

# The Weil conjecture for curves via Jacobian varieties

Kai Fabio Neugebauer

February 8, 2023

Aufgabensteller: Prof. Dr. Christian Liedtke  
Betreuer: Marius Kjærsgaard  
Abgabetermin: 09.02.2023

## Abstract

The most straightforward way to prove the Weil conjectures for a curve  $C$  over a finite field  $k$  is via intersection theory on the surface  $C \times C$  as in [8, V Exerc. 1.10]. We present a different approach, which is historically in the spirit of Weil's original proof. The idea is to associate to  $C$  an abelian variety  $J$ , called the Jacobian of  $C$ . To obtain the Weil conjectures we relate the fixed points of the Frobenius endomorphism of  $C$  to the trace of the induced endomorphism of  $J$ .

In the following we will develop the theory of Abelian and Jacobian varieties enabling us in the end to prove the Weil conjectures for curves.

## Contents

<b>1</b>	<b>Abelian varieties</b>	<b>1</b>
1.1	A summary on the picard functor . . . . .	5
1.1.1	The case when $X(k) \neq \emptyset$ . . . . .	7
1.1.2	The dual abelian variety . . . . .	7
1.2	Endomorphisms of abelian varieties . . . . .	9
<b>2</b>	<b>The Jacobian variety</b>	<b>11</b>
2.1	The canonical map from $C$ to its Jacobian . . . . .	12
2.2	Symmetric powers of a curve . . . . .	13
2.3	The Jacobian as Albanese variety . . . . .	17
2.4	Autoduality . . . . .	18
2.5	The Rosati involution . . . . .	20
2.6	The Lefschetz trace formula and positivity of the Rosati involution . . . . .	21
2.7	The map induced on the Jacobian by an endomorphism of $C$ . . . . .	22
<b>3</b>	<b>The Weil conjectures for curves</b>	<b>24</b>

## 1 Abelian varieties

For this section  $k$  will be a field,  $\bar{k}$  an algebraic closure of  $k$  and  $k_s$  the separable algebraic closure of  $k$  in  $\bar{k}$ .

A variety  $X$  will be a scheme, which is geometrically integral, separated and of finite type over  $k$ . Note that products of varieties will be varieties again. If  $\dim X = 1$  we call  $X$  a curve.

Since we assume the variety  $X$  to be geometrically integral its smooth locus is nonempty and therefore the set of closed points in  $X$  with residue field a separable algebraic field extension of  $k$  is dense in  $X$  (see details at [1, Tag 04QM]).

We will use the notations  $\mathcal{O}_X(D) = \mathcal{O}(D)$  for the sheaf associated to an effective Cartier divisor  $D$  on  $X$ , i.e.  $\mathcal{O}(D) = I_D^{-1}$ .  $\mathcal{L}_X(D) = \mathcal{L}(D)$  will denote the invertible sheaf associated to a Weil-Divisor  $D$  on  $X$ .

The following lemma is due to Mumford.

**Lemma 1.1** (Rigidity lemma). Let  $X, Y$  and  $Z$  be varieties. Suppose that  $X$  is proper. If  $f : X \times Y \rightarrow Z$  is a morphism with the property that, for some  $y \in Y(k)$ , the fibre  $X \times \{y\}$  is mapped to a point  $z \in Z(k)$  then  $f$  factors through the projection  $\text{pr}_Y : X \times Y \rightarrow Y$ .

*Proof.* Suppose the theorem is true for the separable algebraic closure  $k_s$  of  $k$ . Then there exists  $g : Y_{k_s} \rightarrow Z_{k_s}$  such that  $f_{k_s} = g \circ \text{pr}_{Y_{k_s}}$ . Let  $\sigma \in \text{Aut}_k(k_s)$ . Then

$$(1 \times \sigma^{-1}) \circ g \circ (1 \times \sigma) \circ \text{pr}_{Y_{k_s}} = (1 \times \sigma) \circ f_{k_s} \times (1 \times \sigma^{-1}) = f_{k_s} = g \circ \text{pr}_{Y_{k_s}}.$$

$\text{pr}_{Y_{k_s}}$  is an epimorphism because it can be obtained by base change from a faithfully flat morphism. Therefore  $g$  is Galois invariant and by Galois descent [2, Prop. 16.9] there exists a unique morphism  $G : Y \rightarrow Z$  such that  $G_{k_s} = g$ . Therefore  $f_{k_s} = (g \circ \text{pr}_Y)_{k_s}$  and by faithfully flat descent  $f = g \circ \text{pr}_Y$ .

By the above paragraph we can assume  $k = k_s$ . Choose a point  $x_0 \in X(k)$ , and we define  $g : Y \rightarrow Z$  by  $f \circ (x_0, \text{id}_Y)$ . The goal is to show  $f = g \circ \text{pr}_Y$ .

Let  $U$  be an affine open neighborhood of  $z$ . Since  $X$  is proper over  $k$ , the projection  $\text{pr}_Y : X \times Y \rightarrow Y$  is a closed map, so that  $V := \text{pr}_Y(f^{-1}(Z \setminus U))$  is closed in  $Y$  (set theoretic preimage). Let  $P \notin V$  be a  $k$  valued point of  $Y$ . Then  $f(X \times \{P\}) \subseteq U$  by construction of  $V$ .

Every morphism from an irreducible proper variety  $X$  to an affine variety is constant: The scheme-theoretic-image of the morphism is a closed subscheme of an affine variety and therefore an affine variety, say  $W$ . Now  $X$  is proper,  $X \rightarrow W$  is surjective and  $W$  is separated of finite type over  $k$ , hence  $W$  is also a proper variety. Using Grothendieck's finiteness result on proper maps the global sections of  $W$  form a finite dimensional  $k$ -vector space. Hence  $W$  is zero-dimensional and by irreducibility  $W$  must be a point.

Applying the previous paragraph to  $f|_{X \times \{P\}}$  (note:  $X \cong X \times \{P\}$ ) we conclude that  $f(X \times \{P\}) = g(P)$ .

We have shown that the set of points where  $f = g \circ \text{pr}_Y$  contains  $\bigcup_{P \in (X \setminus V)(k)} X \times \{P\}$ . Because  $k = k_s$  the latter set is dense in  $X \times Y$  and we are done by [3, Sect. 10.2.A].  $\square$

Recall that a group variety  $(X, m_X, 0 = e_X, (-1)_X)$  is called abelian if it is proper. We denote its group operation additive.

**Corollary 1.2.** Let  $X$  and  $Y$  be abelian varieties and let  $f : X \rightarrow Y$  be a morphism. Then  $f$  is the composition  $f = t_{f(0)} \circ h$  of a homomorphism  $h : X \rightarrow Y$  and a translation  $t_{f(0)}$  by  $f(0)$  on  $Y$ .

*Proof.* Let  $y = -f(e_X)$  and let  $h = t_y \circ f$ . Define  $g : X \times X \rightarrow Y$  to be the map that one points is given by  $g(x, x') = h(x + x') - h(x) - h(x')$ , i.e.  $g = m_Y \circ (h \circ m_X, m_Y \circ (((-1)_Y \circ h) \times ((-1)_Y \circ h)))$ . Then

$$g(\{e_X\} \times X) = g(X \times \{e_X\}) = -h(e_X) = \{e_Y\}$$

and by the Rigidity lemma this implies that  $g$  factors both through the first and the second projection  $X \times X \rightarrow X$ . Hence  $g$  equals the constant map with value  $e_Y$  and  $h$  must be a homomorphism.  $\square$

**Remark 1.3.** The above Lemma 1.2 applied to  $(-1)_X$  shows that the group law on an abelian variety  $X$  is indeed commutative.

An application of Lemma 1.2 to the identity morphism  $X \rightarrow X$  shows that there is at most one structure of an abelian variety on  $X$  such that  $e \in X(k)$  is the identity element.

We define the kernel of a homomorphism  $f : X \rightarrow Y$  of abelian varieties to be the fiber of  $f$  over  $e_Y \in Y$ .

**Theorem 1.4** (Isogenies). For a homomorphism  $f : X \rightarrow Y$  of abelian varieties the following are equivalent

- a)  $f$  is surjective and has finite kernel.
- b)  $\dim X = \dim Y$  and  $f$  is surjective.
- c)  $\dim X = \dim Y$  and  $f$  has finite kernel.
- d)  $f$  is finite and surjective.

If one of the above conditions is satisfied, we call  $f$  an isogeny.

Moreover, any isogeny  $f$  is flat and the following formula holds for all  $q \in Y$

$$\deg f = \dim_{k(q)} H^0(f^{-1}(q), \mathcal{O}_{f^{-1}(q)}). \quad (1)$$

*Proof.* All nonempty fibers of  $f$  have the same dimension: Choose a point  $p \in f^{-1}(q)(\bar{k})$ . Then  $(\ker f)_{\bar{k}} \xrightarrow{t_p \times_{\bar{k}} t_q} f^{-1}(q)_{\bar{k}}$  defines an isomorphism, where  $t_p$  is the translation of  $X_{\bar{k}}$  by  $p$  and  $t_q$  is defined by mapping  $\{e_y\}_{\bar{k}} \rightarrow \{q\}_{\bar{k}}$ .

Assume that  $f$  is surjective. By [3, Thm. 11.4.1] there exists a nonempty open subset  $U \subseteq Y$  such that for all  $q \in U$  the fiber over  $q$  has pure dimension  $\dim X - \dim Y$ . By the above,  $\dim \ker f = \dim X - \dim Y$ . This proves a)  $\implies$  b)  $\implies$  c).

Note this dimension formula always holds if we replace  $Y$  by the scheme-theoretic image of  $f$ . Hence, if  $f$  has finite kernel,  $\dim X = \dim Y$  implies that the scheme-theoretic image of  $f$  equals  $Y$ . Since  $f$  is closed, this proves c)  $\implies$  a).

Because quasi-finite, proper morphisms are finite, a) implies d). The converse follows because quasi-finite morphisms are finite.

Both  $X$  and  $Y$  have a nonempty smooth locus. By translations we see that  $X$  and  $Y$  are smooth over  $k$ . By c) and [3, thm. 26.2.11] any isogeny is flat.

Now let  $f$  be an isogeny. Because finitely generated, flat modules over Noetherian rings are locally free of finite rank,  $f_* \mathcal{O}_X$  is a locally free quasi-coherent  $\mathcal{O}_Y$  module of finite rank. Since  $Y$  is connected this rank is constant, say  $d \in \mathbb{N}$ .

For any  $q \in Y$  there is an affine open neighborhood  $U = \operatorname{Spec} R$  such that  $(f_* \mathcal{O}_X)|_U \cong \mathcal{O}_Y^d|_U$ .  $f$  is finite and therefore affine, so  $f^{-1}U = \operatorname{Spec}(R')$  for some ring  $R'$ . Then  $f_U^\# : R \rightarrow R'$  makes  $R'$  a free  $R$  module of rank  $d$  and  $f^{-1}(q) \cong \operatorname{Spec}(R' \otimes_R k(q))$  proves that

$$\dim_{k(q)} H^0(f^{-1}(q), \mathcal{O}_{f^{-1}(q)}) = d. \quad (2)$$

For  $q = \eta_Y$  the generic points, we have  $f^{-1}(q) \cong \operatorname{Spec}(R' \otimes_R \operatorname{Quot}(R))$ , and  $R' \otimes_R \operatorname{Quot}(R)$  is a finite  $\operatorname{Quot}(R)$  algebra and moreover an integral domain since  $X$  is assumed to be geometrically integral. Hence  $R' \otimes_R \operatorname{Quot}(R)$  is a field that contains  $R'$  and is contained in  $\operatorname{Quot}(R')$ . Now, by the universal property of the residue field of  $R$  we have  $R' \otimes_R \operatorname{Quot}(R) = \operatorname{Quot}(R')$ . Applying (2) to  $\eta_Y$  therefore completes the prove of (1).  $\square$

**Theorem 1.5** (Theorem of the cube and the square). Let  $X, Y$  be abelian varieties.

1. For  $f, g, h : X \rightarrow Y$  morphisms

$$(f + g + h)^* \mathcal{L} \cong (f + g)^* \mathcal{L} \otimes (g + h)^* \mathcal{L} \otimes (f + h)^* \mathcal{L} \otimes f^* \mathcal{L}^{-1} \otimes g^* \mathcal{L}^{-1} \otimes h^* \mathcal{L}^{-1} \quad (3)$$

2. (*theorem of the square*)

For an invertible sheaf  $\mathcal{L}$  on  $X$ , a  $k$  scheme  $T$  and  $\operatorname{pr}_X, \operatorname{pr}_T$  the projections of  $X_T$ , the map

$$\varphi_{\mathcal{L}} : X(T) \rightarrow \operatorname{Pic}(X_T) : x \mapsto (m(1_X \times x))^* \mathcal{L} \otimes \operatorname{pr}_X^* \mathcal{L}^{-1} \otimes \operatorname{pr}_T^* x^* \mathcal{L}^{-1} \quad (4)$$

is a homomorphism. Note that  $\varphi_{\mathcal{L}}(x) = t_x^* \mathcal{L} \otimes \mathcal{L}^{-1}$  for all  $x \in X(k)$  ( $t_x$  the translation by  $x$ ).

*Proof.* Both parts of the theorem can be seen as corollaries of the *theorem of the cube*, which is a theorem on proper varieties. References are [4, Chp. II §1] or [5, Chp. II.6].  $\square$

**Remark 1.6.** The theorem of the square can be used to prove that all abelian varieties are projective. References are for example [6, thm. 7.1] or [7, sect. 9.6].

For an abelian variety  $X$  and  $n \in \mathbb{Z}$  we define  $n_X : X \rightarrow X$  to be the homomorphism that one points is given by  $x \mapsto nx$  and define  $X[n] := \ker n_X \subseteq X$ . Say we have  $\dim X = g$ .

**Proposition 1.7** (Torsion Points of Abelian Varieties). For  $n \neq 0$  the morphism  $n_X$  is an isogeny of degree  $\deg n_X = n^{2g}$ . If  $\text{char}(k) \nmid n$  then  $n_X$  is étale and  $X[n](k_s) = X[n](\bar{k}) \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$ .

To prove the proposition we need the following lemma.

**Lemma 1.8.** For any line bundle  $\mathcal{L}$  on an abelian variety  $X$  and  $n \in \mathbb{Z}$

$$n_X^* \mathcal{L} \cong \mathcal{L}^{n(n+1)/2} \otimes (-1)^* \mathcal{L}^{n(n-1)/2}.$$

In particular, if  $\mathcal{L}$  is symmetric, i.e.  $\mathcal{L} \cong (-1)^* \mathcal{L}$ , then  $n_X^* \mathcal{L} \cong \mathcal{L}^{n^2}$ .

*Proof.* Apply equation 3 from theorem 1.5 for  $f = n, g = 1$  and  $h = -1$  to obtain

$$n^* \mathcal{L} \cong (n+1)^* \mathcal{L} \otimes (n-1)^* \mathcal{L} \otimes n^* \mathcal{L}^{-1} \otimes (-1)^* \mathcal{L}^{-1} \otimes \mathcal{L}^{-1}$$

and therefore

$$(n+1)^* \mathcal{L} \otimes (n-1)^* \mathcal{L} \cong n^* \mathcal{L}^2 \otimes (-1)^* \mathcal{L} \otimes \mathcal{L}.$$

The assertion now follows from induction, by first checking the cases  $n = -1, 0, 1$  by hand.  $\square$

*Proof of proposition 1.7.* By remark 1.6 there exists a ample line bundle  $\mathcal{L}$  on  $X$ . We can assume  $\mathcal{L}$  to be symmetric, i.e.  $(-1)^* \mathcal{L} \cong \mathcal{L}$ , because when  $\mathcal{L}$  is ample then also  $(-1)^* \mathcal{L} \otimes \mathcal{L}$  will be ample by [8, II Ex. 7.5 (c)]. By lemma 1.8  $n_X^* \mathcal{L} \cong \mathcal{L}^{n^2}$ , so  $n_X^* \mathcal{L}$  is an ample line bundle provided that  $n^2 > 0$ . Its pullback  $\iota^* n_X^* \mathcal{L}$  along the closed immersion  $\iota : X[n] \rightarrow X$  will also be an ample line bundle. But  $n_X \circ \iota$  factors through the zero map and therefore  $\iota^* n_X^* \mathcal{L}$  is trivial.

We proceed to prove that a proper variety admitting a trivial ample line bundle is finite:

By [1, Tag 01QE]  $X[n]$  is quasi-affine. Hence the canonical map  $X[n] \rightarrow \text{Spec}(\Gamma(X[n], \mathcal{O}_{X[n]}))$  is an open immersion. But  $X[n]$  is proper over  $k$ , so this open immersion is moreover proper and therefore a closed immersion. This proves that  $X[n]$  is a proper and affine variety, and therefore finite as asserted. By theorem 1.4 c)  $n_X$  is an isogeny.

Let  $D$  be an divisor such that  $\mathcal{L} \cong \mathcal{L}(D)$ , then  $n_X^* D$  is linearly equivalent to  $n^2 D$ . We now invoke intersection theory on the smooth projective variety  $X$  to conclude

$$n^{2d}(D)^g = (n^2 D)^g = (n_X^* D)^g = \deg(n_X) \cdot (D)^g,$$

where we used [6, Lem. 8.3] for the last equality. Since  $D$  is ample, its self-intersection number is positive by the Nakai-Moishezon criterion, and we can conclude  $n^{2d} = \deg(n_X)$ .

Now assume  $\text{char}(k) \nmid n$ . To prove that  $n_X$  is étale, we may assume that  $k = k_s$ . The locus  $U$ , where  $n_X$  is étale, is open in  $X$ , so, if we prove that its complement doesn't contain any  $k$  valued point, we win. A  $k$ -valued point  $P$  is in  $U$  provided that the induced map on the tangent space at  $P$  is an isomorphism. Since  $n_X \circ t_P = t_{nP} \circ n_X$ , by the chain rule  $d_P n_X \circ d_0 t_P = d_0 t_{nP} \circ d_0 n_X$ . Because translations give isomorphisms on tangent spaces, it suffices to prove that  $d_0 n_X$  is bijective to conclude that  $n_x$  induces bijections on all tangent spaces, which will then imply that  $n_X$  is étale.

Recall that we can identify  $T_{(0,0)}(X \times X)$  with  $T_0(X) \oplus T_0(X)$ , when we set for  $f : Y \rightarrow X \times X$  that  $d_y f = d_y(\text{pr}_1 \circ f) \oplus d_y(\text{pr}_2 \circ f)$ . We claim that for  $x, x' \in T_0(X)$  the equality  $d_{(0,0)} m(x, x') = x + x'$  holds. Let  $a : X \cong \{0\} \times X \rightarrow X \times X$  be the inclusion of the slice  $\{0\} \times X$  into  $X \times X$ . Then

$$d_{(0,0)} m \circ (\text{id}_{T_0 X} \oplus 0) = d_{(0,0)} m \circ d_0 a = d_0(m \circ a) = \text{id}_{T_0 X}$$

yields that  $d_{(0,0)} m$  restricted to the first factor is the identity. By symmetry and linearity we obtain our claim. Hence, for  $f, g : X \rightarrow X$  homomorphisms we have

$$d_0(f + g) = d_0(m \circ (f, g)) = d_0(m) \circ (d_0(\text{pr}_1 \circ (f, g)) \oplus d_0(\text{pr}_2 \circ (f, g))) = d_0 f + d_0 g.$$

So, by induction  $d_0 n_X(x) = nx$  for all  $x \in T_0 X$ , which defines an isomorphism since  $n \in k^*$ .

By equation (1) and  $n_X$  being unramified it directly follows that  $G := X[n](k_s) = X[n](k)$  is an abelian group of order  $n^{2g}$ , which is killed by  $n$ . Further, for every divisor  $d$  of  $n$  the subgroup of elements that is killed by  $d$  is  $X[d](k_s)$  and has order  $d^{2g}$ . An application of the structure theorem of finitely generated abelian groups shows  $X[d](k_s) \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$ .  $\square$

Note that, since  $n_X$  is surjective,  $X(\bar{k})$  is a divisible group.

