemmata 2.12 and 2.14 the question whether N has a principal polarization is equivalent to a numerical conditions:

There exists a sheaf with Euler characteristic 1 iff the polynomial equation of degree $2m$ in $2m$ variables

$$\det(x_0 F_0 + \cdots + x_{m-1} F_{m-1} + y_0 F_0^\lambda + \cdots + y_{m-1} F_{m-1}^\lambda) = \pm 1$$

is solvable in the integers.

A solution to this equation defines a principal polarization iff $x_0 F_0 + \cdots + x_{m-1} F_{m-1} + y_0 F_0^\lambda + y_{m-1} F_{m-1}^\lambda$ has only positive eigenvalues. (Of course, this implies that the determinant had to be 1 in the above equation.)

We now perform these calculations explicitely for $n = 3$.

Under our assumption of non-super-singularity, $\mathrm{End}_k(E)$ is an order in the imaginary quadratic field $\mathrm{End}_k^0(E)$. Let $\mathrm{End}_k^0(E) = \mathbb{Q}(\sqrt{D}), D < 0$ and let $\delta := \sqrt{D}$. There exists an $f \in \mathbb{N}$ such that $\mathrm{End}_k(E)$ is of the form $\mathbb{Z} + f\mathcal{O}$ where $\mathcal{O}$ is the main order in the field $\mathrm{End}_k^0(E)$ (i.e. it is the normal closure of $\mathbb{Z}$). The number f is called the *conductor* of the order.

$D \equiv 2, 3$ *mod* 4 Then $1, f\delta$ is a basis of $\mathrm{End}_k(E)$.

Note that if X is some 2×2-matrix with $\det(X) > 0$ then either X or $-X$ has positive eigenvalues. So there exists a principal polarization on N iff

$$1 \overset{!}{=} \det(xF_0 + yF_0^{f\delta}) = \det \begin{pmatrix} 2x & x + yf\delta \\ x - yf\delta & 2x \end{pmatrix} = 3x^2 + y^2 f^2 D$$

is solvable for $x, y \in \mathbb{Z}$.

$D \equiv 1$ *mod* 4 Then $1, f\frac{1+\delta}{2}$ is a basis of $\mathrm{End}_k(E)$.

$$xF_0 + yF_0^{f\frac{1+\delta}{2}} = \begin{pmatrix} 2x + yf & x + yf\frac{1+\delta}{2} \\ x + yf\frac{1-\delta}{2} & 2x + yf \end{pmatrix}$$

The determinant of this matrix is

$$\begin{gathered} 4x^2 + 4xyf + y^2 f^2 - x^2 - xyf\frac{1+\delta}{2} - xyf\frac{1-\delta}{2} - y^2 f^2 \frac{1-D}{4} = \\ 3x^2 + xy(4f - f) + y^2 f^2 \frac{4 - 1 + D}{4} = \\ 3x^2 + 3xyf + y^2 f^2 \frac{3+D}{4} \end{gathered}$$

So in this case N has a principal polarization iff

$$3x^2 + 3xyf + y^2 f^2 \frac{3+D}{4} = 1$$

is solvable with $x, y \in \mathbb{Z}$.

Theorem 8 *Let $K|k$ be a Galois field extension of perfect fields of degree 3. Let E be a non-super-singular elliptic curve over k. Let N be the trace-zero-surface of the Weil-restriction of E_K with respect to $K|k$.*

If E has no complex multiplication (over k), then the Néron-Severi group of N is a free abelian group on 1 generator, generated by an ample sheaf with kernel $E[3]$. In particular, N is not principally polarized.

If E has complex multiplication (over k), then $\mathrm{NS}(N)$ is a free abelian group on 2 generators. Let $\mathrm{End}_k^0(E) = \mathbb{Q}(\sqrt{D}), D < 0$. Let f be the conductor of the order $\mathrm{End}_k(E)$. Then:

If $D \equiv 2, 3$ mod 4, then N is principally polarized iff $3x^2 + y^2 f^2 D = 1$ is solvable in $\mathbb{Z}$.

If $D \equiv 1$ mod 4 then N is principally polarized iff $3x^2 + 3xyf + y^2 f^2 \frac{3+D}{4} = 1$ is solvable in $\mathbb{Z}$.

2.4 Curves on the trace-zero-hypersurface for degree 3

For this section, let $K|k$ be a Galois field extension of perfect fields of degree 3, E an elliptic k-curve, W the Weil-restriction of A_K with respect to $K|k$ and N the trace-zero-hypersurface on W. [13]

We want to study the trace-zero-surface N using explicit equations and thereby relate the results of the previous section with explicit calculations on N.

By a theorem of A.Weil, a principal polarization of an abelian surface A over some field k is defined by a proper geometrically reduced curve on A which is either non-singular, geometrically irreducible and of genus 2 or geometrically the pointed union of two elliptic curves. In the first case, A is the Jacobian of this curve, in the second $A_{\overline{k}}$ is isomorphic to the direct product of the two elliptic curves; see Proposition A.27 in Subsection A.2.7 in the appendix.

Now let A be a simple abelian surface which is isogenous to a principally polarized abelian surface $\widetilde{A}$, i.e. there exists an isogeny $\pi : \widetilde{A} \longrightarrow A$. Assume that π is not an isomorphism. Then if the polarization on $\widetilde{A}$ is given by a geometrically irreducible curve, the image of this curve on A is a singular curve whose normalization has genus 2, and if the polarization on $\widetilde{A}$ is given geometrically by two elliptic curves, the images of these elliptic curves are still elliptic curves, but they intersect in more than one point.

We want to find these curves in cases in which we know that the trace-zero-hypersurface is isogenous to a principally polarized abelian variety.

We will succeed insofar as for $\text{char}(k) = 3$, we will find a curve on N whose normalization has genus 2. If $\text{char}(k) > 3, \zeta_3 \in k$ and the x-coordinate of a 3-torsion point lies in k, we will find such a curve after possibly a quadratic extension of k.

Before starting with the concrete calculations we remark that by Corollary 2.8 if E is non-super-singular and $\zeta_3 \notin \text{End}_k(E)$, N is simple. Now, curves with j-invariant 0 have an endomorphism algebra which contains ζ_3. Thus with [Mu, Appendix I, p.258, Corollary], we conclude that if k is finite, N is simple provided that E is non-super-singular and $E_{\overline{k}}$ is not isogenous to an elliptic curve with j-invariant 0.

2.4.1 The trace-zero-hypersurface for $\text{char}(k) \neq 2, 3$ [14]

Let $\text{char}(k) \neq 2, 3$ and assume that the 3-rd roots of unity are contained in k. We want to calculate equations of the trace-zero-hypersurface N.

[13] If S is a closed subscheme of a variety V, we say that S is *on* V.

[14] The results in this subsection are based on calculations by G.Frey and N.Naumann. Some corrections and additional remarks are due to the author.

Let $\zeta_3 \in k$ be a third root of unity. (If $k = \mathbb{F}_p$, p prime, this means that $p \equiv 1 \bmod 3$.) By Kummer-theory, there exists an $\alpha \in k$ with $\alpha^3 = a \in k$. Let $\sigma \in \mathrm{Gal}(K|k)$ be given by $\sigma(\alpha) = \zeta_3 \alpha$.

Let the elliptic curve E be defined by the affine equation

$$Y^2 = X^3 + AX + B, \tag{2.8}$$

where $A, B \in k$.

According to the "construction of the Weil-restriction by restriction of scalars" (see Subsection 1.1.3), we make the substitutions

$$\begin{aligned} X &= x_0 \otimes_k 1 + x_1 \otimes_k \alpha + x_2 \otimes_k \alpha^2 \\ Y &= y_0 \otimes_k 1 + x_1 \otimes_k \alpha + x_2 \otimes_k \alpha^2 \end{aligned} \tag{2.9}$$

and get the equation

$$\begin{gathered} (y_0 \otimes_k 1 + x_1 \otimes_k \alpha + x_2 \otimes_k \alpha^2)^2 = \\ (x_0 \otimes_k 1 + x_1 \otimes_k \alpha + x_2 \otimes_k \alpha^2)^3 + A(x_0 \otimes_k 1 + x_1 \otimes_k \alpha + x_2 \otimes_k \alpha^2) + B \otimes_k 1. \end{gathered}$$

Expanding out this equation, we get:

$$\begin{aligned} y_0^2 + 2ay_1y_2 &= x_0^3 + ax_1^3 + a^2x_2^3 + 6ax_0x_1x_2 + Ax_0 + B, \\ ay_2^2 + 2y_0y_1 &= 3x_0^2x_1 + 3ax_0x_2^2 + 3ax_1^2x_2 + Ax_1, \\ y_1^2 + 2y_0y_2 &= 3x_0^2x_2 + 3x_0x_1^2 + 3ax_1x_2^2 + Ax_2. \end{aligned} \tag{2.10}$$

This system of equations defines an open, affine part W_0 of the Weil-restriction of W in $\mathbb{A}^6_k$, the 6-dimensional affine space over k. (The closed subset $W \backslash W_0$ is equal to the support of the divisor D defining the "canonical" polarization of W.)

We want to calculate the intersection of the trace-zero-hypersurface N with W_0. We will denote this surface by N_0. We think of N_0 as a surface in $\mathbb{A}^6_k$.

The trace zero-hypersurface is defined by expanding the equation [15]

$$\begin{gathered} P \oplus \sigma(P) = \ominus\sigma^2(P), \\ (P \text{ a } A \otimes_k K\text{-valued point of E for some } k\text{-algebra } A.) \end{gathered} \tag{2.11}$$

Let P be a $A \otimes_k K$-valued point of E which corresponds to a A-valued point on W_0 and satisfies this equation for the X-coordinate, i.e.:

$$X(P \oplus \sigma(P)) = X(\ominus\sigma^2(P)) = X(\sigma^2(P)) \tag{2.12}$$

Then P satisfies (2.11) or it satisfies

$$P \oplus \sigma(P) = \sigma^2(P) \tag{2.13}$$

If this is the case, $P = \sigma^2(P) \ominus \sigma(P)$, and thus the A-valued point of W corresponding to P factors through E. This means that $P = \sigma(P) = \sigma^2(P)$, and substituting this into (2.13), we get $P = 0$, the zero on E. But this is not possible since the zero on E corresponds to a point of W which does not lie on W_0. Thus we may use equation (2.12) instead of (2.11).

[15] In this section, in order to distinguish the addition on E from addition of coordinates, we write $\oplus$ for the addition on E.

We now want to use the "usual" group law on an elliptic curve E with Weierstraß-equation given as above; see [Si, III,2]. For a $\overline{k}$-valued point P, let $(x(P), y(P))$ denote the coordinates. Then, if P_1, P_2 are two $\overline{k}$-valued points with $x(P_1) \neq x(P_2)$,

$$x(P_1 \oplus P_2) = \left(\frac{y(P_2) - y(P_1)}{x(P_2) - x(P_1)}\right)^2 - x(P_1) - x(P_2). \tag{2.14}$$

To use this formula, we restrict ourselves from $A \otimes_k K$-valued points as above to $\overline{k} \otimes_k K \simeq \overline{k}^3$-valued points. This is possible because the subvariety N_0 of W_0 is uniquely determined by its $\overline{k}$-valued points.

Let P_1 and P_2 be two $\overline{k}^3$-valued points with x-coordinate $x(P_i) = (x^{(1)}(P_i), x^{(2)}(P_i), x_3^{(3)}(P_i))$. Then because of the isomorphism $E(\overline{k}^3) \simeq E(\overline{k})^3$, equation (2.14) remains valid if $x_i(P_1) \neq x_i(P_2)$ for $i = 1, 2, 3$.

Let $X = x_0 \otimes_k 1 + x_1 \otimes_k \alpha + x_2 \otimes_k \alpha^2 \in \overline{k} \otimes_k K$. Then X corresponds to $(x^{(1)}, x^{(2)}, x^{(3)}) \in \overline{k}^3$ where $x^{(i)} = (\mathrm{id}_{\overline{k}} \otimes_k \sigma^{i-1})(X) = x_0 + \zeta_3^{i-1}\alpha x_1 + \zeta_3^{2(i-1)}\alpha^2 x_2$.

Let $P \in E(\overline{k} \otimes_k K)$ with x-coordinate $X = x_0 \otimes_k 1 + x_1 \otimes_k \alpha + x_2 \otimes_k \alpha^2 \in \overline{k} \otimes_k K$. We want to apply the group law (2.14) to X and $\sigma(X)$. This is possible if $x^{(i)} \neq x^{(j)}$ for i, j with $i \neq j$. We have

$$\begin{gathered} x^{(i)} = x^{(j)} \longleftrightarrow \\ x_0 + \zeta^{i-1}\alpha x_1 + \zeta_3^{i-1}\alpha^2 x_2 = x_0 + \zeta_3^{j-1}\alpha x_1 + \zeta_3^{j-1}\alpha^2 x_2 \longleftrightarrow \\ (\zeta_3^{i-1} - \zeta_3^{j-1})x_1 = \alpha(\zeta_3^{2(i-1)} - \zeta_3^{2(j-1)})x_2. \end{gathered} \tag{2.15}$$

Thus the group law (2.14) remains valid outside the intersection of W_0 with the three hyperplanes in $\mathbb{A}_k^6$ defined by (2.15). We denote the union of these hyperplanes by H. We resrict ourselves to the subvariety $W_0 \backslash H$.

Now equation (2.12) is equivalent to

$$\left(\frac{\sigma(Y) - Y}{\sigma(X) - X}\right)^2 = X + \sigma(X) + \sigma^2(X). \tag{2.16}$$

Under the substitutions (2.9), this is equivalent to

$$((y_1 - \zeta_3 y_1) \otimes_k \alpha + (y_2 - \zeta_3^2 y_2) \otimes_k \alpha^2)^2 = 3x_0((x_1 - \zeta_3 x_1) \otimes_k \alpha + (x_2 - \zeta_3^2 x_2) \otimes_k \alpha^2)^2.$$

Expanding out one obtains

$$\begin{gathered} (1 - \zeta_3)(1 - \zeta_3^2)a\,(y_1 y_2 - 3x_0 x_1 x_2) \otimes_k 1 + (1 - \zeta_3^2)^2 a\,(y_2^2 - 3x_0 x_2^2) \otimes_k \alpha + \\ (1 - \zeta_3)^2 a\,(y_1^2 - 3x_0 x_1^2) \otimes_k \alpha^2 = 0. \end{gathered}$$

Thus as a subvariety of $W_0 \backslash H$, $N_0 \backslash H$ is defined by

$$\begin{aligned} y_1 y_2 &= 3x_0 x_1 x_2 \\ y_1^2 &= 3x_0 x_1^2 \\ y_2^2 &= 3x_0 x_2^2. \end{aligned} \tag{2.17}$$

We can insert these equations into (2.10). Thus $N_0\backslash H$ is defined (as a subvariety of $\mathbb{A}_k^6\backslash H$) by (2.17) and

$$\begin{array}{rcl} y_0^2 & = & x_0^3+ax_1^3+a^2x_2^3+Ax_0+B \\ 2y_0y_1 & = & 3x_0^2x_1+3ax_1^2x_2+Ax_1 \\ 2y_0y_2 & = & 3x_0^2x_2+3ax_1x_2^2+Ax_2. \end{array} \tag{2.18}$$

Note that the variety defined by (2.17) and (2.18) in $\mathbb{A}_k^6$ contains E, thus it is not birational to N_0.

Now regard the projection

$$q:\mathbb{A}_k^6\longrightarrow\mathbb{A}_k^4,\ (x_0,x_1,x_2,y_0,y_1,y_2)\mapsto(x_0,x_1,x_2,y_0).$$

The restriction of q to the variety defined by (2.17) and (2.18) is an isomorphism outside $y_0=0$, because for $y_0\neq0$, we can divide the last two equations of (2.18) by $2y_0$ and thus obtain equations for y_1 and y_2. (For $y_0=0$, the projection induces a 2-fold covering: For $y_0=0$, equation (2.18) imposes no condition on y_1,y_2, and by (2.17), (y_1,y_2) is only determined up to a sign.)

Multiplying the resulting equations by $4y_0^2$ and dividing by x_1x_2, x_1^2 and x_2^2 respectively (which is possible outside H), (2.17) becomes

$$(3x_0^2+3ax_1x_2+A)^2=12x_0y_0^2. \tag{2.19}$$

Thus under q, $N_0\backslash(H\cup\{y_0=0\})$ is isomorphic to the variety defined by this equation and the first equation of (2.18), i.e. to the variety defined by the following equations in $\mathbb{A}_k^4\backslash(q(H)\cup\{y_0=0\})$.

$$\begin{array}{rcl} y_0^2 & = & x_0^3+ax_1^3+a^2x_2^3+Ax_0+B \\ (3x_0^2+3ax_1x_2+A)^2 & = & 12x_0(x_0^3+ax_1^3+a^2x_2^3+Ax_0+B) \end{array} \tag{2.20}$$

Let N_1 be the variety defined by these two equations in $\mathbb{A}_k^4$. We now want to show that N_1 has only one irreducible component and thus is birational to $N_0=N\cap W_0$ or – what is the same – to N.

The second equation defines by Krull's Principal Ideal Theorem ([Ei, Theorem 10.1]) a subscheme of pure dimension 2 in $\mathbb{A}_k^3$; the projection $r:\mathbb{A}_k^4\longrightarrow\mathbb{A}_k^3:(x_0,x_1,x_2,y_0)\mapsto(x_0,x_1,x_2)$ restricts to a finite (thus surjective) morphism of degree 2 from N_1 to the scheme defined by the second equation.

We study the scheme defined by the second equation first. We know that this scheme is outside $r\circ q(H)$ isomorphic to $r\circ q(N_0)$. If it had more than one component, the additional component would have to be contained in $r\circ q(H)$. Since it has pure dimension 2, the additional component would have to be the image of one component of H under $r\circ q$. But the intersection of the scheme defined by the second equation with H is at most 1-dimensional and so the scheme does not have such a component.

Since no component of the variety defined by the second equation lies in $r\circ q(H)$, no component of N_1 lies in $r^{-1}(rq(H))=p(H)$. Thus N_1 is birational to N_0, more precisely, the restriction of p to N_1 is a birational map to N_1 which is an isomorphism outside $H\cup\{y_0=0\}$.

There is a fibration by projection onto x_0. We will now examine the resulting curves if we fix x_0. The intersection of these curves with $p(H)$ and $y_0 = 0$ respectively is 0-dimensional and so these curves are birational to curves which lie on N. [16]

Let $x_0 \neq 0$ be fixed.

By (2.19), the fibers under the projections to x_0 consist (geometrically) of two isomorphic components – defined by the second equation of (2.20) (which might itself be reducible), both defined over $k(\sqrt{12x_0})$.

Let C_0 denote the affine k-scheme defined by the second equation. We claim that C_0 is a geometrically irreducible, geometrically reduced k-curve.

Proof Let $f(x_1, x_2) := (3x_0^2 + 3ax_1x_2 + A)^2 - 12x_0(x_0^3 + ax_1^3 + a^2x_2^3 + Ax_0 + B)$ be the defining polynomial of C_0.

Consider the morphism $C_{0\overline{k}} \longrightarrow \mathbb{A}^1_{\overline{k}}$ defined by $(x_1, x_2) \mapsto x_1$, corresponding to the inclusion $\overline{k}[x_1] \hookrightarrow \overline{k}[x_1, x_2]/(f)$.

Under all specializations $\overline{k}[x_1] \longrightarrow \overline{k}$ as well as under the inclusion $\overline{k}[x_1] \longrightarrow \overline{k}(x_1)$, the polynomial f has degree 3.

Thus for some topological point x of $\mathbb{A}^1_{\overline{k}}$, the fiber of the morphism $C_{0\overline{k}} \longrightarrow \mathbb{A}^1_{\overline{k}}$ at the fixed point x is given by a 3-dimensional algebra over the corresponding residue class field at x.

In particular, the generic points of $C_{0\overline{k}}$ are mapped to the generic point of $\mathbb{A}^1_{\overline{k}}$.

This implies that the scheme $C_{0\overline{k}}$ is irreducible iff the fiber over the generic point of $\mathbb{A}^1_{\overline{k}}$ is, i.e. if the nilideal in the spectrum of the algebra $\overline{k}(x_1)[x_2]/(f)$ is prime. Further, since $\overline{k}[x_1, x_2]/(f) \longrightarrow \overline{k}(x_1)[x_2]/(f)$ is an inclusion, the scheme $C_{0\overline{k}}$ is reduced iff the algebra $\overline{k}(x_1)[x_2]/(f)$ is.

Thus $C_{0\overline{k}}$ is integral iff the algebra $\overline{k}(x_1)[x_2]/(f)$ is a field. This is the case iff the polynomial f is irreducible over $\overline{k}(x_1)$.

Now, if f was reducible over $\overline{k}(x_1)$, it would contain a factor of degree 1. This would mean that the the reduced algebra $(\overline{k}(x_1)[x_2]/(f))^{\mathrm{red}}$ splits into the direct sum of $\overline{k}(x_1)$ and another $\overline{k}(x_1)$-algebra which would imply that $C_{0\overline{k}}^{\mathrm{red}}$ would contain a rational curve. This rational curve would be birational to a curve on the abelian surface $N_{\overline{k}}$ which is impossible. □

Let C be the closure of C_0 in $\mathbb{P}^2_k$. This means that C is obtained by writing the second equation of (2.20) in homogeneous form (where x_0 is a constant), i.e. C is given by

$$(3x_0^2z^4 + 3ax_1x_2 + Az^4)^2 = 12x_0(x_0^3z^4 + ax_1^3z + a^2x_2^3z + (Ax_0 + B)z^4).$$

Setting $z = 0$, we obtain

$$(3ax_1x_2)^2 = 0.$$

[16] We use the following fact: Let V be a proper k-variety, C a smooth k-curve, C_0 an open, affine part of C and $C_0 \longrightarrow V$ a k-morphism. Then this morphism can be extended to a k-morphism $C \longrightarrow V$.

Thus there are two points at infinity: $[1:0:0]$ and $[0:1:0]$.

The derivative with respect to z is for $z = 0$

$$12x_0(ax_1^3 + a^2x_2^3),$$

and this is non-zero for the two points at infinity. Thus there are no singularities of C at infinity.

The geometric operation a_σ on W defined by the arithmetic operation σ on A_K is given by $(y_0, x_0, x_1, x_2) \mapsto (y_0, x_0, \zeta_3 x_1, \zeta_3^2 x_2)$. Analogously, one gets an operation on C. In particular, singularities outside $(x_1, x_2) = (0,0)$ occur in triples.

Now, the arithmetic genus of C_0 is $\frac{(4-1)(4-2)}{2} = 3$, and this is equal to the genus of the normalization of C_0 plus the singularity degree. (And the singularity degree is larger or equal the number of singularities.) Thus if C_0 had singularities outside $(0,0)$, it would be a rational curve. But on the other hand, C is birational to a curve on the abelian variety N. Thus it cannot be a rational curve since there are no such curves on abelian varieties.

Thus the only possible singularity of C_0 is $(x_1, x_2) = (0,0)$.

Specializing the defining equation to this point, we get:

$$(3x_0^2 + A)^2 = 12x_0(x_0^3 + Ax_0 + B),$$

i.e.

$$3x_0^4 + 6Ax_0^2 + 12Bx_0 - A^2 = 0$$

This is the 3rd division polynomial of E; see [Si, III,10,Exercise 3.7]. Thus $(0,0)$ is a point on C iff x_0 is the x-coordinate of a 3-torsion point. We now check if $(0,0)$ is a singularity: The derivatives of the defining equation of C with respect to x_1 and x_2 to the point $(0,0)$ are both 0. Thus if $(0,0)$ is a point on C_0, it is a singularity.

Assume that this is the case and furthermore that $\zeta_3 \notin \mathrm{End}_{\overline{k}}(E_{\overline{k}})$. Then by Theorem 5, $N \otimes_k k(\sqrt{12x_0})$ is simple and the genus of the normalization of C is 2.