**Proposition 1.9.** If  $f : X \rightarrow Y$  is an isogeny of degree  $d$  then there exists a unique isogeny  $g : Y \rightarrow X$  such that  $g \circ f = d_X$  and  $f \circ g = d_Y$ .

*Proof.* If  $f : X \rightarrow Y$  is an isogeny of degree  $d$ , then  $\ker f$  is a finite group scheme which is contained in the kernel of  $d_X$  by [4][Exerc.4.4]. Since  $X$  is quasi-projective, we can take the quotient  $X/\ker f$  to get a factorization of  $d_X$  as  $X \rightarrow X/\ker f \xrightarrow{g} X$ . By [5, Sect. 12 Cor. 1] we can identify  $X \rightarrow X/\ker f$  with  $X \xrightarrow{f} Y$ , so that we get  $d_X = g \circ f$ . By theorem 1.4 b)  $g$  is an isogeny. Then  $g \circ d_Y = d_X \circ g = g \circ (f \circ g)$ . Hence  $h = d_Y - (f \circ g)$  maps into the finite  $k$ -scheme  $\ker g$ . The scheme-theoretic image of  $h$  is a closed irreducible subscheme of  $\ker g$ , so  $h$  is constant and  $d_Y = f \circ g$  follows.  $\square$

An non-zero abelian variety  $X$  is called *simple* if  $X$  has no other abelian subvarieties other than  $\{e_X\}$  and  $X$ . Note that abelian subvarieties will be closed subschemes.

For any homomorphism of abelian varieties  $f : X \rightarrow Y$  its scheme-theoretic image is an abelian subvariety of  $Y$ . Further by [4, 5.31] the reduced underlying scheme  $(\ker f)_0^{\text{red}}$  of the identity component of  $\ker f$  is an abelian subvariety of  $X$ .

Hence a non-constant homomorphism  $f : X \rightarrow Y$  of simple abelian varieties is surjective and the identity component of  $\ker f$  is  $\{e_X\}$ . All connected components of a  $\bar{k}$ -group scheme are isomorphic as  $\bar{k}$ -schemes by translating back and forth. In particular, all components of  $\ker f$  have the same dimension and we see by theorem 1.4a) that  $f$  is an isogeny. It follows by Proposition 1.9 that for a simple abelian variety  $X$

$$\text{End}_k^0(X) := \text{End}_k(X) \otimes_{\mathbb{Z}} \mathbb{Q}$$

is an associative division algebra over  $\mathbb{Q}$ . Our goal is to compose an arbitrary abelian variety into simple factors.

**Theorem 1.10** (Poincaré Splitting Theorem). Let  $Y$  be an abelian subvariety of  $X$ , then there exists an abelian subvariety  $Z \subseteq X$  such that the homomorphism  $Y \times Z \rightarrow X$  given by  $(y, z) \mapsto y + z$  is an isogeny.

For a finite dimensional vector space  $V$  admitting an inner product  $V \rightarrow V^\vee, v \mapsto \langle \cdot, v \rangle$  and a subspace  $W \subseteq V$  the subspace  $\ker(V \rightarrow V^\vee \xrightarrow{\text{res}} W^\vee)$  constitutes a complement of  $W$  in  $V$ .

To mimic this prove we need the existence of a dual abelian variety and an isomorphism  $X \rightarrow X^\vee$ .

This can be accomplished using results of the following subsection.

## 1.1 A summary on the picard functor

Given a smooth projective variety  $X \rightarrow k$  over a field.

Note that the contravariant functor  $\text{Sch}/k \rightarrow \text{Ab}, T \mapsto \text{Pic}(X_T)$  is not a Zariski sheaf:

We will denote  $\text{pr}_T : X_T \rightarrow T$  to be the projection. Given  $\mathcal{L} \in \text{Pic}(T)$  such that  $\text{pr}_T^* \mathcal{L}$  is not trivial. Let  $(U_i)_{i \in I}$  an open cover of  $T$  that trivializes  $\mathcal{L}$ . Then  $(X_{U_i})$  constitutes an open cover of  $X_T$  and the pullback of  $\text{pr}_T^* \mathcal{L}$  to  $X_{U_i}$  is trivial. Therefore  $\mathcal{L}$  is in the kernel of the map

$$\text{Pic}(X_T) \mapsto \prod_{i \in I} \text{Pic}(X_{U_i}),$$

while not being trivial.

In hope to get a representable functor we define the (relative) Picard functor of  $X \rightarrow k$  by

$$T \mapsto \text{Pic}(X_T)/\text{pr}_T^* \text{Pic}(T). \quad (5)$$

It turns out that our assumptions on  $X \rightarrow k$  suffice and that the picard functor is indeed representable by a separated scheme  $\text{Pic}_{X/k}$  locally of finite type over  $k$ . Further, every closed subscheme  $Z \hookrightarrow \text{Pic}_{X/k}$  which is of finite type over  $k$  is proper (in fact projective) over  $k$ . A proof is given in [9, Chapt. 8, thm. 3].

Let us denote the connected component of the identity in  $\text{Pic}_{X/k}$  by  $\text{Pic}_{X/k}^0$ . Exploiting the properties of group schemes over fields as in [1, Tag 047J] it can be proven that  $\text{Pic}_{X/k}^0 \hookrightarrow \text{Pic}_{X/k}$  is a flat closed immersion,  $\text{Pic}_{X/k}^0$  is geometrically irreducible and quasi-compact over  $k$ .

Combining the last two paragraphs, we conclude that  $\text{Pic}_{X/k}^0$  is a proper and geometrically irreducible group scheme over  $k$ .

$\text{Pic}_{X/k}^0$  need not necessarily be reduced, let alone geometrically reduced. The latter happens if and only if  $\text{Pic}_{X/k}^0$  is smooth: If  $\text{Pic}_{X/k}^0$  is geometrically reduced it is a variety and will have non-empty smooth-locus. Using the translation morphism of its group structure we see that it is smooth. Conversely, if  $\text{Pic}_{X/k}^0$  is smooth then its base change to the algebraic closure will be regular. Any regular local ring is a domain and hence  $\text{Pic}_{X/k}^0$  must be geometrically reduced.

Luckily, there is a criterion for when  $\text{Pic}_{X/k}^0$  is smooth.

**Theorem 1.11.** The tangent space of  $\text{Pic}_{X/S}$  at the identity element is isomorphic to  $H^1(X, \mathcal{O}_X)$ . Further,  $\text{Pic}_{X/k}^0$  is smooth over  $k$  if and only if  $\dim \text{Pic}_{X/k}^0 = \dim H^1(X, \mathcal{O}_X)$ .

*Proof.* Let  $S := \text{Spec}(k[\varepsilon])$  where  $k[\varepsilon]$  is the ring of the dual numbers over  $k$ . For any  $k$  algebra  $A$  every element in  $A \otimes_k k[\varepsilon]$  can be written as an product of element in  $A$  and a unit. Therefore the map  $A \rightarrow A \otimes_k k[\varepsilon]$  induces a homeomorphism onto its image when passing to spectra. The map  $A \rightarrow A \otimes_k k[\varepsilon]$  is also finite and injective, so it will actually induce a homeomorphism. Looking at affine patches as above, we can identify the topological spaces  $X$  and  $X_S$ .

On this space we have a short exact sequence of sheaves

$$0 \rightarrow \mathcal{O}_X \xrightarrow{h} \mathcal{O}_{X_S}^* \xrightarrow{\text{res}} \mathcal{O}_X^* \rightarrow 1 \quad (6)$$

where  $h$  is given on sections by  $f \mapsto 1 + \varepsilon f$  and  $\text{res}$  by  $a + \varepsilon b \mapsto a$ . Since this sequence also yields an exact sequence on global sections, we get an exact sequence on the first cohomology groups

$$0 \rightarrow H^1(X, \mathcal{O}_X) \rightarrow \text{Pic}(X_S) \xrightarrow{\text{res}} \text{Pic}(X). \quad (7)$$

(Cohomology in the category of sheaves of abelian groups on  $X$ .)

Let  $s : \text{Spec}(k) \rightarrow S$  be the canonical morphism. Then  $\text{Pic}(X_S) \xrightarrow{\text{res}} \text{Pic}(X)$  can be identified with the pull back along  $X \xrightarrow{(1_X, s)} X_S$ .

Since  $\text{Pic}(S)$  and  $\text{Pic}(k)$  are trivial, we have  $\text{Pic}_{X/k}(k) = \text{Pic}(X)$  and  $\text{Pic}_{X/k}(S) = \text{Pic}(X_S)$ . Further, the pullback along  $(1_X, s)$  is by definition of the contra-variant functor  $\text{Pic}_{X/k}$  the induced map  $\text{Pic}_{X/k}(S) \rightarrow \text{Pic}_{X/k}(k)$ . Its kernel  $T$  consists of  $f : S \rightarrow \text{Pic}_{X/k}$  such that  $f \circ s = 0$ , where  $0$  is the identity of the group scheme  $\text{Pic}_{X/k}$ . In [1, Tag 0B28]  $T$  is identified with the tangent space of  $\text{Pic}_{X/k}$  at  $0$ , where the  $k$  action on  $T$  is induced by  $k[\varepsilon] \rightarrow k[\varepsilon], \varepsilon \mapsto \lambda\varepsilon$ . Therefore the sequence (7) identifies the underlying abelian group of the tangent space of  $\text{Pic}_{X/S}$  at zero with the abelian group  $H^1(X, \mathcal{O}_X)$ . The  $k$ -vector space structure on  $H^1(X, \mathcal{O}_X)$  is given by  $\lambda \cdot \{f_{\alpha\beta} \in \mathcal{O}_X(U_\alpha \cap U_\beta)\} = \{\lambda f_{\alpha\beta} \in \mathcal{O}_X(U_\alpha \cap U_\beta)\}$  for any Čech 1-cocycle given a covering  $(U_\alpha)$ .

The first map in the sequence (7), sends such a Čech 1-cocycle  $\{f_{\alpha\beta} \in \mathcal{O}_X(U_\alpha \cap U_\beta)\}$  to a line bundle on  $X_S$  that trivializes on the  $U_\alpha$  and has transition functions  $1 + \varepsilon f_{\alpha\beta}$ . Hence the  $k$ -vector space structure on  $T$  as tangent space exactly matches the  $k$ -action we obtain when identifying  $T$  via sequence (7) with the vector space  $H^1(X, \mathcal{O}_X)$ . This proves that  $H^1(X, \mathcal{O}_X) \cong T_0(\text{Pic}_{X/k})$  as  $k$ -vector spaces.

The only if part of the second statement of the theorem follows from  $H^1(X, \mathcal{O}_X) \cong T_0(\text{Pic}_{X/k}^0)$ .

Conversely, assuming  $\dim \text{Pic}_{X/k}^0 = \dim H^1(X, \mathcal{O}_X)$  we conclude that  $\dim \text{Pic}_{X/k}^0 = \dim T_0(\text{Pic}_{X/k}^0)$ . Hence, the stalk of  $\Omega_{\text{Pic}_{X/k}^0}^1$  at 0 is generated by  $\dim(\text{Pic}_{X/k}^0)$  elements. Therefore  $\text{Pic}_{X/k}^0$  is smooth over  $k$  at 0 of relative dimension  $\dim(\text{Pic}_{X/k}^0)$ . The locus of smoothness of fixed relative dimension is open and by translating it on  $\text{Pic}_{X/k}^0$  we win.  $\square$

### 1.1.1 The case when $X(k) \neq \emptyset$

We assume there is  $\varepsilon : k \rightarrow X$  a section to  $X \rightarrow k$ . Then for any  $k$ -scheme  $T$  the projection  $\text{pr}_T : X \times T \rightarrow T$  admits a section  $\varepsilon_T : T \cong k \times T \xrightarrow{\varepsilon \times 1} X \times T$ .

Hence  $\text{pr}_T^* : \text{Pic}(T) \rightarrow \text{Pic}(X_T)$  is a section to the pullback  $\varepsilon_T^* : \text{Pic}(X_T) \rightarrow \text{Pic}(T)$  along  $\varepsilon_T$ , and therefore the maps

$$\ker(\varepsilon_T^*) \hookrightarrow \text{Pic}(X_T) \twoheadrightarrow \text{Pic}(X_T)/\text{pr}_T^* \text{Pic}(T) \quad (8)$$

compose to an isomorphism with inverse  $\mathcal{L} \mapsto \mathcal{L} \otimes \text{pr}_T^* \varepsilon_T^* \mathcal{L}^{-1}$ . If we consider both left and right hand side of (8) as contravariant functors in  $T$  then (8) defines a natural isomorphism between those and we obtain that  $\text{Pic}_{X/k}$  also represents the functor

$$T \mapsto \{\mathcal{L} \in \text{Pic}(X_T) : \varepsilon_T^* \mathcal{L} \text{ is trivial}\}. \quad (9)$$

**Proposition 1.12** (The Poincaré Bundle). There is an isomorphism class of line bundles  $\mathcal{P}$  on  $X \times_k \text{Pic}_{X/k}$  such that  $\varepsilon_{\text{Pic}_{X/k}}^* \mathcal{P}$  is trivial, that satisfies the following universal property: For any  $\mathcal{L} \in \text{Pic}(X_T)$  with  $\varepsilon_T^* \mathcal{L}$  trivial, there exists a unique  $g : T \rightarrow \text{Pic}_{X/k}$  such that  $(1_X \times g)^* \mathcal{P} = \mathcal{L}$ .

Moreover,  $\mathcal{P}|_{X \times 0}$  is trivial for  $0 \in \text{Pic}_{X/k}(k)$  representing the identity in  $\text{Pic}(X)$ .

*Proof.* This is the contravariant Yoneda Lemma applied to (9). See the diagram below. The last assertion is clear from the first statement by taking  $\mathcal{L} = \mathcal{O}_X \in \text{Pic}(X)$ .  $\square$

$$\begin{array}{ccc} \text{Hom}_k(\text{Pic}_{X/k}, \text{Pic}_{X/k}) & \xrightarrow{\text{Hom}(g, \text{Pic}_{X/k})} & \text{Hom}_k(T, \text{Pic}_{X/k}) \\ \downarrow \wr & \begin{array}{ccc} \text{id}_{\text{Pic}_{X/k}} & \xrightarrow{\quad} & g \\ \downarrow & & \downarrow \\ \mathcal{P} & \xrightarrow{\quad} & \mathcal{L} \end{array} & \downarrow \wr \\ \{\mathcal{L} \in \text{Pic}(X \times_k \text{Pic}_{X/k}) : \varepsilon_{\text{Pic}_{X/k}}^* \mathcal{L} \text{ is trivial}\} & \xrightarrow{(1 \times g)^*} & \{\mathcal{L} \in \text{Pic}(X_T) : \varepsilon_T^* \mathcal{L} \text{ is trivial}\} \end{array} \quad (10)$$

We will call  $\mathcal{P}_X := \mathcal{P}$  from Proposition (1.12) the *Poincaré bundle*.

### 1.1.2 The dual abelian variety

In the case that  $X$  is an abelian variety, we will always take  $\varepsilon$  to be the inclusion of the identity, which we denote 0, into  $X$ . Let  $\mathcal{L}$  be a line bundle on  $X$ . On  $X \times X$  we define the *Mumford line bundle*  $\Lambda(\mathcal{L})$  by

$$\Lambda(\mathcal{L}) := m^* \mathcal{L} \otimes \text{pr}_1^* \mathcal{L}^{-1} \otimes \text{pr}_2^* \mathcal{L}^{-1}.$$

Then  $\varepsilon_X^* \Lambda(\mathcal{L})$  is trivial and by proposition (1.12) there is a unique  $\varphi_{\mathcal{L}} : X \rightarrow \text{Pic}_{X/k}$  such that  $(1 \times \varphi_{\mathcal{L}})^* \mathcal{P} = \Lambda(\mathcal{L})$ .

On  $T$  valued-points this map is given by mapping  $x : T \rightarrow X$  to  $\varphi_{\mathcal{L}} \circ x$  and diagram (10) tells us that this point represents  $(1 \times \varphi_{\mathcal{L}} \circ x)^* \mathcal{P} \in \text{Pic}(X_T)$ . Moreover, since

$$(1 \times \varphi_{\mathcal{L}} \circ x)^* \mathcal{P} = (1 \times x)^* \Lambda(\mathcal{L}) = (m \circ (1 \times x))^* \mathcal{L} \otimes \text{pr}_X^* \mathcal{L}^{-1} \otimes \text{pr}_T^* x^* \mathcal{L}^{-1} \quad (11)$$

we can identify  $\varphi_{\mathcal{L}}$  on  $T$ -valued points with the map from the theorem of the square (1.5). Now theorem (1.5) part b) proves that  $\varphi_{\mathcal{L}}$  is a homomorphism. In particular,  $\varphi_{\mathcal{L}}(0) = 0$  and because  $X$  is connected  $\varphi_{\mathcal{L}}$  factors through  $\text{Pic}_{X/k}^0$ .

**Lemma 1.13.** Let us denote the kernel of  $\varphi_{\mathcal{L}} : X \rightarrow \text{Pic}_{X/k}^0$  by  $K(\mathcal{L})$ .

- (i) We have  $\Lambda(\mathcal{L})|_{X \times K(\mathcal{L})} \cong \mathcal{O}_{X \times K(\mathcal{L})}$ ,
- (ii) If  $\mathcal{L}$  is ample, then  $K(\mathcal{L})$  is finite. Conversely, if  $\mathcal{L}$  has a non-zero global section and  $K(\mathcal{L})$  is finite, then  $\mathcal{L}$  is ample.

*Proof.* Let  $T = K(\mathcal{L})$  and  $x : K(\mathcal{L}) \rightarrow X$  be the inclusion. Then  $\Lambda(\mathcal{L})|_{X \times K(\mathcal{L})} = (1 \times x)^* \Lambda(\mathcal{L})$  represents  $\varphi_{\mathcal{L}} \circ x$ , which is trivial by definition of  $K(\mathcal{L})$ .

For (ii) let  $\mathcal{L}$  be an ample line bundle on  $X$ . Then its pullback  $\mathcal{L}'$  to  $K(\mathcal{L})$  is ample because  $x : K(\mathcal{L}) \rightarrow X$  is a closed immersion. By (i) the bundle  $(1 \times x)^* \Lambda(\mathcal{L})$  is trivial on  $X \times K(\mathcal{L})$ . Hence also  $(x, (-1))^* (1 \times x)^* \Lambda(\mathcal{L}) \cong \mathcal{L}'^{-1} \otimes (-1)^* \mathcal{L}'^{-1}$  is trivial on  $K(\mathcal{L})$ . So,  $\mathcal{L}' \otimes (-1)^* \mathcal{L}'$  is an ample and trivial sheaf on the closed subscheme  $K(\mathcal{L})$  of the proper scheme  $X$ .

In the first paragraph of the proof of proposition (1.7) we showed that if the structure sheaf of a proper scheme over  $k$  is ample, then the scheme is finite over  $k$ . This proves the first assertion of statement (ii). The converse statement is proposition 2.2 in [4].  $\square$

**Theorem 1.14.** For an abelian variety  $X$  over  $k$  the *dual abelian variety*  $X^\vee := \text{Pic}_{X/k}^0$  is an abelian variety over  $k$ . If  $\mathcal{L} \in \text{Pic}(X)$  is ample, then  $\varphi_{\mathcal{L}} : X \rightarrow X^\vee$  is an isogeny and, further,  $\dim X = \dim_k H^1(X, \mathcal{O}_X) = \dim X^\vee$ . In particular, if  $X$  is a curve, it's a curve of genus one.

*Proof.* Choose an ample line bundle  $\mathcal{L} \in \text{Pic}(X)$ , which exists by (1.6). Then the map  $\varphi_{\mathcal{L}} : X \rightarrow \text{Pic}_{X/k}^0$  has finite fiber over 0 by (1.13) and we conclude  $\dim X \leq \dim \text{Pic}_{X/k}^0$ .