If x_0 is not the x-coordinate of a 3-torsion point, C_0 is non-singular. Being a quadric curve in $\mathbb{P}^2_{k(\sqrt{12x_0})}$, it is a so-called canonical curve; see [Ha, IV, Example 5.2.1.].

We get the following result:

For any $x_0 \neq 0$, there are two curves on $N \otimes_k k(\sqrt{12x_0})$ which are birational to the curve C (which depends on x_0). If $x_0 \neq 0$ is not the x-coordinate of a 3-torsion point, C is a non-singular curve which is a so-called canonical curve of genus 3. However, if x_0 is the x-coordinate of a 3-torsion point, C is singular, and under the assumption $\zeta_3 \notin \mathrm{End}_{\overline{k}}(E_{\overline{k}})$, the genus of the normalization of C is 2.

Now let $x_0 = 0$.

Then the second equation of (2.20) becomes

$$3ax_1x_2 + A = 0.$$

Let $A \neq 0$. Substituting $x_2 = -\frac{A}{3a}x_1^{-1}$ into the first equation of (2.20), we get (with $x_0 = 0$)

$$y_0^2 = ax_1^3 - \frac{A^3}{27a^2}x_1^{-3} + B.$$

Multiplication by x_1^4 and substitution $y = y_0x_1^2$ gives

$$y^2 = ax_1^7 + Bx_1^4 - \frac{A^3}{27a}x_1. \tag{2.21}$$

Let C be the projective closure of C_0 in $\mathbb{P}_k^2$. Then C is either a rational curve or a hyperelliptic curve whose normalization has genus ≤ 3. The first case is impossible since it is a curve on an abelian surface.

So, if the discriminant of the polynomial on the right-hand side is non-zero, the normalization of C has genus 3, and in general it is a hyperelliptic curve whose normalization has genus ≤ 3. If N is simple, then the normalization of C has genus 2 or 3.

If N is simple, this curve is defined even without the assumption $\zeta_3 \in k$. One takes the intersection of N with the surface defined by "expanding out" $\sigma(Y) = Y$. The normalization of the resulting curve is still hyperelliptic, since every non-singular curve with genus ≥ 2 which is hyperelliptic over some field is hyperelliptic wherever it is defined. (This holds since its function field contains a *unique* rational subfield of index 2.)

For $A = 0$ i.e. $j = 0$, we get two elliptic curves. Note that in this case $\zeta_3 \in \mathrm{End}_k^0(E)$ and thus this is consistent with the decomposition of W in Subsection 2.1.3.

By (2.16), condition $x_0 = 0$ is – outside of H – equivalent to $Y = \sigma(Y)$. Thus we get the following result:

Under the condition $j \neq 0$, the intersection of N with the subvariety of W defined by $Y = \sigma(Y)$ is a hyperelliptic curve C whose normalization has genus $\leq$ 3. (3 is the "generic" case.)

We now translate the idea of intersecting N_0 with the variety defined by "expanding out" $\sigma(Y) = Y$ to characteristic 2 and 3.

The curves constructed in this way will also be used as examples in the next chapter (Section 3.3) where we outline attacks on the DL-problem in $E(K)$.

2.4.2 The curve defined by $\sigma(Y) = Y$

We explain the idea first independently of the characteristic.

Let E be given by the following affine Weierstraß-equation:

$$Y^2 + A_1XY + A_3Y = X^3 + A_2X^2 + A_4XA_6, \tag{2.22}$$

where all A_i lie in k.

We now intersect the subvariety of W_0 which is given by the expansion of the equation

$$Y = \sigma(Y) \tag{2.23}$$

with N_0, the open, affine part of the trace-zero-hypersurface N.

We restrict ourselves to the affine parts $W_0 \backslash H$ and $N_0 \backslash H$ of W and N defined as above.

To define N_0, we can just as for $\mathrm{char}(k) > 3$ restrict ourselves to the equation for the X-coordinate. Under (2.23), we have

$$X(P \oplus \sigma(P)) = -A_2 - X - \sigma(X).$$

Thus under (2.23), we get the following easy defining equation for N_0.

$$X + \sigma(X) + \sigma^2(X) = -A_2 \tag{2.24}$$

Let C_0 be the subscheme of W_0 which is defined by (2.23) and (2.24). It will turn out to be a curve.

$\mathbf{char}(k) > 3$

This case was treated above. Stating with an elliptic curve with j-invariant $\neq 0$ defined by equation (2.8), we obtain a curve which is (possibly after a base-change $k(\zeta_3)|k$) birational to the curve given by (2.21).

$\mathbf{char}\ (k) = 2$

Again assume that $\zeta_3 \in k$ and assume that $j \neq 0$. (If ζ_3 is not contained in k, the curve C_0 is after the base-change $k(\zeta_3)|k$ given by the equations which now follow.)

Let α, a and σ be defined as above. Let E be given by an affine equation

$$Y^2 + XY = X^3 + A_2X^2 + B, \tag{2.25}$$

where $A_2, B \in k,\ B \neq 0$; see [Si, Appendix A, Proposition 1.1. (c)].

Again we make the substitutions (2.9). Then the subscheme C_0 is given by

$$y_1 = y_2 = 0,\ x_0 = -A_2 = A_2,$$

and (2.25) becomes

$$\begin{gathered}(1 \otimes y_0)^2 + (1 \otimes A_2 + \alpha \otimes x_1 + \alpha^2 \otimes x_2)(1 \otimes y_0) = \\ (1 \otimes A_2 + \alpha \otimes x_1 + \alpha^2 \otimes x_2)^3 + A_2(1 \otimes A_2 + \alpha \otimes x_1 + \alpha^2 \otimes x_2)^2 + B.\end{gathered} \tag{2.26}$$

This expands to the following three equations, which describe C_0 in $\mathbb{A}_k^4$.

$$\begin{aligned} y_0^2 + A_2y_0 &= A_2^3 + ax_1^3 + a^2x_2^3 + A_2^2 + B \\ x_1y_0 &= A_2^2x_1 + aA_2x_2^2 + ax_1^2x_2 + aA_2x_2^2 \\ x_2y_0 &= A_2^2x_2 + A_2x_1^2 + ax_1x_2^2 + A_2x_1^2 \end{aligned} \tag{2.27}$$

The second and third equation can be simplified to

$$\begin{aligned} x_1y_0 &= A_2^2x_1 + ax_1^2x_2 \\ x_2y_0 &= A_2^2x_2 + ax_1x_2^2, \end{aligned} \tag{2.28}$$

and for $(x_1, x_2) \neq (0, 0)$, this is equivalent to

$$y_0 = A_2^2 + ax_1x_2.$$

Substituting this into the first equation of (2.27), we get the following equation for C_0

$$A_2^4 + a^2x_1^2x_2^2 + A_2^3 + aA_2x_1x_2 = A_2^3 + ax_1^3 + a^2x_2^3 + A_2^2 + B.$$

The scheme C_0 is a geometrically irreducible, geometrically reduced curve. The *proof* of this fact is analogous to the one on page 64.

The curve C_0 is an open affine part of the projective curve C defined by the corresponding homogeneous equation

$$a^2x_1^2x_2^2 + aA_2x_1x_2z^2 + ax_1^3z + a^2x_2^3z + (A_2^2 + A_2^4 + B)z^4 = 0. \tag{2.29}$$

As this equation has degree 4, C has arithmetic genus 3. Just as in the case of $\mathrm{char}(k) > 3$ discussed above, singularities outside infinity and $(0, 0)$ have to occur in triples. So again, if the curve had such singularities, the genus of its normalization would be 0, what is impossible. Thus the only possible singularities are $(0, 0)$ and the points at infinity.

We examine the singularities at infinity. The curve C has the infinite points $[1 : 0 : 0]$ and $[0 : 1 : 0]$. Taking the derivative of (2.29) with respect to z (note that $\mathrm{char}(k) = 2$) gives

$$ax_1^3 + a^2x_2^3.$$

This is $\neq 0$ for both infinite points $\neq 0$. Thus C has no singularities at infinity.

We now look at the possible singularity at $(0, 0)$. Firstly, $(0, 0)$ would have to lie on C_0. Thus

$$A_2^2 + A_2^4 + B = 0.$$

Secondly, the derivatives with respect to x_1 and x_2 at $(0, 0)$ would both have to be 0. This implies $A_2 = 0$ and thus also $B = 0$. This is impossible because it would mean that E is singular.

We arrive at the following characterization of the curve C:

C is a canonical curve of degree 4 and genus 3 which is the normalization of a curve on N.

$\mathbf{char}(k) = 3$

Now let k be a field with characteristic 3. According to Artin-Schreier theory, $K|k$ is generated by some α with $\alpha^3 - \alpha = a \in k$. The Galois group is generated by σ with $\sigma(\alpha) = \alpha + 1$.

For later use, we calculate

$$\begin{aligned} \sigma(\alpha^2) &= (\alpha+1)^2 = \alpha^2 - \alpha + 1 \\ \sigma^2(\alpha^2) &= (\sigma^2(\alpha))^2 = (\alpha-1)^2 = \alpha^2 + \alpha + 1 \end{aligned} \tag{2.30}$$

and

$$\begin{aligned} \alpha^3 &= \alpha + a \\ \alpha^4 &= \alpha^2 + \alpha a \\ \alpha^5 &= \alpha^2 a + \alpha + a \\ \alpha^6 &= \alpha^2 - \alpha a + a^2. \end{aligned} \tag{2.31}$$

Let E be given by the equation

$$Y^2 = X^3 + A_2X^2 + B, \tag{2.32}$$

where according to the assumptions $A_2, B \in k$ and are both non-zero; see [Si, Appendix A, Proposition 1.1. (c)].

Again under the substitutions (2.9), (2.24) becomes

$$x_2 = A_2, y_1 = y_2 = 0,$$

and (2.32) gives

$$\begin{gathered} 1 \otimes y_0^2 = 1 \otimes x_0^3 + (\alpha \otimes x_1^3 + 1 \otimes ax_1^3) + (\alpha^2 A_2^3 - \alpha \otimes aA_2^3 + 1 \otimes a^2 A_2^3) \\ +A_2[1 \otimes x_0^2 + \alpha^2 \otimes x_1^2 + \alpha^2 A_2^2 + \alpha \otimes aA_2^2 \\ -\alpha \otimes x_0x_1 - \alpha^2 \otimes A_2x_0 - \alpha \otimes A_2x_1 - 1 \otimes aA_2x_1] + B \end{gathered}$$

Thus C_0 is given by the following three equation in $\mathbb{A}_k^4$.

$$\begin{gathered} y_0^2 = x_0^3 + ax_1^3 + a^2A_2^3 + A_2x_0^2 - aA_2^2x_1 + B \\ 0 = x_1^3 - aA_2^3 + aA_2^3 - A_2x_0x_1 - A_2^2x_1 \\ 0 = A_2^3 + A_2x_1^2 + A_2^3 - A_2^2x_0. \end{gathered} \tag{2.33}$$

The third equation can be divided by $A_2 \neq 0$ and is equivalent to

$$0 = x_1^2 - A_2^2 - A_2x_0.$$

This equation also implies the second equation of (2.33) and is equivalent to

$$x_0 = A_2^{-1}x_1^2 - A_2. \tag{2.34}$$

This implies

$$x_0^2 = A_2^{-2}x_1^4 + x_1^2 + A_2^2. \tag{2.35}$$

If we insert (2.34) and (2.35) in the first equation of (2.33), we are given the curve C_0, described by

$$y_0^2 = A_2^{-3}x_1^6 - A_2^3 + ax_1^3 + a^2A_2^3 + A_2^{-1}x_1^4 + A_2x_1^2 + A_2^3 - aA_2^2x_1 + B,$$

i.e.

$$y_0^2 = A_2^{-3}x_1^6 + A_2^{-1}x_1^4 + ax_1^3 + A_2x_1^2 - aA_2^2x_1 + a^2A_2^3 + B. \tag{2.36}$$

This is a hyperelliptic curve of degree 6.

Let C be the projective closure of C_0 in $\mathbb{P}_k^2$. We obtain the following characterization of C:

The normalization of C is a hyperelliptic curve of genus 1 or 2. (If N is simple, the genus is 2.) In particular, if N is simple, it is isogenous to the Jacobian variety of the normalization of C.

Chapter 3

Coverings of curves and the discrete-logarithm problem

Introduction and results

This chapter is devoted to cryptoanalytic applications.

Let k be a finite field, $K|k$ a field extension of prime degree n. Let X' be a non-singular, geometrically irreducible (i.e. geometrically integral), proper curve over K. [1] Assume that X' has "cryptographically good" properties. Especially, the group $\mathrm{Pic}^0(X') \cong \mathrm{Cl}^0(K(X'))$ should have a large prime factor. We try to transform the discrete-logarithm problem in $\mathrm{Cl}^0(K(X'))$ into the discrete-logarithm problem in $\mathrm{Cl}^0(k(C))$ for a suitable non-singular, geometrically irreducible, proper k-curve C.

The idea is that if the genus of C is not "too large", perhaps the discrete-logarithm problem in the group $\mathrm{Cl}^0(k(C))$ is "easier" than the discrete-logarithm problem in the original group $\mathrm{Cl}^0(K(X'))$. This is suggested by [En], [EG] and [Gau].

In [GHS], the following approach was introduced:

Let $C_K \longrightarrow X'$ be a covering. Then $K(X')$ is included in $K(C_K)$. Consider the group-homomorphism

$$\mathrm{norm}_{K(C_K)|k(C)} \circ \mathrm{con}_{K(C_K)|K(X')} : \mathrm{Cl}^0(K(X')) \longrightarrow \mathrm{Cl}^0(k(C)). \tag{3.1}$$

Two conditions should be fulfilled:

1. The large prime factor of $\mathrm{Cl}^0(K(X'))$ is preserved.

2. The curve C has "reasonably nice" cryptographic properties. Especially the genus of C should not be "too large" in relation to n and the genus of X'. For example, if we consider a family of curves X' for different extension degree n, by the state of the art of cryptoanalysis in class groups of high

[1] In this chapter, X' or X always denotes a curve and never a variable.

genus curves, the genus of C should be at most quadratic in n; see [En]. Other interesting properties of C are hyperellipticity or automorphisms.

For 1., no "theoretical result" is known to the author. [2] However, using the Weil-restriction of $J(X')$ with respect to $K|k$, we motivate very strongly that the kernel of (3.1) is small in certain situations; see Subsections 3.1.1 and 3.1.2, especially Theorem 9, p. 77.

Then we show how to use Galois theory to construct appropriate coverings of curves (or equivalently finite extensions of function fields of transcendence degree 1). In the case that the Jacobian $J(X')$ is a new abelian variety (for definition see foreword), we give the construction of [GHS] as an example. For the case that X' is already defined over k, we first proof a theoretical result (Theorem 9, p. 77), then we give examples based this result (see Subsection 3.3).

3.1 Coverings as curves on the Weil-restriction

Let k be a finite field of characteristic p, $K|k$ be an extension of finite fields of prime degree n. Identify $\mathrm{Gal}(K|k)$ with its opposite group and denote the Frobenius automorphism of $K|k$ by σ_k^K.

Let X' be a geometrically integral, proper, non-singular curve over K with a K-rational point P_0. Let W be the Weil-restriction of X' with respect to $K|k$.

Let C be a non-singular, irreducible proper curve over k. (We do not assume that C is geometrically irreducible.) Then by the definition of the Weil-restriction, k-morphisms $C \longrightarrow W$ are in bijection to K-morphisms $C_K := C \otimes_k K \longrightarrow X'$: If $c : C_K \longrightarrow X'$ is a K-morphism, then there is a unique $b : C \longrightarrow W$ such that $c = u \circ (b \otimes \mathrm{id}_K)$.

Again let $c : C_K \longrightarrow X'$ be a K-morphism, and let $b : C \longrightarrow W$ be the unique morphism with $c = u \circ (b \otimes_k \mathrm{id}_K)$. Then the image of c is a point iff c factors through the structure morphism $C_K \longrightarrow \mathrm{Spec}(K)$ iff b factors through the structure morphism $C \longrightarrow \mathrm{Spec}(k)$ iff the image of b on W is a point. [3] Thus:

Lemma 3.1 *c is dominant iff the image of b on W is a curve.*

From now on, let c be a dominant, finite morphism. We call such a morphism a *covering* of non-singular, proper, irreducible curves.

[2] Of course, it is possible to check that the large prime factor is preserved in specific cases, for example with the help of a computer.

[3] More generally, let D be some k-scheme. Then by functoriality, $b : C \longrightarrow W$ has the form $b = ed$ for some $d : C \longrightarrow D$ and $e : D \longrightarrow W$ iff c has the form $c = f \circ (d \otimes \mathrm{id}_K)$ for some $d : C \longrightarrow D$, $f : D \otimes_k K \longrightarrow X'$. (In fact, $f = u \circ (e \otimes_k \mathrm{id}_K)$.)

We have a commutative diagram

$$\begin{tikzcd}
C_K \arrow[r, "b\otimes_k \mathrm{id}_K"'] \arrow[rr, bend left, "c"] \arrow[d] & W_K \arrow[r, "u"] \arrow[d] & X' \\
C \arrow[r, "b"] & W. &
\end{tikzcd}$$

This induces a commutative diagram

$$\begin{tikzcd}
\mathrm{Pic}^0(C_K) \arrow[d, "\mathrm{N}"] & \mathrm{Pic}^0(W_K) \arrow[l, "(b\otimes_k \mathrm{id}_K)^*"] \arrow[d, "\mathrm{N}"] & \mathrm{Pic}^0(X') \arrow[l, "u^*"] \arrow[ll, bend right, "c^*"'] \\
\mathrm{Pic}^0(C) & \mathrm{Pic}^0(W). \arrow[l, "b^*"] &
\end{tikzcd}$$

We have already seen that the group-homomorphism $\mathrm{N}\circ u^* : \mathrm{Pic}^0(X') \longrightarrow \mathrm{Pic}^0(W)$ is bijective; see Corollary 1.19. In the case that X' is an elliptic curve E', this homomorphism is – under the identifications of E' and W with its duals via their canonical principal polarizations – nothing but the canonical isomorphism $E'(K) \xrightarrow{\sim} W(k)$.

If $k(C)$, $K(C_K)$ and $K(X')$ are the function fields of C, C_K and X' respectively, then $\mathrm{N} \circ c^*$ corresponds to

$$\mathrm{norm}_{K(C_K)|k(C)} \circ \mathrm{con}_{K(C_K)|K(X')} : \mathrm{Cl}^0(K(X')) \longrightarrow \mathrm{Cl}^0(k(C)). \qquad (3.2)$$

We want to study the kernel of (3.2) or – equivalently – the kernel of $\mathrm{N}\circ c^* : \mathrm{Pic}^0(X') \longrightarrow \mathrm{Pic}^0(C)$.

We note first that in practice we can restrict ourselves to the case that C is geometrically irreducible. For, let that not be the case. Let $\lambda := k(C) \cap \overline{k}$, where $\overline{k}$ is the algebraic closure of k (intersection in some common overfield). We now make the *assumption* that n does not divide $[\lambda : k]$. (To use this construction for an attack on the DLP in $\mathrm{Cl}^0(K(X'))$, $[\lambda : k]$ should be much smaller than n.) The fields K and λ are linearly disjoint over k, i.e. $K \otimes_k \lambda$ is a field, denoted $K\lambda$. If we consider C as a λ-curve, it is geometrically irreducible and $C_K = C \otimes_k K \simeq C \otimes_\lambda (K \otimes_k \lambda) \simeq C \otimes_\lambda K\lambda$. [4] As

$$\begin{gathered}
\mathrm{norm}_{K(C_K)|k(C)} \circ \mathrm{con}_{K(C_K)|K(X')} = \\
\mathrm{norm}_{K\lambda(C_K)|\lambda(C)} \circ \mathrm{con}_{K\lambda(C_K)|K\lambda(X_\lambda)} \circ \mathrm{con}_{K\lambda(X'_\lambda)|K(X')} : \\
\mathrm{Cl}^0(K(X')) \longrightarrow \mathrm{Cl}^0(k(C)),
\end{gathered}$$

[4] For definition of "linear disjoint" see Subsection A.3.1 in the appendix.

we only have to consider the kernel of (3.2) for geometrically irreducible curves.

Let C be a geometrically irreducible (i.e. geometrically integral) k-curve.

The kernel of $\mathrm{N}\circ c^*$: $\mathrm{Pic}^0(X') \longrightarrow \mathrm{Pic}^0(C)$ is isomorphic to the kernel of $b^* : \mathrm{Pic}^0(W) \longrightarrow \mathrm{Pic}^0(C)$. Let $J(C)$ be the Jacobian variety of C. Then this kernel is isomorphic to the kernel of $b^* : \mathbf{Pic}^0(W)(k) \longrightarrow J(C)(k)$. (This holds even if C has no k-rational points. In this case, we still have an injective homomorphism $\mathrm{Pic}^0(C) \longrightarrow J(C)(k)$; see [Mi-J, Remark 1.5.].)

By Corollary 1.18, $\mathbf{Pic}^0(W)$ is an abelian variety which is canonically isomorphic $\mathbf{Res}_k^K(J(X))$, the Weil-restriction of the Jacobian variety of X'. To study the kernel of $b^* : \mathbf{Pic}^0(W)(k) \longrightarrow J(C)(k)$, we ask if the morphism $b^* : \mathbf{Pic}^0(W) \longrightarrow J(C)$ is an isogeny on large isogeny factors of $\mathbf{Pic}^0(W)$. If this is the case and $\mathrm{Pic}^0(X') \simeq \mathrm{Pic}^0(W)$ has a large prime factor, then we *expect* that this prime factor is preserved under b^* and thus under $\mathrm{N}\circ c^*$, i.e. under (3.2).

We make the following general assumption:

The Jacobian variety of X' is simple and its endomorphism ring is commutative.

The assumption that the Jacobian variety is simple is natural in the case of a cryptographic application since $\mathrm{Pic}^0(X')$ should have a large prime factor.

The second condition is for example fulfilled if X' is a non-super-singular elliptic curve.

3.1.1 Curves with Jacobians which are new abelian varieties

Let X' be a curve which is not defined over k such that its Jacobian $J(X')$ is a new abelian variety, i.e. $J(X')$ is not isogenous to an abelian variety defined over k. For example, X' could be an elliptic curve which is not isogenous to an elliptic curve defined over k.

In this case, $\mathbf{Pic}^0(W) \simeq \mathbf{Res}_k^K(J(X'))$ is simple; see Corollary 1.18 and Theorem 3.

So in this case, the kernel of (3.2) is bounded by the separability degree of the morphism from $\mathbf{Pic}^0(W)$ onto its image in $J(C')$. Thus we expect the kernel of c^* to be small. In particular, if $\mathrm{Pic}^0(X')$ contains a large prime factor, as is the case in cryptographic applications, then we expect this factor to be preserved.

3.1.2 Curves which are defined over the small field

Let X be a curve over k, $X' := X \otimes_k K$. We assumed that X' has a K-rational point P_0. Let $\iota : X' \longrightarrow J(X')$ be the embedding defined by $P_0 \mapsto 0$.

Diagram (3.1) extends to the following diagram

$$\begin{tikzcd}
C_K \arrow[rr, "c"] \arrow[dr, "b\otimes_k \mathrm{id}_K"] \arrow[dd] & & X_K \arrow[rr, "\iota"] & & J(X_K) \\
& X_K^n \arrow[ur, "u"] \arrow[rr] \arrow[dd] & & J(X_K)^n \arrow[ur] \arrow[dd] & \\
C \arrow[dr, "b"] & & & & \\
& W \arrow[rr, "j:=\mathbf{Res}_k^K(\iota)"] & & V := \mathbf{Res}_k^K(J(X_K)). &
\end{tikzcd}$$

Lemma 3.2 $j^* := \mathbf{Res}_k^K(\iota)^* : \widehat{V} = \widehat{\mathbf{Res}_k^K(J(X_K))} \longrightarrow \mathbf{Pic}^0(W)$ *is an isomorphism of abelian varieties.*

Proof This follows from the diagram

$$\begin{tikzcd}
\mathbf{Res}_k^K(J(X_K)) \arrow[d, "\mathbf{T}"] & \mathbf{Res}_k^K(\widehat{J(X_K)}) \arrow[l, "\mathbf{Res}_k^K(\iota^*)"', "\sim"] \arrow[d, "\mathbf{T}"] \\
\mathbf{Pic}^0(W) & \widehat{\mathbf{Res}_k^K(J(X_K))} \arrow[l, "j^*"]
\end{tikzcd} .$$

Here, the down-arrows are the morphisms defined in Subsection 1.2.3. They are isomorphism since X_K is a curve and $J(X_K)$ an abelian variety; see Corollary 1.18 and Proposition 1.20. □

Instead of asking which isogeny factors of $\mathbf{Pic}^0(W)$ are preserved under $b^* : \widehat{W} \longrightarrow J(C)$, we now ask which isogeny factors of $\mathbf{Res}_k^K(J(X_K))$ are preserved under $b^* \circ j^* : \widehat{V} \longrightarrow J(C)$. This approach is more convenient since $V = \mathbf{Res}_k^K(J(X_K))$ is itself an abelian variety.

We already assumed that $J(X_K)$ is simple and that the endomorphism ring of $J(X_K)$ is commutative. We now *assume* furthermore that – after an inclusion of $\mathrm{End}_k^0(J(X))$ into $\overline{\mathbb{Q}}$ – $\mathrm{End}_k^0(J(X)) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$. Then we know by Theorem 5 that V has exactly two simple isogeny factors, $J(X)$ itself and the trace-zero-hypersurface N. We expect the kernel of b^* to be small if the image of N under $b^* \circ j^*$ is non-trivial.

There exists an extension $\lambda|k$ of degree prime to $n = [K : k]$ such that C_λ has a λ-rational point P and such that $\mathrm{End}_{\lambda K}(J(X')_{\lambda K})$ is still commutative (i.e. $\mathrm{End}_{\lambda K}(J(X')_{\lambda K}) = \mathrm{End}_K(J(X'))$).

[*Proof* If $\lambda|k$ has degree m and there exists no two roots x_1, x_2 of the characteristic polynomial of the Frobenius of $J(X')$ (in $\overline{\mathbb{Q}}$) and no l such that $\zeta_m^l x_1 = x_2$, then the roots of the characteristic polynomial of the Frobenius of $J(X'_{\lambda K})$ are distinct. Choose such an extension $\lambda|k$ whose degree is high enough (and prime to n) such that by the "Riemann-hypothesis", C_λ has a λ-rational point.]

Now $K|k$ and $\lambda|k$ are linearly disjoint, so if $K\lambda$ is some composite of $K|k$ and $\lambda|k$, then $K\lambda \simeq K \otimes_k \lambda$ and $K\lambda|\lambda$ is again a field extension of degree n.

Since "base-restriction" commutes with "base-extension" (see Lemma 1.1), V_λ is again isogenous to $J(X_K)_\lambda \times N_\lambda$ and N_λ is again simple.

Let $\beta := j \circ b$. The morphism $\beta^P := T_{(-\beta\otimes_k \mathrm{id}_\lambda)\circ P} \circ (\beta \otimes_k \mathrm{id}_\lambda) : C_\lambda \longrightarrow V_\lambda$ maps the λ-rational point P of C_λ to 0. Let $f^P : C_\lambda \longrightarrow J(C)_\lambda$ be the immersion defined by $P \mapsto 0$. By the universal property of the Jacobian (see [Mi-J, Proposition 6.1]), there exists a unique morphism of abelian varieties $\gamma^P : J(C_\lambda) \longrightarrow V_\lambda$ such that

$$\begin{tikzcd}
J(C)_\lambda \arrow[dr, "\gamma^P"] & \\
C_\lambda \arrow[u, "f^P"] \arrow[r, "\beta^P"] & V_\lambda .
\end{tikzcd}$$

After dualizing, we obtain

$$\begin{tikzcd}
\widehat{J(C)}_\lambda \arrow[d, "f^{P*}"] & \\
J(C)_\lambda & \widehat{V}_\lambda , \arrow[ul, "\gamma^{P*}"'] \arrow[l, "\beta^*"']
\end{tikzcd}$$

where $f^{P*} : \widehat{J(C)}_\lambda \longrightarrow J(C)\lambda$ is the canonical isomorphism. In the last line we can write β^* instead of β^{P*} since $T^*_{-\beta\circ P} : \mathcal{P}\mathrm{ic}^0(V_\lambda) \longrightarrow \mathcal{P}\mathrm{ic}^0(V_\lambda)$ is the identity by the definition of $\mathcal{P}\mathrm{ic}^0(V_\lambda)$.

In particular, $\ker(\beta^*) = \ker(\gamma^{P*})$. Under the identification of V_λ with $\widehat{V}_\lambda$ via the principal polarization induced by the canonical principal polarization of $J(X')$, the reduced connected component of the zero of $\ker(\beta^*)$ is the orthogonal complement of the image of γ^P; see Subsection A.2.4 in the appendix, in particular Lemma A.22, i.e. β^{P^*} induces an isogeny of $\gamma^P(J(C))_\lambda$ with its image and is trivial on the orthogonal complement of this abelian subvariety.

We are mainly interested in the question whether β^* induces an isogeny of N_λ with its image, i.e. if the image of γ^P contains N_λ.

Now, the image of γ^P is the smallest abelian subvariety of N_λ which contains $\beta^P(C)$. Thus N_λ is *not* contained in the image of γ^P iff $\beta^P(C)$ is contained in $J(X)_\lambda$.

We identified $\mathrm{Gal}(K|k)$ with its opposed group and denote the Frobenius automorphism of $K|k$ by $\sigma_k^K \in \mathrm{Gal}(K|k)$. The automorphism σ_k^K of K induces an automorphism of $\mathrm{Spec}(K)$, and this induces the "arithmetic Frobenius automorphism" of $J(X_K)$ which we also denote by σ_k^K; cf. Subsection A.3.4.

Let $a = a_{\sigma_k^K}$ be the k-automorphism of V corresponding to the automorphism σ_k^K on $J(X')$; see subsection 1.1.5. Then $\beta^P(C)$ is contained in $J(X)_\lambda$ iff $((a \otimes_k \mathrm{id}_\lambda) - \mathrm{id}) \circ \beta^P(C_\lambda)$ is a point, i.e. iff $(((a - \mathrm{id}) \circ \beta) \otimes_k \mathrm{id}_\lambda)(C_\lambda)$ is a point, i.e. iff $(a - \mathrm{id}) \circ \beta(C)$ is a point.

Let $p_k : C \longrightarrow \mathrm{Spec}(k)$, $p_K : C_K \longrightarrow \mathrm{Spec}(K)$ be the structure morphisms.

Then $(a - \mathrm{id}) \circ \beta(C)$ is a point $\longleftrightarrow$ $(a - \mathrm{id}) \circ \beta$ factors through p_k $\longleftrightarrow$ there exists a $q \in V(k)$ with $a \circ \beta - \beta = q \circ p_k$.

For $q \in V(k)$, let $Q := u \circ (q \otimes_k \mathrm{id}_K)$ be the corresponding element in $J(X)(K)$. Then the last equation is equivalent to $\sigma_k^K(\iota c) - \iota c = Q \circ p_K$, i.e. $\sigma_k^K(\iota c) = T_Q \circ \iota c$ by the definition of T_Q.

Similar arguments for $J(X)$ instead of N lead to

Proposition 3.3 *Let $c : C \longrightarrow X'$ be a morphism where C is a curve. Then $\beta^* : V \longrightarrow J(C)$ induces an isogeny of*

- *N with its image iff there does not exist a $Q \in J(X)(K)$ with $\sigma_k^K(\iota c) - \iota c = Q \circ p_K$, i.e. $\sigma_k^K(\iota c) = T_Q \circ \iota c$,*
- *$J(X)$ with its image iff there does not exist a $Q \in J(X)(K)$ with $\iota c + \cdots + \sigma_k^{K^{n-1}}(\iota c) = Q \circ p_K$.*

So if there does not exist a $Q \in J(X)(K)$ with $\sigma_k^K(\iota c) = T_Q \circ \iota c$, then the kernel of

$$\mathrm{norm}_{K(C_K)|k(C)} \circ \mathrm{con}_{K(C_K)|K(X_K)} : \mathrm{Cl}^0(K(X_K)) \longrightarrow \mathrm{Cl}^0(k(C))$$

is bounded by the separability degree of the isogeny β^* between N and its image times $\mathrm{Pic}^0(X)$. So we expect the kernel to be small.

In particular, if $\mathrm{Pic}^0(X_K)$ contains a large prime factor, as is the case in cryptographic applications, then we expect that this prime factor is preserved.

Theorem 9 *Let $K|k$ be an extension of finite fields of prime degree n. Let σ_k^K be the Frobenius automorphism of $K|k$. Let X be a non-singular, proper, geometrically irreducible curve over k of genus g with a k-rational point P_0. Assume that the Jacobian $J(X_K)$ of X_K is simple, and the endomorphism ring of $J(X_K)$ is commutative. Assume further that – after an inclusion of $\mathrm{End}_k^0(J(X))$ into $\overline{\mathbb{Q}}$ – $\mathrm{End}_k(J(X)) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$.*

Let W be the Weil-restriction of X_K with respect to $K|k$. Then $\mathbf{Pic}^0(W)$ *is an $n \cdot g$-dimensional abelian variety which is canonically isogenous to $J(X) \times_k N$, where N is a simple $(n-1) \cdot g$-dimensional abelian variety.*

Let C be a non-singular, proper, geometrically irreducible curve over k, and let $c : C \longrightarrow X$ be a covering.

Assume that C has an automorphism t of degree n which is not *an c-automorphism, i.e. such that $c \circ t \neq c$ and that there does* not *exist a $Q \in J(X)(K)$ such that $\iota c t \otimes_k id_K = T_Q \circ (\iota c \otimes_k id_K)$.*

Let C^t be the twist of C with respect to $K|k$ and t, i.e. $C^t = C_K / < \sigma_k^K t >$. Then C^t is a non-singular, geometrically irreducible curve, and t defines an automorphism on C^t of order n.

Then the morphism $c \otimes_k \mathrm{id}_K : C_K^t \simeq C_K \longrightarrow X_K$ induces a morphism

$b^t : C^t \longrightarrow W$.

$$\begin{tikzcd}
C^t_K \arrow[r, "b^t \otimes_k \mathrm{id}_K"'] \arrow[rr, bend left, "c"] \arrow[d] & W_K \arrow[r, "u"] \arrow[d] & X_K \\
C^t \arrow[r, "b^t"] & W &
\end{tikzcd}$$

Now, the morphism $b^{t*} : \mathbf{Pic}^0(W) \longrightarrow J(C^t)$ induces an isogeny of N with its image. [5]

Proof We only have to check the last statement. By Proposition 3.3, we have to show that there does not exist a $Q \in J(X)(K)$ with

$$\sigma_k^K(\iota c \otimes_k \mathrm{id}_K)(t^{-1} \otimes_k \mathrm{id}_K){\sigma_k^K}^{-1} = T_Q \circ (\iota c \otimes_k \mathrm{id}_K). \ (*)$$

Now, $\sigma_k^K(\iota c \otimes_k \mathrm{id}_K)(t^{-1} \otimes_k \mathrm{id}_K){\sigma_k^K}^{-1} = \iota c t^{-1} \otimes_k \mathrm{id}_K$. Thus (*) is equivalent to $T_{-Q} \circ (\iota c \otimes_k \mathrm{id}_K) = (\iota ct \otimes_k \mathrm{id}_K)$. This is impossible by assumption. □

Remark Under the assumption that $ct \neq c$, the condition that there does not exist a $Q \in J(X)(K)$ with $\iota ct \otimes_k \mathrm{id}_K = T_Q \circ (\iota c \otimes_k \mathrm{id}_K)$ is especially fulfilled under one of the following two conditions:

- t has a geometric fixed point
- $J(X)(K)$ does not have an element of order n

Proof Firstly, if t has a geometric fixed point, and the equation is satisfied for some Q, then $Q = 0$ thus $\iota c = \iota ct$. Since ι is an immersion, $c = ct$, contradicting the assumption.

Secondly, if a Q exists then it follows that $\iota c \otimes_k \mathrm{id}_K = {\sigma_k^K}^n(\iota c \otimes_k \mathrm{id}_K) = T_{nQ} \circ (\iota c \otimes_k \mathrm{id}_K)$. Let $P \in C(\overline{k})$. Then $(\iota c \otimes_k \mathrm{id}_{\overline{k}}) \circ P = nQ + (\iota c \otimes_k \mathrm{id}_{\overline{k}}) \circ P$ thus $nQ = 0$. □

3.2 Coverings of curves whose Jacobian variety is a simple new abelian variety

3.2.1 Construction of coverings

Let $K|k$ be an extension of finite fields of prime degree n, let X' be a geometrically irreducible curve over K with a K-rational point.

[5] In particular, in the context of the theorem, if $\mathrm{Pic}^0(X_K)$ has a large prime factor, then we *expect* this prime factor to be preserved under $\mathrm{N} \circ c^* : \mathrm{Pic}^0(X_K) \longrightarrow \mathrm{Pic}^0(C)$.

General assumptions for this section Assume that $J(X')$ is a simple new abelian variety, i.e. that it is not isogenous to an abelian variety defined over k. (This implies that X' is not defined over k, i.e. there exists no k-curve X with $X_K \approx X'$.) Assume that the endomorphism ring of $J(X')$ is commutative.

Let $K(X')$ be the function field of X'. Suppose that $K(X')|K(x)$ is an abelian extension, included in $K(x)^{\mathrm{sep}}|K(x)$, and the degree $[K(X') : K(x)]$ is prime to n. As above, we denote the Frobenius automorphism of $K|k$ by σ_k^K.

Let $L' = K(X')\sigma_k^K(K(X')) \cdots \sigma_k^{K^{n-1}}(K(X'))$ be the Galois closure of $K(X')$ over $k(x)$ in $K(x)^{\mathrm{sep}}$.

Then by Galois theory, we get the exact sequence

$$1 \longrightarrow \mathrm{Gal}(L'|K(x)) \longrightarrow \mathrm{Gal}(L'|k(x)) \longrightarrow \mathrm{Gal}(K|k) \longrightarrow 1. \tag{3.3}$$

Lemma 3.4 *Sequence (3.3) splits.*

Proof Note that $\mathrm{Gal}(L'|K(x))$ is isomorphic to $(\mathrm{Gal}(K(X')|K(x)))^m$ for some $m \leq n$. The order of this group is prime to n, since by assumption $[K(X') : K(x)]$ is prime to n. Thus the lemma follows from the following group-theoretic lemma. □

Lemma 3.5 *Let* $1 \longrightarrow A \longrightarrow E \longrightarrow G \longrightarrow 1$ *be an exact sequence of finite groups where* A *is abelian,* G *is cyclic and the order of* A *is prime to the order of* G*. Then this sequence splits.*

Proof First let A be a general abelian group. Then if an extension E of G by A is given, G operates on A by taking preimages and conjugation inside E. Such an operation given, the extensions E of G by A are classified by the elements of $H^2(G, A)$, the trivial element in this group corresponding to the semi-direct product defined by the given operation of G on A; see [Se, VII,par. 3].

We now show that under the assumption that the orders of G and A are coprime, $H^2(G, A)$ is trivial. Thus every extension of G by A is a semi-direct product.

Firstly, $H^2(G, A)$ is annihilated by the order of G; see [Se, VIII, par. 2, p.130, Corollary 1]. Secondly, $H^2(G, A) \simeq \widehat{H}^0(G, A) = A^G/\mathrm{N}(A)$ (see [Se, VIII, par. 4, p.133, Corollary]), and this group being the quotient of a subgroup of A is annihilated by the exponent of A.

Since the orders of A and G where assumed to be coprime, $H^2(G, A) = 1$. □

Assume that $L'|K(x)$ *is regular over* K*.* [6]

[6] For definition of "regular" see Subsection A.3.1 in the appendix.

Fix a section of (3.3). Let L be the fixed field of the subgroup of $\mathrm{Gal}(L'|k(x))$ defined by this section. Then by construction, L and $K(x)$ are linearly disjoint over $k(x)$ and $LK = L'$. Thus $L'|K(x)$ is defined over k.

Note however, that $L'|K(x)$ is not defined over k with its Galois group. For if this was the case, every subextension of $L'|K(x)$ would be defined over k thus $K(X')|k(x)$ would be defined over k which is by assumption not the case.

Because of the simplicity of the Weil-restriction the map

$$\mathrm{norm}_{KL|L} \circ \mathrm{con}_{KL|K(X')} : \mathrm{Cl}^0(K(X')) \longrightarrow \mathrm{Cl}^0(L)$$

is expected to have small kernel.

Now assume that $L'|K(x)$ is not regular. The argumentation is now similar to the one on page 73: Assume further that $[L' \cap \overline{k} : K]$ is prime to n. (In fact, to use this construction as an attack on the DLP in $\mathrm{Cl}^0(K(X'))$, $[L' \cap \overline{k} : K]$ should be much smaller than n.) Then there exists an extension of finite fields $\lambda|k$ such that $K \otimes_k \lambda \simeq \lambda K = L' \cap \overline{k}$. Now $L'|K\lambda$ is regular, and $L'|\lambda(x)$ is Galois. By the same arguments as above, there exists a regular subextension $L|\lambda$ with $L \otimes_\lambda K\lambda \simeq KL = L'$. Therefore $L \otimes_k K \simeq L \otimes_\lambda (K \otimes_k \lambda) \simeq L'$.

Because of the simplicity of the Weil-restriction of X'_λ, with respect to $K\lambda|\lambda$, we still expect the kernel of

$$\begin{gathered}\mathrm{norm}_{KL|L} \circ \mathrm{con}_{KL|K(X')} = \mathrm{norm}_{KL|L} \circ \mathrm{con}_{K\lambda KL|K\lambda(X')} \circ \mathrm{con}_{K\lambda(X')|K(X')} : \\ \mathrm{Cl}^0(X') \longrightarrow \mathrm{Cl}^0(L)\end{gathered}$$

to be small.

Geometric interpretation of the construction

Let L' still be the Galois closure of $K(X')|k(x)$. Assume that $[L' \cap \overline{k} : K]$ is prime to n. We have seen that in this case there exists a function field $L|k$ with $L \otimes_k K \simeq LK = L'$. The diagram

$$\begin{tikzcd}
L \otimes_k K \arrow[d, dash] \arrow[dr, dash] & \\
K(X') \arrow[d, dash] & L \arrow[dd, dash] \\
K(x) \arrow[dr, dash] & \\
 & k(x)
\end{tikzcd}$$

corresponds to a diagram

$$\begin{tikzcd}
C_K := C \otimes_k K \arrow[d, "c"] \arrow[dr] & \\
X' \arrow[d] & C \arrow[dd] \\
\mathbb{P}^1_K \arrow[dr] & \\
& \mathbb{P}^1_k
\end{tikzcd} \tag{3.4}$$

of coverings of irreducible non-singular proper curves. (C is geometrically irreducible iff $L|k$ is regular, that is, if $L'|K$ is regular.)

Let W be the Weil-restriction of X' with respect to $K|k$, $b : C \longrightarrow W$ the morphism corresponding to $c : C_K \longrightarrow X'$.

If we consider C as a covering of $\mathbb{P}^1_k$, then $c \in \mathfrak{R}\mathrm{es}_{\mathbb{P}^1_k}^{\mathbb{P}^1_K}(X')$. By Lemma 1.2, this is equal to $\mathfrak{R}\mathrm{es}_k^K(X') \times_{\mathfrak{R}\mathrm{es}_{\mathbb{P}^1_k}^{\mathbb{P}^1_K}(X')} \mathbb{P}^1_k$. So $b : C \longrightarrow W$ factors through $W \times_{\mathbf{Res}_k^K(\mathbb{P}^1)} \mathbb{P}^1_k \simeq \mathbf{Res}_{\mathbb{P}^1_k}^{\mathbb{P}^1_K}(X')$.

We get the following diagram of coverings

$$\begin{tikzcd}
C \otimes_k K \arrow[d] \arrow[dr] & \\
X' \times_{\mathbb{P}^1_K} \sigma_k^K(X') \times_{\mathbb{P}^1_K} \cdots \times_{\mathbb{P}^1_K} \sigma_k^{K^{n-1}}(X') \arrow[d, "p_{\mathrm{id}}"] \arrow[dr] & C \arrow[d] \\
X' \arrow[d] & \mathbf{Res}_{\mathbb{P}^1_k}^{\mathbb{P}^1_K}(X') \arrow[dd] \\
\mathbb{P}^1_K \arrow[dr] & \\
& \mathbb{P}^1_k,
\end{tikzcd}$$

where $C \otimes_k K \longrightarrow X' \times_{\mathbb{P}^1_K} \sigma_k^K(X') \times_{\mathbb{P}^1_K} \cdots \times_{\mathbb{P}^1_K} \sigma_k^{K^{n-1}}(X')$ is given by $(\sigma_k^{K^i}(a))_{i=0,\ldots,n-1}$. By construction, this morphism identifies an open part of C_K with the open part of one component of $X' \times_{\mathbb{P}^1_K} \sigma_k^K(X') \times_{\mathbb{P}^1_K} \cdots \times_{\mathbb{P}^1_K} \sigma_k^{K^{n-1}}(X')$ (since $K(X') \otimes_{K(x)} \sigma_k^K(K(X')) \otimes_{K(x)} \cdots \otimes_{K(x)} \sigma_k^{K^{n-1}}(K(X')) \longrightarrow K(C)$ is surjective) and the same is true for C and $\mathbf{Res}_{\mathbb{P}^1_k}^{\mathbb{P}^1_K}(X')$.

In particular, $C \longrightarrow \mathbf{Res}_{\mathbb{P}^1_k}^{\mathbb{P}^1_K}(X')$ induces a closed immersion of an open part of C. So is also $\mathbf{Res}_{\mathbb{P}^1_k}^{\mathbb{P}^1_K}(X') \simeq W \times_{\mathbf{Res}_k^K(\mathbb{P}^1)} \mathbb{P}^1_k \longrightarrow \mathbf{Res}_k^K(X')$, since $\mathbb{P}^1_k \longrightarrow$

$\mathbf{Res}_k^K(\mathbb{P}^1_K)$ is (see Lemma 1.5) and "closed immersion" is stable under base-change (see [Ha, II,ex. 3.11.]). Thus:

Proposition 3.6 *$b : C \longrightarrow W$ induces a closed immersion of an open part of C.*

3.2.2 An application

Let n be odd. Let H' be a hyperelliptic curve as above. A Weierstraß-equation of H' defines a covering $H' \longrightarrow \mathbb{P}^1_K$ of degree 2. Let L' be the Galois closure of $K(H')|K(x)$. Then if $L'|K(x)$ is regular, by the general theory presented above, it can be defined over k. [7]

char(k) = 2

Let the elliptic K-curve E' be given by the Weierstraß-equation

$$y^2 + xy = x^3 + \alpha x^2 + \beta; \ \alpha, \beta \in K$$

So $K(E')|k(x)$ is a (Galois) extension of degree 2, and via this extension we regard $K(E')$ as a intermediate field of $K(x)^{\mathrm{sep}}|K(x)$. After division by x^2 and substitution $s := y/x + \beta^{\frac{1}{2}}/x$, the extension $K(E')|K(x)$ is given by

$$s^2 + s + \beta^{\frac{1}{2}}x^{-1} + \alpha + x = 0.$$

(Note that since K is perfect, $\beta^{\frac{1}{2}} \in K$.) Thus the Galois closure L' of $K(E')|K(x)$ is given by the Artin-Schreier equation

$$\begin{aligned} &s_0^2 + s_0 + \beta^{\frac{1}{2}}x^{-1} + \alpha + x = 0 \\ &s_1^2 + s_1 + \sigma_k^{K^1}(\beta)^{\frac{1}{2}}x^{-1} + \sigma_k^{K^1}(\alpha) + x = 0 \\ &\quad \vdots \\ &s_{n-1}^2 + s_{n-1} + \sigma_k^{K^{n-1}}(\beta)^{\frac{1}{2}}x^{-1} + \sigma_k^{K^{n-1}}(\alpha) + x = 0 \end{aligned}$$

with $s_0 = s$. It is shown in [GHS] that L' is a regular field extension of $K(z)$ of degree $\leq 2^n$, and furthermore that it is hyperelliptic and that its genus is bounded by 2^{n-1}.