It can be shown that for any group variety over a field  $\dim H^1(X, \mathcal{O}_X) \leq \dim X$ , see [4, Cor. 6.15] and therefore

$$\dim X \leq \dim \text{Pic}_{X/k}^0 \leq \dim T_0(\text{Pic}_{X/k}^0) \stackrel{1.11}{=} \dim_k H^1(X, \mathcal{O}_X) \leq \dim X.$$

Hence  $\text{Pic}_{X/k}$  is an abelian variety by (1.11) and the discussion above (1.11).  $\varphi_{\mathcal{L}}$  will be an isogeny by theorem (1.4) using that its kernel is finite by lemma 1.13 (ii).  $\square$

Consider two line bundles  $\mathcal{L}, \mathcal{L}'$  on  $X$ . If  $\mathcal{L} \cong \mathcal{L}'$ , then  $\Lambda(\mathcal{L}) \cong \Lambda(\mathcal{L}')$  and therefore  $\varphi_{\mathcal{L}} = \varphi_{\mathcal{L}'}$ . Hence we obtain a morphism

$$\varphi : \text{Pic}(X) \rightarrow \text{Hom}_k(X, X^\vee), \mathcal{L} \mapsto \varphi_{\mathcal{L}}. \quad (12)$$

Further  $\Lambda(\mathcal{L} \otimes \mathcal{L}') \cong \Lambda(\mathcal{L}) \otimes \Lambda(\mathcal{L}')$  and therefore  $\varphi_{\mathcal{L} \otimes \mathcal{L}'} = \varphi_{\mathcal{L}} + \varphi_{\mathcal{L}'}$ , i.e.  $\varphi$  is a homomorphism.

An isogeny  $\lambda : X \rightarrow X^\vee$  will be called *polarization*, if there exists some invertible ample sheaf  $\mathcal{L}$  on  $X_{\bar{k}}$  such that  $\lambda_{\bar{k}} = \varphi_{\mathcal{L}}$ . By theorem (1.14) and remark (1.6) there always exists at least one polarization.

If  $f : X \rightarrow Y$  is a homomorphism of abelian varieties over  $k$  then  $(f \times 1)^* \mathcal{P}_Y$  is trivial when pulled back to  $\{0\} \times Y^\vee$ . Therefore, by proposition (1.12) there exists a unique  $f^\vee : Y^\vee \rightarrow X^\vee$  such that

$$(1 \times f^\vee)^* \mathcal{P}_X \cong (f \times 1)^* \mathcal{P}_Y. \quad (13)$$

Note that  $f \mapsto f^\vee$  is a contravariant functor. Moreover, it can be shown that  $(f + g)^\vee = f^\vee + g^\vee$  for  $f, g : X \rightarrow Y$  homomorphisms, see [4, Chap. 7]. In particular,  $n_X^\vee = n_{X^\vee}$  and proposition (1.9) shows that the dual of an isogeny of degree  $d$  is again an isogeny of degree  $d$ . The existence of such dual homomorphisms justifies the name *dual abelian variety*.

For  $x \in Y^\vee(T)$  represented by  $\mathcal{L} \in \text{Pic}(Y_T)$  we obtain from proposition 1.12 that  $f^\vee(x)$  is represented by

$$(1 \times f^\vee \circ x)^* \mathcal{P}_X = (1 \times x)^* (f \times 1)^* \mathcal{P}_Y = (f \times 1)^* (1 \times x)^* \mathcal{P}_Y = (f \times 1)^* \mathcal{L}. \quad (14)$$



## 1.2 Endomorphisms of abelian varieties

In this chapter  $X$  and  $Y$  will be abelian varieties over the field  $k$ ,  $X$  will have dimension  $g$  and  $l$  will be a prime number not equal to  $\text{char}(k)$ . We give a proof of the Poincaré Splitting Theorem (1.10).

*Proof.* Let  $\iota : Y \rightarrow X$  be the inclusion and  $\lambda : X \rightarrow X^\vee$  a polarization.

For  $K := \ker(X \xrightarrow{\lambda} X^\vee \xrightarrow{\iota^\vee} Y^\vee)$  define  $Z$  to be the connected components of  $K$  with its reduced subscheme structure. Then  $Z$  is an abelian variety of dimension  $\dim X - \dim Y$ . By [4, Exerc. 11.1]  $\iota^\vee \circ \lambda \circ \iota$  is a polarization of  $Y$ . In particular,  $Z \cap Y$  is finite. Now the kernel of the homomorphism  $Y \times Z \rightarrow X$  in consideration is contained in  $(Y \cap Z) \times (Y \cap Z)$  and therefore finite. The proposition follows from theorem (1.4) part c).  $\square$

**Corollary 1.15.** There exist simple abelian varieties  $Y_1, \dots, Y_n$ , non two of which are  $k$ -isogenous, and there are positive integers  $m_1, \dots, m_n$  such that  $X$  is isogenous to  $Y_1^{m_1} \times Y_2^{m_2} \times \dots \times Y_n^{m_n}$ . The factors are unique up to  $k$ -isogeny and permutation.

*Proof.* This follows from the Poincaré Splitting Theorem (1.10) and the fact that any homomorphism of simple abelian varieties is constant or an isogeny.  $\square$

**Definition 1.16** (The Tate module). We define the *Tate module* of  $X$  by

$$T_l X := \lim \left( \{0\} \xleftarrow{l} X[l](k_s) \xleftarrow{l} X[l^2](k_s) \xleftarrow{l} \dots \right).$$

It follows from theorem (1.4) that  $T_l X$  is (non-canonically) isomorphic to  $\mathbb{Z}_l^{2g}$  and we introduce the  $2g$  dimensional  $\mathbb{Q}_l$  vector space  $V_l(X) := T_l(X) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l = T_l(X) \otimes_{\mathbb{Z}_l} (\mathbb{Z}_l \otimes_{\mathbb{Z}} \mathbb{Q}) = T_l(X) \otimes_{\mathbb{Z}} \mathbb{Q}$ .

A homomorphism of abelian varieties  $f : X \rightarrow Y$  induces a homomorphism  $T_l f : T_l X \rightarrow T_l Y$ . It sends a point  $(0, x_1, x_2, \dots) \in T_l X$  to  $(0, f(x_1), f(x_2), \dots) \in T_l Y$ . It follows from the definition that this is functorial. In particular,  $\text{End}_k(X) \rightarrow \text{End}_{\mathbb{Z}_l}(T_l X), f \mapsto T_l f$ , as well as,

$$V_l : \text{End}_k(X) \otimes_{\mathbb{Z}} \mathbb{Q} \rightarrow \text{End}_{\mathbb{Q}_l}(V_l X), f \otimes c \mapsto c \cdot (T_l(f) \otimes_{\mathbb{Z}_l} \text{id}_{\mathbb{Q}_l}) \quad (15)$$

are algebra homomorphisms.

**Remark 1.17.**  $\mathbb{Q}_l/\mathbb{Z}_l$  is the union of its subgroups  $l^{-n}\mathbb{Z}_l/\mathbb{Z}_l$ , which we identify with  $\mathbb{Z}/l^n\mathbb{Z}$ . Therefore as rings  $\mathbb{Q}_l/\mathbb{Z}_l = \text{colim}(\mathbb{Z}/l^n\mathbb{Z})$ , where the colimit is taken over the homomorphisms  $\mathbb{Z}/l^n\mathbb{Z} \hookrightarrow \mathbb{Z}/l^{n+1}\mathbb{Z}$  given by  $(1 \bmod l^n) \mapsto (l \bmod l^{n+1})$  and we see that  $T_l X = \text{Hom}(\mathbb{Q}_l/\mathbb{Z}_l, X(k_s))$ . Using this characterization of the Tate module and the long exact sequence of  $\text{Ext}_{\mathbb{Z}}(\mathbb{Q}_l/\mathbb{Z}_l, \cdot)$  modules it can be shown that for any isogeny  $f : X \rightarrow Y$  the induced map  $T_l f : T_l X \rightarrow T_l Y$  is injective with cokernel isomorphic to the  $l$ -Sylow group of  $(\ker f)(k_s)$  and further that  $V_l f : V_l X \rightarrow V_l Y$  is an isomorphism, see [4, Cor. 10.7].

**Lemma 1.18.** Let  $f : X \rightarrow Y$  be a homomorphism. If  $T_l f \in \text{Hom}_{\mathbb{Z}_l}(T_l X, T_l Y)$  is divisible by  $l^n$  then  $f$  is divisible by  $l^n$  in  $\text{Hom}(X, Y)$ .

*Proof.* The divisibility of  $T_l(f)$  means that  $f$  vanishes on  $X[l^n](k_s)$ .  $X[l^n]$  is étale over  $k$  and therefore  $f$  vanishes on  $X[l^n]$ . By [5, Sect. 12 Cor. 1] the isogeny  $l_X^n : X \rightarrow X$  gives  $X$  the structure of the quotient  $X/X[l^n]$ . Therefore  $f$  factors through  $l_X^n$  and hence is divisible by  $l_X^n$ .  $\square$

If  $f \in \text{Hom}_k(X, Y)$  and  $n \in \mathbb{Z} \setminus \{0\}$  then  $n \cdot f = 0 \implies n_Y \circ f = f \circ n_X = 0$ , but  $[n_X]$  is surjective, so  $f = 0$ . Hence,  $\text{Hom}_k(X, Y)$  is a torsion-free abelian group. In particular, the canonical map  $\text{End}(X) \rightarrow \text{End}^0(X)$  is injective.

For  $f \in \text{End}(X)$  we define  $\deg f$  to be the degree of  $f$  if  $f$  is an isogeny and zero otherwise. Because the degree is multiplicative we can extend this to  $\deg : \text{End}^0(X) \rightarrow \mathbb{Q}$  via  $\deg(\frac{f}{n}) := n^{-2g} \deg f$ .

**Theorem 1.19.** The map  $\deg : \text{End}_k^0(X) \rightarrow \mathbb{Q}$  is a homogeneous polynomial mapping of degree  $2g$ , i.e. if  $e_1, \dots, e_n$  are independent elements of  $\text{End}_k^0(X)$  then there is a homogeneous polynomial  $P \in \mathbb{Q}[x_1, \dots, x_n]$  of degree  $2g$  such that  $\deg(x_1 e_1 + \dots + x_n e_n) = P(x_1, \dots, x_n)$  for all  $x_1, \dots, x_n \in \mathbb{Q}$ .

*Proof.* By corollary 1.15 and proposition 1.9 we may assume that  $X$  is simple. Note that  $\deg(nf) = n^{2g} \deg(f)$  for all  $n \in \mathbb{Q}$  and all  $f$ . So, if  $P$  is a polynomial mapping, it must be homogeneous of degree  $2g$ . [6, Lem. 12.3] shows via an induction argument that it suffices to prove that for all  $f, g \in \text{End}_k^0(X)$  there exists  $P \in \mathbb{Q}[x]$  of degree  $\leq 2g$  such that  $\deg(nf + g) = P(n)$  for all  $n \in \mathbb{Q}$ . By multiplying with a big enough integer and using that  $\deg(nf) = n^{2g} \deg(f)$  we may assume that  $f, g \in \text{End}(X)$  and that  $n \in \mathbb{Z}$ .

Let  $D$  be a very ample divisor on  $X$  and let  $D_n := (nf + g)^*D$ . Then by [6, Lem. 8.3]  $\deg(nf + g)(D)^g = (D_n^g)$ , since  $nf + g$  is either an isogeny or the zero map. Hence, it suffices to prove that  $(D_n^g)$  is a polynomial in  $n$  of degree  $\leq 2g$ .

By theorem 1.5 part a) applied to the maps  $nf + g, f, f : X \rightarrow X$  and  $\mathcal{L} = \mathcal{L}(D)$  shows that  $D_{n+2} - 2D_{n+1} + D_n$  is linearly equivalent to  $D' := (2f)^*D - 2(f^*D)$ . So by induction  $D_n$  is linearly equivalent to  $\frac{n(n-1)}{2}D' + nD_1 - (n-1)D_0$ . By the multilinearity of the  $g$ -fold intersection number we conclude that  $(D_n)^g = \left(\frac{n(n-1)}{2}\right)^g (D')^g + \dots$  is a polynomial in  $n$ .  $\square$

**Theorem 1.20.** The  $\mathbb{Z}_l$ -linear map  $\text{Hom}_k(X, Y) \otimes \mathbb{Z}_l \rightarrow \text{Hom}_{\mathbb{Z}_l}(T_l X, T_l Y)$  given by  $f \otimes c \mapsto c \cdot T_l(f)$  is injective.

*Proof.* Claim: If  $X$  is simple, then the map  $\text{End}(X) \otimes \mathbb{Z}_l \rightarrow \text{End}(T_l X)$  is injective:

Suppose the map is not injective. Then there exist  $f_1, \dots, f_n \in \text{End}(X)$  and  $l$ -adic integers  $c_1, \dots, c_n$  such that  $c_1 T_l f_1 + c_2 T_l f_2 + \dots + c_n T_l f_n = 0$ .

Let  $M$  be the  $\mathbb{Z}$  submodule of  $\text{End}^0(X)$  generated by the  $\{f_1, \dots, f_n\}$ . By theorem 1.19 the map  $\deg : \mathbb{Q}M := \mathbb{Q} \otimes M \rightarrow \mathbb{Q}$  is continuous for the real topology and so  $U := \{v \in \mathbb{Q}M \mid \deg(v) < 1\}$  is an open neighborhood of 0. Since  $X$  is simple, every nonzero endomorphism of  $X$  has degree a positive integer and therefore  $(\mathbb{Q}M \cap \text{End}(X)) \cap U = \{0\}$  and we see that  $\mathbb{Q}M \cap \text{End}(X)$  is discrete in  $\mathbb{Q}M$ . By [10, Prop. 4.15] this is equivalent to  $\mathbb{Q}M \cap \text{End}(X)$  being a finitely generated  $\mathbb{Z}$ -module. Since  $\text{End}(X)$  is torsion-free there is  $r > 0$  such that  $\mathbb{Q}M \cap \text{End}(X) = e_1 \mathbb{Z} \oplus \dots \oplus e_r \mathbb{Z}$  for certain  $e_i \in \text{End}(X)$ . Moreover, there are  $a_1, \dots, a_r \in \mathbb{Z}_l$  such that  $\sum_{i=1}^r a_i T_l(e_i) = 0$ .

Since the integers are dense in the  $l$ -adic integers, for any  $m \in \mathbb{N}$  there exists  $n_1(m), \dots, n_r(m) \in \mathbb{Z}$  such that for all  $i = 1, \dots, r$  we have  $n_i(m) - a_i$  is divisible through  $l^m$ . Then also

$$T_l \left( \sum_{i=1}^r n_i(K) e_i \right) = \sum_{i=1}^r n_i(K) T_l(e_i) = \sum_{i=1}^r (n_i - a_i) T_l(e_i)$$

is divisible through  $l^m$  and by lemma 1.18  $\sum_{i=1}^r n_i(m) e_i \in \text{End}(X)$  is divisible by  $l^m$  in  $\text{End}(X)$  and therefore in  $\mathbb{Q}M \cap \text{End}(X)$  by definition of  $\mathbb{Q}M$ . On the other hand, since  $|n_i(m) - a_i|_l \leq l^{-m}$  there exist  $M_i, K_i \in \mathbb{Z}$  such that  $v_l(n_i(m)) = K_i$  for all  $m \geq M_i$ . Let  $M = \max M_i$  and  $K = \max K_i$ . Then  $\sum_{i=1}^r n_i(m) e_i$  is not divisible by a power of  $l$  higher than  $K$  for all  $m \geq M$  in  $\mathbb{Q}M \cap \text{End}(X)$  since the  $e_1, \dots, e_r$  form a free generating system. This contradicts the earlier statement.

Now we prove the general case. Note that since ‘limits commute’  $T_l(X \times Y) = T_l(X) \times T_l(Y)$ .

There exists isogenies  $X \rightarrow \prod_{i=1}^r X_i$  and  $Y \rightarrow \prod_{j=1}^s Y_j$ , where the  $X_i, Y_j$  are simple abelian varieties. Proposition 1.9 lets us map  $\text{Hom}(X, Y)$  into  $\text{Hom}(\prod_{i=1}^r X_i^{m_i}, \prod_{j=1}^s Y_j^{n_j})$  and since  $n_X$  is an epimorphism for all  $n \in \mathbb{Z}$  this is injective. Since every nonzero homomorphism of simple abelian varieties is an isogeny,  $\text{Hom}(\prod_{i=1}^r X_i^{m_i}, \prod_{j=1}^s Y_j^{n_j}) = \prod_{i,j} \text{Hom}(X_i, Y_j)$  and if  $X_i$  and  $Y_j$  are isogenous then  $\text{Hom}(X_i, Y_j)$  embeds into  $\text{End}(X_i)$ , else  $\text{Hom}(X_i, Y_j) = 0$ . So, the theorem follows from the special case proven above.  $\square$

**Corollary 1.21.**  $\text{Hom}^0(X, Y) := \text{Hom}_k(X, Y) \otimes \mathbb{Q}$  has  $\mathbb{Q}$  dimension  $\leq 4 \dim X \dim Y$ .

*Proof.* For an abelian variety  $X$  the  $\mathbb{Z}_l$ -module  $T_l X$  is free of rank  $2 \dim X$  and therefore  $\text{Hom}_{\mathbb{Z}_l}(T_l X, T_l Y)$  is free of rank  $4 \dim X \dim Y$ . Since  $\mathbb{Z}_l$  is a principal ideal domain we can conclude from theorem 1.20 that  $\mathbb{Z}_l \otimes \text{Hom}(X, Y)$  is a free  $\mathbb{Z}_l$  module of rank  $\leq 4 \dim X \dim Y$ . This bounds the rank of the torsion free abelian group  $\text{Hom}(X, Y)$  by  $4 \dim X \dim Y$ .  $\square$

Given  $f \in \text{End}_k^0(X)$  there is a necessarily unique polynomial  $P_f \in \mathbb{Q}[x]$  of degree  $2d$  such that  $P_f(n) = \deg(n_X - f)$  for all  $n \in \mathbb{N}$  by theorem 1.19. The next theorem justifies that we will refer to  $P_f$  as the *characteristic polynomial* of  $f$ .

**Theorem 1.22.** For  $f \in \text{End}^0(X)$  let  $P_{f,l} \in \mathbb{Q}_l[x]$  be the characteristic polynomial of  $V_l f \in \text{End}_{\mathbb{Q}_l}(V_l X)$ . Then  $P_{f,l} = P_f$  is independent of  $l$  and has integer coefficients whenever  $f \in \text{End}(X)$ .

*Proof.* We only give a sketch, whereas a detailed proof can be found in [6, Chapt. 12] or [4, thm. 12.8]. It can be assumed that  $f \in \text{End}(X)$  and, further, using corollary 1.15 that  $X$  is simple.

Set  $g = \text{id}$ . We start with the notation of the proof of theorem 1.19 for a chosen ample symmetric divisor  $D$  and interchange the roles of  $f$  and  $g$ . Lemma 1.8 shows that  $D' \sim -2D$  and we conclude from the last equation in the proof of theorem 1.19 that  $P_f$  has integer coefficients and leading coefficient 1.

Let  $P_f = \prod_{i=1}^{2g} (x - a_i)$  and let  $P_{f,l} = \prod_{i=1}^{2g} (x - b_i)$ . Let  $F \in \mathbb{Z}[t]$ . Using the properties of the determinant it can be proven that  $\det V_l(F(f)) = \pm \prod_{i=1}^{2g} F(b_i)$  and similarly using the multiplicativity of the degree it can be shown that  $\deg(F(f)) = \pm \prod_{i=1}^{2g} F(a_i)$ .

Let  $\alpha := F(f)$ . Using the Smith-Normal form on  $T_l \alpha$  to assume it in diagonal form, we can see that  $\frac{1}{\#(\text{coker}(T_l \alpha))} = |\det(T_l \alpha)|_l$ . Further by remark 1.17  $\text{coker}(T_l \alpha)$  is isomorphic to the  $l$ -Sylow-group  $N_l$  of  $(\ker \alpha)(k_s)$ .  $N_l$  is an étale group scheme over  $k$  by [4, Cor. 4.48] provided that  $l$  is relatively prime to  $\text{char}(p)$  and hence  $\#N_l = |\deg(\alpha)|_l^{-1}$  by equation (1). Summarized we have,

$$\left| \prod_{i=1}^{2g} F(a_i) \right|_l = |\deg(\alpha)|_l = \frac{1}{\#N_l} = \frac{1}{\#(\text{coker}(T_l \alpha))} = |\det(T_l \alpha)|_l = \left| \prod_{i=1}^{2g} F(b_i) \right|_l$$

for all  $F \in \mathbb{Z}[t]$ . By lemma 1 in [11, lem. VII 1.], this implies that  $P_{f,l} = P_f$  as elements of  $\mathbb{Q}_l[x]$ . (The proof of the cited lemma relies on the denseness of the integers in the  $l$ -adic integers and the continuity of the given polynomials with respect to the  $l$ -adic topology).  $\square$

We define the trace of  $f \in \text{End}^0(X)$  via the following equation  $P_f(x) = x^{2g} - \text{tr}(f)x^{2g-1} + \dots + \deg(f)$ .

## 2 The Jacobian variety

In this section  $C$  shall be a non-singular proper curve of genus  $g$  over a field  $k$ . Curves are assumed to be geometrically integral one-dimensional schemes of finite type and separated over  $k$ .

**Proposition 2.1.**  $\text{Pic}_{C/k}$  is smooth over  $k$ .

*Proof.* We already know that  $\text{Pic}_{C/k}$  is locally of finite type over  $k$  and therefore it suffices to proof that  $\text{Pic}_{C/k}$  is formally smooth. To show this let  $Z$  be an affine scheme over  $k$  and  $i : Z_0 \hookrightarrow Z$  a closed subscheme cut out by an ideal  $I \subseteq \mathcal{O}_Z$  that satisfies  $I^2 = 0$ . Passing to the functor that the scheme  $\text{Pic}_{C/k}$  represents we have to proof the following: The pullback along  $(1 \times i)$  induces a surjection  $\text{Pic}(C \times Z)/\text{pr}_Z^* \text{Pic}(Z) \rightarrow \text{Pic}(C \times Z_0)/\text{pr}_{Z_0}^* \text{Pic}(Z_0)$ .

Note that  $b + I \in \mathcal{O}_{Z_0}(Z_0)$  is invertible if and only if  $b \in \mathcal{O}_Z(Z)^\times$ : If  $b = 1 + c$  for  $c \in I$  then  $b^{-1} = (1 - c)$ . Hence we obtain an exact sequence of sheaves of abelian groups on the topological space  $|Z| = |Z_0|$  given by  $0 \rightarrow I \rightarrow \mathcal{O}_Z^\times \xrightarrow{i^\#} \mathcal{O}_{Z_0}^\times \rightarrow 1$ , where the first map sends  $s$  to  $1 + s$ .

This gives the following short exact sequence on the topological space  $|C \times Z| = |C \times Z_0|$

$$0 \rightarrow \text{pr}_Z^* I = \mathcal{O}_C \otimes_k I \xrightarrow{n \mapsto 1+n} \mathcal{O}_{C \times Z}^\times \xrightarrow{(1 \times i)^\#} \mathcal{O}_{C \times Z_0}^\times \rightarrow 1.$$

We apply the pushforward along  $\text{pr}_Z$  to obtain a long exact sequence

$$\begin{aligned} 0 \rightarrow R^0(\text{pr}_Z)_*(\mathcal{O}_C \otimes_k I) &\rightarrow R^0(\text{pr}_Z)_*\mathcal{O}_{C \times Z}^\times \rightarrow R^0(\text{pr}_Z)_*\mathcal{O}_{C \times Z_0}^\times \\ &\rightarrow R^1(\text{pr}_Z)_*(\mathcal{O}_C \otimes_k I) \rightarrow R^1(\text{pr}_Z)_*\mathcal{O}_{C \times Z}^\times \rightarrow R^1(\text{pr}_Z)_*\mathcal{O}_{C \times Z_0}^\times \rightarrow \dots \end{aligned}$$

The map  $(\text{pr}_Z)_*\mathcal{O}_{C \times Z}^\times \rightarrow (\text{pr}_Z)_*\mathcal{O}_{C \times Z_0}^\times$  is a surjective map of sheaves on  $Z$  and therefore  $R^1(\text{pr}_Z)_*(\mathcal{O}_C \otimes_k I) \rightarrow R^1(\text{pr}_Z)_*\mathcal{O}_{C \times Z}^\times$  is injective. Further,  $R^2(\text{pr}_Z)_*(\mathcal{O}_C \otimes_k I)$  vanishes because  $\text{pr}_Z$  is proper,  $I$

is quasi-coherent and  $H^2(C, \mathcal{O}_C) = 0$ , see [12, 7.7.10 and 7.7.5 (II)]. Therefore we obtain an exact sequence

$$0 \rightarrow R^1(\mathrm{pr}_Z)_*(\mathcal{O}_C \otimes_k I) \rightarrow R^1(\mathrm{pr}_Z)_*\mathcal{O}_{C \times Z}^\times \rightarrow R^1(\mathrm{pr}_Z)_*\mathcal{O}_{C \times Z_0}^\times \rightarrow 1.$$

We apply the global section functor  $H^0(Z, \cdot)$  to see that the obstruction for

$$\mathrm{Pic}_{X/k}(Z) = H^0(Z, R^1(\mathrm{pr}_Z)_*\mathcal{O}_{C \times Z}^\times) \rightarrow H^0(Z_0, R^1((\mathrm{pr}_Z))_\times \mathcal{O}_{C \times Z_0}^*) = \mathrm{Pic}_{C/k}(Z_0)$$

being surjective is  $H^1(Z, R^1(\mathrm{pr}_Z)_*(\mathcal{O}_C \otimes_k I))$ , which vanishes because  $Z$  is affine and  $(\mathrm{pr}_Z)_*(\mathcal{O}_C \otimes_k I)$  is quasi-coherent by properness of  $\mathrm{pr}_Z$ .  $\square$

The given proof that  $\mathrm{Pic}_{C/k}$  is formally smooth can be found in [9, Prop. 8.4.2] and relies on  $H^2(C, \mathcal{O}_C)$  vanishing. So, our assumption that  $C$  is a curve plays a crucial role in this proof of smoothness of  $\mathrm{Pic}_{C/k}$ .

A regular local ring is reduced and therefore  $\mathrm{Pic}_{C/k}^0$  is geometrically reduced over  $k$ . Moreover, we have seen in section 1.1 that  $\mathrm{Pic}_{C/k}^0$  is also proper and geometrically irreducible, i.e.  $\mathrm{Pic}_{C/k}^0$  is an abelian variety. We will refer to  $J := \mathrm{Pic}_{C/k}^0$  as *Jacobian variety* or short *Jacobian* of  $C$ . By theorem 1.11  $J$  has dimension  $g$  and its tangent space at the zero is isomorphic to  $H^1(C, \mathcal{O}_C)$ . In particular, if  $g = 0$  then  $J = \mathrm{Spec}(k)$ .

## 2.1 The canonical map from $C$ to its Jacobian

In this subsection we assume  $C$  to have a  $k$ -rational point  $P \in C(k)$  corresponding to a  $k$ -morphism  $\varepsilon : k \rightarrow C$ . By [1, Tag 0C6U], if  $g = 0$  then  $C \cong \mathbb{P}_k^1$  and we will assume in the following subsection that  $g > 0$ .

Further, we will denote the canonical line bundle on  $C \times J$  from Proposition 1.12 by  $\mathcal{M}^P$ .

Since  $C \times C$  is regular, we can associate an invertible sheaf  $\mathcal{L}^P$  to the Weil-Divisor

$$\Delta - C \times \{P\} - \{P\} \times C \quad (16)$$

on  $C \times C$ . Then  $\varepsilon_C^* \mathcal{L}^P \cong \mathcal{L}(P) \otimes \mathcal{L}(P)^{-1} \otimes \varepsilon_C^*((\varepsilon_C)_* \mathcal{O}_C)^{-1}$  is trivial, since  $\varepsilon_C$  is a closed immersion.

By proposition 1.12 there exists a unique map  $f : C \rightarrow \mathrm{Pic}_{C/k}$  such that  $(1 \times f)^* \mathcal{M}^P = \mathcal{L}^P$ .

For  $K/k$  a field extension and  $Q \in C(K) \setminus P$  with corresponding map  $x : K \rightarrow C$  we have  $(1 \times x)^* \mathcal{L}^P = \mathcal{L}_{C_K}(Q) \otimes \mathcal{L}_{C_K}(P)^{-1}$ .

Consulting diagram 10 we deduce that  $f$  is given on  $K$ -valued by

$$f(Q) = \mathcal{L}_{C_K}(Q) \otimes \mathcal{L}_{C_K}(P)^{-1}. \quad (17)$$

Since  $C$  is connected and  $f(P) = \mathcal{O}_X$  the map  $f$  factors through  $\mathrm{Pic}_{X/k}^0 = J$ .

The canonical map  $h_J : \Gamma(J, \Omega_J^1) \rightarrow \Omega_{J,0}^1 = (T_0 J)^\vee$  is an isomorphism for any group variety over a field, see [9, 4.2 Prop. 2]. Serre-duality gives a canonical isomorphism  $\mathrm{ser} : \Gamma(C, \Omega_C^1) \rightarrow H^1(C, \mathcal{O}_C)^\vee$ . These isomorphisms are related via the pullback along  $f$ . This is encoded in the next proposition, whose proof can be found in [4, Thm. 14.4].

**Proposition 2.2.** For  $\nu : H^1(C, \mathcal{O}_C) \rightarrow T_0 J$  the isomorphism from theorem 1.11 and  $f^* : \Gamma(J, \Omega_J^1) \rightarrow \Gamma(C, \Omega_C^1)$  the canonical map the diagram

$$\begin{array}{ccc} \Gamma(J, \Omega_J^1) & \xrightarrow{f^*} & \Gamma(C, \Omega_C^1) \\ \downarrow h_J & & \downarrow \mathrm{ser} \\ T_0(J)^\vee & \xrightarrow{\nu^\vee} & H^1(C, \mathcal{O}_C)^\vee \end{array}$$

commutes. In particular,  $f^* : \Gamma(J, \Omega_J^1) \rightarrow \Gamma(C, \Omega_C^1)$  is an isomorphism.

**Theorem 2.3.**  $f : C \rightarrow J$  is a closed immersion. If  $C$  has genus  $g = 1$  then  $f$  is an isomorphism.

*Proof.* Whether a morphism is a closed immersion, can be checked after faithfully flat base change, so we may assume  $k = \bar{k}$ . Since  $f$  is a morphism of smooth, projective  $k$ -varieties, it is a closed immersion if it separates points and tangent vectors. (The proof is the same as the “if” part of [8, II 7.3]). To see that  $f$  separates points, assume that  $Q_1, Q_2 \in C(k)$  have the same image under  $f$ . Then  $\mathcal{L}(Q_1) \otimes \mathcal{L}(Q_2)^{-1}$  is trivial, i.e.  $Q_1 - Q_2$  is the divisor of a function  $f$ . But then  $f$  defines an isomorphism  $C \rightarrow \mathbb{P}_C^1$ , contradicting our assumption  $g > 0$ .

We will only sketch the proof of  $f$  separating tangent vectors. To see that  $(df_Q) : T_Q C \rightarrow T_{f(Q)} J$  is injective, we may assume that  $Q = P$ . It can be shown that the dual map of  $df_P$  is  $\Gamma(J, \Omega_J^1) \xrightarrow{f^*} \Gamma(C, \Omega_C^1) \xrightarrow{\text{can}} (T_P C)^\vee$ . We have seen in Proposition 2.2 that the first of these maps is an isomorphism. Therefore it suffices to proof that  $\Gamma(C, \Omega_C^1) \xrightarrow{\text{can}} (T_P C)^\vee$  is surjective. The kernel of this map can be identified with  $\{\omega \in \Gamma(C, \Omega_C^1) \mid \omega(P) = 0\}$  and by Serre duality the latter is dual to  $H^1(C, \mathcal{L}(P))$ . Since  $T_P C$  is one-dimensional, we now only have to proof that  $\dim H^1(C, \mathcal{L}(P)) < \dim \Gamma(C, \Omega_C^1)$ . Moreover, we know that  $\dim \Gamma(C, \Omega_C^1) = g$  by Serre duality and  $h^1(C, \mathcal{L}(P)) = h^0(C, \mathcal{L}(P)) + g - 2$  by the Riemann-Roch theorem. Because we assumed  $g > 0$ , there exist no meromorphic functions on  $C$  that only have one simple pole and are regular elsewhere, as such define an isomorphism  $C \rightarrow \mathbb{P}_k^1$ . We conclude that  $H^0(C, \mathcal{L}(P)) = H^0(C, \mathcal{O}_C) \cong k$  and hence  $h^1(C, \mathcal{L}(P)) = g - 1 < g = \dim \Gamma(C, \Omega_C^1)$ . In summary, we have shown that  $f$  also separates tangent vectors and hence must be a closed immersion.

In the case  $g = 1$  both  $J$  and  $C$  are proper, regular curves and hence  $f$  must be an isomorphism.  $\square$

**Remark 2.4** (*Elliptic Curves*). Due to theorem 1.14 abelian varieties of dimension one have genus one. By the last theorem 2.3, a nonsingular, proper curves of genus one, which admits a  $k$ -valued point, is isomorphic to its own Jacobian variety. We conclude that these notions coincide and refer to abelian varieties of dimension one as *elliptic curves*. Let  $C$  be an elliptic curve and  $Q_1, Q_2 \in C(\bar{k})$ . Then we can read from  $f$ 's action on closed points, that there exists a unique  $Q_3 \in C(\bar{k})$  such that  $\mathcal{L}(Q_1 + Q_2 - 2P) \cong \mathcal{L}(Q_3 - P)$ . Further,  $(Q_1, Q_2) \mapsto Q_3$  defines the unique group law on  $C$  such that  $f$  is a homomorphism of abelian varieties.

## 2.2 Symmetric powers of a curve

In this subsection we assume there exists  $P \in C(k)$  and that  $g > 0$ . We will write  $f$  for the canonical closed immersion  $C \rightarrow J$  from theorem 2.3.

For  $n > 0$  let  $S_n$  be the symmetric group on  $n$  letters.  $S_n$  acts on  $C^n$  by permuting the factors. A morphism  $\varphi : C^n \rightarrow T$  is said to be symmetric if  $\varphi \circ \sigma = \varphi$  for all  $\sigma \in S_n$ .

Since quasi-projective schemes admit quotients by finite groups, see [5, p. 66], there exists a variety  $C^{(n)}$  and a symmetric morphism  $\pi : C^n \rightarrow C^{(n)}$ , such that

1. as topological space  $(C^{(n)}, \pi)$  is the quotient of  $C^n$  by  $S_n$ .
2. for any open affine subset  $U$  of  $C$ ,  $U^{(n)}$  is an open affine subset of  $C^{(n)}$  and  $\mathcal{O}_{C^{(n)}}(U^{(n)})$  is the subring  $\mathcal{O}_{C^n}(U^n)^{S_n}$  of  $\mathcal{O}_{C^n}(U^n)$  given by elements fixed by the action of  $S_n$ .

The pair  $(C^{(n)}, \pi)$  has the following universal property: every symmetric  $k$ -morphism  $\varphi : C^n \rightarrow T$  factors uniquely through  $\pi$ . Moreover, the map  $\pi$  is finite and surjective. Since  $C^n$  is proper this implies that  $C^{(n)}$  is proper over  $k$ .

For  $m_1, \dots, m_k \in \mathbb{N}_0$  a partition  $n = m_1 + \dots + m_r$  the natural isomorphism  $C^{m_1} \times \dots \times C^{m_r} \rightarrow C^n$  induces a natural morphism  $s = s_{m_1, \dots, m_r} : C^{(m_1)} \times \dots \times C^{(m_r)} \rightarrow C^{(n)}$  that we will refer to the sum map.

**Proposition 2.5.** Suppose given a partition  $n = m_1 + \dots + m_r$  and points  $P_1, \dots, P_r \in C(k)$  with  $P_i \neq P_j$  if  $i \neq j$ . Write  $m_i P_i \in C^{(m_i)}(k)$  for the image of the point  $(P_i, \dots, P_i) \in C^{m_i}$  under the quotient map  $C^{m_i} \rightarrow C^{(m_i)}$ .

- (i) Then the sum morphism  $C^{(m_1)} \times \dots \times C^{(m_r)} \rightarrow C^{(n)}$  is étale at the point  $(m_1 P_1, \dots, m_r P_r)$ .

(ii) The symmetric power  $C^{(n)}$  of a non-singular curve is regular of dimension  $n$  for any  $n > 0$ .

In particular,  $\pi : C^n \rightarrow C^{(n)}$  is finite and flat of degree  $n!$ .

*Proof.* We won't give a proof of part (i) here, a proof can be found in [4, Lem. 14.7].

For the proof of part (ii) we may assume that  $k$  is algebraically closed. It suffices to check that for all  $k$ -valued points  $Q$  of  $C^{(n)}$  the stalks at  $Q$  is regular. By part (i) we only have to check this on points of the form  $Q := np$  for given  $p \in C(k)$ . Let us denote  $P := (p, \dots, p) \in C^n(k)$ . Note that the formation of the fixed ring under the action of  $S_n$  is a finite categorical limit. Finite limits commute with filtered colimits, e.g. localization, as well as, all categorical limits. In particular,  $\mathcal{O}_{C^{(n)}, Q} = (\mathcal{O}_{C^n, P})^{S_n}$ . The ideal  $\mathfrak{m}$  cutting out the closed point  $P$  in  $\mathcal{O}_{C^n, P}$  is invariant under the action of  $S_n$  and equals the ideal cutting out the closed point  $Q$  in  $\mathcal{O}_{C^{(n)}, P}$ . Therefore

$$\begin{aligned} (\widehat{\mathcal{O}_{C^n, P}})^{S_n} &= (\lim_m \mathcal{O}_{C^n, P} / \mathfrak{m}^m)^{S_n} = \lim_m (\mathcal{O}_{C^n, P} / \mathfrak{m}^m)^{S_n} = \lim_m (\mathcal{O}_{C^n, P})^{S_n} / \mathfrak{m}^m \\ &= \lim_m \mathcal{O}_{C^{(n)}, Q} / \mathfrak{m}^m = \widehat{\mathcal{O}_{C^{(n)}, Q}}. \end{aligned}$$

Since  $C^n$  is regular,  $\widehat{\mathcal{O}_{C^n, P}} \cong k[[x_1, \dots, x_n]]$ , where  $S_n$  acts on  $\widehat{\mathcal{O}_{C^n, P}}$  by permuting the variables. By the fundamental theorem on symmetric polynomials  $k[[x_1, \dots, x_n]] \rightarrow k[[x_1, \dots, x_n]]^{S_n}$ ,  $x_i \rightarrow \sigma_i$ , for  $\sigma_i$  being the  $i$ -th symmetric polynomial in  $n$  variables, is an isomorphism. Since a local Noetherian ring is regular if and only if its completion is regular, we have proven that  $C^{(n)}$  is regular at  $Q$ .

For the last assertion note that a quasi-finite morphism of regular varieties is flat by [3, 26.2.11.]. As in the proof of theorem 1.4, we can compute the degree of  $\pi$  as the dimension of the  $k$ -vector space of global sections of any fiber. Choosing a fiber containing a point  $(P_1, \dots, P_n)$  with  $P_i \neq P_j$  for all  $i \neq j$ , we see by (i) that the fiber is étale over  $k$ . So,  $\deg \pi$  equals the number of closed points of this fiber, which is the cardinality of the  $S_n$  orbit of  $(P_1, \dots, P_n)$  in  $C^n$ . Hence,  $\deg \pi = n!$ .  $\square$

Recall that for  $C \rightarrow T$  a morphism of  $k$ -schemes a *relative effective Cartier divisor*  $D$  on  $C_T := C \times T$  over  $T$  is a closed subscheme  $D \subseteq C_T$ , which is flat over  $T$  and such that the ideal sheaf  $\mathcal{I}_D \subseteq \mathcal{O}_{C_T}$  is an invertible  $\mathcal{O}_{C_T}$  module.