More precisely, let

$$\begin{aligned} U &:= \mathrm{span}_{\mathbb{F}_2}(\{\sigma_k^{K^i}(\beta)^{\frac{1}{2}}x^{-1} + \sigma_k^{K^i}(\alpha) + x\}_{i=0,\dots,n-1}), \\ U' &:= \mathrm{span}_{\mathbb{F}_2}(\{(\sigma_k^{K^i}(\beta)^{\frac{1}{2}}, \sigma_k^{K^i}(\alpha), 1)\}_{i=0,\dots,n-1}). \end{aligned}$$

Let $m :=\dim_{\mathbb{F}_2}(U/\mathcal{P}(\overline{K(x)}) \cap U) =\dim_{\mathbb{F}_2}(U'/U' \cap \{(0, \mathcal{P}(\xi), 0), \xi \in \overline{K}\})$, where $\mathcal{P}(\xi) := \xi^2 + \xi$. Then it follows from Artin-Schreier theory that $2^m = [L' : K(x)]$; see [Ne, IV, (3.3) with (3.4)] for the statement of the Artin-Schreier theory we use here. Calculations show that $g(L) = g(L') = 2^{m-1}$ or $g(L) = g(L') = 2^{m-1} - 1$.

[7] This construction was introduced by Galbraith and Smart and analyzed in detail by Gaudry, Hess and Smart in characteristic 2; cf. [GHS]. Additional remarks were made by Menezes and Qu; cf. [MQ]. It was generalized to certain hyperelliptic curves of characteristic 2 by Galbraith; cf. [Gal]. The analysis in the odd-characteristic case is due to the author.

For n prime to 2, let $\varphi_2(n) := \mathrm{ord}(2)$ for $2 \in (\mathbb{Z}/n\mathbb{Z})^*$.

Then for $k = \mathbb{F}_2$, m can only assume the values $\varphi_2(n)i + 1$ for $i \geq 1$, thus $g(L) = 2^{\varphi_2(n)i}$ or $g(L) = 2^{\varphi_2(n)i} - 1$; see [MQ].

Let $n = 127$. Then $\varphi_2(n) = 7$, and for this value of n, an explicit extension $K(E')|K(x)$ can be constructed for which L has genus $2^7 - 1 = 127$; see [GHS].

$\mathbf{char}(k) \neq 2$

Let n still be odd. Let H' be a hyperelliptic curve of genus g which satisfies the "general assumptions". Let H' be given by the Weierstraß-equation

$$y^2 = f(x),$$

where f is a polynomial of degree $2g+1$ or $2g+2$. Again regard $K(H')$ as an intermediate field of $K(x)^{\mathrm{sep}}|k(x)$, let L' be the Galois closure of $K(H')|K(x)$ inside $K(x)^{\mathrm{sep}}$.

We identify the places of $\overline{K}(x)|\overline{K}$ with $\overline{K} \cup \{\infty\}$ (via x). Let $e_1, e_2, \ldots \in \overline{K}$ and possibly ∞ be the ramified places of the extension $\overline{K}L'|\overline{K}(x)$. (The place ∞ is ramified iff $\deg(f) = 2g+1$.)

The absolute Galois-group $\mathrm{Gal}(\overline{K}|K)$ operates on the covering and thus also on the ramified places. It fixes ∞ and operates on the e_i.

On the other hand, the set $S := \{e_1, e_2, \ldots\}$ is not invariant under $\mathrm{Gal}(\overline{K}|k)$. For if it was, $f(x) = (x-e_1)(x-e_2)\cdots$ would have coefficients in k, and thus H' would be defined over k.

Assume that $\sigma_k(e_1), \ldots, \sigma_k(e_l) \notin S$ and $\sigma_k(e_{l+1}), \ldots \in S$. Then all elements $\sigma_k^i(e_j)$, $i = 0, \ldots, n-1$, $j = 1, \ldots, l$ are distinct and for $i \geq 1$, they do not lie in S.

Lemma 3.7 *$L'|K(x)$ is regular over K and has degree 2^n.*

proof (by induction) Let $i = 2, \ldots, n$. Assume that $L' \cdots \sigma_k^{K^{i-1}}(L')|K(x)$ is regular over K and has degree 2^{i-1}. This is equivalent to $[\overline{K}L' \cdots \sigma_k^{i-1}(\overline{K}L') : \overline{K}(x)] = 2^{i-1}$. Now ${\sigma_k}^i(e_1)$ is in the ramification locus of ${\sigma_k}^i(\overline{K}L')|\overline{K}(x)$ but not in the ramification locus of $\overline{K}L' \cdots {\sigma_k}^{i-1}(\overline{K}L')|\overline{K}(x)$. Thus $\sigma_k^i(\overline{K}L')$ cannot be contained in $\overline{K}L' \cdots \sigma_k^i(\overline{K}L')$, and thus they are linearly disjoint over $\overline{K}(x)$, defining an extension of degree 2^i. This implies that $L' \cdots \sigma_k^{K^{i-1}}(L')$ is regular of degree 2^i. $\square$.

By the general theory, there exists a regular extension $L|k(x)$ such that $K \otimes L \simeq KL = L'$. The ramification of $L|k(x)$ or – what is the same – the ramification of $L'|K(X)$ can be calculated using Abhyankar's Lemma; see [Po, Lemma (2.14)].

Lemma 3.8 (Abhyankar) *Let F be a field, $\overline{F}$ a Galois closure of F, v a discrete valuation of F of rank 1. Let F_1, F_2 be finite Galois extension fields of F in $\overline{F}$. Let v_1, v_2 be extensions of v in F_1, F_2, $e_1 = e(v_1|v), e_2 = e(v_2|v)$ the corresponding* *ramification indices. Assume that v is tamely ramified in $F_1|F$ and in $F_2|F$ and that e_1 divides e_2.*

Then: If F' is the composite of F_1 and F_2 in $\overline{F}$ and v' is an extension of v in F', then v' is unramified *in the extension $F'|F_2$.*

With this lemma, we conclude that all ramification indices of the ramified places of $\overline{K}L'|\overline{K}(X)$ are 2.

Let r be the number of ramified places of $\overline{K}L'|\overline{K}(x)$. Then r equals the number of elements in the set $\{\sigma_k^{K^i}(e_j)|\ i = 0, \ldots, n-1, j = 1, 2, \ldots\}(\cup\{\infty\})$. So by the remarks before Lemma 3.7,

$$2g + n + 1 \leq r \leq (2g + 2)n.$$

The lower bound is obtained if the degree of f is $2g + 1$ and all e_i lie in k expect one (which lies in K), the upper bound is obtained if the degree of f is $2g + 2$ and no e_i lies in k.

With the Riemann-Hurwitz-formula we calculate

$$g(L) = g(L') = 2^n(0-1) + \frac{1}{2}r\frac{e-1}{e}2^n + 1 = -2^n + r2^{n-2} = 2^{n-2}(r-4) + 1. \quad (3.5)$$

So

$$2^{n-2}(2g + n - 3) + 1 \leq g(L) \leq 2^{n-1}((g+1)n - 2) + 1.$$

In particular, let H' be an elliptic curve. Then there always exists a Weierstraß-equation such that f has degree 3. So $3 + n \leq r \leq 3n + 1$ and

$$2^{n-2}(n-1) + 1 \leq g(L) \leq 3 \cdot 2^{n-2}(n-1) + 1.$$

3.3 Coverings of curves defined over the small field

3.3.1 Construction of coverings

Let still $K|k$ be a prime extension of finite fields of characteristic p, $n := [K : k]$, X a non-singular, proper, geometrically irreducible curve over k with a k-rational point. Assume that $\mathrm{End}_K(J(X_K))$ is commutative and – after an inclusion of $\mathrm{End}_k^0(J(X))$ into $\overline{\mathbb{Q}}$ – $\mathrm{End}_k^0(J(X)) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$. As proven in Theorem 5, under these assumptions, the trace-zero-hypersurface of the Weil-restriction of $J(X_K)$ with respect to $K|k$ is simple.

We want to construct coverings of X which fulfill the conditions of Theorem 9, i.e. we want to construct coverings $c : C \longrightarrow X$ such that C has an automorphism t with $c \circ t \neq c$. Furthermore we want that t has a geometric fixed point. (If $\mathrm{Cl}^0(X_K)$ has no element of order n, this assumption is not needed.)

Analogously to Subsection 3.2.1, let $k(X)$ be the function field of X, $k(X)|k(x)$ an extension, included in $k(x)^{\mathrm{sep}}|k(x)$, such that n divides $[k(X) : k(x)]$. Let L be the Galois closure of $k(X)|k(x)$ in $k(x)^{\mathrm{sep}}$.

Assume that n does not divide $[L : k(X)]$. Then $L|k(x)$ has an automorphism of order n which does not fix $K(X)$ which we denote by $t^{\#}$. Assume that this automorphism is contained in some inertia group of $L|k(x)$ or that $\mathrm{Cl}^0(X_K)$ has *no* element of order n. Let C be a proper, non-singular model of $k(X)$, $c : C \longrightarrow X$ the covering corresponding to the extension $k(C)|k(X)$. Let t be the automorphism of C corresponding to $t^{\#}$.

Now, if $L|k$ is regular, we can apply Theorem 9. (If $L|k$ is not regular but L is regular over some extension $\lambda|k$ such that n does not divide $[\lambda : k]$, we can work over λ instead of k and then still apply the theorem.)

A first example

Let $c : E \longrightarrow E$ be the identity and let $t : E \longrightarrow E$ be the elliptic involution, i.e. $t \circ P = -P$. Now if $K|k$ is a field extension of degree 2 (not necessarily of finite fields) then by the theorem, the twist of E by the involution is mapped into the Weil-restriction. By construction, this morphism is given by the closed immersion $(\mathrm{id}, -\mathrm{id}) : E_K \longrightarrow E_K^2 \simeq W_K$. This corresponds to the well-known fact that the trace-zero-hypersurface is isomorphic to E^t, and W is isogenous to $E \times_k E^t$.

Geometric interpretation of the construction

Let $c : C \longrightarrow X$ be the covering defined by $L|k(X)$. The field extension $k(X)|k(x)$ defines a covering $X \longrightarrow \mathbb{P}^1_k$. Let W be the Weil-restriction of X_K with respect to $K|k$, $b : C \longrightarrow W$ the morphism corresponding to $c \otimes_k \mathrm{id}_k : C_K \longrightarrow X_K$. Let $b^t : C^t \longrightarrow W$ be the morphism corresponding to $C^t_K \simeq C_K \longrightarrow X_K$ as in Theorem 9.

Then both b and b^t factor through the closed immersion $\mathbf{Res}_{\mathbb{P}^1_k}^{\mathbb{P}^1_K}(X_K) \longrightarrow \mathbf{Res}_k^K(X_K)$.

We want to give conditions under which b^t induces a closed immersion of an open part of C^t. This is the case iff $b^t \otimes_k \mathrm{id}_K = (ct^{i-1} \otimes_k \mathrm{id}_K)_{i=0}^{n-1} : C^t_K \simeq C_K \longrightarrow \mathbf{Res}_{\mathbb{P}^1_k}^{\mathbb{P}^1_K}(X_K) \otimes_k K \simeq \overbrace{X_K \times_{\mathbb{P}^1_K} \cdots \times_{\mathbb{P}^1_K} X_K}^{n \text{ fold}}$ induces a closed immersion of an open part of C^t_K. This in turn is the case iff the ring-homomorphism $\overbrace{K(X_K) \otimes_{K(x)} \cdots \otimes_{K(x)} K(X_K)}^{n \text{ fold}} \longrightarrow KL$ induced by $t^{\#^i}\iota^{\#}$ for $i = 0, \ldots, n-1$ is surjective (where $\iota^{\#} : k(x) \hookrightarrow k(X)$ is the inclusion).

Proposition 3.9 *Let $[k(X) : k(x)] = n$. Then $b^t : C^t \longrightarrow \mathbf{Res}_k^K(X_K)$ induces a closed immersion of an open part of C^t.*

Proof Let $\iota_i^{\#}$, $i = 1, \ldots, n : k(x) \longrightarrow k(X)$ be the inclusions. We know that t

operates non-trivially on the set of $\iota_i^\#$. Thus by assumption, it operates by cyclic permutation, i.e. the set of $t^{\#^i}\iota^\#$ for $i = 0, \ldots, n-1$ equals the set of $\iota_i^\#$ for $i = 1, \ldots, n$.

Thus the ring-homomorphism $\overbrace{k(X) \otimes_{k(x)} \cdots \otimes_{k(x)} k(X)}^{n \text{ fold}} \longrightarrow L$ induced by $t^{\#^i}\iota^\#$ for $i = 0, \ldots, n-1$ equals (up to permutation of the factors) the ring-homomorphism induced by the injections $\iota_i^\#$. We know that this homomorphism is surjective. (L is generated by the roots of a primitive element of $k(X)|k(x)$.) □

A second example

Let E be a non-super-singular elliptic curve which is not isogenous to an elliptic curve with j-invariant $\neq 0$. A Weierstraß-equation of E defines a field extension $k(E)|k(y)$ of degree 3. Since by assumption $k(E)$ does not have an automorphism of order 3, this extension is non-Galois.

Let L be a Galois closure of this extension. Then $L|k(E)$ is an extension of degree 2, the Galois group of $K(E)|k(y)$ is isomorphic to the symmetric group on three elements.

There are two possibilities: 1. $L = \lambda(E_\lambda)$, where $\lambda|k$ is the unique extension of degree 2, 2. L is regular over k. Since L has an automorphism of order 3 and we assumed that E does not have j-invariant 0, the first case is impossible. Thus $L|k(E)$ is regular.

Let $c : C \longrightarrow E$ be the covering of non-singular, proper, irreducible curves which corresponds to the extension $L|k(E)$. Since we assumed that E is not isogenous to a curve with j-invariant 0, the genus of C is at least 2.

Let $K|k$ be the field extension of degree 3 and let σ_k^K be the Frobenius automorphism of $K|k$. Let $t \in \mathrm{Gal}(L|k(x))$ be of of the two elements of exact order 3. Let C^t be the twisted curve defined by $\sigma_k^K \mapsto t\sigma_k^K$. By construction, just as C, C^t is a covering of $\mathbb{P}_k^1$.

If we substitute t be t^2, the other element of exact order 3 in $\mathrm{Gal}(L|k(x))$, we obtain another covering $C^{t^2} \longrightarrow \mathbb{P}_k^1$. However, the elements t and t^2 are conjugated in $\mathrm{Gal}(L|k(x))$, $st = t^2 s$ for some element s of order 2 in $\mathrm{Gal}(L|k(x))$ and such an s defines an isomorphism from $C_K^t \longrightarrow \mathbb{P}_K^1$ to $C_K^{t^2} \longrightarrow \mathbb{P}_K^1$ which is compatible with the Galois-operation. Therefore the two $\mathbb{P}_k^1$-coverings C^t and C^{t^2} are isomorphic. [This corresponds to the fact that there are exactly two elements in the pointed set $H^1(\mathrm{Gal}(K|k), \mathrm{Aut}(C_K \longrightarrow \mathbb{P}_K^1))$.]

The covering $C^t \longrightarrow \mathbb{P}_k^1$ corresponds to a morphism $b^t : C^t \longrightarrow \mathbf{Res}_{\mathbb{P}_k^1}^{\mathbb{P}_K^1}(E_K)$. (Where $E_K \longrightarrow \mathbb{P}_K^1$ is the covering induced by the extension $K(E_K)|K(y)$.) By Proposition 3.9, this morphism induces a closed immersion of an open part of C^t.

All in all, the reducible K-curve $\mathbf{Res}_{\mathbb{P}_k^1}^{\mathbb{P}_K^1}(E_K)_K \simeq E_K \times_{\mathbb{P}_K^1} E_K \times_{\mathbb{P}_K^1} E_K$ has five irreducibility components: E_K itself, and four components which are birational to C_K. [The ring $K(E_K) \times_{K(x)} K(E_K) \times_{K(x)} K(E_K)$ is isomorphic to $K(E_K) \times L^3$.]

One of the components of $\mathbf{Res}_{\mathbb{P}^1_k}^{\mathbb{P}^1_K}(E_K)_K \simeq E_K \times_{\mathbb{P}^1_K} E_K \times_{\mathbb{P}^1_K} E_K$ is the image of $C^t_K \simeq C_K$ under $b^t \otimes_k \mathrm{id}_K = (c, ct, ct^2)$. The other components which are isomorphic to C_K are the images of C_K under (ct, c, c), (c, ct, c), (c, c, ct) respectively. These components are permuted under the Galois-operation on $\mathbf{Res}_{\mathbb{P}^1_k}^{\mathbb{P}^1_K}(E_K)_K$. They descend to an irreducible k-curve on $\mathbf{Res}_{\mathbb{P}^1_k}^{\mathbb{P}^1_K}(E_K)$ which is birational to C_K considered as k-curve. Thus apart from E itself, the image of C^t is the only geometrically irreducible k-curve on $\mathbf{Res}_{\mathbb{P}^1_k}^{\mathbb{P}^1_K}(E_K)$.

Let E be given by a "nice" Weierstraß-equation as in [Si, Appendix A, Proposition 1.1]. Then C^t is birational to the geometrically irreducible curves constructed in Subsection 2.4.2, the last subsection of the previous chapter. (In particular, the image of C^t in $\mathbf{Res}_k^K(E_K)$ under b^t lies on the trace-zero-hypersurface of E.) If $\mathrm{char}(k) = 3$, it is birational to the curve given by (2.36). If $\mathrm{char}(k) > 3$ and the third roots of unity are contained in k, it is birational to the curve given by (2.21). If $\mathrm{char}(k) = 2$, again under the assumption that the third roots of unity are contained in k, it is birational to the curve given by (2.29).

In particular:

- If $\mathrm{char}(k) \neq 2, 3$, C^t is a hyperelliptic curve of genus ≤ 3.
- If $\mathrm{char}(k) = 2$, C^t is a "canonical curve" of genus 3.
- If $\mathrm{char}(k) = 3$, C^t is a curve of genus 2.

3.3.2 An application

Definition For n prime to p, let $\varphi_p(n) := \mathrm{ord}(p)$ for $p \in (\mathbb{Z}/n\mathbb{Z})^*$. We might call φ_p the *local Euler-function for p.*

Lemma 3.10 $\mathbb{F}_p(\zeta_m) = \mathbb{F}_{p^{\varphi_p(m)}}$.

Let $c : \mathrm{Gal}(\mathbb{F}_p(\zeta_m)|\mathbb{F}_p) \longrightarrow (\mathbb{Z}/m\mathbb{Z})^*$ be the m-th cyclotomic character, i.e. $\sigma(\zeta_m) = \zeta_m^{c(\sigma)}$. Then c induces a bijection of $\mathrm{Gal}(\mathbb{F}_p(\zeta_m)|\mathbb{F}_p)$ with the subgroup generated by p in $(\mathbb{Z}/m\mathbb{Z})^*$. □

For the following construction, let n be an odd prime and assume that the n-th *roots of unity are contained in k*, i.e. k contains $\mathbb{F}_{p^{\varphi_p(n)}}$.

Let H be a hyperelliptic k-curve and let $g(x, y)$ be some Weierstraß-"equation" (i.e. polynomial) defining H. Let L be a Galois closure of the extension of $k(x)$

given by $z^n = x, g(z,y) = 0$.

$$\begin{tikzcd}
L \arrow[d, dash] \\
k(H) \arrow[d, dash, "2"] \\
k(z) \arrow[d, dash, "n"] \\
k(x)
\end{tikzcd}$$

Let $\zeta = \zeta_n$ be an n-th root of unity in $\overline{k}$. Then the field L is given by the equations

$$z^n = x,\ g(z,y_0) = 0,\ g(\zeta z, y_1) = 0,\ \ldots,\ g(\zeta^{n-1}z, y_{n-1}) = 0 \text{ (with } y_0 = y).$$

So $L|k(H)$ is a composite of extensions of degree 2, and $[L : k(H)] = 2^a$ for some $a \leq n-1$.

The place $\mathfrak{p}_0$ is ramified in $L|k(x)$, its ramification index equals n. Let $t^\#$ be an element of the inertia group of $L|k(x)$ of order n. Now $t^\#$ does not fix $k(H)$ because $[L : k(H)] = 2^a$ and n is odd, and $t^\#$ has a fixed point.

Let $\lambda := L \cap \overline{k}$ (intersection in some common overfield) be the Galois closure of k in L. Then the extension $L|\lambda(H_\lambda)$ and the automorphism t fulfill the requirements of the theorem.

Let $\iota^\# : k(H) \longrightarrow L$ be the inclusion. Then the set $t^\# \iota^\#(k(H))$ equals the set of images of $k(H)$ under all inclusions into L (over $k(x)$). Thus the homomorphism $\overbrace{k(H) \otimes_{k(x)} \cdots \otimes_{k(z)} k(H)}^{n \text{ fold}} \longrightarrow L$ induced by $t^{\#^i}\iota^\#$ is surjective, and as in the case of Proposition 3.9, $b^t : C^t \longrightarrow \mathbf{Res}_k^K(X_K)$ induces a *closed immersion of an open part of* C^t.

It is a priori not clear whether $L|k$ is regular. However, since $\mathrm{Gal}(L|k(z))$ has exponent 2, if $L|k$ is not regular, it is regular over the unique extension of k of degree 2.

As above, let λ be the Galois closure of k in L. Then L and $\lambda(z)$ are linearly disjoint over $\lambda(x)$. Thus $[L : k(x)] = [L : \lambda(z)] \cdot [\lambda(x) : k(z)] = [\overline{k}L : \overline{k}(z)] \cdot [\lambda : k]$ and $[\lambda : k] = \frac{[\overline{k}L:\overline{k}(z)]}{[L:k(z)]}$.

We now address the extension-degrees in question for special Weierstraß-equations. Then we calculate the genus of L (which equals the genera of C and C^t).

$\mathbf{char}(k) = 2$

We still assume that the n-th roots of unity are contained in k.

Let E be an elliptic curve, given by the Weierstraß-equation

$$y^2 + xy = x^3 + \alpha x^2 + \beta;\ \ \alpha, \beta \in k$$

After division by x^2 and substitution $s := y/x + \beta^{\frac{1}{2}}/x$, the extension $k(E)|k(x)$ is given by the Artin-Schreier equation

$$s^2 + s + \beta^{\frac{1}{2}} x^{-1} + \alpha + x = 0.$$

Now substitute x by z. Then the extension $L|k(x)$ defined above is given by

$$\begin{aligned} & z^n = x \\ & s_0^2 + s_0 + \beta^{\frac{1}{2}} z^{-1} + \alpha + z = 0 \\ & s_1^2 + s_1 + \beta^{\frac{1}{2}} (\zeta z)^{-1} + \alpha + \zeta z = 0 \\ & \quad \vdots \\ & s_{n-1}^2 + s_{n-1} + \beta^{\frac{1}{2}} (\zeta^{n-1} z)^{-1} + \alpha + \zeta^{n-1} z = 0 \end{aligned}$$

with $s_0 = s$.