When we tensor the inclusion  $\mathcal{I}_D \hookrightarrow \mathcal{O}_{C_T}$  with  $\mathcal{L}(D)$  we obtain an inclusion  $\mathcal{O}_{C_T} \hookrightarrow \mathcal{L}(D)$  and hence a canonical global section  $s_D$  of  $\mathcal{L}(D)$ . The map  $D \mapsto (\mathcal{L}(D), s_D)$  defines a bijection between relative effective divisors on  $C_T$  over  $T$  and isomorphism classes of pairs  $(\mathcal{L}, s)$  where  $\mathcal{L}$  is an invertible sheaf on  $C_T$  and  $s \in \Gamma(C_T, \mathcal{L})$  is such that

$$\mathcal{L}/s\mathcal{O}_{C_T} := \text{Coker}(\mathcal{O}_{C_T} \xrightarrow{s} \mathcal{L})$$

is flat over  $T$ . Here two pairs  $(\mathcal{L}, s)$  and  $(\mathcal{L}', s')$  are considered to be isomorphic if there is an isomorphism of  $\mathcal{O}_{C_T}$ -modules  $h : \mathcal{L} \rightarrow \mathcal{L}'$  with  $h(s) = s'$ . The inverse of the above bijection associates to  $(\mathcal{L}, s)$  the zero scheme  $D = Z(s) \subseteq C_T$  of the section  $s$ .

Relative effective Cartier divisors on  $C_T$  over  $T$  can be added. If  $D$  corresponds to the pair  $(\mathcal{L}, s)$  and  $D'$  to the pair  $(\mathcal{L}', s')$  then  $D + D'$  is cut out by  $\mathcal{I}_D \cdot \mathcal{I}_{D'}$  and corresponds to  $(\mathcal{L} \otimes \mathcal{L}', s \otimes s')$ . To see that  $D + D'$  is again flat over  $T$  consult [1, Tag 0B8U].

While the pullback of an effective Cartier divisor might not be effective, the charm of relative effective Cartier divisors is that they behave nicely with respect to base-changes:

If  $D \subseteq C_T$  is a relative effective Cartier divisor over  $T$  and  $h : T' \rightarrow T$  is a morphism of  $k$ -schemes then we can pull  $D$  back to an relative effective Cartier divisor  $D_{T'} = h^*D \subseteq C_{T'}$  on  $C_{T'}$  over  $T'$ . A proof of this property can be found at [1, Tag 056Q].

Consider an relative effective Cartier divisor  $D$  on  $C_T$  over  $T$ . Then for any  $t \in T$  the pullback  $D_t$  of  $D$  along  $t \rightarrow T$  is a Cartier Divisor on the curve  $C_{k(t)}$  and therefore finite. We conclude that  $D \rightarrow T$  is quasi-finite. As  $C$  is proper over  $k$ ,  $D$  is proper over  $T$  too, and quasi-finite + proper implies finite. So,  $D$  is finite and flat over  $T$  and hence  $\mathcal{O}_D$  is finite locally free as an  $\mathcal{O}_T$  module. The rank of  $\mathcal{O}_D$  as an  $\mathcal{O}_T$  module (which is a locally constant function on  $T$ ) is called the degree of  $D$  and denoted  $\deg D$ . It is straightforward to check that, if  $D$  has constant degree  $n$  over  $T$  then the same holds for  $D_{T'}$  over  $T'$  for any  $h : T' \rightarrow T$ . It is proven in [13, Lem. 1.2.6] that for two relative

effective Cartier divisors  $D_1, D_2$  on  $C_T$  over  $T$  their sum  $D_1 + D_2$  has degree  $\deg(D_1) + \deg(D_2)$  over  $T$ .

We obtain a contravariant functor  $\text{Div}_{C/k}^{\text{eff},n} : \text{Sch}/k \rightarrow \text{Sets}$  with

$$\text{Div}_{C/k}^{\text{eff},n}(T) = \{\text{relative effective Cartier divisors } D \subseteq C_T \text{ of constant degree } n \text{ over } T\}. \quad (18)$$

If  $P \in C(T)$  is a  $T$ -valued point of  $C$  then this gives a section  $T \rightarrow C_T$  of the structural morphism, whose image is a relative effective Cartier divisor  $P \subseteq C_T$  of constant degree 1 over  $T$  by [13, Lem. 1.2.2]. More generally, for  $P_1, \dots, P_n \in C(T)$  we get an relative effective Cartier divisor  $P_1 + \dots + P_n$  on  $C_T$  of constant degree  $n$  over  $T$ . In this way we obtain a morphism  $C^n \rightarrow \text{Div}_{C/k}^{\text{eff},n}$ . Since this morphism is  $S_n$  invariant, it factors through a morphism  $h : C^{(n)} \rightarrow \text{Div}_{C/k}^{\text{eff},n}$ . Checking on closed points motivates that  $h$  defines an isomorphism. This is proven in [6, Thm. 3.13].

**Remark 2.6.** We will henceforth identify  $C^{(n)}$  with  $\text{Div}_{C/k}^{\text{eff},n}$  via the above isomorphism  $h$ .

Let  $f^n$  be the map  $C^n \rightarrow J$  sending  $(P_1, \dots, P_n)$  to  $f(P_1) + \dots + f(P_n)$ . Here  $f$  is the canonical closed immersion from theorem 2.3. On  $k$ -valued points  $f^n$  is given by  $(P_1, \dots, P_n) \mapsto \mathcal{L}(P_1) \otimes \dots \otimes \mathcal{L}(P_n) \otimes \mathcal{L}(P)^{-n}$ . Since  $f^n$  is symmetric, it induces a map  $f^{(n)} : C^{(n)} \rightarrow J$ .

Given a  $k$ -scheme  $T$ . We can pull back  $P \rightarrow C$  along  $C_T \rightarrow C$  to obtain a relative effective divisor on  $C_T$  of degree 1 over  $T$ .

We claim that, in terms of Cartier divisors  $f^{(n)}$  sends a relative effective Cartier divisor  $D$  on  $C_T$  of degree  $n$  over  $T$  to the class in  $J(T)$  represented by  $\mathcal{O}_{C_T}(D) \otimes \mathcal{O}_{C_T}(P_T)^{-n}$ , in short

$$f^{(n)}(D) = \mathcal{O}_{C_T}(D) \otimes \mathcal{O}_{C_T}(P_T)^{-n} \quad \text{for all } D \in C^{(n)}(T). \quad (19)$$

To see this, note that (19) defines a natural transformation between the functors represented by  $C^{(n)}$  and  $\text{Pic}_{C/k}$ . Thus, there exists a morphism  $\widetilde{f^{(n)}} : C^{(n)} \rightarrow \text{Pic}_{C/k}$  that on  $T$ -valued points is given by (19). Since  $C^{(n)}$  is connected and  $\widetilde{f^{(n)}}$  sends  $nP \in C^{(n)}(k)$  to zero, we can consider  $\widetilde{f^{(n)}}$  as a map to  $J = \text{Pic}_{C/k}^0$ . It remains to be proven that  $\widetilde{f^{(n)}} = f^{(n)}$ . We know by proposition 2.5 that  $C^{(n)}$  is reduced, so looking at the locus where  $\widetilde{f^{(n)}}$  and  $f^{(n)}$  agree, as in [3, 10.2. A], it suffices to proof that they induce the same map on  $\bar{k}$  valued points. But this readily follows from equation (17).

Via the description of  $f^{(n)}$  in 19 in the case that  $T = k$ , we see that the  $k$ -valued points of the fibre of  $f^{(n)}$  containing  $D \in C^{(n)}(k)$  will correspond to the complete linear system  $|D|$ . The set  $|D|$  is in natural bijection with  $(\Gamma(X, \mathcal{O}(D)) \setminus \{0\})/k^\times$  via  $D + (f) \mapsto \{\lambda f \mid \lambda \in k^\times\}$ . This observation on  $k$ -valued points has a scheme-theoretic reformulation.

**Theorem 2.7** (Abel's theorem). Let  $\mathcal{L}$  be a line bundle of degree  $n$  on  $C$ . Then the scheme-theoretic fibre of  $f^{(n)} : C^{(n)} \rightarrow J$  over the point  $p \in J(k)$  represented by  $\mathcal{L} \otimes \mathcal{L}(P)^{-n} \in \text{Pic}^0(C)$  is

$$f^{(n)-1}(p) = \mathbb{P}(H^0(C, \mathcal{L})) := \text{Proj}(\text{Sym}(H^0(C, \mathcal{L}))) \cong \mathbb{P}_k^m,$$

for  $m = h^0(C, \mathcal{L}) - 1$ .

*Proof.* Write  $\Phi \subseteq C^{(n)}$  for the scheme-theoretic fibre of  $f^{(n)}$  over  $p$  and let  $\mathbb{P} := \mathbb{P}(H^0(C, \mathcal{L}))$ . Let  $g : T \rightarrow \text{Spec}(k)$  be a  $k$ -scheme and consider the cartesian diagram

$$\begin{array}{ccc} C_T & \xrightarrow{\text{pr}_C} & C \\ \downarrow \text{pr}_T & & \downarrow h \\ T & \xrightarrow{g} & \text{Spec}(k) \end{array}.$$

Considering the functors represented by  $J$  and  $C^{(n)}$  we get natural isomorphisms

$$\begin{aligned} \Phi(T) &\cong \{D \subseteq C_T \text{ rel. eff. divisor of degree } n \text{ over } T \text{ with } \mathcal{O}_{C_T}(D) \cong \text{pr}_C^* \mathcal{L} \mod \text{pr}_T^* \text{Pic}(T)\} \\ &\cong \left\{ \begin{array}{l} \text{isomorphism classes } (\mathcal{L}', s) \text{ with } s \in H^0(C_T, \mathcal{L}') \text{ such that} \\ \mathcal{L}'/s\mathcal{O}_{C_T} \text{ is flat over } \mathcal{O}_T \text{ and } \exists M \in \text{Pic}(T) \text{ with } \mathcal{L}' = \text{pr}_C^* \mathcal{L} \otimes \text{pr}_T^* M \end{array} \right\} \end{aligned} \quad (20)$$

By definition,  $\mathbb{P} = \text{Proj}(\text{Sym}((h_*\mathcal{L})))$ , which is isomorphic to  $\mathbb{P}_k^m$ .  $T$ -valued points of such a projective space can be described as follows:

A map  $T \rightarrow \mathbb{P}$  is given by a line bundle  $M$  on  $T$  together with a surjective homomorphism of  $\mathcal{O}_T$  modules  $t : g^*((h_*\mathcal{L})) \rightarrow M$ , where two such pairs  $(M, t)$  and  $(M, t')$  are considered equivalent if there exists an isomorphism  $\alpha : M \xrightarrow{\sim} M'$  with  $\alpha \circ t = t'$ .

Such a map  $t$  determines and is determined by an element  $t \in H^0(T, (g^*h_*\mathcal{L}) \otimes M)$  such that  $t(x) \neq 0$  for all  $x \in T$ :

$g^*(h_*\mathcal{L})$  is non-canonically isomorphic to  $\mathcal{O}_T^{\oplus(m+1)}$ , therefore  $(g^*h_*\mathcal{L}) \otimes M$  is isomorphic to  $M^{\oplus(m+1)}$ . Since  $M$  is a line bundle, a homomorphism  $\mathcal{O}_T^{\oplus(m+1)}$  is determined by  $(m+1)$  sections in  $M$  and the map being surjective translates to the non-vanishing condition via Nakayama's Lemma.

By flat base change along  $g$  we have a canonical isomorphism  $g^*h_*\mathcal{L} \cong \text{pr}_{T*}\text{pr}_C^*\mathcal{L}$ .

By the projection formula the canonical map  $\text{pr}_{T*}(\text{pr}_C^*\mathcal{L} \otimes \text{pr}_T^*M) \rightarrow (\text{pr}_{T*}\text{pr}_C^*\mathcal{L}) \otimes M$  is an isomorphism.

We get the following isomorphism that is natural in  $T$ :

$$\begin{aligned} H^0(T, (g^*h_*\mathcal{L}) \otimes M) &\cong H^0(T, (\text{pr}_{T*}\text{pr}_C^*\mathcal{L}) \otimes M) \cong H^0(T, \text{pr}_{T*}(\text{pr}_C^*\mathcal{L} \otimes \text{pr}_T^*M)) \\ &= H^0(C_T, \text{pr}_C^*\mathcal{L} \otimes \text{pr}_T^*M) \end{aligned} \quad (21)$$

And we conclude

$$\mathbb{P}(T) \cong \left\{ \begin{array}{l} \text{isomorphism classes } (M, \text{pr}_{T*}s) \text{ with } s \in H^0(C_T, \text{pr}_C^*\mathcal{L} \otimes \text{pr}_T^*M) \\ \text{and } (\text{pr}_{T*}s)(x) \neq 0 \text{ for all } x \in T \end{array} \right\} \quad (22)$$

It can be checked that the isomorphism in (21) lets the notion of isomorphism classes of pairs in (20) and (22) coincide, if one identifies the appearing sets  $\mathbb{P}(T)$  and  $\Phi(T)$  in the canonical way. We omit the proof that the notion of flatness in (20) matches up with the notion of non vanishing in (22).

We have proved that  $\Phi(T)$  and  $\mathbb{P}(T)$  are isomorphic, naturally in  $T$ , and conclude  $\Phi \cong \mathbb{P}$  by the Yoneda-Lemma.  $\square$

**Theorem 2.8** (Jacobi's inversion theorem). For  $0 \leq n \leq g$  the morphism  $f^{(n)} : C^{(n)} \rightarrow J$  is birational onto its scheme-theoretic image, denoted  $W^n$ , which is irreducible. For  $n \geq g$  the morphism  $f^{(n)}$  is surjective. In particular,  $f^{(g)} : C^{(g)} \rightarrow J$  is a birational equivalence.

*Proof.* Note that since  $f^{(n)}$  is proper the scheme theoretic image agrees with the set-theoretic image on the level of sets, so the assertion for the case  $n = g$  follows from the other two statements. Further,  $W^n$  is irreducible as image of the irreducible topological space  $C^{(n)}$  under the continuous map  $f^{(n)}$ .

Whether a morphism is surjective or birational can be detected after quasi-compact, faithfully flat base change, see [14, B.2].  $(C^{(n)})_{\bar{k}}$  represents the functor  $\text{Div}_{C_{\bar{k}}/\bar{k}}^{\text{eff}, n}$  and  $J_{\bar{k}}$  represents the functor  $\text{Pic}_{C_{\bar{k}}/\bar{k}}^0$  and moreover the formation of  $f^{(n)}$  commutes with base change to  $\bar{k}$ . This can be seen by checking the given definitions of these functors. Hence, we may assume that  $k$  is algebraically closed.

For proving surjectivity, it suffices to show that the map is surjective on  $k$  valued points. Let  $n \geq g$ . For any  $\mathcal{L} \in \text{Pic}^0(C) = J(k)$  the Riemann-Roch theorem implies that  $\mathcal{L} \otimes \mathcal{L}(P)^n$  is effective, and therefore  $\mathcal{L}$  is in the image of  $f^{(n)}$ .

Now assume  $0 \leq n \leq g$ . We try to find a non-empty open set  $U \subseteq C^{(n)}$  where the fibers of  $f^{(n)}$  are zero-dimensional. Since the dimension of the fibers change in an upper-semicontinuous manner on the domain, it suffices by Abel's theorem 2.7 to find an effective divisor  $D$  of degree  $n$  on  $C$  such that  $h^0(C, \mathcal{O}_C(D)) = 1$ . We proceed by induction on  $n \leq g$ . For  $n = 1$  the assertion follows, because  $h^0(C, \mathcal{L}(P)) = 1$  using that  $g > 0$  and a meromorphic function with exactly one zero would define an isomorphism  $C \rightarrow \mathbb{P}_k^1$ . Suppose then that  $2 \leq n \leq g$  and that we have an effective divisor  $E$  of degree  $n - 1$  with  $h^0(E) = 1$ . Let  $K = \Omega_C^1$  be the canonical divisor on  $C$ . By Serre duality  $h^1(K - E) = 1$  and so by the Riemann-Roch theorem

$$h^0(K - E) - 1 = 1 - g + \deg(K - E) = 1 - g + (2g - 2) - (n - 1) = g - n \geq 0. \quad (23)$$



Thus  $[K - E]$  is effective. Choose a point  $Q \in C(k)$  which is not a base point of the linear system  $|K - E|$ . Then  $h^0(K - E - Q) = h^0(K - E) - 1 \stackrel{23}{=} g - n$ , where the first equality follows from  $[K - E]$  being effective because there is no meromorphic function  $f \in K(C)$ , whose only pole is  $Q$ , since else  $f$  would define an isomorphism  $C \rightarrow \mathbb{P}^1$ .

Thus, by the Riemann-Roch theorem and then Serre duality

$$h^0(E + Q) = 1 - g + n + h^1(E + Q) = 1 - g + n + h^0(K - E - Q) = 1.$$

This proves there exists  $\emptyset \neq U \subseteq C^{(n)}$  such that  $f^{(n)}|_U : U \rightarrow J$  has only zero-dimensional fibers. By Abel's theorem 2.7 the non-empty fibers of  $f^{(n)}|_U$  over  $k$ -valued points are isomorphic to  $\mathbb{P}_k^0 \cong \text{Spec}(k)$ .

By [3, 10.1.P] a morphism of finite type schemes over an algebraically closed field  $k$  is universally injective if and only if the induced map on  $k$  valued points is injective. We conclude from the above paragraph that that  $f|'_U : U' \rightarrow W^n$  is indeed universally injective. In particular, the field extension  $k(C^{(n)})/k(W^n) = k(U)/k(W^n)$  is purely inseparable, see [1, Tag 01S2].

The morphism  $f^{(n)} : C^{(n)} \rightarrow W^n$  is surjective and closed. Hence  $\dim C^{(n)} \geq \dim W^n$ . But on the other hand, taking  $p \in U$  and  $q = f^{(n)}(p)$ , we see that  $\dim C^{(n)} \leq \dim W^{(n)} + \dim(f^{(n)})^{-1}(Q) = \dim W^{(n)}$ .

So,  $\dim W^n = \dim C^{(n)}$ , and the residue field extension  $k(C^{(n)})/k(W^n)$  is algebraic.

Since  $W^n$  is reduced and  $K$  algebraically closed, the field extension  $k(W^n)/k$  is separable. Similarly, the field extension  $k(C^{(n)})/k$  is separable. But then  $k(C^{(n)})/k(W^n)$  must be separable, too:

To see this take  $K$  a purely transcendental extension  $K/k$  such that  $K \subseteq k(W^n)$  and  $k(W^n)/K$  is separable algebraic. Then also  $k(C^{(n)})/K$  is separable, since  $k(C^{(n)})/k$  is. Hence

$$\begin{aligned} [k(C^{(n)}) : k(W^n)]_s [k(W^n) : K]_s &= [k(C^{(n)}) : K]_s = [k(C^{(n)}) : K] = [k(C^{(n)}) : k(W^n)] [k(W^n) : K] \\ &= [k(C^{(n)}) : k(W^n)] [k(W^n) : K]_s, \end{aligned}$$

therefore  $k(C^{(n)})/k(W^n)$  is separable and algebraic. We have already proven that this field extension is purely inseparable and the only way to not obtain a contradiction is  $[k(C^{(n)}) : k(W^n)] = 1$ , i.e.  $f^{(n)} : C^{(n)} \rightarrow W^n$  is birational. □

We define the theta divisor by  $\Theta := W^{g-1} \subseteq J$ . By theorem 2.8  $\Theta$  is indeed a divisor on  $J$ .