Let U' be the $\mathbb{F}_2$-vector space

$$U' := \mathrm{span}_{\mathbb{F}_2}(\{\beta^{\frac{1}{2}}\zeta^{-i}, \alpha, \zeta^i)\}_{i=0,\dots,n-1}) \subseteq \overline{\mathbb{F}_2}^3.$$

Let $\mathcal{P}(\xi) := \xi^2 + \xi$. By Artin-Schreier theory in the form of [Ne, IV, (3.3) with (3.4)], $[L : k(z)] = 2^d$ with $d = \dim_{\mathbb{F}_2}(U'/U' \cap \{(0, \mathcal{P}(\xi), 0) | \xi \in k\})$, $[L\overline{k} : \overline{k}] = 2^m$ with $m = \dim_{\mathbb{F}_2}(U'/U' \cap \{(0, \xi, 0) | \xi \in \overline{k}\})$. Let

$$V' := \mathrm{span}_{\mathbb{F}_2}(\{\beta^{\frac{1}{2}}\zeta^{-i}, \zeta^i)\}_{i=0,\dots,n-1}).$$

Then $m = \dim_{\mathbb{F}_2}(V')$.

$$\varphi_2(n) \leq m \leq 2\varphi_2(n) \tag{3.6}$$

The second inequality follows from the inclusion $V' \subseteq \beta^{\frac{1}{2}}\mathbb{F}_2(\zeta) \oplus \mathbb{F}_2(\zeta)$. The first inequality follows from projection of V' onto $\mathbb{F}_2(\zeta)$ (projection to the second coordinate).

Of course, since we only have n generating vectors, we also have the inequality $\dim_{\mathbb{F}_2}(U') \leq n$ which is for example a better bound if $\varphi_2(n) = n - 1$.

We now study over which constant field L is regular. We have the following cases:

case 1: $\alpha = 0$. In this case, $[L : k(x)] = [\overline{k}L : \overline{k}(x)] = \dim(V') = m$ and the extension $L|k$ is regular.

case 2: $\alpha \neq 0$. Since the sum over all n-th roots of unity is 0, $(0, \alpha, 0) \in U'$. Now the extension $L|k$ is regular iff $\alpha \in \mathcal{P}(k)$, and it is regular over the constant field extension of degree 2 otherwise.

We calculate the genus of L. We use the following lemma. [8]

[8] This idea was pointed out to the author by H. Stichtenoth.

Lemma 3.11 (Accola; Kani; Garcia, Stichtenoth) *Let λ be a field, l a prime number, m a natural number and $L|\lambda(z)$ a Galois extension, regular over λ, with Galois group isomorphic to $(\mathbb{Z}/l\mathbb{Z})^m$. Then $L|\lambda(z)$ has exactly $e := (l^m - 1)/(l - 1)$ subfields $L_i|\lambda(z)$ with $[L_i : k(z)] = l$. We have*

$$g(L) = \sum_{i=1}^{e} g(L_i).$$

Proof See [GS, Theorem 2.1] with [Kan, Theorem 1]. (The conditions on λ stated in [GS] are not necessary.) □

We apply this lemma with $l = 2$, L, m as above and λ the Galois closure of k in L.

Then $e = 2^m - 1$ and all $L_i|\lambda(z)$ are Artin-Schreier extensions. – They correspond bijectively to cyclic subgroups of V', i.e. to non-trivial elements of V'. Such an element $(\beta^{\frac{1}{2}}c_i, d_i) \in V'$ defines an extension $L_i|\lambda(z)$ given by the Artin-Schreier equation

$$t^2 + t + \beta^{\frac{1}{2}}c_i z^{-1} + d_i z = 0.$$

Thus $g(L_i) \leq 1$ and we get the following proposition.

Proposition 3.12 *Either $L|k$ is regular or it is regular over the constant field extension of degree 2. Let $m := \dim_{\mathbb{F}_2}(V')$. Then $[L\overline{k} : \overline{k}(x)] = 2^m$, and L has genus $\leq 2^m - 1 \leq 2^{2\varphi_2(n)} - 1$.*

We can now apply Theorem 9. We have motivated: [9]

Proposition 3.13 *Let n be an odd prime number. Let E be an elliptic curve over $\mathbb{F}_{2^{\varphi_2(n)}}$ such that $E(\mathbb{F}_{2^{\varphi_2(n)n}})$ contains a prime factor of order $\sim 2^{\varphi_2(n)n-\varphi_2(n)}$. Then a geometrically irreducible curve C^t of genus $\leq 2^{2c\varphi_2(n)} - 1$ defined over $\mathbb{F}_{2^{2\varphi_2(n)}}$ with an automorphism of order n can be constructed such that via the homomorphism (3.2), we expect the DL-problem in $E(\mathbb{F}_{2^{\varphi_2(n)n}})$ to be transformed into the DL-problem of $\mathrm{Cl}^0(C^t)$.*

An interesting special case is the following: Let $n = 2^c - 1$ be a prime number. Then $\varphi_2(n) = c$ since $2^c = n + 1 \equiv 1 \bmod n$. So:

Let $n = 2^c - 1$, be a prime number, e.g. $n = 3, 7, 31, 127$. Let E be an elliptic curve over $\mathbb{F}_{2^c}$ such that $E(\mathbb{F}_{2^{cn}})$ contains a prime factor of order $\sim 2^{cn-c}$. Then a geometrically irreducible curve C^t of genus $\leq 2^{2c} - 1$ defined over $\mathbb{F}_{2^{2c}}$ with an automorphism of order n can be constructed such that via the homomorphism (3.2), we expect the DL-problem in $E(\mathbb{F}_{2^{cn}})$ to be transformed into the DL-problem of $\mathrm{Cl}^0(C^t)$.

[9] We write "motivated" instead of "proven" because the result relies on the fact that we *expect* the large prime factor in $E(K)$ to be preserved; see Theorem 9 for details.

In particular, let E be a curve defined over $\mathbb{F}_{2^5}$ such that $E(\mathbb{F}_{2^{155}})$ contains a prime factor of order 2^{150}. Then we have associated to E a geometrically irreducible curve C^t of genus $\leq 2^{10} - 1$, defined over $\mathbb{F}_{2^{10}}$ with an automorphism of order 31, such that via the homomorphism (3.2), the DL-problem in $E(\mathbb{F}_{2^{155}})$ is expected to be transformed into the DL-problem of $\mathrm{Cl}^0(C^t)$.

$\mathbf{char}(k) \neq 2$

Let $k(H)$ be a hyperelliptic function field of genus g and let $k(H)|k(z)$ be a degree-2 extension defined by a Weierstraß-equation of degree $d := 2g+1$ or $d := 2g+2$ (in z). We identify the places of $\overline{k}(z)|\overline{k}$ with $\overline{k} \cup \{\infty\}$ (via z).

Then $\overline{k}(E)|\overline{k}(z)$ is ramified over d places $e_1, e_2, \ldots, e_d \in \overline{k}$ and additionally over ∞ if d is odd.

There are several different cases depending on whether some ramification points lie in the same orbit under of the action of the Galois group of $k(z)|k(x)$. The most generic one is the following:

All e_i lie in different orbits of the Galois group of $k(z)|k(x)$.

There are two sub-cases:

case 1: $e_i \neq 0$ for all i. Then $\overline{k}L|\overline{k}(z)$ is ramified at $(2g+1)n+1$ or $(2g+2)n$ places (depending on whether the Weierstraß-"equation" (i.e. polynomial) has odd or even order).

case 2: $e_i = 0$ for some e_i. Then $\overline{k}L|\overline{k}(z)$ is ramified at $2gn+2$ or $(2g+1)n+1$ places.

In both cases, exactly as in the proof of Lemma 3.7, one sees that $L|k(z)$ is regular and has degree 2^n.

Using Abhyankar's Lemma (Lemma 3.8), we conclude that the ramification order at the ramified places is always 2. We can calculate the genus of L (which equals the genera of C and C^t) using formula (3.5):

$$g(L) = 2^{n-2}(r-4) + 1,$$

where r is the number of ramified places in $L|k(z)$. Thus $2gn + 2 \leq r \leq (2g+2)n$ and

$$2^{n-1}(gn-1) + 1 \leq g(L) \leq 2^{n-1}((g+1)n-2).$$

Appendix A

Some auxiliary results

A.1 Some results about the Picard scheme

The functor $\mathcal{P}\mathrm{ic}(X)$ of a non-singular, projective, integral k-variety X with a k-rational point as well as the group-schemes $\mathbf{Pic}(X)$ and $\mathbf{Pic}^0(X)$, the Picard scheme, where already introduced in Subsection 1.2.2. Here we give some additional properties. We are only interested in "geometric" questions like the dimension of $\mathbf{Pic}^0(X)$, so we work over an algebraically closed field only.

A.1.1 The dimension of the Picard scheme

Let k be an algebraically closed field, X a non-singular, projective, integral k-variety.

The dimension of the Picard scheme $\mathbf{Pic}^0(X)$ can be calculated via étale cohomology or via the étale fundamental group.

Lemma A.1 *For any prime* $l \neq \mathrm{char}(k)$*:* [1]

$$\dim(\mathbf{Pic}^0(X)) = \frac{1}{2}\dim_{\mathbb{Q}_l}(H^1(X_{ét}, \mathbb{Z}_l) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l) =$$
$$\frac{1}{2}\dim_{\mathbb{Q}_l}(\mathrm{Hom}_{\mathrm{cont}}(\pi_1(X), \mathbb{Z}_l) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l)$$

Proof of the first equation Let $n \in \mathbb{N}$ with $\mathrm{char}(k) \nmid n$. The Kummer exact sequence (in the étale topology)

$$0 \longrightarrow \mu_n \longrightarrow \mathbb{G}_m \xrightarrow{\cdot n} \mathbb{G}_m \longrightarrow 0$$

[1] We should write the fundamental group relative to some base point. However the fundamental groups relative to different base points are (non-canonically) isomorphic.

gives rise to a long exact sequence

$$\begin{tikzcd}
0 \arrow[r] & \mu_n(X) \arrow[r] & \Gamma(X,\mathcal{O}_X)^* \arrow[r, "\cdot n"] & \Gamma(X,\mathcal{O}_X)^* \arrow[r] & {} \\
H^1(X_{\text{ét}},\mu_n) \arrow[r] & H^1(X_{\text{ét}},\mathbb{G}_m) \arrow[r] \arrow[d, equal, "\sim"] & H^1(X_{\text{ét}},\mathbb{G}_m) \arrow[r] \arrow[d, equal, "\sim"] & \cdots \\
 & \operatorname{Pic}(X) \arrow[r, "\cdot n"] & \operatorname{Pic}(X) &
\end{tikzcd}$$

Since X is projective, $\cdot n : \Gamma(X,\mathcal{O}_X)^* \longrightarrow \Gamma(X,\mathcal{O}_X)^* \simeq k^*$ is an isomorphism. We thus have an isomorphism

$$H^1(X_{\text{ét}},\mu_n)\xrightarrow{\sim}\operatorname{Pic}(X)_n{}^2$$

Choosing an isomorphism $\mu_n \longrightarrow \mathbb{Z}/n\mathbb{Z}$ we get a *non-canonical* isomorphism

$$H^1(X_{\text{ét}},\mathbb{Z}/n\mathbb{Z}) \approx \operatorname{Pic}(X)_n.$$

Now let $l \neq$char(k) be a prime. We can choose isomorphism $\mu_{l^i}\xrightarrow{\sim}\mathbb{Z}/l^i\mathbb{Z}$ in a way that is compatible with the projective systems. Taking the limit, we obtain an isomorphism

$$H^1(X_{\text{ét}},\mathbb{Z}_l)\xrightarrow{\sim}T_l(\operatorname{Pic}(X)).^3$$

It follows

$$H^1(X_{\text{ét}},\mathbb{Z}_l)\otimes_{\mathbb{Z}_l}\mathbb{Q}_l \approx T_l(\mathbf{Pic}(X))\otimes_{\mathbb{Z}_l}\mathbb{Q}_l \simeq T_l(\mathbf{Pic}^0(X))\otimes_{\mathbb{Z}_l}\mathbb{Q}_l \simeq T_l(\mathbf{Pic}^0(X)^{\text{red}})\otimes_{\mathbb{Z}_l}\mathbb{Q}_l$$

On the other hand, $\mathbf{Pic}^0(X)^{\text{red}}$ is an abelian variety and with [Mi-A, Theorem 15.1], we can conclude that

$$\dim(\mathbf{Pic}^0(X)) = \dim(\mathbf{Pic}^0(X)^{\text{red}})$$
$$\frac{1}{2}\dim_{\mathbb{Q}_l}T_l(\operatorname{Pic}(X))\otimes_{\mathbb{Z}_l}\mathbb{Q}_l = \frac{1}{2}\dim_{\mathbb{Q}_l}H^1(X_{\text{ét}},\mathbb{Z}_l)\otimes_{\mathbb{Z}_l}\mathbb{Q}_l$$

Proof of the second equation (outline) There is a canonical isomorphism

$$\operatorname{Hom}_{\text{cont}}(\pi_1(X),\mathbb{Z}_l) \simeq H^1(X_{\text{ét}},\mathbb{Z}_l)$$

This follows from the following facts:

- $H^1(X_{\text{ét}},\mathbb{Z}/n\mathbb{Z}) \simeq \overset{\vee}{H^1}(X_{\text{ét}},\mathbb{Z}/n\mathbb{Z})$. [4] [Mi-É, III.2, Theorem 2.17.]

[2] For some abelian group G, we denote the kernel of the multiplication of n by G_n. In particular, if A is an abelian variety over the algebraically closed field k, then $A[n](k) \simeq A(k)_n$.

[3] For an abelian group G and some prime l, we denote $\lim_{\longleftarrow i} G_{l^i}$ by $T_l(G)$. In particular, if A is an abelian variety over the algebraically closed field k, then $T_l(A) = T_l(A(k))$.

[4] We use the same notation for a finite group, the corresponding group scheme and the corresponding étale/flat sheaf over some scheme.

- The set of isomorphism classes of principal homogeneous spaces for $\mathbb{Z}/n\mathbb{Z}$ over X is in bijection with $\overset{\vee}{H}{}^1(X_{\mathrm{et}}, \mathbb{Z}/n\mathbb{Z})$. [Mi-É, III.4, Corollary 4.7., Remark 4.8.]

- Principal homogeneous spaces for $\mathbb{Z}/\ltimes\mathbb{Z}$ over X correspond to Galois coverings of X with given Galois action of $\mathbb{Z}/n\mathbb{Z}$ and vice versa, and the set of isomorphism classes of these is in bijection with $\mathrm{Hom}_{\mathrm{cont}}(\pi_1(X), \mathbb{Z}/n\mathbb{Z})$. ([SGA I, V.2] and definition of the étale fundamental group) □

If $\mathbf{Pic}(X)$ is reduced (smooth) – thus an abelian variety – can also be read of from cohomology:

Lemma A.2

$$\dim(\mathbf{Pic}^0(X)) \leq \dim_k H^1(X, \mathcal{O}_X)$$

Equality holds iff $\mathbf{Pic}^0(X)$ *is reduced. In particular, this is the case if char*$(k) = 0$.

Proof See [BLR, 8.4, Theorem 1]. The last statement follows from the fact that all projective group schemes over fields in characteristic zero are reduced. □

For the following proposition we need the definition:

Definition Let $\mathrm{char}(k) > 0$, let X be a projective k-variety. A smooth proper global lifting is a separated scheme $\mathcal{X}$ defined over the spectrum of a discrete valuation ring R such that

- The function field of R has characteristic zero and the residue field is k
- The "geometric fiber" $\mathcal{X}_0 := \mathcal{X} \otimes_R k$ is isomorphic to X
- $\mathcal{X}$ is smooth and proper over $\mathrm{Spec}R$.

Let $\mathcal{X}_\eta := \mathcal{X} \otimes_R \mathrm{Quot}(R)$ be the "generic fiber" of $\mathcal{X}$. Then in particular, $\mathcal{X}_\eta$ is a non-singular, proper, integral $\mathrm{Quot}(R)$-variety. We denote $\mathcal{X}_\eta \otimes_{\mathrm{Quot}(R)} \overline{\mathrm{Quot(R)}}$ be $\overline{\mathcal{X}_\eta}$.

Remark We will use that the Picard-scheme of $\mathcal{X}_\eta$ exists and is proper. Since up to now we have only talked about the Picard-scheme of a *projective* non-singular integral variety, we assume furthermore that the generic fiber of $\mathcal{X}_\eta$ is projective. However, the Picard-scheme also exists in the proper case and is proper; see [BLR, 8.2. Theorem 3 ,8.4, Theorem 3].

Lemma A.3 *Let k be a field with positive characteristic. Let X have a smooth proper global lifting. Then* $\mathbf{Pic}^0(X)$ *is reduced.*

Proof By Lemma A.2 we have to show that $\dim(\mathbf{Pic}^0(X)) = \dim H^1(X, \mathcal{O}_X)$.

Let $\mathcal{X}$ be a global lifting for k over the spectrum of the discrete valuation ring R.

Let $l \neq$char(k) be a prime. By the above lemmata,

$$\frac{1}{2}\dim_{\mathbb{Q}_l} H^1(\overline{\mathcal{X}_\eta}_{\text{ét}}, \mathbb{Z}_l) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l = \dim_{\overline{\text{Quot}(R)}} H^1(\overline{\mathcal{X}_\eta}, \mathcal{O}_{\mathcal{X}_\eta}).$$

We now use the theorems of cohomology and base change to "transfer" this equation to $\mathcal{X}_0 \approx X$.

$$\dim_{\overline{\text{Quot}(R)}} H^1(\overline{\mathcal{X}_\eta}, \mathcal{O}_{\mathcal{X}_\eta}) = \dim_{\text{Quot}(R)} H^1(\mathcal{X}_\eta, \mathcal{O}_{\mathcal{X}_\eta}) = \dim_k H^1(\mathcal{X}_0, \mathcal{O}_{\mathcal{X}_\eta})$$

The first equation is a special case of [Ha, III, Proposition 9.3], and the second equation follows from [Ha, III, Corollary 12.9].

By [Mi-É, VI, Corollary 4.2],

$$H^1(\overline{\mathcal{X}_\eta}_{\text{ét}}, \mathbb{Z}/n\mathbb{Z}) \cong H^1(\mathcal{X}_{0\,\text{ét}}, \mathbb{Z}/n\mathbb{Z}).$$

These equations imply

$$\dim(\mathbf{Pic}^0(X)) = \frac{1}{2}\dim_{\mathbb{Q}_l}(H^1(X_{\text{ét}}, \mathbb{Z}_l) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l) = \dim_k H^1(X, \mathcal{O}_X).$$

Thus by Lemma A.2, X is reduced. □

A.1.2 The Picard scheme of a product

Let k be an algebraically closed field and let X_1, X_2 be two non-singular projective integral k-varieties. Let P_1 and P_2 be k-rational points of X_1, X_2 respectively. Let $q_i : X_1 \times_k X_2 \longrightarrow X_i$ $(i = 1, 2)$ be the projections.

Let Z be a k-scheme. By bull-back, we have morphisms

$$\text{Pic}(X_1 \times_k Z)/\text{Pic}(Z) \times \text{Pic}(X_1 \times_k Z)/\text{Pic}(Z) \longrightarrow \text{Pic}(X_1 \times_k X_2 \times_k Z)/\text{Pic}(Z)$$
$$(\overline{\overline{\mathcal{M}_1}}, \overline{\overline{\mathcal{M}_2}}) \mapsto \overline{\overline{q_1^*(\mathcal{M}_1) \otimes q_2^*(\mathcal{M}_2)}}.$$

By applying $(P_i \times_k \text{id}_Z)^*$ we see that these morphism are *injective.*

Thus we get an injective natural transformation

$$\mathcal{U} : \mathcal{P}\text{ic}(X_1) \times \mathcal{P}\text{ic}(X_1) \longrightarrow \mathcal{P}\text{ic}(X_1 \times_k X_2).$$

This induces a morphism

$$\mathbf{U} : \mathbf{Pic}^0(X_1) \times \mathbf{Pic}^0(X_1) \longrightarrow \mathbf{Pic}^0(X_1 \times_k X_2).$$

Proposition A.4 *If k has characteristic zero or if X_1 and X_2 have smooth proper global liftings, then* $\mathbf{U}$ *is an isomorphism between abelian varieties.*

In general, $\mathbf{U}$ *induces an isomorphism between the corresponding reduced objects, which are abelian varieties.*

Proof By Lemma A.1,

$$\begin{gathered}\dim(\mathbf{Pic}^0(X_1 \times_k X_2)) = \tfrac{1}{2}\dim_{\mathbb{Q}_l}(\mathrm{Hom}_{\mathrm{cont}}(\pi_1(X_1 \times_k X_2), \mathbb{Z}_l) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l) = \\ \tfrac{1}{2}\dim_{\mathbb{Q}_l}(\mathrm{Hom}_{\mathrm{cont}}(\pi_1(X_1) \times \pi_1(X_2), \mathbb{Z}_l) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l) = \\ \tfrac{1}{2}\dim_{\mathbb{Q}_l}(\mathrm{Hom}_{\mathrm{cont}}(\pi_1(X_1), \mathbb{Z}_l) \times \mathrm{Hom}_{\mathrm{cont}}(\pi_1(X_2), \mathbb{Z}_l)) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l) = \\ \dim(\mathbf{Pic}^0(X_1)) \cdot \dim(\mathbf{Pic}^0(X_2)).\end{gathered} \tag{A.1}$$

Here we use

$$\pi_1(\mathbf{Pic}^0(X_1) \times_k \mathbf{Pic}^0(X_2)) \cong \pi_1(\mathbf{Pic}^0(X_1)) \times \pi_1(\mathbf{Pic}^0(X_2))$$

(relative so some base points); see [SGA I, X, Corollaire 1.7].

Alternatively, we could also use the Künneth-formula of étale cohomology to derive $(A.1)$.

Since k is an algebraically closed field, the corresponding reduced objects on both sides are abelian varieties. $\mathbf{U}$ has trivial kernel, thus induces an isomorphism of abelian varieties.

If X_1 and X_2 have global liftings, so has the product and by Lemma A.3, both sides are reduced, thus $\mathbf{U}$ is an isomorphism. □

Remark If X_1 and X_2 are irreducible non-singular *curves*, then a smooth global lifting exists; see [Po, Satz 10.1]. Thus in this case, $\mathbf{U}$ is an isomorphism of abelian varieties.

A.2 Some results about abelian varieties

The results is this section are mostly well-known. Some of the results are discussed in [Mu] over algebraically closed fields at least implicitly. However, for most of the results we lack a suitable reference and because of that we include them with proofs.

A.2.1 Isogenies

Let K be a field, A, B and C three abelian K-varieties.

Lemma A.5 *Let $\alpha, \beta : B \longrightarrow C$ be some morphisms, $\pi : A \longrightarrow B$ an isogeny. Assume that $\alpha\pi = \beta\pi$. Then $\alpha = \beta$.*

Proof π is surjective on $\overline{K}$-valued points, and thus $\alpha = \beta : B(\overline{K}) \longrightarrow C(\overline{K})$. This implies $\alpha = \beta : B \longrightarrow C$. □

We also have the following analogous result:

Lemma A.6 *Let $\alpha, \beta : A \longrightarrow B$ be some morphisms, $\pi : B \longrightarrow C$ an isogeny. Assume that $\pi\alpha = \pi\beta$. Then $\alpha = \beta$.*

Proof Since $\pi : b \longrightarrow C$ is an isogeny, $\ker(\pi)$ is a closed subscheme of $\ker([n])$ for some $n \in \mathbb{N}$. Thus there exists a $\rho : C \longrightarrow B$ such that $\rho\pi = n\,\mathrm{id}_C$. Thus $[n]\,\alpha = [n]\,\beta$, so $\alpha[n] = \beta[n]$. Since $[n]$ is an isogeny, we get $\alpha = \beta$ by the preceding lemma. □

For any two abelian varieties A and B, let as usual $\mathrm{Hom}^0_K(A,B) := \mathrm{Hom}_K(A,B) \otimes_{\mathbb{Z}} \mathbb{Q}$. $\mathrm{Hom}_K(A,B)$ is a free abelian group (since $[n] = n\,\mathrm{id}$ is an isogeny), thus $\mathrm{Hom}_K(A,B) \longrightarrow \mathrm{Hom}^0_K(A,B)$ is an inclusion.

If $\alpha : A \longrightarrow B$, $q \in \mathbb{Q}$, we write $q\,\alpha$ for $\alpha \otimes q$.