## 2.3 The Jacobian as Albanese variety

Throughout this section  $C$  will again be a proper nonsingular curve of genus  $g > 0$  over a field  $k$ ,  $J$  will be its Jacobian variety and  $P \in C(k)$  will be a  $k$ -rational point. We will continue with all notations from the previous section. In particular, the definition of  $f$  from (2.1).

**Proposition 2.9** (Universal property of the canonical map  $f : C \rightarrow J$ ). For any map  $g : C \rightarrow X$  from  $C$  into an abelian variety  $X$  sending  $P$  to 0, there is a unique homomorphism  $h : J \rightarrow X$  such that  $g = h \circ f$ .

*Proof.* Consider the map  $g^g : C^g \rightarrow X$  that on points is given by  $(P_1, \dots, P_g) \mapsto \sum_{i=1}^g g(P_i)$ . Since this is symmetric, it factors as  $g^{(g)} \circ \pi = g^g$  for  $g^{(g)} : C^{(g)} \rightarrow X$  and  $\pi : C^g \rightarrow C^{(g)}$  the canonical morphism. Now by Jacobi's Inversion theorem 2.8 we obtain a rational map  $h : J \rightarrow X$  such that  $h \circ f^{(g)} = g^{(g)}$ , where this expression is defined. But a rational map from a smooth variety  $J$  to an abelian variety  $X$  is defined on the whole of  $J$ , by [6, Thm. 3.1]. Let  $\varphi : C \rightarrow C^{(g)}$  on closed points be given by  $Q \mapsto \pi(Q, P, \dots, P)$ . Then  $f = f^{(g)} \circ \varphi$  and therefore  $h \circ f = h \circ f^{(g)} \circ \varphi = g^{(g)} \circ \varphi = g$ . In particular,  $h$  sends 0 to 0, and corollary 1.2 shows it is a homomorphism.

If  $h'$  is another such homomorphism, then  $h' \circ f^g = h \circ f^g$ . Since  $X$  is separated,  $J$  is reduced and  $f^g$  is surjective by theorem 2.8, we must have  $h = h'$ . (This is because the "coincidence scheme" of  $h$  and  $h'$ , as in [7, 7.4 ex. 3], equals  $J$ .) □

**Corollary 2.10.** Let  $C_1$  and  $C_2$  be nonsingular, proper curves over  $k$ ,  $P_1 \in C_1(k)$  and  $P_2 \in C_2(k)$  be their Jacobians. Let  $f^{P_i} : C_i \rightarrow J_i$  be the canonical maps from section 2.1. The map

$\text{Hom}_k(J_1, J_2) \rightarrow \{\mathcal{L} \in \text{Pic}(C_2 \times C_1) : \mathcal{L}|_{C_2 \times \{P_1\}} \text{ and } \mathcal{L}|_{\{P_2\} \times C_1} \text{ are trivial}\}, h \mapsto (1_{C_2} \times (h \circ f^{P_1}))^* \mathcal{M}^{P_2}$

is an isomorphism.

*Proof.* The map is well-defined because  $\mathcal{M}^{P_2}|_{\{P_2\} \times C_2}$  and  $\mathcal{M}^{P_2}|_{C_2 \times \{0\}}$  is trivial by definition of  $\mathcal{M}^{P_2}$  in section 2.1, (also see proposition 1.12).

Now given  $\mathcal{L} \in \text{Pic}(C_2 \times C_1)$  such that both  $\mathcal{L}|_{C_2 \times \{P_1\}}$  and  $\mathcal{L}|_{\{P_2\} \times C_1}$  are trivial. Since  $\mathcal{M}^{P_2}$  is the universal bundle on  $C_2 \times J_2$  from proposition 1.12, there is a unique map  $g : C_1 \rightarrow J_2$  such that  $(1_{C_2} \times g)^* \mathcal{M}^{P_2} \cong \mathcal{L}$ . It follows from diagram 10 that  $g(P_1)$  is represented by  $\mathcal{L}|_{C_2 \times P_1}$  which is trivial. Hence  $g$  sends  $P_1$  to 0 and by proposition 2.9 there exists a unique homomorphism  $h : J_1 \rightarrow J_2$  such that  $g = h \circ f^{P_1}$ .  $\square$

## 2.4 Autoduality

Let  $\mathcal{P}$  denote the Poincaré bundle on  $J \times J^\vee$ .

Consider the Mumford line bundle  $\Lambda(\mathcal{L}(\Theta)) = m^* \mathcal{L}(\Theta) \otimes \text{pr}_1^* \mathcal{L}(\Theta)^{-1} \otimes \text{pr}_2^* \mathcal{L}(\Theta)^{-1}$  on  $J \times J$  from section 1.1.2. We obtain a polarization  $\varphi_{\mathcal{L}(\Theta)} : J \rightarrow J^\vee$  with  $(1 \times \varphi_{\mathcal{L}(\Theta)})^* \mathcal{P} \cong \Lambda(\mathcal{L}(\Theta))$ .

Write  $\Theta^-$  for the pullback of  $\Theta$  along  $(-1)_J : J \rightarrow J$  and  $\Theta_a$  for  $t_{-a}^* \Theta = \Theta + a$ ,  $a \in J(k)$ .

**Remark 2.11.** It is shown in [4, 14.22 and 14.28 (ii)] that  $\Theta$ ,  $\Theta^-$  and  $\Theta_a$  are numerically equivalent and this implies that  $\varphi_{\mathcal{L}(\Theta)} = \varphi_{\mathcal{L}(\Theta^-)} = \varphi_{\mathcal{L}(\Theta_a)}$  for all  $a \in J(k)$  by [4, 7.26].

In particular, by lemma 1.8 the divisors  $n^* \Theta$  and  $n^2 \Theta$  are numerically equivalent for all  $n \in \mathbb{Z}$ .

We abbreviate  $(\Theta^-)_a$  as  $\Theta_a^-$ .

Consider the invertible sheaf  $(f \times 1)^* \mathcal{P}$  on  $C \times J^\vee$ . Its restriction to  $\{P\} \times J^\vee$  is trivial because  $f(P) = 0$  and  $\mathcal{P}$  restricted to  $\{0\} \times J^\vee$  is trivial. Applying proposition 1.12 to the universal bundle  $\mathcal{M}^P$  on  $C \times J$  we obtain a unique morphism  $f^\vee : J^\vee \rightarrow J$  such that  $(f \times 1)^* \mathcal{P} \cong (1 \times f^\vee)^* \mathcal{M}^P$ .

**Theorem 2.12.** The maps  $-f^\vee : J^\vee \rightarrow J$  and  $\varphi_{\mathcal{L}(\Theta)} : J \rightarrow J^\vee$  are inverses.

*Proof.*  $(J^\vee)_{\bar{k}}$  represents  $(J_{\bar{k}})^\vee$  and  $J_{\bar{k}}$  represents  $\text{Pic}_{C_{\bar{k}}/\bar{k}}^0$ , moreover the formation of  $f$  and therefore also the formation of  $\Theta$ ,  $\varphi_{\mathcal{L}(\Theta)}$  and  $f^\vee$  commutes with base change to  $\bar{k}$ . Whether a morphism is an isomorphism can be detected after faithfully flat, quasi-compact base change by [14, B.2].

Therefore we may assume that  $k$  is algebraically closed.

Let  $U$  be the largest open subset of  $J$  such that:

- (i) the fiber of  $f^{(g)} : C^{(g)} \rightarrow J$  at any point of  $U$  has dimension zero; and
- (ii) if  $a \in U(k)$  and  $D(a)$  is the, by Abel's theorem necessarily unique, element of  $C^{(g)}(k)$  mapping to  $a$ ; then  $D(a)$  is a sum of  $g$  distinct points of  $C(k)$ .

Note that  $U$  can be obtained in two steps: First, by removing the subset over which the fibers have dimension  $> 0$ , which is closed because the fiber dimension changes upper-semi-continuously on the target. (Note that  $f^{(g)}$  is proper and see [3, 11.4.2]). Secondly, by removing images of certain closed sets of the form  $\Delta_C \times C^{g-2}$  under the proper map  $f^g$ . The first step yields a nonempty open set by (the proof of) Jacobi's inversion theorem 2.8. In the second step a proper closed subset of  $J$  gets removed, so, by irreducibility of  $J$  the set  $U$  is a nonempty open dense subset of  $J$ .

$$\textbf{Claim: } f^{-1}(\Theta_a^-) = D(a) \text{ for all } a \in U(k) \quad (24)$$

Let  $a \in U(k)$  and let  $D(a) = \sum_{i=1}^g P_i$  with  $P_i \neq P_j$  for all  $i \neq j$ . A point  $Q_1$  maps to  $\Theta_a^-$  if and only if there exists a divisor  $\sum_{i=2}^g Q_i$  on  $C$  such that  $f(Q_1) = -\sum_{i=2}^g Q_i + a$ . This equality implies  $\sum_{i=1}^g Q_i \sim D$ , and the fact that  $|D|$  has dimension 0 by Abel's theorem 2.7 implies that  $\sum_{i=1}^g Q_i = D$ . It follows that the support of  $f^{-1}(\Theta_a^-)$  is  $\{P_1, \dots, P_g\}$ , and it remains to show that  $f^{-1}(\Theta_a^-)$  has degree  $\leq g$  for all  $a \in U(k)$ .

Consider the map  $\Psi : C \times \Theta \rightarrow J$  sending  $(Q, b)$  to  $f(Q) + b$ . By Jacobi's inversion theorem 2.8 and proposition 2.5, the maps  $f^{g-1} : C^{g-1} \rightarrow \Theta$  and  $f^g : C^g \rightarrow J$  have degree  $(g-1)!$  and  $g!$  respectively. As,  $\Psi$  composed with  $1 \times f^{g-1} : C \times C^{g-1} \rightarrow C \times \Theta$  is  $f^g$ , we conclude that  $\Psi$  has degree  $g$ . Also,  $\Psi$  is proper as  $C \times \Theta$  is a proper variety and therefore  $\Psi' := \Psi|_{\Psi^{-1}(V)}$  is proper and quasi-finite, hence finite. Moreover,  $\Psi'$  is flat by [3, 26.2.11] using that  $C \times \Theta$  and  $J$  are regular of dimension  $g$ . It follows as in the proof of theorem 1.4 that all fibers of  $\Psi'$  have global sections a  $g$  dimensional  $k$  vector space. In particular, all fibers have less then  $g$  points. But for  $a \in U$  the  $k$  valued points of  $\Psi^{-1}(a)$  are exactly the  $k$  valued points of  $f^{-1}(\Theta_a^-)$  and the claim follows.

**Claim:** (i) Let  $a \in J(k)$ , and let  $f^{(g)}(D) = a$ ; then  $f^* \mathcal{L}(\Theta_a^-) \cong \mathcal{L}(D)$ . (25)

(ii) The sheaves  $(f \times (-1))_*^* \Lambda(\mathcal{L}(\Theta^-))$  and  $\mathcal{M}^P$  on  $C \times J$  are isomorphic. (26)

Note that the map

$$C \xrightarrow{Q \mapsto (Q, a)} C \times \{a\} \xrightarrow{f \times (-1)} J \times J \xrightarrow{m} J$$

equals  $t_{-a} \circ f$ , where  $t_{-a}$  is the translation on  $J$  by  $a$ . Therefore

$$(f \times (-1))^* m^* \mathcal{L}(\Theta^-)|_{C \times \{a\}} \cong (t_{-a} \circ f)^* \mathcal{L}(\Theta^-) \cong f^* \mathcal{L}(\Theta_a^-)$$

On the other hand,  $\mathcal{M}^P$  is an invertible sheaf on  $C \times J$  such that

- a)  $\mathcal{M}^P|_{C \times \{a\}} \cong \mathcal{L}(D - gP)$  if  $D$  is an effective divisor of degree  $g$  on  $C$  such that  $f^{(g)}(D) = a$  (see the definition of  $f$ ).
- b)  $\mathcal{M}^P|_{\{P\} \times J}$  is trivial (see the definition of  $\mathcal{M}^P$ ).

Hence,  $\mathcal{M}^P \otimes \text{pr}_1^* \mathcal{L}(gP)|_{C \times \{a\}}$  is isomorphic to  $\mathcal{L}(D)$ , whenever  $f^{(g)}(D) = a$  for  $D \in C^{(g)}(k)$  an effective divisor of degree  $g$  on  $C$ . Hence (i) is equivalent to  $(f \times (-1))^* m^* \mathcal{L}(\Theta^-)|_{C \times \{a\}}$  being isomorphic to  $\mathcal{M}^P \otimes \text{pr}_1^* \mathcal{L}(gP)|_{C \times \{a\}}$  for all  $a \in J(k)$ . By claim 24 we know that (i) holds on a nonempty dense open and therefore

$$\mathcal{N} := ((f \times (-1))^* m^* \mathcal{L}(\Theta^-)) \otimes (\mathcal{M}^P \otimes \text{pr}_1^* \mathcal{L}(gP))^{-1}$$

is trivial, when restricted to sets of the form  $C \times \{a\}$  for all  $a$  in a dense open subset of  $J$ .

The set of all  $a \in J$  such that  $\mathcal{N}$  restricted to  $C \times \{a\}$  is trivial is closed in  $J$ , by [6, 5.3]. (This is because on the proper variety  $C$  an invertible sheaf is trivial if and only if  $\mathcal{N}$  and its dual  $\mathcal{N}^{-1}$  have nonzero global sections; but the dimensions of global sections of  $\mathcal{N}|_{C \times \{a\}}$  and  $\mathcal{N}^{-1}|_{C \times \{a\}}$  vary in an upper-semicontinuous manner on  $J$  by [3, 28.1.1].) Because a closed set in  $J$  that contains a dense set is equal to  $J$ , we obtain that claim (i) holds.

Taking  $a = 0$  we obtain  $f^* \mathcal{L}(\Theta^-) \cong \mathcal{L}(gP)$  and therefore

$$(f \times (-1))^* \text{pr}_1^* \mathcal{L}(\Theta^-) \cong (f \circ \text{pr}_1)^* \mathcal{L}(\Theta^-) \cong \text{pr}_1^* \mathcal{L}(gP).$$

Now for all  $a \in J(k)$  the sheaves

$$(f \times (-1))^* \left( m^* \mathcal{L}(\Theta^-) \otimes (\text{pr}_1^* \mathcal{L}(\Theta^-))^{-1} \right)|_{C \times \{a\}}$$

and  $\mathcal{M}^P|_{C \times \{a\}}$  are isomorphic on  $C$ . Now by the so-called Seesaw principle [6, 5.1], which is a theorem on proper varieties, there exists an invertible sheaf  $\mathcal{F}$  on  $J$  such that

$$(f \times (-1))^* \left( m^* \mathcal{L}(\Theta^-) \otimes (\text{pr}_1^* \mathcal{L}(\Theta^-))^{-1} \right) \cong \mathcal{M}^P \otimes \text{pr}_2^* \mathcal{F}$$

On computing the restriction to  $\{P\} \times J$  of the above equation, we obtain

$$\mathcal{F} \cong (f \times (-1))^* \left( m^* \mathcal{L}(\Theta^-) \otimes (\text{pr}_1^* \mathcal{L}(\Theta^-))^{-1} \right)|_{\{P\} \times J} \cong (-1)^* \mathcal{L}(\Theta^-).$$

and therefore

$$\mathcal{M}^P \cong (f \times (-1))^* (m^* \mathcal{L}(\Theta^-) \otimes \text{pr}_1^* \mathcal{L}(\Theta^-)^{-1}) \otimes \text{pr}_2^* (-1)^* \mathcal{L}(\Theta^-)^{-1}$$

But  $(f \times (-1))^* \text{pr}_2^* \mathcal{L}(\Theta^-)^{-1} \cong \text{pr}_2^* (-1)^* \mathcal{L}(\Theta^-)^{-1}$  and therefore claim (ii) in equation 26 follows from the definition of  $\Lambda(\Theta^-)$

Now we are ready to proof the theorem: We have  $\varphi_{\mathcal{L}(\Theta)} = \varphi_{\mathcal{L}(\Theta^-)}$  and

$$\begin{aligned} (1 \times -\varphi_{\mathcal{L}(\Theta)})^* (1 \times f^\vee)^* \mathcal{M}^P &\cong (1 \times -\varphi_{\mathcal{L}(\Theta)})^* (f \times 1)^* \mathcal{P} \cong (f \times (-1))^* (1 \times \varphi_{\mathcal{L}(\Theta^-)})^* \mathcal{P} \\ &\cong (f \times (-1)^*) \Lambda(\mathcal{L}(\Theta^-)) \end{aligned}$$

and therefore by the claim in (26) we have  $(1 \times (-\varphi_{\mathcal{L}(\Theta)} \circ f^\vee))^* \mathcal{M}^P \cong \mathcal{M}^P$ .

Hence  $-\varphi_{\mathcal{L}(\Theta)} \circ f^\vee = \text{id}_{J^\vee}$  by definition of  $\mathcal{M}^P$  as the universal line bundle on  $C \times J$  and the uniqueness assertion in proposition 1.12. By theorem 1.4 both  $\varphi_{\mathcal{L}(\Theta)}$  and  $f^\vee$  are isogenies. Now their degree must be equal to one and the theorem follows from proposition 1.9.  $\square$

**Corollary 2.13.** a)  $(f \times (-1)_J)^* \Lambda(\mathcal{L}(\Theta)) \cong (f \times 1_J)^* \Lambda(\mathcal{L}(\Theta)^{-1}) \cong \mathcal{M}^P$  on  $C \times J$ .

b) For  $\mathcal{L}^P$  the sheaf on  $C \times C$  from equation (16) we have an isomorphism  $\mathcal{L}^P \cong (f \times f)^* \Lambda(\mathcal{L}(\Theta)^{-1})$ .

c) The divisor  $\Theta$  on  $J$  is ample and has self-intersection number  $(\Theta)^g = g!$ . Moreover,  $H^0(J, \mathcal{L}(\Theta)) = k$  and  $H^i(J, \mathcal{L}(\Theta)) = 0$  for  $i \geq 1$ .

*Proof.* We have

$$\begin{aligned} (f \times (-1)_J)^* \Lambda(\mathcal{L}(\Theta)) &\cong (f \times (-1)_J)^* (1_J \times \varphi_{\mathcal{L}(\Theta)})^* \mathcal{P} \cong (1_J \times -\varphi_{\mathcal{L}(\Theta)})^* (f \times 1_J)^* \mathcal{P} \\ &\cong (1_J \times -\varphi_{\mathcal{L}(\Theta)})^* (1 \times f^\vee)^* \mathcal{M}^P \cong (1_J \times (f^\vee \circ (-\varphi_{\mathcal{L}(\Theta)})))^* \mathcal{M}^P \stackrel{2.12}{=} \mathcal{M}^P \end{aligned}$$

Since  $\mathcal{L} \rightarrow \varphi_{\mathcal{L}}$ , as in equation (12), is a homomorphism, we have  $\varphi_{\mathcal{L}(\Theta)^{-1}} = -\varphi_{\mathcal{L}(\Theta)}$  and so

$$\mathcal{M}^P \cong (f \times 1_J)^* (1_J \times -\varphi_{\mathcal{L}(\Theta)})^* \mathcal{P} = (f \times 1_J)^* (1_J \times \varphi_{\mathcal{L}(\Theta)^{-1}})^* \mathcal{P} \cong (f \times 1_J)^* \Lambda(\mathcal{L}(\Theta)^{-1}).$$

Now b) follows from a) because  $(f \times f)^* \Lambda(\mathcal{L}(\Theta)^{-1}) \cong (1_C \times f)^* \mathcal{M}^P \cong \mathcal{L}^P$  by definition of  $f$ .