The class of abelian varieties with morphisms between two abelian varieties A and B being $\mathrm{Hom}^0_K(A,B)$ forms a category which is called the "category of abelian varieties up to isogeny"; cf. [Mu, par. 19].

Lemma A.7 *Let $\pi : A \longrightarrow B$ be an isogeny. We want to show that π has a unique inverse in the category of abelian varieties up to isogeny. By this we mean the following: There exists a $\rho \in \mathrm{Hom}^0_K(B,A)$ with $\rho\pi = \mathrm{id}_A$, $\pi\rho = \mathrm{id}_B$. Moreover, ρ is uniquely determined by $\pi\rho = \mathrm{id}_A$ or $\rho\pi = \mathrm{id}_B$.*

Proof There exists some isogeny $\rho : B \longrightarrow A$ and some $n \in \mathbb{N}$ with $\rho\pi = n\,\mathrm{id}_A$. Thus $\frac{1}{n}\rho\pi = \mathrm{id}_A$, i.e. $\frac{1}{n}\rho$ is the left inverse of π in the category of abelian varieties up to isogeny. Now, $\frac{1}{n}\beta$ is also the right inverse for π. In fact, $\pi\rho\pi = n\pi$, and by Lemma A.5, $\pi\rho = n\,\mathrm{id}_B$. Again by the preceding lemmata, the left and right inverses of π in the category of abelian varieties up to isogeny are unique. Thus ρ is *the* unique inverse of π in the category of abelian varieties up to isogeny. □

We will denote the inverse of the isogeny π by π^{-1}.

The next lemma is now obvious.

Lemma A.8 *Let $\pi : A \longrightarrow B$ be an isogeny of abelian varieties. Then $\mathrm{End}^0_K(A) \longrightarrow \mathrm{End}^0_K(B)$ $\alpha \mapsto \pi\alpha\pi^{-1}$ is an isomorphism.*

□

Remark Let the kernel of $\pi : A \longrightarrow B$ be contained in $\ker([n])$ for some $n \in \mathbb{N}$. For example, A and B might be elliptic curves and π an isogeny of degree n.

Then the above lemma may be strengthened in the following way: For some ring Λ and an element $f \in \Lambda$, let $\Lambda_{(f)}$ be the localization of Λ at the multiplicative set $\{f^i | i \geq 0\}$. Then π induces an isomorphism $\mathrm{End}(A)_{(f)} \longrightarrow \mathrm{End}(B)_{(f)}$.

A.2.2 The Néron-Severi group and polarizations

Let k be a field and let A be an abelian k-variety, $\widehat{A}$ the dual variety. Let $\mathcal{L}$ be an invertible sheaf on A. Let $\phi_{\mathcal{L}} : A \longrightarrow \widehat{A}$ be the morphism which is associated to the natural transformation $\mathrm{Hom}(-,A) \longrightarrow \mathcal{P}\mathrm{ic}^0(A)$, given for Z-valued points P by $P \mapsto T_P^* q_Z^*(\mathcal{L}) \otimes q_Z^*(\mathcal{L})^{-1}$, where $q_Z : A \times_k Z \longrightarrow A$ is the projection. The map $\phi : \mathrm{Pic}(A) \longrightarrow \mathrm{Hom}_K(A, \widehat{A})$ itself is a group homomorphism. The kernel of ϕ is $\mathrm{Pic}^0(A)$, the group of classes of invertible sheaves on A being algebraically equivalent to $\mathcal{O}_A$.

The group $\mathrm{Pic}(A)/\mathrm{Pic}^0(A)$ is called the *Néron-Severi group* of A, denoted $\mathrm{NS}(A)$. As usual, we denote $\mathrm{NS}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ by $\mathrm{NS}^0(A)$. If $x \in \mathrm{NS}(A)$ is given by some sheaf $\mathcal{M}$ on A, we denote $\phi_{\mathcal{M}}$ also by ϕ_x. By construction, the map $\phi : \mathrm{NS}(A) \longrightarrow \mathrm{Hom}_k(A, \widehat{A})$ is an injective group homomorphism. It extends to an injective group homomorphism $\phi : \mathrm{NS}^0(A) \longrightarrow \mathrm{Hom}_k^0(A, \widehat{A})$.

Let $K|k$ be an algebraic field extension. Let A' be an abelian K-variety. As usual, any k-morphism $\sigma : \mathrm{Spec}(K) \longrightarrow \mathrm{Spec}(K)$ induces an isomorphism $\sigma^* : \mathrm{Pic}(A') \longrightarrow \mathrm{Pic}(\sigma^{-1}(A'))$. This isomorphism corresponds to the isomorphism $\sigma^{-1}(\ldots) = (\ldots)^\sigma : \mathbf{Pic}(A') \longrightarrow \mathbf{Pic}(\sigma^{-1}(A'))$. (For $K|k$ Galois and $A' = A_K$ this is a special case of Lemma 1.16, if one forgets the last equality of the proof of Lemma 1.16, this proof also implies the general case.)

Lemma A.9 *Let σ be a k-automorphism of* $\mathrm{Spec}(K)$*, let $\mathcal{L}$ be an invertible sheaf on A'. Then*

$$\phi_{\sigma^*(\mathcal{L})} = \sigma^{-1}\phi_{\mathcal{L}}\sigma = \sigma^{-1}(\phi_{\mathcal{L}}) = \phi_{\mathcal{L}}^\sigma : \sigma^{-1}(A') \longrightarrow \sigma^{-1}(\widehat{A'}).$$

Proof Let $\sigma'^{\#}$ be a k-automorphism with $\sigma'^{\#}|K = \sigma^{\#}$. This defines a K-automorphism σ' of $\mathrm{Spec}(\overline{K})$. Denote the pull-back of $\mathcal{L}$ to $A'_{\overline{K}}$ again by $\mathcal{L}$. Applying the base change $\overline{K}|K$ to the above equality, we get the following equality of morphisms of abelian $\overline{K}$-varieties, which is equivalent to the equality in the statement of the lemma.

$$\phi_{\sigma'^*(\mathcal{L})} = \sigma'^{-1}\phi_{\mathcal{L}}\sigma' = \sigma'^{-1}(\phi_{\mathcal{L}}).$$

We show that this equality holds for $\overline{K}$-valued points. This implies the equality in the statement of the lemma.

Let P be a $\overline{K}$-valued point of $\sigma^{-1}(A'_{\overline{K}}) \simeq \sigma'^{-1}(A')_{\overline{K}}$. We use that $\sigma' T_P \sigma'^{-1} = \sigma'(T_P) = T_{\sigma'(P)} : A'_{\overline{K}} \longrightarrow A'_{\overline{K}}$.

Now, $\phi_{\sigma'^*(\mathcal{L})} \circ P$ (which is a $\overline{K}$-valued point of $\sigma'^{-1}(\widehat{A'}_{\overline{K}})$) corresponds to the class of sheaves $T_P^*(\sigma'^*(\overline{\mathcal{L}})) \otimes \sigma'^*(\overline{\mathcal{L}})^{-1} = (\sigma' T_P)^*(\overline{\mathcal{L}}) \otimes \sigma'^*(\overline{\mathcal{L}})^{-1} = (T_{\sigma'(P)}\sigma')^*(\overline{\mathcal{L}}) \otimes \sigma'^*(\overline{\mathcal{L}})^{-1} = \sigma'^*(T_{\sigma'(P)}^*(\overline{\mathcal{L}}) \otimes \overline{\mathcal{L}}^{-1})$. This sheaf in turn corresponds to $\sigma'^{-1}(\phi_{\mathcal{L}} \circ \sigma'(P)) = \sigma'^{-1} \circ \phi_{\mathcal{L}} \circ \sigma' \circ P \circ \sigma'^{-1} \circ \sigma' = \sigma'^{-1}(\phi_{\mathcal{L}}) \circ P$. □

Galois extensions

Now let $K|k$ be Galois. Let A be an abelian k-variety, $A' = A_K$.

Then the last lemma implies in particular that $\mathrm{Pic}^0(A_K)$ is invariant under pull-back by σ. (This follows for example also from the fact that the operation of G on $\mathbf{Pic}(A_K)(K)$ restricts to an operation on $\mathbf{Pic}^0(A_K)(K) = \widehat{A}(K)$.)

Since $\mathrm{Pic}^0(A) = \mathrm{Pic}^0(A_K) \cap \mathrm{Pic}(A)$, $\mathrm{NS}(A)$ is naturally a subgroup of $\mathrm{NS}(A_K)$. Because $\mathrm{Pic}^0(A)$ is invariant under the Galois-operation, G operates on $\mathrm{NS}(A_K)$.

With the notations as in the lemma, $\mathcal{L}$ defines an element in $\mathrm{NS}(A_K)^G$ iff $\phi_{\mathcal{L}}$ is invariant under G, i.e. iff it is defined over k.

We want to study the cokernel of the injective group homomorphism

$$\mathrm{NS}(A) \hookrightarrow \mathrm{NS}(A_K)^G. \tag{A.2}$$

Lemma A.10 *The cokernel of (A.2) has exponent 2.*

Proof This is a special case of [Mu, 20, p.188, Theorem 2]:

Let $x \in \mathrm{NS}(A_K)^G$. This induces the morphism $\phi_x : A \longrightarrow \widehat{A}$.

Choose a prime $l \neq \mathrm{char}(k)$. The bilinear form $e_l(.,\phi_x(.))$ on $T_l(A_{\overline{K}})$ is skew-symmetric since $\phi_x \otimes_k \mathrm{id}_K = \phi_{\mathcal{L}}$ on A_K. Let $\mathcal{P}$ be a universal divisional correspondence on $A \times \widehat{A}$, and let $\mathcal{M} := (\mathrm{id}, \phi_x)^*(\mathcal{P})$. Then one calculates that $2e_l(.,\phi_x(.)) = e_l(.,\phi_{\mathcal{M}}(.))$. It follows that $2\phi_x = \phi_{\mathcal{M}}$ because of the non-degeneracy of e_l.

This implies that $\overline{\mathcal{M}}$ is class of $2x$ in $\mathrm{NS}(A_K)^G$. □

Warning The proof of the remark following [Mu, par. 20, p.188, Theorem 2] (i.e. [Mu, par. 23, p.231, Theorem 3]) does not hold since it is assumed that $\mathrm{Pic}(A)$ is divisible. Thus one cannot conclude that the cokernel of (A.2) is trivial.

Now we study the cokernel of (A.2) with a cohomological approach.

By definition of the Néron-Severi group we have a short exact sequence

$$1 \longrightarrow \mathrm{Pic}^0(A_K) \longrightarrow \mathrm{Pic}(A_K) \longrightarrow \mathrm{NS}(A_K) \longrightarrow 1.$$

Taking invariants under the action by the Galois group G, we get a long exact sequence

$$\begin{gathered} 1 \longrightarrow \mathrm{Pic}^0(A) \longrightarrow \mathrm{Pic}(A) \longrightarrow \mathrm{NS}(A_K)^G \longrightarrow \\ H^1(G, \mathrm{Pic}^0(A_K)) \longrightarrow H^1(G, \mathrm{Pic}(A_K)) \longrightarrow \cdots \end{gathered}$$

Thus $\mathrm{coker}(\mathrm{Pic}(A) \longrightarrow \mathrm{NS}(A_K)^G) = \ker(H^1(G, \mathrm{Pic}^0(A_K)) \longrightarrow H^1(G, \mathrm{Pic}(A_K)))$.

Lemma A.11 *If the order of G is finite and odd then* $\mathrm{NS}(A) \longrightarrow \mathrm{NS}(A_K)^G$ *is an isomorphism.*

Proof We already know that the cokernel has exponent 2. On the other hand, since G is a finite group and the order of G odd, so are the orders of its Tate-cohomology groups; see [Se, VIII, 2, p.130, Corollary 1]. Thus the cokernel has to be trivial. □

Lemma A.12 *Let k be finite. Then $H^1(\mathrm{Gal}(\overline{k}|k), A(\overline{k})) = 0$ and thus $\mathrm{NS}(A) \longrightarrow \mathrm{NS}(A_{\overline{k}})^{\mathrm{Gal}(\overline{k}|k)}$ is an isomorphism.*

Proof We only have to show the result for all finite subextensions. Let $K|k$ be such a subextension with Galois group G.

Every 1-cocycle $(P_\sigma)_{\sigma\in G}$ defines by $\sigma \mapsto T_{P_\sigma}$ (= translation by P_σ) a twist of A_K. Such a twist is isomorphic to A iff $(P_\sigma)_{\sigma\in G}$ is a 1-coboundary, i.e. if there exists a $Q \in A(K)$ with $\sigma^{-1}(Q) - Q = P_\sigma$ for all $\sigma \in G$, i.e. iff $\sigma^{-1}(Q) = T_{P_\sigma} \circ Q$, i.e. iff $Q = \sigma \circ T_{P_\sigma} \circ Q \circ \sigma^{-1}$. And this means that Q is invariant under the Galois-operation of G on A_K and thus is a k-rational point of A.

Now, a theorem by S.Lang says that over a finite field k, all k-schemes which are "geometrically" abelian varieties have a rational point; see [Mu, p.205, Theorem 3].

So $(P_\sigma)_{\sigma\in G}$ is a 1-coboundary and thus $H^1(G, A_K)$ is trivial.

Note: The argument can be reformulated by saying that all principal homogeneous spaces of A_K are equivalent, or – what is the same – that the Weil-Châtelet-group of A is trivial; see [Si, X, 3] for details, the results formulated there hold for general abelian varieties. □

The Néron-Severi group as functor

Lemma A.13 *Let $\psi : A \longrightarrow B$ be a morphism of abelian k-varieties, $x \in \mathrm{NS}^0(B_{k^{\mathrm{sep}}})^{\mathrm{Gal}(k^{\mathrm{sep}}|k)}$, given by some $\overline{\mathfrak{L}} \in \mathrm{Pic}(B_{k^{\mathrm{sep}}})$. Then*

$$\phi_{\psi^*(\mathfrak{L})} = \widehat{\psi} \otimes_k \mathrm{id}_{k^{\mathrm{sep}}} \circ \phi_{\mathfrak{L}} \circ \psi \otimes_k \mathrm{id}_{k^{\mathrm{sep}}} : A_{k^{\mathrm{sep}}} \longrightarrow \widehat{A}_{k^{\mathrm{sep}}}.$$

The *proof* is analogous to the one of Lemma A.9.

We can assume that $k = \overline{k}$.

Let P be a $k = \overline{k}$-valued point of A. We use that $\psi\, T_P = T_{\psi\circ P}\, \psi$.

Now, $\phi_{\psi^*(\mathfrak{L})} \circ P$ (which is a k-valued point of $\widehat{A}$) corresponds to the class of sheaves $T_P^*(\psi^*(\overline{\mathfrak{L}}))\otimes\psi^*(\overline{\mathfrak{L}})^{-1} = (\psi T_P)^*(\overline{\mathfrak{L}})\otimes\psi^*(\overline{\mathfrak{L}})^{-1} = (T_{\psi\circ P}\psi)^*(\overline{\mathfrak{L}})\otimes\psi^*(\overline{\mathfrak{L}})^{-1} = \psi^*(T_{\psi\circ P}^*(\overline{\mathfrak{L}}) \otimes \overline{\mathfrak{L}}^{-1})$. This sheaf in turn corresponds to $\widehat{\psi}\phi_{\mathfrak{L}}\psi \circ P$. □

In particular, $\mathrm{Pic}^0(A)$ is invariant under ψ^*. Thus NS is a contravariant functor from the category of abelian k-varieties to the category of abelian groups. (And so are NS^0, $\mathrm{NS}((.)_{k^{\mathrm{sep}}})^{\mathrm{Gal}(k^{\mathrm{sep}}|k)}$ and $\mathrm{NS}^0((.)_{k^{\mathrm{sep}}})^{\mathrm{Gal}(k^{\mathrm{sep}}|k)}$.)

If $\psi : A \longrightarrow B$, the corresponding homomorphism between Néron-Severi groups will also be denoted by ψ^*.

Polarizations and the category of polarized abelian varieties

Definition [Mi-A, 13] A *polarization* of A is a morphism $\varphi : A \longrightarrow \widehat{A}$ such that $\varphi\otimes_k \mathrm{id}_{\overline{k}} = \phi_{\mathfrak{L}} : A_{\overline{k}} \longrightarrow A_{\overline{k}}$ for some ample sheaf $\mathfrak{L}$ on $A_{\overline{k}}$. A *principal polarization* is a polarization with trivial kernel.

By Lemma A.9, ϕ induces a bijection between the subset of element of $\mathrm{NS}(A_{k^{\mathrm{sep}}})^{\mathrm{Gal}(k^{\mathrm{sep}}|k)}$ defined by ample sheaves and the set of polarizations on A.

Definition The *category of polarized abelian varieties* over k consists of the following:

Objects are abelian varieties A with some element $x \in \mathrm{NS}(A_{\overline{k}})$ where x is defined by an ample sheaf and – after the choice of a dual abelian variety $\widehat{A}$ – $\phi_x : A_{\overline{k}} \longrightarrow \hat{A}_{\overline{k}}$ is defined over k. (If k is perfect, this is the same as saying that $x \in \mathrm{NS}(A_{\overline{k}})^{\mathrm{Gal}(\overline{k}|k)}$.)

The morphisms between two objects (A, x) and (B, y) are morphisms $\alpha : A \longrightarrow B$ with $\alpha^*(x) = y$. [5]

Analogously, one defines the *category of polarized abelian varieties with polarizations defined by sheaves over* k. Here, the objects are abelian varieties A with some $x \in \mathrm{NS}(A)$. The morphisms are defined as above.

There is a forget-functor from the category of polarized abelian varieties with polarizations defined by sheaves over k to the category of polarized abelian varieties varieties. This functor is fully faithful.

And there is a forget-functor from the category of polarized abelian varieties to the category of abelian varieties. This functor is also faithful and for a fixed abelian variety A, the preimages under this functor correspond in a natural way to the polarizations on A.

The results about the Néron-Severi group translate to results of polarizations. For example, if $\varphi : A \longrightarrow \widehat{A}$ is a polarization, then 2φ is defined by a sheaf on A. And if k is finite, every polarization is defined by a sheaf on A.

The *proof* is [Mu, 20, p.188, Theorem 2] again plus the fact that "ample" is a geometric property and depends only on the class of a sheaf in the Néron-Severi group.

For the next two lemmata, let k be perfect.

Lemma A.14 *Let $\varphi : A \longrightarrow \widehat{A}$ be a polarization. This polarization induces an injective group homomorphism $\mathrm{NS}^0(A_{\overline{k}})^{\mathrm{Gal}(\overline{k}|k)} \longrightarrow \mathrm{End}^0_k(A)$. The image of this inclusion consists of the elements of $\mathrm{End}^0_k(A)$ which are fixed by the Rosati involution (with respect to φ).*

Now let φ be a principal polarization. Then we have an injective group homomorphism $\mathrm{NS}(A_{\overline{k}})^{\mathrm{Gal}(\overline{k}|k)} \longrightarrow \mathrm{End}_k(A)$. Again, the image of this inclusion consists of the elements which are fixed by the Rosati involution (with respect to φ).

Proof Both statements follow from the corresponding statements over algebraically closed fields by taking Galois-invariants. Thus we restrict ourselves to algebraically closed fields.

[5] With this definition for the category of polarized abelian varieties we avoid the (simultaneous) choosing of a dual abelian variety for every abelian variety.

Let k be algebraically closed. The first statement is well-known; see [Mu, p.190 (3)]. For the second statement, let $\lambda \in \operatorname{End}(A)$. By the first statement, there exists an $n \in \mathbb{N}$ and sheaf $\mathcal{M}$ on A such that $\varphi^{-1}\phi_{\mathcal{M}} = n\lambda$, i.e. $\phi_{\mathcal{M}} = n\varphi\lambda$. Since φ is an isomorphism, $\ker(\phi_{\mathcal{M}})$ contains $A[n]$, the group scheme of n-torsion points of A. Since we assumed k to be algebraically closed, by [Mu, par. 23, p.231, Theorem 3], there exists a sheaf $\mathcal{N}$ on A such that $\overline{\mathcal{N}}^n = \overline{\mathcal{M}}$, and the class of this sheaf in the Néron-Severi group is mapped to λ. □

Lemma A.15 *Let φ be a polarization on A. With respect to this polarization, let $(\ldots)'$ denote the Rosati involution.*

Let $x \in \operatorname{NS}(A_{\overline{k}})^{\operatorname{Gal}(\overline{k}|k)}$ corresponding under the polarization φ to the endomorphism m on A. Let ψ be an endomorphism on A. Then $\psi^*(x)$ corresponds – again under φ – to $\psi' m \psi \in \operatorname{End}_k^0(A)$.

Proof The element in $\operatorname{End}_k^0(A)$ we are looking for is $\varphi^{-1}\phi_{\psi^*(x)}$, and this equals $\varphi^{-1}\widehat{\psi}\phi_x\psi = \varphi^{-1}\widehat{\psi}\varphi\varphi^{-1}\phi_x\psi = \psi' m\psi$. □

A.2.3 Products and the Rosati involution

Let k be a field, let B_i for $i = 1, \ldots, n$ and A_j for $j = 1, \ldots, m$ be abelian k-varieties. Let $A := \prod_{j=1,\ldots,m} A_j$, $B := \prod_{i=1,\ldots,n} B_i$. 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.) Then, since a finite product of abelian varieties is also the sum of the these abelian varieties in the category of abelian varieties,

$$\begin{array}{ccc} \operatorname{Hom}_k(A,B) & \longrightarrow & \bigoplus_{i,j} \operatorname{Hom}_k(A_j, B_i) \\ \psi & \mapsto & (p_i^B \psi \iota_j^A)_{i=1,\ldots,n,\, j=1,\ldots,m} \end{array} \tag{A.3}$$

is an isomorphism. (The same is true for the corresponding groups $\operatorname{Hom}_k^0(\ldots, \ldots)$ of both sides.)

Thus every morphism from A to B is uniquely determined by its "matrix", and conversely, every "matrix" determines a morphism. Further, the composition of morphisms corresponds to the usual composition of matrices.

In particular, under (A.3), $\operatorname{End}_k(A)$ is isomorphic to the "matrix ring" $\bigoplus_{i,j} \operatorname{Hom}_k(A_j, A_i)$.

There is a notational difficulty: For $j = 1$, a morphism $\psi = (\psi_1, \ldots, \psi_n) : A \longrightarrow B = \prod_{i=1,\ldots,n} B_i$ is represented by the *column vector*

$$\begin{pmatrix} \psi_1 \\ \psi_2 \\ \vdots \\ \psi_n \end{pmatrix}.$$

We now 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 $\psi \in \mathrm{Hom}_k^0(X,Y)$, we denote $\varphi_X^{-1}\widehat{\psi}\varphi_Y \in \mathrm{Hom}_k^0(Y,X)$ by ψ' and call it the *Rosati involution with respect to the polarizations φ_X and φ_Y.*

Now for $i = 1,\dots,n,\ j = 1,\dots,m$, let $\varphi_{B_i} : B_i \longrightarrow \widehat{B_i}$ and $\varphi_{A_j} : A_j \longrightarrow \widehat{A_j}$ be polarizations. Let $\varphi_A : A \longrightarrow \widehat{A}$ and $\varphi_B : B \longrightarrow \widehat{B}$ be the corresponding product polarizations.