$\Theta$  is ample by lemma 1.13. By the vanishing theorem for line bundles on abelian varieties from [4, prop. 9.14] we have  $H^i(J, \Theta) \neq 0$  only for  $i = 0$ . By the Riemann-Roch theorem for abelian varieties as in [4, thm. 9.11]  $\chi(\mathcal{L}(\Theta))^2 = \deg(\varphi_{\mathcal{L}(\Theta)}) = 1$  and  $(\Theta)^g = g! \cdot \chi(\mathcal{L}(\Theta)) = g!$ , so c) follows.  $\square$

## 2.5 The Rosati involution

**Definition 2.14.** The Rosati involution corresponding to  $\varphi_{\mathcal{L}(\Theta)}$  is defined as the involution on  $\text{End}^0(J)$  given by

$$h \mapsto h^\dagger := \varphi_{\mathcal{L}(\Theta)}^{-1} \circ h^\vee \circ \varphi_{\mathcal{L}(\Theta)} = f^\vee \circ h^\vee \circ \varphi_{\mathcal{L}(\Theta)^{-1}}.$$

Let  $g, h \in \text{End}^0(J)$ . It is clear from the definition that  $(hg)^\dagger = g^\dagger h^\dagger$  and because  $(h + g)^\vee = h^\vee + g^\vee$  also  $(h + g)^\dagger = h^\dagger + g^\dagger$ . Moreover,  $g^\dagger = g$  if  $g \in \mathbb{Q}$ .

Let  $\sigma : C \times C \rightarrow C \times C$  be the  $k$  morphism that switches the above factors. Then  $\sigma$  acts on

$$F := \{ \mathcal{L} \in \text{Pic}(C \times C) : \mathcal{L}|_{C \times \{P\}} \text{ and } \mathcal{L}|_{C \times \{P\}} \text{ is trivial} \}$$

by pullback. By corollary 2.10 this corresponds to an action on  $\text{End}(J)$ .

**Lemma 2.15.** The action on  $F$  by  $\sigma$  agrees with the Rosati involution when  $F$  is identified with  $\text{End}(J)$  via the isomorphism in corollary 2.10.

*Proof.* Let  $h \in \text{End}(J)$ . Since

$$\begin{aligned}
(1_C \times (h^\dagger \circ f))^* \mathcal{M}^P &= (1_C \times (f^\vee \circ h^\vee \circ \varphi_{\mathcal{L}(\Theta)^{-1}} \circ f))^* \mathcal{M}^P \cong (1 \times h^\vee \circ \varphi_{\mathcal{L}(\Theta)^{-1}} \circ f)^*(1 \times f^\vee)^* \mathcal{M}^P \\
&\cong (1 \times h^\vee \circ \varphi_{\mathcal{L}(\Theta)^{-1}} \circ f)^*(f \times 1)^* \mathcal{P} \cong (f \times 1)^*(1 \times \varphi_{\mathcal{L}(\Theta)^{-1}} \circ f)^*(1 \times h^\vee)^* \mathcal{P} \\
&\cong (f \times 1)^*(1 \times \varphi_{\mathcal{L}(\Theta)^{-1}} \circ f)^*(h \times 1)^* \mathcal{P} \\
&\cong ((h \circ f) \times 1)^*(1 \times f)^*(1 \times \varphi_{\mathcal{L}(\Theta)^{-1}})^* \mathcal{P} \cong ((h \circ f) \times 1)^*(1 \times f)^* \Lambda(\mathcal{L}(\Theta)^{-1}) \\
&\stackrel{2.13}{\cong} ((h \circ f) \times 1)^* \mathcal{M}^P \cong \sigma^*(1_C \times (h \circ f))^* \mathcal{M}^P,
\end{aligned}$$

the assertions follows from corollary 2.10.  $\square$

Since  $\sigma^2 = \text{id}$  we conclude from the previous lemma 2.15 that  $(h^\dagger)^\dagger = h$  for all  $h \in \text{End}(J)$ . Since  $g^\dagger = g$  for all  $g \in \mathbb{Q}$ , this result extends to  $\text{End}^0(J)$ .

## 2.6 The Lefschetz trace formula and positivity of the Rosati involution

We invoke intersection theory on the surface  $C \times C$ . Notation will be as in Hartshorne [8] chapter V.1 but we won't assume that  $k$  is necessarily algebraically closed. For effective divisors  $D, C$  on  $C \times C$  we define their intersection number  $C \cdot D := \deg_C \mathcal{L}_{C \times C}(D)|_C$  and extend this definition to a symmetric, bilinear map  $\text{Div}(C \times C) \times \text{Div}(C \times C) \rightarrow \mathbb{Z}$  that only depends on the linear equivalence class of the inputs. To see that there exists a unique such pairing consult [8, V1, Thm. 1.1].

**Theorem 2.16** (Lefschetz trace formula). Let  $h \in \text{End}(J)$  and let  $X$  be a divisor on  $C \times C$  such that  $\mathcal{L}(X) \cong (1_C \times (h \circ f))^* \mathcal{M}^P$ . Then the negative intersection number of the diagonal divisor  $\Delta_C \subseteq C \times C$  with  $X$  equals  $\text{tr}(h)$ , i.e.  $-\Delta_C \cdot X = \text{tr}(h)$ .

Before we can proof the theorem we need the following relation between trace and intersection theory on  $J$ .

**Lemma 2.17.** Let  $h \in \text{End}(J)$ . Let  $D_\Theta(h) := (h + 1)^* \Theta - h^* \Theta - \Theta$ . Then

$$\text{tr}(h) = \frac{g}{(\Theta^g)} (\Theta^{g-1} \cdot D_\Theta(h)) = \frac{1}{(g-1)!} (\Theta^{g-1} \cdot D_\Theta(h)) = (f(C) \cdot D_\Theta(h)) = \deg f^* \mathcal{L}(D_\Theta(h)).$$

*Sketch of a proof.* In the last paragraph of theorem 1.19 we computed, that for all  $n \in \mathbb{N}$  we have  $\deg(h + n) = \frac{(D_n)^g}{(D)^g}$ , where we can choose

$$D = \Theta, \quad D' = 2^* D - 2D, \quad D_n = (n + h)^* D = \frac{n(n-1)}{2} D' + n(h + 1)^* D - (n-1)h^* D.$$

By remark 2.11  $D'$  is numerically equivalent to  $2D$  and, so,  $D_n$  is numerically equivalent to  $n^2 D + n D_\Theta(h) + h^* D$ .

Since by definition  $P_h(-n) = \deg(h + n) = \frac{(D_n)^g}{(D)^g}$  for all  $n \in \mathbb{N}$  we have that  $\text{tr}(h)$  is the coefficient in front of  $n^{2g-1}$  in the expression  $\frac{(D_n)^g}{(D)^g}$ , which we can identify with  $\frac{g}{(D)^g} (D^{g-1} \cdot D_\Theta(h))$  by using the linearity of the intersection number.

We have proven the first equality of the assertion and the second follows from corollary 2.13.

To show that  $(\Theta^{g-1} \cdot D_\Theta(h)) = (g-1)!(f(C) \cdot D_\Theta(h))$  one proceeds as in [11, IV §3 Thm 5] to relate intersection numbers with taking sums of divisors via the addition of  $J$ . For this one considers the so-called Pontrjagin product  $*$  on the Chow ring of  $J$ ; its definition can be found in [11, p. 8]. It is shown in [11, II §3 prop. 4] that for the  $r$ -fold Pontrjagin product of  $f(C)$  one has  $f(C)^{*r} = r! W^r$ .

Further one shows that taking images (in the sense of intersection theory) under endomorphisms  $h : J \rightarrow J$  induces a endomorphism of the group of cycles of  $J$  with the Pontrjagin product. Whereas taking inverses images under  $h$  induces an endomorphism of the chow ring with the intersection product. These two operations are adjoint to each other:  $(h(\xi) \cdot \nu) = (\xi \cdot h^{-1}(\nu))$ . (This is [11, IV §3 Thm 5]).

Using the above two properties is can be computed that  $(\Theta^{g-1} \cdot D_\Theta(h)) = (g-1)!(W^1 \cdot D_\Theta(h))$ . This is done here [11, p.112].

Now it only remains to justify  $(f(C) \cdot D_\Theta(h)) = \deg f^* \mathcal{L}(D_\Theta(h))$ . This is [15, Exmp. 7.1.17].  $\square$

*Proof of theorem 2.16.* By Corollary 2.13 we have that

$$\begin{aligned}\Delta_C^* \mathcal{L}(X) &\cong \Delta_C^*(1_C \times (h \circ f)^*) \mathcal{M}^P \cong \Delta^*(1_C \times (h \circ f))^*(f \times 1_J)^* \Lambda(\mathcal{L}(\Theta))^{-1} \\ &\cong ((1_J \times h) \circ (f \times f) \circ \Delta_C)^* \Lambda(\mathcal{L}(\Theta))^{-1} \cong f^*(1_J, h)^* \Lambda(\mathcal{L}(\Theta))^{-1} \\ &= f^*(1_J, h)^*(m^* \mathcal{L}(\Theta)^{-1} \otimes \text{pr}_1^* \mathcal{L}(\Theta) \circ \text{pr}_2^* \mathcal{L}(\Theta)) = f^* D_\Theta(h)^{-1}\end{aligned}$$

So, by the previous lemma 2.17,  $\text{tr}(h) = \deg f^* D_\Theta(h) = \deg \Delta_C^* \mathcal{L}(X)^{-1} = \Delta_C.(-X) = -\Delta_C.X$ .  $\square$

**Corollary 2.18** (Positivity of the Rosati involution). Let  $h, g \in \text{End}(J)$  then

$$\text{tr}(h^\dagger \circ g) = \deg((h \circ f, g \circ f)^* \Lambda(\mathcal{L}(\Theta))) \text{ and } \text{tr}(h^\dagger \circ h) = 2 \deg((h \circ f)^* \mathcal{L}(\Theta)) = 2((h \circ f)(C) \cdot \Theta).$$

The *trace form*

$$\text{End}^0(J) \times \text{End}^0(J) \rightarrow \mathbb{Q}, (g, h) \mapsto \text{tr}(g \circ h^\dagger)$$

is bilinear, symmetric and positive definite.

*Proof.* It can be read of the proof of lemma 2.19 that  $(1_C \times h^\dagger)^* \mathcal{M}^p \cong ((h \circ f) \times 1)^* \Lambda(\mathcal{L}(\Theta))^{-1}$ . So, by the Lefschetz trace formula 2.16,

$$\begin{aligned}\text{tr}(h^\dagger \circ g) &= -\deg \Delta_C^*(1_C \times (h^\dagger \circ g \circ f)) = -\deg \Delta_C^*((h \circ f) \times (g \circ f))^* \Lambda(\mathcal{L}(\Theta))^{-1} \\ &= \deg((h \circ f, g \circ f)^* \Lambda(\mathcal{L}(\Theta))).\end{aligned}$$

In particular,  $\text{tr}(h^\dagger, h) = \deg((h \circ f, h \circ f)^* \Lambda(\mathcal{L}(\Theta)))$ . We compute

$$\begin{aligned}(h \circ f, h \circ f)^* \Lambda(\mathcal{L}(\Theta)) &= (h \circ f, h \circ f)^*(m^* \mathcal{L}(\Theta) \otimes \text{pr}_1^* \mathcal{L}(\Theta)^{-1} \otimes \text{pr}_2^* \mathcal{L}(\Theta)^{-1}) \\ &\cong (h \circ f)^*(2_J)^* \mathcal{L}(\Theta) - (h \circ f)^* \mathcal{L}(\Theta)^2\end{aligned}$$

and, since after taking degree only the numerical equivalence class of  $\Theta$  matters, we obtain

$$\deg((h \circ f, h \circ f)^* \Lambda(\mathcal{L}(\Theta))) = 2^2 \deg((h \circ f)^* \mathcal{L}(\Theta)) - 2 \deg((h \circ f)^* \mathcal{L}(\Theta))$$

by remark 2.11. So,  $\text{tr}(h^\dagger \circ h) = 2 \deg((h \circ f)^* \mathcal{L}(\Theta)) = 2((h \circ f)(C) \cdot \Theta)$ , where the last equality is by [15, Exmp. 7.1.17].

By lemma 2.15 and theorem 2.16  $\text{tr}(h^\dagger) = -\Delta_C.\sigma^* X = -\Delta_C.X = \text{tr}(h)$ . In particular, the trace form is symmetric. Bilinearity follows from linearity of the Rosati involution and the properties of the trace.

If  $h \neq 0$ , then  $Y := (h \circ f)(C)$  is a nontrivial integral closed subscheme of dimension 1 on  $J$ . By the Nakai-Moishezon criterion for ampleness, the intersection number  $(Y \cdot \Theta)$  is positive. In other words,  $\text{tr}(h^\dagger \circ h) > 0$ .  $\square$

## 2.7 The map induced on the Jacobian by an endomorphism of $C$

Throughout this section  $C$  will again be a proper non-singular curve of genus  $g > 0$  over a field  $k$ ,  $J$  will be its Jacobian variety and  $P \in C(k)$  will be a  $k$ -rational point.  $f$  will be defined as in section 2.1.

Let  $\alpha : C \rightarrow C$  be a non-constant  $k$ -morphism. Note that  $\alpha$  will necessarily be finite and flat.

There are two approaches to obtain a homomorphism  $J \rightarrow J$  induced by  $\alpha$ .

- a) Let  $t_{-f(\alpha(P))}$  be the translation on  $J$  by  $-f(\alpha(P))$ . Then  $t_{-f(\alpha(P))} \circ f \circ \alpha : C \rightarrow J$  maps  $P$  to 0 and by proposition 2.9 there is a unique homomorphism  $\alpha' : J \rightarrow J$  such that

$$t_{-f(\alpha(P))} \circ f \circ \alpha = \alpha' \circ f.$$

- b) For a given  $k$ -scheme  $T$  and  $\mathcal{L} \in \text{Pic}(C \times T)$  the map  $\mathcal{L} \mapsto (\alpha \times 1_T)^* \mathcal{L}$  is natural in  $T$  and therefore defines a map  $\text{Pic}_{C/k} \rightarrow \text{Pic}_{C/k}$ . Since the trivial line bundle in  $\text{Pic}_{C/k}(k)$  is sent to itself, this defines a homomorphism  $\alpha^* : J \rightarrow J$ .

Using that for  $\mathcal{L} \in \text{Pic}(C \times T)$  the degree function  $T \ni t \mapsto \deg(\mathcal{L}|_{C \times \{t\}})$  is locally constant, it can be shown that  $J(k)$  can be identified with  $\text{Pic}^0(C)$ , the degree 0 line bundles on  $C$ , see [4, 14.1]. So,  $\alpha^*$  is on  $k$ -valued points literally given by the pullback of degree 0 line bundles along  $\alpha$ .

The following lemma says that the Rosati involution translates one approach into the other. In particular,  $\alpha'$  is independent of the choice of  $P$ .

**Lemma 2.19.** We have  $(\alpha')^\dagger = \alpha^*$  as  $k$ -morphisms  $J \rightarrow J$  and

$$(1 \times (\alpha' \circ f))^* \mathcal{M}^P \cong \sigma^* \mathcal{L}(\Gamma_\alpha - C \times \{\alpha(P)\} - \alpha^{-1}(P) \times C),$$

for  $\sigma : C \times C \rightarrow C \times C$  the morphism that switches the factors.

*Proof.* The sheaf  $\mathcal{C} = \mathcal{L}(\Gamma_\alpha - C \times \{\alpha(P)\} - \alpha^{-1}(P) \times C)$  on  $C \times C$  is trivial, when restricted to  $C \times \{P\}$ , as well as, when restricted to  $\{P\} \times C$ .

By proposition 1.12 applied to  $\mathcal{M}^P$  we obtain a unique  $k$ -morphism  $g : C \rightarrow J$  such that  $(1_C \times g)^* \mathcal{M}^P \cong \mathcal{C}$ . Let  $K$  be a field extension of  $k$ . By diagram 10 for  $K$ -valued point  $R$  of  $C$  with inclusion  $R \xrightarrow{x} C$  we have  $g(R)$  is represented by  $(1 \times x)^* \mathcal{C} \cong \mathcal{L}_{C_K}(\alpha^{-1}(R)) \otimes \mathcal{L}_{C_K}(\alpha^{-1}(P))^{-1} \cong \alpha^* \mathcal{L}_{C_K}(R - P)$ . Since  $g(P) = 0$  there is a homomorphism  $h : J \rightarrow J$  such that  $g = h \circ f$ . Now  $f(R)$  is represented by  $\mathcal{L}_{C_K}(R - P)^{-1}$  by equation (17). We conclude that  $h \circ f^g$  and  $\alpha^* \circ f^g$  agree on  $K$  valued points. It follows as in the last paragraph of the proof of proposition 2.9 that  $h = \alpha^*$ . By corollary 2.10 it therefore suffices to proof that  $(1_C \times (\alpha' \circ f))^* \mathcal{M}^P \cong \sigma^* \mathcal{C}$ , we win by direct computation:

$$\begin{aligned} (1_C \times (\alpha' \circ f))^* \mathcal{M}^P &= (1_C \times (t_{-f(\alpha(P))} \circ f \circ \alpha))^* \mathcal{M}^P \cong (1_C \times \alpha)^* (1 \times (t_{-f(\alpha(P))} \circ f))^* \mathcal{M}^P \\ &\cong (1_C \times \alpha)^* \mathcal{L}(\Delta - \{\alpha(P)\} \times C - C \times \{P\}) \\ &\cong \mathcal{L}(\sigma^{-1} \Gamma_\alpha - \{\alpha(P)\} \times C - C \times \alpha^{-1}(P)) \\ &\cong \sigma^* \mathcal{L}(\Gamma_\alpha - C \times \{\alpha(P)\} - \alpha^{-1}(P) \times C), \end{aligned}$$

where  $(t_{-f(\alpha(P))} \circ f)^* \mathcal{M}^P \cong \mathcal{L}(\Delta - \{\alpha(P)\} \times C - C \times \{P\})$  because the unique map  $\varphi : C \rightarrow J$  such that  $(1 \times \varphi)^* \mathcal{M}^P \cong \mathcal{L}(\Delta - \{\alpha(P)\} \times C - C \times \{P\})$  agrees with  $t_{-f(\alpha(P))} \circ f$ . Note that this can be checked on  $\overline{K}$ -valued points and  $\varphi$  can be computed on these points via diagram 10.  $\square$

We now try to relate  $\text{tr}(\alpha') = \text{tr}(\alpha^*)$  with the fixed points of  $\alpha$ .

**Theorem 2.20** (Lefschetz fixed point formula). We have  $\Delta_C \cdot \Gamma_\alpha = 1 - \text{tr}(\alpha^*) + \deg(\alpha)$ .

*Proof.* By lemma 2.19 we have  $(1 \times (\alpha^* \circ f))^* \mathcal{M}^P \cong \mathcal{L}(\Gamma_\alpha - C \times \{\alpha(P)\} - \alpha^{-1}(P) \times C)$  and so by the Lefschetz trace formula 2.16

$$\text{tr}(\alpha^*) = -\Delta_C \cdot (\Gamma_\alpha - C \times \{\alpha(P)\} - \alpha^{-1}(P) \times C) = -\Delta_C \cdot \Gamma_\alpha + 1 + \Delta_C \cdot (C \times \alpha^{-1}(P)).$$

Since  $\Delta_C$  and  $C \times \alpha^{-1}(P)$  have no components in common and have scheme-theoretic intersection  $\alpha^{-1}(P)$  we conclude  $\Delta_C \cdot (C \times \alpha^{-1}(P)) = h^0(\alpha^{-1}(P), \mathcal{O}_{\alpha^{-1}(P)})$ . Because  $\alpha$  is flat and finite,  $\deg \alpha = h^0(\alpha^{-1}(P), \mathcal{O}_{\alpha^{-1}(P)})$  by exactly the same proof as in theorem 1.4.  $\square$

**Example 2.21.** Applying the Lefschetz fixed point formula to  $\text{id}_C$  yields  $\Delta_C^2 = 1 - 2g - 1$ .

The interpretation of theorem 2.20 as fixed point formula is justified by the following proposition.