Lemma A.16 *Let $\psi \in \mathrm{Hom}_k^0(A,B)$ be by the "matrix" $(\psi_{i,j})_{i=1,\dots,n,\, j=1,\dots,m}$, $\psi_{i,j} \in \mathrm{Hom}_k^0(A_j,B_i)$. Then with respect to φ_A and φ_B, the Rosati involution of ψ is given by the "matrix" $(\psi'_{j,i})_{i=1,\dots,m,\, j=1,\dots,n}$ with $\psi'_{j,i} \in \mathrm{Hom}_k^0(B_j,A_i)$.*

Proof Under the identification of $\widehat{A}$ with $\prod_{j=1,\dots,n} \widehat{A}_j$, $\widehat{p_j^A}$ equals (by definition) $\iota_j^{\widehat{A}}$. Analogously, $\widehat{p_j^{\widehat{A}}} = \iota_j^{\widehat{\widehat{A}}} = \iota_j^A$ and thus $p_j^{\widehat{A}} = \widehat{\iota_j^A}$. Further, $\varphi\iota_j^B = \iota_j^{\widehat{B}}\varphi_{B_j}$ and $\varphi_{A_i}p_i^A = p_i^{\widehat{A}}\varphi$, i.e. $p_i^A\varphi_A^{-1} = \varphi_{A_i}^{-1}p_i^{\widehat{A}}$.

We have to show that $p_i^A\psi'\iota_j^B = \psi'_{j,i}$. Now,

$$p_i^A\psi'\iota_j^B = p_i^A\varphi_A^{-1}\widehat{\psi}\varphi_B\iota_j^B = \varphi_{A_i}^{-1}p_i^{\widehat{A}}\widehat{\psi}\iota_j^{\widehat{B}}\varphi_{B_j} = \varphi_{A_i}^{-1}\widehat{\iota_i^A}\widehat{\psi}\widehat{p_j^B}\varphi_{B_j} = \\ \varphi_{A_i}^{-1}(\widehat{p_j^B\psi\iota_i^A})\varphi_{B_j} = \varphi_{A_i}^{-1}\widehat{\psi_{j,i}}\varphi_{B_j} = \psi'_{j,i}$$

□

A.2.4 Orthogonal complements and the Complete Reducibility Theorem

In this subsection, let k be a perfect field. Let X be an abelian variety over k. Let $\lambda|k$ be a subfield of $\overline{k}|k$, $\mathcal{L}$ an an ample sheaf on X_λ defining a polarization $\varphi : X \longrightarrow \widehat{X}$. Let Y be an abelian subvariety of X, let $\iota_Y : Y \hookrightarrow X$ be the inclusion, and let $\widehat{\iota_Y} : \widehat{X} \longrightarrow \widehat{Y}$ be the corresponding dual morphism.

The sheaf $\iota_Y^*(\mathcal{L})$ is again ample (this is true for any pull-back of an ample sheaf), and by Lemma A.13, the polarization defined by $\iota_Y^*(\mathcal{L})$ can be calculated as follows:

Lemma A.17 $\widehat{\iota_Y}\varphi\iota_Y \otimes_k \mathrm{id}_\lambda = \phi_{\iota_Y^*(\mathcal{L})}$. *In particular,* $K(\mathcal{L}) = \ker(\widehat{\iota_Y}\varphi\iota_Y) \otimes_k \mathrm{id}_\lambda$.

Definition Let Z be the reduced connected component of the zero of $\varphi^{-1}(\ker(\widehat{\iota_Y})) = \ker(\widehat{\iota_Y}\varphi)$. With other words, it is reduced induced closed subscheme associated to the connected component of the zero of $\ker(\widehat{\iota_Y}\varphi)$. (Thus there exists a natural closed immersion $Z \hookrightarrow \ker(\widehat{\iota_Y}\varphi)$.) We call Z the *orthogonal complement of* Y *in* X *with respect to* $\mathcal{L}$. The reduced and irreducible sub-group scheme Z of X is geometrically irreducible by lemma A.28 and geometrically reduced because we assumed k to be perfect, thus Z is an abelian variety. From this it also follows that “orthogonal complement” commutes with base extension (of fields). Since $\phi_{\iota_Y^*}$ is surjective, $\widehat{\iota_Y}$ is surjective.

Let $l \neq$char(k) be a prime. Let $E^{\mathfrak{L}}$ be the Riemann form associated with $\mathfrak{L}$ and l; cf. [Mu, p.186]. The term “orthogonal complement” is justified by the following lemma.

Lemma A.18 *$Z_{\overline{k}}$ is the largest abelian subvariety $Z'_{\overline{k}}$ of $X_{\overline{k}}$ with the property that $E^{\mathfrak{L}}(Y_{\overline{k}}, Z'_{\overline{k}}) = 1$.*

Proof Let $P \in T_l(X_{\overline{k}})$, $Q \in T_l(Y_{\overline{k}})$. Then

$$E^{\mathfrak{L}}_{X_{\overline{k}}}(T_l(\iota_Y)(Q), P) = e_{l\,X_{\overline{k}}}(T_l(\iota_Y)(Q), T_l(\phi_{\mathfrak{L}})(P)) = e_{l\,Y_{\overline{k}}}(Q, T_l(\widehat{\iota_Y})T_l(\phi_{\mathfrak{L}})(P)).$$

So,

$$E^{\mathfrak{L}}_{X_{\overline{k}}}(T_l(\iota_Y Y_{\overline{k}}), P) = 1 \longleftrightarrow e_{l\,Y_{\overline{k}}}(T_l(Y_{\overline{k}}), T_l(\widehat{\iota}\phi_{\mathfrak{L}})(P)) = 1 \longleftrightarrow T_l(\widehat{\iota}\phi_{\mathfrak{L}})(P) = 1.$$

Especially, the orthogonal complement $Z_{\overline{k}}$ of $Y_{\overline{k}}$ has the desired property. On the other hand, if $Z'_{\overline{k}}$ is any abelian subvariety with $E^{\mathfrak{L}}(Y_{\overline{k}}, Z'_{\overline{k}}) = 1$, then $T_l(Z'_{\overline{k}}) \subseteq T_l(\phi_{\mathfrak{L}}^{-1}(\ker(\widehat{\iota})))$. This implies $T_l(Z'_{\overline{k}}) \subseteq T_l(Z_{\overline{k}})$.

[Assume $P \in T_l(Z'_{\overline{k}}), P \notin T_l(Z_{\overline{k}})$. Let $i > 0$ such that $l^i P = 0$. For all $m \in \mathbb{N}$, let $Q_m \in T_l(Z'_{\overline{k}})$ with $l^{im} Q_m = P$. Then for $m_1 < m_2, Q_{m_2} - Q_{m_1} \notin T_l(Z_{\overline{k}})$ because otherwise $P = l^{im_2}(Q_{m_2} - Q_{m_1}) \in T_l(Z_{\overline{k}})$. So all sets $Q_{m_1} + T_l(Z_{\overline{k}}), Q_{m_2} + T_l(Z_{\overline{k}})$ are disjoint. By construction they are also contained in $T_l(\phi_{\mathfrak{L}}^{-1}(\ker(\widehat{\iota})))$, thus this set has infinitely many elements, a contradiction.]

Now the result follows by the injectivity of the l-adic representation. □

Lemma A.19 *$Y \cap Z := Y \times_X Z =: \iota_Y^{-1}(Z)$ is a closed subscheme of* $\ker(\widehat{\iota_Y}\varphi\iota_Y)$.

Proof The closed immersion $Z \hookrightarrow \ker(\widehat{\iota_Y}\varphi)$ induces a closed immersion $\iota_Y^{-1}(Z) \hookrightarrow \iota_Y^{-1}(\ker(\widehat{\iota_Y}\varphi)) = \ker(\widehat{\iota_Y}\varphi\iota_Y)$. (“Closed immersion” is “stable under base extension”.) □

Since $\iota_{Y_\lambda}^*(\mathfrak{L})$ is ample, so $K(\iota_{Y_l}^*(\mathfrak{L}))$ is finite, and so is $Y \times_X Z$. This implies the “Complete Reducibility Theorem”.

Proposition A.20 *[Mu, p.173] Let (X, φ) be a polarized abelian k-variety and Y an abelian subvariety, Z the orthogonal complement of Z with respect to $\mathfrak{L}$. Then* $\dim(X) = \dim(Y) + \dim(Z)$ *and X is isogenous to $Y \times_k Z$.*

Remark Let $\iota : Y \times_k Z \longrightarrow X$ be the isogeny, defined by ι_X and ι_Y. Then under this isogeny, φ becomes a product polarization, i.e. $\widehat{\iota}\varphi\iota$ is a product polarization. This is obvious since by definition of Z, $\widehat{\iota_Z}\varphi\iota_Y = 0$ and similarly with Y and Z interchanged, since the definition is “orthogonal complement” is symmetric by Lemma A.18 for example.

Already assuming the Complete Reducibility Theorem, one can easily proof

Lemma A.21 *Let X and Z be abelian k-varieties, $p : X \longrightarrow Z$ a surjective morphism. Then $\widehat{p} : \widehat{X} \longrightarrow \widehat{Z}$ has finite kernel.*

Proof Let Y be the reduced connected component of the zero of the kernel of $p : X \longrightarrow Z$, $\iota_{Z'} : Z' \hookrightarrow X$ the orthogonal complement of Y with respect to some polarization. Then the kernel of $p\iota_{Z'} : Z' \longrightarrow Z$ is immersed in $Z' \cap \ker(p)$ which is finite since $Z' \cap Y$ is finite. So $p\iota_{Z'} : Z' \longrightarrow Z$ is an isogeny, and so is $\widehat{\iota_{Z'}}\widehat{p} : Z \longrightarrow Z'$. Thus $\widehat{p}$ has finite kernel. □

This implies:

Lemma A.22 *Let $(X, \varphi), (\widetilde{X}, \widetilde{\varphi})$ be a principally polarized abelian k-varieties, let $f : \widetilde{X} \longrightarrow X$ and $f' := \widetilde{\varphi}^{-1}\widehat{f}\varphi$ the "Rosati involution" of f with respect to φ and $\widetilde{\varphi}$, $Y :=$ im(f). Then the orthogonal complement of Y is the reduced connected component of the zero of* $\ker(f')$.

Proof Let $f = \iota_Y g$, where $g : X \longrightarrow Y$ is surjective. The orthogonal complement is given as the reduced connected component of the kernel of $\widehat{\iota_Y}\varphi$, which by the last lemma is the same as the reduced connected component of the zero of the kernel of $\varphi^{-1}\widehat{g\iota_Y}\varphi = \varphi^{-1}\widehat{\iota_Y g}\varphi = f'$. □

Lemma A.23 *Let (X, φ) be a principally polarized abelian k-variety, f an endomorphism, f' the Rosati involution with respect to φ. Assume that* $\ker(f')$ *is reduced and irreducible. Let $Y =$* im(f) *and $Z =$* $\ker(f')$. *Then $Y \cap Z := Y \times_k Z =$* $\ker(\widehat{\iota_Y}\varphi\iota_Y)$.

Proof As above, let $f = \iota_Y g$. Since by assumption $\ker(f') = \ker(\varphi^{-1}\widehat{g\iota_Y}\varphi)$ is reduced and irreducible, so is $\ker(\widehat{\iota_Y}\varphi)$. Thus $Z = \ker(\widehat{\iota_Y}\varphi)$ and $Y \cap Z = \iota_Y^{-1}(Z) = \iota_Y^{-1}(\ker(\widehat{\iota_Y}\varphi) = \ker(\widehat{\iota_Y}\varphi\iota_Y)$. □

A.2.5 The decomposition of the endomorphism ring of an abelian variety

Let A be an abelian variety over a perfect field k.

Let $A^{(i)} \hookrightarrow A$, $i = 1, \ldots$ be abelian subvarieties such that the induced morphism $\prod_i A^{(i)} \longrightarrow A$ is an isogeny. Let $e^{(i)}$, $i = 1, \ldots$ be the elements of $\mathrm{End}_k(A)$ which correspond under the isogeny to the projections on the left hand side. Then $1 = \sum_i e^{(i)}$ and the $e^{(i)}$ are idempotent. Now if $a^{(i)} \in \mathbb{N}$ such that $a_i e^{(i)}$ are morphisms, then $A^{(i)} = a^{(i)}e^{(i)}(A)$ and $A^{(i)}$ is the reduced connected component of the zero of the kernel of $a^{(i)}(1 - e^{(i)})$.

Conversely, if a decomposition of the unity $1 = \sum_i e^{(i)}$ where the e_i are idempotent is given, define $A_{(i)} := a^{(i)}e^{(i)}(A)$ for suitable $a^{(i)} \in \mathbb{N}$. Then again $\prod_i A^{(i)} \sim A$ and the $e^{(i)}$ correspond to the projections on the left hand side.

Now fix a polarization φ on A. With the help of the Complete Reducibility Theorem, A can be decomposed into a product of simple abelian varieties.

There exist simple abelian subvarieties $\iota_{i,j} : A_{i,j} \hookrightarrow A$ with $A_{i,j} \sim A_{i',j'}$ iff $i = i'$ such that the $\iota_{i,j}$ induce an isogeny

$$\prod_{i=1}^{s} \prod_{j=1}^{k_i} A_{i,j} \sim A \tag{A.4}$$

and such that $A'_{i,j}$:=(abelian variety generated by $A_{i',j'}$ for $(i,j) \neq (i',j')$) is orthogonal of $A_{i,j}$ with respect to φ. Under this isogeny, φ becomes a product polarization on the left-hand side. In particular, the projections on the left-hand side are invariant under the Rosati involution. As above, let $e_{i,j}$ be the idempotents in $\mathrm{End}_K(A_K)$ which correspond to these projections. Then also the $e_{i,j}$ are invariant under the Rosati involution, $e'_{i,j} = e_{i,j}$, and thus by Lemma A.22, $A'_{i,j}$ is the orthogonal complement of $A_{i,j}$.

Let A_i be the abelian subvariety generated by the $A_{i,1}, \ldots, A_{i,k_i}$. Then the A_is are independent of the particular decomposition chosen. We call them the *isotypic components* of the abelian variety A (over k).

$$A \sim \prod_{i=1}^{s} A_i \tag{A.5}$$

Let A'_i := abelian subvariety in A generated by the A_j, $j \neq i$.

Decomposition (A.4) induces an isomorphism

$$\mathrm{End}^0_k(A) \simeq \prod_{i=1}^{s} \mathrm{End}^0_k(A_i). \tag{A.6}$$

The $\mathrm{End}^0_k(A_i)$ are simple rings (simple meaning that they do not have a proper two sided ideal) with $\mathrm{End}^0(A_i) \approx \mathrm{M}_{k_i}(D_i)$, where $D_i \approx \mathrm{End}^0_k(A_{A_{i,j}})$ is a division ring.

It is a fact from the theory of semisimple rings that (A.6) is the unique way to decompose $\mathrm{End}^0_K(A_K)$ into a product of simple rings (i.e. the if a decomposition $\mathrm{End}^0_K(A_K) \simeq \prod_i R_i$ is given, the R_i are uniquely determined inside $\mathrm{End}^0_k(A)$ up to a permutation); see [FD, Theorem 1,13].

Now let e_i be the image of the unity of $\mathrm{End}^0_k(A_i)$ in $\mathrm{End}^0_k(A)$ under the above isomorphism. Then the e_i are central and idempotent and $1 = \sum_{1=1}^{s} e_i$, and again $e'_i = e_i$ and A_i is orthogonal to A'_i.

Now all polarizations of $\prod_{i=1}^{s} A_i$ are multiples of product polarizations and, in particular, $e_i = e'_i$ and the A_i are orthogonal with respect to any polarization.

Proof $\mathrm{End}^0_k(\prod_{i=1}^{s} A_i) \simeq \prod_{i=1}^{s} \mathrm{End}^0_k(A_i)$. This implies $\mathrm{NS}^0(\prod_{i=1}^{s} A_{i\overline{k}})^{\mathrm{Gal}(\overline{k}|k)} \simeq \prod_{i=1}^{s} \mathrm{NS}^0_k(A_{i\overline{k}})^{\mathrm{Gal}(\overline{k}|k)}$. (Use the characterization [Mu, p.208, application III] with the product polarization φ on the left-hand side and the φ_i on the right-hand side; see also Proposition A.9.)

Now, classes of ample sheaves on the left hand side correspond to tuples of classes of ample sheaves on the right hand side. These classes on the left hand side define multiples of polarizations, and on the right hand side, they define multiples of product polarizations. □

A.2.6 Ample sheaves

Let K be a field and let A be an abelian K-variety of dimension n with an ample sheaf $\mathcal{L}$.

Recall the Vanishing Theorem:

Proposition A.24 *[Mu, par. 16, p.150] Let $\mathcal{M}$ be a non-degenerate invertible sheaf on A, i.e. $K(\mathcal{M})$ is finite.*

Then there exists a unique integer $i(\mathcal{M}), 0 \leq i(\mathcal{M}) \leq n$, called the index *of $\mathcal{M}$, such that $H^p(X, \mathcal{M}) = 0$ for $p \neq i(\mathcal{M})$ and $H^{i(\mathcal{M})}(X, \mathcal{M}) \neq 0$.*

The index can be calculated as follows:

Proposition A.25 *[Mu, par. 16, p.155] With $\mathcal{L}$ and $\mathcal{M}$ as above, the function $z \mapsto \chi(\mathcal{L}^z \otimes \mathcal{M})$ is a polynomial function of degree n whose roots are all real and non-zero. The index $i(\mathcal{M})$ is the number of positive roots.*

This implies:

Lemma A.26 *Let $\mathcal{M}$ be a non-degenerate invertible sheaf on A. The following are equivalent:*

1. *$\mathcal{M}$ is ample, i.e. a power of $\mathcal{M}$ is very ample.*
2. *$\mathcal{M}$ is defined by an effective divisor.*
3. *The index $i(\mathcal{M})$ is 0, i.e. $H^0(X, \mathcal{M}) \neq 0$ and $H^p(X, \mathcal{M}) = 0$ for $p \neq 0$.*
4. *The polynomial $\chi(\mathcal{L}^z \otimes \mathcal{M})$ has only negative roots.*

Proof 2. $\longleftrightarrow$ 3. $\longleftrightarrow$ 4. follows from the Vanishing Theorem.

1. $\longrightarrow$ 3.: By the Vanishing Theorem applied to the ample sheaf $\mathcal{M}$ (!) and the non-degenerate sheaf $\mathcal{M}$, the index $i(\mathcal{M})$ is equal to the number of positive roots of the polynomial defined by $z \mapsto \chi(\mathcal{M}^z \otimes \mathcal{M}) = \chi(\mathcal{M}^{z+1}) \overset{\text{Riemann-Roch}}{=} (z+1)^n \chi(\mathcal{M})$. The roots of this polynomial are all at $-1 < 0$, so the index is zero.

2. $\longrightarrow$ 1.: see [Mu, p. 60, application 1]. □

A.2.7 Principally polarized abelian surfaces

The following proposition is due to A.Weil. Because Weil uses in his proof his own language which is out of fashion today, we include a proof.

Proposition A.27 (A. Weil) *[We-T, Satz 2] Let A be an abelian surface over an algebraically closed field k. Let $\mathcal{L}$ be an ample sheaf on A which defines a principal polarization. Then $\mathcal{L}$ is defined by an effective divisor D which is unique up to translation.*

Either D is a non-singular geometrically irreducible proper curve of genus 2, and if $\iota : D \longrightarrow A$ is the inclusion, $\iota^* : A \longrightarrow J(D)$ is an isomorphism.

Or A is isomorphic to the product $E \times_k E'$ of elliptic curves, and via this isomorphism, D has the form $E \times_k a + a' \times_k a'$ where a, a' are two points on E, E' respectively.

Before we come to the proof of this proposition, we show how the arithmetic genus of a curve on an abelian surface A can be calculated from the Euler-characteristic of the sheaf it defines on A.

Let D be a (not necessarily irreducible) curve on A. Then we have the exact sequence

$$0 \longrightarrow \mathcal{L}(-D) \longrightarrow \mathcal{L}(A) \longrightarrow \mathcal{O}_D \longrightarrow 0.$$

Here, we make the usual identification of $\mathcal{O}_D$ with $\iota_*(\mathcal{O}_D)$ where $\iota : D \longrightarrow A$ is the inclusion. [Ha, Remark 2.10.1] This identification is justified by the fact that $H^i(D, \mathcal{O}_D) = H^i(A, \iota_* \mathcal{O}_D)$. [Ha, III,Lemma 2.10]

By the additivity of the Euler-characteristic we get

$$\chi(\mathcal{L}(-D)) + \chi(\mathcal{O}_D) = \chi(\mathcal{O}_A) = 0.$$

Because of the Riemann-Roch Theorem, $\chi(\mathcal{L}(-D)) = \frac{1}{2}(D, D) = \chi(\mathcal{L}(D))$ and thus

$$\chi(\mathcal{O}_D) = -\chi(\mathcal{L}(D)).$$

In particular, if D is connected, $H^1(D, \mathcal{O}_D) = \chi(\mathcal{L}(D)) + 1$.

proof of the proposition Let D be an effective divisor defining $\mathcal{L}$, unique up to translation on A. Let $D = \sum_{i=1}^{l} n_i D_i$, where $n_i > 1$ and D_i, $i = 1, \dots, l$ are irreducible proper curves. Then by the Riemann-Roch Theorem

$$2 = (D, D) = \sum_{i,j} n_i n_j (D_i, D_j).$$

We claim that there are only two cases:

$l = 1, n_1 = 1$, $(D_1, D_1) = 2$, and D_1 is a non-singular geometrically irreducible proper curves of genus 2

$l = 2, n_1 = n_2 = 1$, $(D_1, D_1) = 0, (D_2, D_2) = 0, (D_1, D_2) = 1$, and D_1, D_2 are elliptic curves

Without loss of generality, we can assume that $(D_1, D_1) \neq 0$ or $(D_1, D_2) \neq 0$.

Assume that $(D_1, D_1) \neq 0$. Since again by the Riemann-Roch Theorem, the self-intersection of any divisor on an abelian surface is divisible by 2, $(D_1, D_1) = 2$, thus $n_1 = 1$ and $(D_1, D_i) = 0$ for $i > 1$. Now D_1 is an ample divisor, and by the criterion of Nakai-Moishezon [Ha, V,Theorem 1.10], $k = 1$. By the remarks before the proof of the proposition, the arithmetic genus of D is 2. The geometric genus of the normalization of D is also 2, and so D itself is non-singular. For assume that the genus of the normalization would be 0 or 1. It cannot be zero because there exist no rational curves on abelian varieties, and it cannot be 1 because then than the map from the normalization of D to A would be the inclusion of an elliptic curve combined with a translation in A. In particular, D would be an elliptic curve and its arithmetic genus would be 1, not 2.

Now assume that $(D_1, D_2) \neq 0$. Then $(D_1, D_2) = 1, n_1 = n_2 = 1$ and $D_1 + D_2$ is ample. Now $(D_1 + D_2, D_i) = 0$ for any $i > 2$ and by the criterion of Nakai-Moishezon, $k = 2$. By the remarks before the proof, the arithmetic genera of D_1, D_2 are 1. The geometric genera can again not be 0, so D_1 and D_2 are elliptic curves.

In the case $l = 2$, D_1 and D_2 intersect in one point and A has the universal property of the sum of D_1 and D_2 in the category of abelian varieties.

We come back to the case $k = 1$. We want to proof that $\iota^* : A \longrightarrow J(D)$ is an isomorphism. Let $P \in D(\overline{k})$, $f^P : D \longrightarrow J(D)$ be the canonical immersion defined by $P \mapsto 0$. By a translation of A, we can assume that $\iota(P) = 0$ on A. By the universal property of the Jacobian, there exists a morphism $\alpha^P : J(D) \longrightarrow A$ with $\alpha^P \circ f^P = \iota$.

We already know that α^P is an isogeny and claim that it is in fact an isomorphism. Then $\widehat{\alpha}$ and also ι^* are isomorphisms.

f^P induces a morphism $\phi : D \times_k D \longrightarrow J(D)$, given on .-valued points by $(Q, R) \mapsto P + Q$. This factors through $D \times_k^S D$, the symmetric product. The induced morphism $D \times_k^S D \longrightarrow J(D)$ is birational, thus the degree of ϕ is 2.

The composition $\alpha^P \circ \phi$ is given by $(Q, R) \longrightarrow \iota \circ Q + \iota \circ R$. We claim that the degree of $\alpha^P \circ \phi$ is 2, thus the degree of α^P is 1.

The divisor D is algebraically equivalent to $(-\mathrm{id}_A)^{-1}(D)$ (see [Mu, par. 8, p.75, (iv)]), and this divisor is algebraically equivalent to $(-\mathrm{id}_A)^{-1}(D) + T$ for all $T \in A(\overline{k})$.

Thus the equation $(D, D) = 2$ implies $(D, (-\mathrm{id}_A)^{-1}(D) + T) = 2$ for any $T \in A(\overline{k})$. There exists an open subset $U \subseteq A$ such that for $T \in U(\overline{k})$, D and $(-\mathrm{id}_A)^{-1}(D) + T$ intersect transversely. Thus for $T \in U(\overline{k})$, there exist exactly 2 points $(P, Q) \in (D \times_k D)(\overline{k})$ with $\phi \circ (P, Q) = \iota \circ P + \iota \circ Q = T$.

Since U is dense in A, the degree of the morphism $\phi : D \times_k D \longrightarrow A$ is 2. □

Remark Let the conditions be as in the proposition but let k be an arbitrary field. Then again $\mathfrak{L}$ is defined by an effective divisor D, unique up to translation.

Now, D is a geometrically reduced proper curve. There are two cases: Either D is geometrically irreducible, non-singular and has genus 2 or it is geometrically the pointed union of two elliptic curves. In the first case, A is again isomorphic to $J(D)$ (over k).

A.3 Some results about schemes and varieties

In this section we present some results from various sources as well as some other rather technical results.

A.3.1 Regular function fields and geometrically irreducible varieties

Definition Let $K|k$ be an algebraic extension, let $L|k$ be any extension. Then K and L are *linearly disjoint* over k iff $K \otimes_k L$ is a field.

Assume that this is the case and let K and L be included in some common overfield. Then the compositum KL of K and L in this overfield together with the inclusions $K \longrightarrow KL$ and $L \longrightarrow KL$ is (canonically isomorphic to) the tensor product of K and L over k, $K \otimes_k L \simeq KL$.

Again let K and L be included in some common overfield and assume that $K|k$ is Galois. Then K and L are linearly disjoint iff $K \cap L = k$; see [La, VII, par. 3,4]. [6]

An function field $L|k$ is called *regular* over k, if L and $\overline{k}$ are linearly disjoint over k. An extension $L|k(x)$ is called regular iff $L|k$ is regular or – what is the same – if L and $\overline{k}(x)$ are linearly disjoint over $k(x)$.

Let $K|k$ be an algebraic field extension. A regular extension $L'|K(x)$ is said to be *defined over k*, if there exists a subextension $L|k(x)$ of $L'|k(x)$ which is linearly disjoint from $K(x)|k(x)$ with $LK = L'$. (This implies that $L|k(x)$ is regular.)

A regular extension $L'|K(x)$ is said to be *defined over k with its Galois group*, if there exists such a subextension $L|k(x)$ which is *Galois*.

All the above statements can easily be translated into statements about varieties. For example, Let X' be an irreducible k-variety. Then X is geometrically integral iff the function field $k(X)|k$ is regular.

Lemma A.28 *Let X be a connected k-scheme with a k-rational point. Then X is geometrically connected. If additionally X is smooth (and thus irreducible) it is geometrically irreducible.*

Proof We have to show that $X \otimes_k k^{\text{sep}}$ is irreducible.

Let $K|k$ be some finite Galois extension with Galois group G. Then so is $X \otimes_k K \longrightarrow X$. (Galois is stable under base extension.) So $(X \otimes_k K)/G \simeq X$.

[6] **Caution!** The notation KL does not mean that K and L are necessarily linearly disjoint. It can also just be the compositum in a common overfield. We write $KL \simeq K \otimes_k L$ if K and L are linearly disjoint.

This means in particular that the underlying topological space of X is the quotient of the underlying topological space of $X \otimes_k K$ by G. Thus G operates transitively on the components of $X \otimes_k K$.

Let $P : \mathrm{Spec} k \longrightarrow X$ be a k-rational point. By base change, P defines a K-rational point of $X \otimes_k K$ which we also denote by P. Let X_0' be the component of the image of P in $X \otimes_k K$.

Now assume that $X \otimes_k K$ has more than one component.

Let $\tau \in G^{\mathrm{opp}}$ such that τ moves X_0 to another component. Then the image of τP is *not* in X_0, and so is the image of $\tau \circ P = \tau P \tau^{-1}$, a contradiction, since also $P = \tau(P)$.

Since $K|k$ was arbitrary finite Galois, $X \otimes_k k^{\mathrm{sep}}$ is connected.

If X is smooth, so is $X \otimes_k k^{\mathrm{sep}}$, and thus is is connected. □

A.3.2 Pull-back of effective divisors

Let k be a field and let X be a non-singular connected (irreducible) k-variety. Then the group of Weil-divisors and Cartier-divisors on X are isomorphic. [Ha, Proposition 6.11.] Under this isomorphism, effective Weil-divisors correspond to effective Cartier-divisors, and they correspond to closed subschemes of X of pure codimension 1.

We will now discuss the last isomorphism in greater detail.

Let D be a closed subscheme of pure codimension 1. Then there exists an open covering U_i of X such that on every U_i, D is defined by a single element $f_i \in \Gamma(U_i, \mathcal{O}_{U_i}^*)$. Let 0 denote the k-rational point of $\mathbb{A}_k^1$ corresponding to $k[x] \longrightarrow k$, $x \mapsto 0$. Then f_i defines a morphism $U_i \longrightarrow \mathbb{A}_k^1$ and $D|_{U_i} = f_i^{-1}(0)$. [7] Now the covering $(U_i)_i$ and the $(f_i)_i$ define the corresponding Cartier-divisor which we denote by D^C.

Now let Y be another non-singular connected k-variety and let $a : Y \longrightarrow X$ be a morphism. Then $a^{-1}(D)|_{a^{-1}(U_i)} = a^{-1} f_i^{-1}(0) = (f_i a)^{-1}(0)$. (The last equality is equivalent to $a^{-1}(U_i) \times_{U_i} (U_i \times_{\mathbb{A}_k^1} 0) = a^{-1}(U_i) \times_{\mathbb{A}_k^1} 0$.)

Assume that $a(Y) \not\subseteq D$ as *sets*. (Since we assumed that Y is irreducible this is equivalent to that the inverse image of D in Y is not the whole space.) This condition is especially fulfilled if a is an immersion and the support of D (i.e. the corresponding reduced subscheme) does not contain Y or if a is surjective.

Then $f_i a \neq 0$ and $a^{-1}(D)$ is again a subscheme of pure codimension 1, and the corresponding Cartier-divisor is defined by the open covering $a^{-1}(U_i)$ of Y and the set $(f_i a)_i$. This divisor is usually denoted by $a^*(D^C)$. Thus $a^{-1}(D)^C = a^*(D^C)$.

The groups of Weil-divisor classes, Cartier divisor classes and classes invertible sheaves are also naturally isomorphic.

[7] Recall that for a closed immersion of schemes $\iota : X \hookrightarrow Y$, and some morphism $a : Z \longrightarrow Y$, by $a^{-1}(X)$ we always mean the *scheme-theoretic* preimage, i.e. $\alpha^{-1}(X) := X \times_Y Z$ where the product is taken relative to ι and α.

Furthermore, again under the condition $a(Y) \nsubseteq D$, we have $a^*(\mathcal{L}(D^C)) \simeq \mathcal{L}(a^*(D^C))$. Thus

Lemma A.29 *Let X, Y be nonsingular connected varieties, $a : Y \longrightarrow X$ a morphism. Let D be a subscheme on X, purely of codimension 1, let D^C be the associated Cartier divisor. Assume that the support of D does not contain the* set *$a(Y)$.*

Then $a^{-1}(D)^C = a^*(D^C)$ and $a^*(\mathcal{L}(D^C)) \simeq \mathcal{L}(a^{-1}(D)^C)$.

Remark If X is an abelian variety and $Y \longrightarrow X$ is a closed immersion, then the condition of the proposition can always be fulfilled by translating D.

A.3.3 Galois-operation and descent

Let X and Y be schemes and let $\pi : X \longrightarrow Y$ be a Galois covering with Galois group G. For any quasi-coherent $\mathcal{O}_X$-sheaf $\mathcal{L}$ and $\boldsymbol{\sigma} \in G$, choose a pull-back via $\sigma : Y \longrightarrow X$. As usual, denote this sheaf by $\sigma^*(\mathcal{L})$.

Now let $\mathcal{L}$ be a quasi-coherent $\mathcal{O}_X$-module on X.

For any $\sigma, \tau \in G$ and any morphism $a : \mathcal{L} \longrightarrow \tau^{-1^*}(\mathcal{L})$, denote by $\tau(a)$ the composition $\sigma^{-1^*}(\mathcal{L}) \longrightarrow \sigma^{-1^*}(\tau^{-1^*}(\mathcal{L})) \simeq (\sigma\tau)^{-1^*}(\mathcal{L})$, where the first morphism is defined by base-change.

Then a *1-cocycle datum* of $\mathcal{L}$ is a map $G \in \tau \mapsto a_\tau$, where a_τ is an $\mathcal{O}_X$-morphism $\mathcal{L} \longrightarrow (\sigma^{-1})^*(\mathcal{L})$ such that for all $\sigma, \tau \in G$, $a_{\sigma\tau} = \sigma(a_\tau) \circ a_\sigma : \mathcal{L} \longrightarrow (\sigma\tau)^{-1^*}(\mathcal{L})$.

A quasi-coherent $\mathcal{O}_X$-module $\mathcal{L}$ on X with a 1-cocycle datum is called a quasi-coherent *G-sheaf.*

Proposition A.30 *The functor $\mathcal{F} \mapsto \pi^*(\mathcal{F})$ is an equivalence of categories of quasi-coherent $\mathcal{O}_Y$-modules and that of quasi-coherent G-sheaves on X. Coherent sheaves correspond to coherent sheaves and locally free sheaves correspond to locally free sheaves of the same rank.*

Proof This is a special case of the "faithfully flat descent" of $\mathcal{O}_X$-modules; see [BLR, par. 6.1]. □

Caution! The proposition would be wrong if one would call an $\mathcal{O}_X$-module a G-sheaf if its *class* is invariant under pull-back by elements of G. Note however that the following proposition is a special case of formula (1.16):

Proposition A.31 *Let $K|k$ be a Galois field extension. Let Y be a projective k-variety with a k-rational point. Let $\mathcal{L}$ be an invertible free sheaf on $Y \otimes_k K$, such that for every $\boldsymbol{\sigma} \in$* Gal$(K|k)$, *$\sigma^*(\mathcal{L}) \approx \mathcal{L}$. Then $\mathcal{L}$ is isomorphic to the inverse image of a sheaf on Y.*

Remark A 1-cocycle-datum on a $\mathcal{O}_X$-sheaf can be interpreted as follows:

By definition, $(\sigma^{-1})^*(\mathcal{L}) = (\sigma^{-1})^{-1}(\mathcal{L}) \otimes_{(\sigma^{-1})^{-1}(\mathcal{O}_X)} \mathcal{O}_X$. Now, $(\sigma^{-1})^{-1}(\mathcal{O}_X)$ is canonically isomorphic to $\sigma_*(\mathcal{O}_X)$, and the same is true for $\mathcal{L}$. Thus $(\sigma^{-1})^*(\mathcal{L}) \simeq \sigma_*(\mathcal{L}) \otimes_{\sigma_*(\mathcal{O}_X)} \mathcal{O}_X$, where $\sigma_*(\mathcal{O}_X) \longrightarrow \mathcal{O}_X$ is given by $\sigma^{\#^{-1}}$. This means that $\mathcal{L}$ is canonically isomorphic to $\sigma_*(\mathcal{L})$ regarded as $\mathcal{O}_X$ module via $\sigma^{\#} : \mathcal{O}_X \longrightarrow \sigma_*(\mathcal{O}_X)$. Under this identification, the $\mathcal{O}_X$-morphism $a_\sigma : \mathcal{L} \longrightarrow \sigma^{-1^*}(\mathcal{L})$ corresponds to a morphism $a_\sigma : \mathcal{L} \longrightarrow \sigma_*(\mathcal{L})$ with $a_\sigma(\lambda x) = \sigma^{\#}(\lambda)a_\sigma(x)$ for $\lambda \in \mathcal{O}_X(U)$, $x \in \mathcal{L}(U)$, U open in X.

Now, $\pi_*(\mathcal{L}) = \pi_*\sigma_*(\mathcal{L})$ and a_σ becomes an automorphism of $\pi_*(\mathcal{L})$, which we denote by $\sigma^{\#}$. This morphism satisfies $\sigma^{\#}(\lambda x) = \sigma^{\#}(\lambda)\sigma^{\#}(x)$, where $\lambda \in \pi_*(\mathcal{O}_Y)(U)$, $x \in \pi_*(\mathcal{L})(U)$, U open in Y. We thus have a G-operation on $\pi_*(\mathcal{L})$ which "covers" the G-operation on $\pi_*(\mathcal{O}_X)$. Taking invariants, we get a presheaf $\pi_*(\mathcal{L})^G$ which is in fact a sheaf because $\sigma^{\#}(x) = x$ is a local property.

If $\mathcal{M}$ is a $\mathcal{O}_X$-sheaf on X, $(\pi_*(\pi^*(\mathcal{M})))^G \simeq \mathcal{M}$. If $\mathcal{L}$ is a $\mathcal{O}_Y$-sheaf on Y with a 1-cocycle datum, and $\mathcal{M}$ is a $\mathcal{O}_X$-sheaf on X such that $\pi^*(\mathcal{M}) \approx \mathcal{L}$ such that under the isomorphic the cocycle-data of the two sheaves agree, then $\mathcal{M} \simeq (\pi_*(\pi^*(\mathcal{M})))^G \approx \pi_*(\mathcal{L})^G$. Thus $\mathcal{L} = \pi^*(\mathcal{M}) \approx \pi^*(\pi_*(\mathcal{L})^G)$.

A.3.4 Schemes over finite fields

Definitions Let q be the power of a prime number p, k the finite field with q elements, $K|k$ an algebraic extension of fields. We identify the Galois group $\mathrm{Gal}(K|k)$ with its dual and denote its elements with usual letters. The Frobenius automorphism of $K|k$ is denoted by σ_k^K.

There exist two (or even three) different concepts of Frobenius morphisms for K-schemes. We want to distinguish between them carefully.

Let X' be a K-scheme.

The k-automorphism σ_k^K of K induces an automorphism of $\mathrm{Spec}(K)$ which we again denote by σ_k^K. We call the automorphism $\sigma_k^K : \sigma_k^{K^{-1}}(X') \longrightarrow X'$ the *arithmetic Frobenius isomorphism.*

Let F_k^K be the automorphism of X' which is defined as follows: F_k^K is the identity on the underlying topological space and it is given by $f \mapsto f^q$ on $\mathcal{O}_{X'}$.

By definition, we have a commutative diagram

$$\begin{tikzcd}
X' \arrow[r, "F_k^K"] \arrow[d] & X' \arrow[d] \\
\mathrm{Spec}(K) \arrow[r, "\sigma_k^K"] & \mathrm{Spec}(K).
\end{tikzcd}$$

In particular, if the extension $K|k$ is non-trivial, F_k^K is not a $\mathrm{Spec}(K)$-morphism.

Now define the *geometric Frobenius morphism* by $\pi_k := \sigma_k^{K^{-1}} \circ F_k^K : X' \longrightarrow \sigma_k^{K^{-1}}(X')$ – this is a K-morphism.

Let X' be affine and of finite type, $K[x_1, \dots, x_m]/(f_1, \dots, f_l)$ a presentation of the coordinate ring of X'. Then the coordinate ring of $\sigma^{-1}(X')$ is given by $K[x_1, \dots, x_m]/({\sigma_k^K}^{\#}(f_1), \dots, {\sigma_k^K}^{\#}(f_l))$, and π_k is given by the identity on K and $x_i \mapsto x_i^q$. For a general K-scheme X' of finite type, π_k is defined like this locally.

The definition of π_k behaves well with respect to base-change: If $L|K$ is some algebraic field extension, then $({\sigma_k^K}^{-1} \circ F_k^K) \otimes_K \mathrm{id}_L = {\sigma_k^L}^{-1} \circ F_k^L : X' \longrightarrow {\sigma_k^K}^{-1}(X') \otimes_K L \simeq {\sigma_k^L}^{-1}(X' \otimes_K L)$.

Note In [Ha], the morphism F_k^K is called "Frobenius morphism" and the geometric Frobenius morphism π_k is called "K-linear Frobenius morphism"; see [Ha, IV, 2, p. 301].

In [Mi-A], the "Frobenius morphism" is only defined for the case that $k = K$, and under this assumption, σ_k^K is trivial and F_k^K and π_k agree; see [Mi-A, par. 20].

In [Mu], the "Frobenius morphism" is first defined for $k = K$ and then generalized to $\overline{k}$-schemes which are defined over k. Again it equals the geometric Frobenius morphism π_k.

From now on, we restrict ourselves to the case $K = \overline{k}$. We write σ_k for the arithmetic Frobenius automorphism $\sigma_k^{\overline{k}}$ and denote $F_k^{\overline{k}}$ by F_k.

Let P be a $\overline{k}$-valued point of X'. Then $F_k \circ P \circ \sigma_k^{-1} = P$. In fact, the left-hand side is also a $\overline{k}$-valued point of X' and its image coincides with the one of P.

The equation $F_k \circ P = P \circ \sigma_k$ implies $\pi_k \circ P = \sigma_k^{-1} \circ F_k \circ P = \sigma_k^{-1} \circ P \circ \sigma_k = \sigma_k^{-1}(P) = P^{\sigma_k}$.

Lemma A.32 *Let X' be a $\overline{k}$-scheme. Then for all $\overline{k}$-valued points P of X',*

$$\pi_k \circ P = \sigma_k^{-1}(P) = P^{\sigma_k} \in \sigma_k^{-1}(X').$$

If X' is an irreducible variety, the field extension $\overline{k}(\sigma_k(X'))|\overline{k}(X')$ is purely inseparable. If X' is an abelian variety, then π_k is an isogeny of p-power degree whose kernel is connected (local in the language of [Mu]).

□

Lemma A.33 *Let V' and W' be $\overline{k}$-varieties, $\lambda : V' \longrightarrow W'$ a $\overline{k}$-morphism. Then $\lambda^{\sigma_k} \pi_k = \pi_k \lambda : V' \longrightarrow \sigma_k^{-1}(W')$.*

Proof We only have to show this for $\overline{k}$-rational points. Let $P \in V'(\overline{k})$. Then

$$\lambda^{\sigma_k} \circ \pi \circ P = \lambda^{\sigma_k} \circ P^{\sigma_k} = (\lambda \circ P)^{\sigma_k} = \pi_k \circ \lambda \circ P.$$

□

This implies:

Lemma A.34 *Let V, W be k-varieties, $\lambda : V_{\overline{k}} \longrightarrow W_{\overline{k}}$ a morphism. Then λ is defined over k iff $\pi_k \, \lambda = \lambda \, \pi_k$.*

□

Using Lemma A.8, we also get

Lemma A.35 *Let A' be an abelian $\overline{k}$-variety, $\lambda \in \mathrm{End}^0_{\overline{k}}(A')$. Then $\lambda^{\sigma_k} = \pi \, \lambda \, \pi^{-1} \in \mathrm{End}^0_{\overline{k}}(\sigma_k^{-1}(A'))$.*

□

Remark A consequence of Lemma A.32 is that for an abelian k-variety A, the operation of the two Frobenius morphisms π_k and σ_k on the Tate-module (for some prime l) are equal (where σ_k operates by $(\ldots)^{\sigma_k}$). Because of this, we speak of *the* operation of the Frobenius on the Tate-module and the characteristic polynomial of this operation.

Bibliography

[BLR] Bosch, S. Lütkebohmert W., Raynaud, M.: Néron Models, Springer-Verlag, Berlin (1980)

[CR] Curtis, W., Reiner, I.: Methods of Representation Theory, Wiley, New York (1988)

[EGA II] Grothendieck, A. mit Dieudonné, J.: Elementes de Geometrie Algebrique II, Publications Mathematiqués **8**, IHES (1961)

[Ei] Eisenbud, D.: Commutative Algebra, Springer-Verlag, New York (1996)

[En] Enge, A.: Computing discrete logarithms in high-genus hyperelliptic Jacobians in provably subexponential time, Combinatorics and Optimization Research Report CORR 99-04, University of Waterloo (1999), to be published in Mathematics of Computation

[EG] Enge, A, Gaudry, P.: A general framework for subexponential discrete logarithm algorithms, Laboratoire d'Informatique, Ecole Polytechnique (2000)

[FD] Farb, B., Dennis, K.: Noncommutative Algebra, Springer-Verlag, New York (1993)

[Fr] Frey, G., How to disguise an elliptic curve (Weil descent), Talk at the 2nd Elliptic Curve Cryptography Workshop (ECC '98) in Waterloo, www.cacr.math.uwaterloo.ca/conferences/1998/ecc98/slides.html

[Gal] Galbraith, S.: Weil Descent of Jacobians, preprint (2000)

[Gau] Gaudry, P.: An algorithm for solving the discrete log problem on hyperelliptic curves, Advances in Cryptology, Eurocrypt'2000, Springer-Verlag, LNCS 1807, 19-34 (2000)

[GHS] Gaudry, P., Hess, F., Smart, N.P.: Constructive and destructive facets of Weil descent on elliptic curves, preprint (2000)

[GS] Garcia, A., Stichtenoth, H.: Elemetary Abelian p-Extensions of Algebraic Function Fields, Manuscripta math. **72**, 67-79, Springer-Verlag (1991)

[Ha] Hartshorne, R.: Algebraic Geometry, Springer-Verlag, New York (1977)

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

[Kan] Kani, E.: Relations Between the Genera and between the Hasse-Witt Invariants of Galois Coverings of Curves, Canad.Math.Bull. **28**, 321-327 (1985)

[Kar] Karpilovsky, G.: Group Representations, North-Holland, Amsterdam (1992)

[La] Lang S.: Algebra, 3. Edition, Addison-Wesley, Reading (1993)

[Lo] Lorenz, F.: Algebra I, Spektrum Akademischer Verlag Berlin (1996)

[Mi-AA] Milne, J.S.: On the Arithmetic of Abelian Varieties, Inventiones math. **17**, 177-190 (1972)

[Mi-A] Milne, J.S.: Abelian Varieties, Cornell, G., Silverman, J. (ed.) et al.: Arithmetic Geometry, Springer-Verlag, New York (1986)

[Mi-É] Milne, J.S.: Étale Cohomology, Princeton University Press, Princeton (1980)

[Mi-J] Milne, J.S.: Jacobian Varieties, Cornell, G., Silverman, J. (ed.) et al.: Arithmetic Geometry, Springer-Verlag, New York (1986)

[Mu] Mumford, D.: Abelian Varieties, Tata Institute for Fundamental Research, Bombay (1970)

[MQ] Menezes, A., Qu, M.: Analysis of the Weil Descent Attack of Gaudry, Hess and Smart, preprint (2000)

[Na] Naumann, N.: Weil-Restriktion, "Diplomarbeit" at the Universität-GHS Essen, Essen (1999)

[Ne] Neukirch, J.: Algebraische Zahlentheorie, Springer-Verlag, Berlin (1991)

[Po] Popp, H.: Fundamentalgruppen algebraischer Mannigfaltigkeiten, Springer-Verlag, Berlin (1970)

[Se] Serre, J.-P.: Local Fields, Springer-Verlag, New York (1976)

[SGA I] Grothendieck, A.: Séminaire de Geometrie Algebrique 1960-61: Revêtements Etales et Groupe Fondamentale (SGA I), Institut des Hautes Etudes Scientifiques, Paris (1961)

[Si] Silverman, J.: The Arithmetic of Elliptic Curves, Springer-Verlag, New-York (1986)

[We-F] Weil, A.: The field of definition of a variety, Amer. J. of Maths. **78**, 509-524 (1958)

[We-T] Weil, A.: Zum Beweis des Torellischen Satzes, Gött. Nachr. **2**, 33-53 (1957)