**Proposition 2.22.** Assume  $k$  to be algebraically closed. Let  $\alpha : C \rightarrow C$  be non-constant such that

a)  $\alpha(x) = x$  for only finitely many  $x \in C(k)$  and

b)  $d_x \alpha \neq \text{id}_{T_x C}$  for all  $x \in C(k)$  with  $\alpha(x) = x$ ,

then  $\Gamma_\alpha \cdot \Delta_C = \#\{x \in C(k) : \alpha(x) = x\}$ .

*Proof.* Condition a) implies  $(\Delta_C \times_{C \times C} \Gamma_\alpha)(k) = \{x \in C(k) : \alpha(x) = x\} < \infty$ .

So,  $\Gamma_\alpha \cap \Delta_C := \Gamma_\alpha \times_{C \times C} \Delta_C$  is finite and  $\Gamma_\alpha$  and  $\Delta_C$  have no components in common. Hence  $\Gamma_\alpha \cdot \Delta_C = \dim_k \Gamma(\Gamma_\alpha \cap \Delta_C, \mathcal{O}_{\Gamma_\alpha \cap \Delta_C})$ .

Let  $i : \Delta_C \rightarrow C$  and  $j : \Gamma_\alpha \rightarrow C$  be the inclusion. Then for  $P \in (\Gamma_\alpha \cap \Delta_C)(k)$  we have  $\text{im}(di)_P = \text{span}(\pi, \pi)$  and  $\text{im}(dj)_P = \text{span}(\pi, d\alpha_P(\pi))$ , where  $\pi$  is a generator of  $T_P(C)$  and we identify  $T_P(C \times C)$  as  $T_P(C) \oplus T_P(C)$ . Hence by assumption b)  $T_P(C \times C) = \text{im}(di)_P + \text{im}(dj)_P$ .

Let  $f$  be the local equation for  $\Delta_C$  in  $C \times C$  at  $P$  and  $g$  the local equation for  $\Gamma_\alpha$  in  $C \times C$  at  $P$ . Then  $T_P(C \times C) = \text{im}(di)_P + \text{im}(dj)_P$  shows that  $f$  and  $g$  generate  $m_P$  at  $\mathcal{O}_{C \times C, P}$ . Hence  $\mathcal{O}_{\Gamma_\alpha \cap \Delta_C, P} = \mathcal{O}_{C \times C, P} / (f, g) = k$  and therefore

$$\Gamma_\alpha \cdot \Delta_C = \dim_k \Gamma(\Gamma_\alpha \cap \Delta_C, \mathcal{O}_{\Gamma_\alpha \cap \Delta_C}) = \#(\Gamma_\alpha \cap \Delta_C)(k) = \{x \in C(k) : \alpha(x) = x\}.$$

□

### 3 The Weil conjectures for curves

Let  $C$  be a proper non-singular curve of genus  $g$  over a finite field  $\mathbb{F}_q$  with  $q$  elements. Let  $k$  be an algebraic closure of  $\mathbb{F}_q$  and denote  $C_k := C \times_{\mathbb{F}_q} k$ . Let  $F_C : C \rightarrow C$  be the absolute Frobenius morphism of  $C$ , which is the identity on the underlying topological space and acts as the  $q$ -th power map on  $\mathcal{O}_C$ . Let  $F_{C,k} := F_C \times_{\mathbb{F}_q} 1_k$  be the  $k$  linear Frobenius morphism of  $C_k$ .

Let  $J$  be the Jacobian variety of  $C$  over  $\mathbb{F}_q$ . Then the base change of  $J$  to  $k$ , denoted by  $J_k$ , is the Jacobian variety of  $C_k$ . Further, the induces map on  $J_k$  by  $F_{C,k}$  as in section 2.7 a) is  $\text{Fr} := F_J \times 1_k$ , where  $F_J$  is the absolute Frobenius of  $J$ . This follows from the naturality of the absolute Frobenius.

**Theorem 3.1** (Weil conjectures for curves).

Let  $P$  be the characteristic polynomial of  $\text{Fr} \in \text{End}(J_k)$  and  $\alpha_1, \dots, \alpha_{2g} \in \mathbb{C}$  its roots. The Weil conjectures for curves state:

1. (*Rationality of the zeta function*)

$$\exp \left( \sum_{n=1}^{\infty} \#C(\mathbb{F}_{q^n}) \frac{x^n}{n} \right) = \frac{\prod_{i=1}^{2g} (1 - \alpha_i x)}{(1-x)(1-qx)}$$

$$\text{and } \prod_{i=1}^{2g} (1 - \alpha_i x) = x^{2g} P\left(\frac{1}{x}\right) \in \mathbb{Z}[x].$$

2. (*Riemann hypothesis*)  $|\alpha_i| = q^{\frac{1}{2}}$  for all  $i = 1, \dots, 2g$ .
3. (*Hesse-Weil bound*)

$$\#C(\mathbb{F}_{q^n}) = 1 - \sum_{i=1}^{2g} \alpha_i^n + q^n$$

$$\text{and in particular } |\#C(\mathbb{F}_{q^n}) - (q^n + 1)| \leq 2gq^{\frac{n}{2}}.$$

Moreover, whenever  $C$  has an  $\mathbb{F}_{q^n}$  valued point

$$\#\text{Pic}^0(C_{\mathbb{F}_{q^n}}) = \prod_{i=1}^{2g} (1 - \alpha_i^n), \tag{27}$$

where  $\text{Pic}^0(C_{\mathbb{F}_{q^n}})$  denotes the group of isomorphism classes of degree zero line bundles on the curve  $C_{\mathbb{F}_{q^n}} := C \times_{\mathbb{F}_q} \mathbb{F}_{q^n}$  over  $\mathbb{F}_{q^n}$ .

*Proof.* Let  $F_k : \text{Spec}(k) \rightarrow \text{Spec}(k)$  denote the absolute Frobenius of  $k$ .

The Lefschetz fixed point formula 2.20 applied to  $F_{C,k}^n$  yields

$$\Delta_C \cdot \Gamma_{F_{C,k}^n} = 1 - \text{tr}(\text{Fr}^n) + \deg(F_{C,k}^n).$$

Using theorem 1.22 we have  $\text{tr}(\text{Fr}^n) = \sum_{i=1}^{2g} \alpha_i^n$ . Further,  $\deg(F_{C,k}^n) = \deg(F_{C,k})^n$ .

**Claim 1:**  $\deg(F_{C,k}) = q$ . By [7, 8.5 Prop. 13] there is a nonempty open neighborhood  $U \subseteq C_k$  and an étale  $k$ - morphism  $g : U \rightarrow \mathbb{A}_k^1$ . It suffices to prove that  $F_{C,k}|_U : U \rightarrow U$  has degree  $q$ .



Now  $g \circ F_{C,k} = (F_{\mathbb{A}_{\mathbb{F}_q}^1} \times 1_k) \circ g$ . By the multiplicativity of the degree it is enough to prove that  $\deg(F_{\mathbb{A}_{\mathbb{F}_q}^1} \times 1_k) = q$  (Note that  $g$  induces a finite residue field extension). To see this, observe that  $F_{\mathbb{A}_{\mathbb{F}_q}^1}$  fixes coefficients and maps coordinates to their  $q$ -th power. The induced residue field extension is  $\mathbb{F}_q(x) \hookrightarrow \mathbb{F}_q(x)[t]/(t^q - x)$ , which has degree  $q$ .

So, we obtain

$$\Delta_C \cdot \Gamma_{F_{C,k}^n} = 1 - \sum_{i=1}^{2g} \alpha_i^n + q^n. \quad (28)$$

$\#C(\mathbb{F}_{q^n}) = \Delta_C \cdot \Gamma_{F_{C,k}^n}$ . For the  $k$ -variety  $C_k$  we have a bijection between the  $k$ -valued points of  $C_k$  and the  $k$ -valued points of the  $\mathbb{F}_q$  variety  $C$  given by

$$C_k(k) \rightarrow C(k), (x : k \rightarrow C_k) \mapsto (k \xrightarrow{x} C_k \xrightarrow{\text{pr}_C} C) \quad (29)$$

a)  $C(k)$  has an action given by pre-composition with  $F_k$ .

b)  $C_k(k)$  has an action given by post-composition with  $F_{C,k}$ .

**Claim 2:** The bijection in (29) identifies both actions a) and b):

Let  $x \in C_k(k)$ . Then  $\text{pr}_C \circ F_{C,k} \circ x = F_C \circ \text{pr}_C \circ x = F_S \circ \text{pr}_C \circ x$ , where we used the naturality of the absolute Frobenius in the last equation.

Let  $C(k)^{F_k^n}$  denote the elements of  $C(k)$  fixed by pre-composition with  $F_k^n$ .

**Claim 3:**  $C(\mathbb{F}_{q^n}) \rightarrow C(k)^{F_k^n}, (x : \text{Spec}(\mathbb{F}_{q^n}) \rightarrow C) \mapsto (\text{Spec}(k) \rightarrow \text{Spec}(\mathbb{F}_{q^n}) \xrightarrow{x} C)$  is a bijection.

The map is injective, because  $\text{Spec}(k) \rightarrow \text{Spec}(\mathbb{F}_{q^n})$  is faithfully flat and therefore an epimorphism. Next we show surjectivity. Say,  $y \in C(k)^{F_k^n}$ . Take any  $\text{Spec}(R) = U \subseteq C$  open affine such that  $y$  factors as  $k \rightarrow U \hookrightarrow C$ . Then  $k \rightarrow U$  corresponds to a  $\mathbb{F}_q$  algebra homomorphism  $\varphi : R \rightarrow k$  such that  $\mathfrak{f} \circ \varphi = \varphi$ , for  $\mathfrak{f}(r) = r^{q^n}$ . This implies that  $\varphi$  factors through  $\mathbb{F}_{q^n} \hookrightarrow k$ . Hence,  $y$  factors as  $\text{Spec}(k) \rightarrow \mathbb{F}_{q^n} \rightarrow U \hookrightarrow C$ .

If we denote elements of  $C_k(k)$  fixed by post-composition with  $F_{C,k}^n$  with  $C_k(k)^{F_{C,k}^n}$ , then applying claim 3 and then claim 2 shows that

$$\#C(\mathbb{F}_{q^n}) = \#C(k)^{F_k^n} = \#C_k(k)^{F_{C,k}^n} = \#\{x \in C_k(k) : F_{C,k}^n(x) = x\}. \quad (30)$$

We want to apply proposition 2.22 to  $F_{C,k}^n : C_k \rightarrow C_k$ .

For a) note that  $\#C(\mathbb{F}_{q^n}) < \infty$  because  $C$  admits a closed immersion into  $\mathbb{P}_k^m$  for  $m$  big enough and  $\mathbb{P}_k^m(\mathbb{F}_{q^n}) = ((q^n)^{m+1} - 1)/(q^n - 1) < \infty$ . So, by equation 30  $F_{C,k}^n(x) = x$  for only finitely many  $x \in C_k(x)$ .

For b) observe that for  $x \in C_k(k)$  we have  $(dF_{C,k})_x = 0$ , because  $q^n = 0$  in  $k$ . This can be proven very explicitly by using an étale morphisms as in the proof of claim 1. Then  $(dF_{C,k})_x = 0$  follows because the endomorphism of  $\mathbb{A}_{\mathbb{F}_q}$  that fixes the coefficients and raises the coordinates to their  $q^n$  power induces the zero map on tangent spaces.

All in all, we can apply proposition 2.22 to obtain

$$\#C(\mathbb{F}_{q^n}) \stackrel{(30)}{=} \#\{x \in C_k(k) : F_{C,k}^n(x) = x\} = \Delta_C \cdot \Gamma_{F_{C,k}^n} \stackrel{(28)}{=} 1 - \sum_{i=1}^{2g} \alpha_i^n + q^n. \quad (31)$$

For showing the Riemann hypothesis for the curve  $C$  we proceed to proof the following statement.

**Claim 4:**  $\text{Fr}^\dagger \circ \text{Fr} = q_J$ , or in other words  $\text{Fr}^\vee \circ \varphi_{\mathcal{L}(\Theta)} \circ \text{Fr} = q_J \cdot \varphi_{\mathcal{L}(\Theta)}$ .

Given  $P \in J$  and let  $g$  be a local equation cutting out  $\Theta$  on the neighborhood  $U$  of  $P$ . Note that, since  $\Theta$  can be defined over  $\mathbb{F}_q$ , we have  $\text{Fr}_U^\#(g) = g^q$  and this is a local equation cutting out  $\text{Fr}^*\mathcal{L}(\Theta)$  at  $P$ . But  $\text{div}(g^q) = q \cdot \text{div}(g)$  and thus  $\text{Fr}^*\mathcal{L}(\Theta) \cong \mathcal{L}(q\Theta) \cong \mathcal{L}(\Theta)^q$ .

Now given a  $k$ -valued point  $x \in J_k(k)$  we can compute via equation (14) and (4) that  $\text{Fr}^\vee \circ \varphi_{\mathcal{L}(\Theta)} \circ \text{Fr}(x)$  is represented by the line bundle

$$\text{Fr}^*(t_{\text{Fr}(x)}^* \mathcal{L}(\Theta) \otimes \mathcal{L}^{-1}(\Theta)) \cong t_x^* \text{Fr}^* \mathcal{L}(\Theta) \otimes (\text{Fr}^* \mathcal{L}(\Theta))^{-1} \cong t_x^* \mathcal{L}(\Theta)^q \otimes (\mathcal{L}(\Theta)^q)^{-1} = \varphi_{\mathcal{L}(\Theta)^q}(x)$$

But  $\varphi_{\mathcal{L}(\Theta)^q} = q\varphi_{\mathcal{L}(\Theta)}$  because  $\mathcal{L}' \mapsto \varphi_{\mathcal{L}'}$  is a homomorphism, see equation (12). So,  $\text{Fr}^\vee \circ \varphi_{\mathcal{L}(\Theta)} \circ \text{Fr}$  and  $q_J \cdot \varphi_{\mathcal{L}(\Theta)}$  agree on  $k$ -valued points. Since  $k$  is algebraically closed, claim 4 follows.

**Claim 5:** Every complex root  $\alpha$  of  $P$  has absolute value  $|\alpha| = \sqrt{q}$ .

Note that  $\mathbb{Q}[\text{Fr}] \subseteq \text{End}^0(J_k)$  is a commutative ring. Further  $\text{End}^0(J_k)$  is finite dimensional as  $\mathbb{Q}$ -vector space by corollary 1.21 and therefore  $\mathbb{Q}[\text{Fr}]$  is a finite commutative  $\mathbb{Q}$ -algebra.

By the relation  $\text{Fr}^{-1} = \text{Fr}^\dagger/q$  from claim 4 we see that  $\text{Fr}$  is not a zero divisor in  $\text{End}(J_k)^0$ . Hence the  $\mathbb{Q}$  linear endomorphism of  $\mathbb{Q}[\text{Fr}]$  given by multiplication by  $\text{Fr}$  is injective. Because  $\mathbb{Q}[\text{Fr}]$  is finite dimensional the endomorphism is also surjective and therefore  $\text{Fr}^{-1} \in \mathbb{Q}[\text{Fr}]$ . Again by the relation in claim 4 we obtain  $\text{Fr}^\dagger \in \mathbb{Q}[\text{Fr}]$ . So, by the properties of the Rosati involution from section 2.5  $(\cdot)^\dagger : \mathbb{Q}[\text{Fr}] \rightarrow \text{End}^0(J_k)$  maps into  $\mathbb{Q}[\text{Fr}]$ .

Let  $0 \neq a \in \mathbb{Q}[\text{Fr}]$ . Then  $b := a^\dagger \cdot a$ . By the positivity of the Rosati involution 2.18  $\text{tr}(b) = \text{tr}(a^\dagger \cdot a) > 0$ . So,  $b \neq 0$ . As  $b^\dagger = b$  also  $\text{tr}(b^2) = \text{tr}(b^\dagger b) > 0$  by the positivity of the Rosati involution 2.18 and hence  $b^2 \neq 0$ . Similarly,  $b^4 \neq 0$  and by induction  $b^{2n} \neq 0$ . Hence  $b$  is not nilpotent. Because  $\mathbb{Q}[\text{Fr}]$  is commutative, if  $a$  was nilpotent, then also  $b$  would be nilpotent. We conclude that  $\mathbb{Q}[\text{Fr}]$  is reduced.

Since  $\mathbb{Q}[\text{Fr}]$  is a finite commutative  $\mathbb{Q}$ -algebra, i.e. Artinian, it has a finite number of prime ideals  $\mathfrak{m}_1, \dots, \mathfrak{m}_j$  each of which is maximal. Since  $\mathbb{Q}[\text{Fr}]$  is reduced, we see that  $\bigcap_{i=1}^j \mathfrak{m}_i = 0$ . So, by the chinese remainder theorem  $\mathbb{Q}[\text{Fr}] \cong \prod_{i=1}^j K_i$  for  $K_i := \mathbb{Q}[\text{Fr}]/\mathfrak{m}_i$  a field. Any automorphism  $\tau$  of  $\mathbb{Q}[\text{Fr}]$  maps a maximal ideal to a maximal ideal, i.e. there is a permutation  $\sigma \in S_j$ , for  $S_j$  the symmetric group in  $j$ -letters, and isomorphisms  $\tau_i : K_i \rightarrow K_{\sigma(i)}$  such that  $\tau(a_1, \dots, a_j) = (b_1, \dots, b_j)$  for  $b_{\sigma(i)} = \tau_i(a_i)$  and  $a_i, b_i \in K_i$ . The Rosati involution is an automorphism of  $\mathbb{Q}[\text{Fr}]$  as we have seen that it restricts to a map  $\mathbb{Q}[\text{Fr}] \rightarrow \mathbb{Q}[\text{Fr}]$  is linear and its own inverse. Further,  $(\cdot)^\dagger$  is multiplicative because  $\mathbb{Q}[\text{Fr}]$  is commutative. For  $\tau = \dagger$  the permutation  $\sigma$  from above must be trivial: Else, for  $\sigma(i) \neq i$  and  $a := (0, \dots, 0, 1, 0 \dots 0) \in \mathbb{Q}[\text{Fr}]$ , 1 in the  $i$ -th spot,  $\text{tr}(a^\dagger \cdot a) = 0$ , which contradicts corollary 2.18.

Hence  $\dagger$  preserves the factors of  $\mathbb{Q}[\text{Fr}]$  and is a positive-definite involution on each of them. The involution extends by linearity (equivalently by continuity) to a positive-definite involution of  $\mathbb{Q}[\text{Fr}] \otimes \mathbb{R}$ , i.e.  $(\cdot)^\dagger : \mathbb{Q}[\text{Fr}] \otimes \mathbb{R} \rightarrow \mathbb{Q}[\text{Fr}] \otimes \mathbb{R}$  is an  $\mathbb{R}$ -automorphism that is its own inverse and there exists  $\text{tr} : \mathbb{Q}[\text{Fr}] \otimes \mathbb{R} \rightarrow \mathbb{R}$ , which is  $\mathbb{R}$ -linear such that  $\text{tr}(a^\dagger \circ a) > 0$  for all  $a \in \mathbb{Q}[\text{Fr}] \otimes \mathbb{R}$ .

The above remarks also apply to  $\mathbb{Q}[\text{Fr}] \otimes \mathbb{R}$ : it is a finite  $\mathbb{R}$  algebra and a product of fields, where  $\dagger : \mathbb{Q}[\text{Fr}] \otimes \mathbb{R} \rightarrow \mathbb{Q}[\text{Fr}] \otimes \mathbb{R}$  is a positive-definite involution that preserves each factor of  $\mathbb{Q}[\text{Fr}] \otimes \mathbb{R}$ .

Since any finite field extension of  $\mathbb{R}$  is either  $\mathbb{R}$  itself or isomorphic to  $\mathbb{C}$ , each factor of  $\mathbb{Q}[\text{Fr}] \otimes \mathbb{R}$  is either  $\mathbb{R}$  or  $\mathbb{C}$ .

The field  $\mathbb{R}$  has no nontrivial automorphisms at all, and so  $(\cdot)^\dagger$  must act on a real factor of  $\mathbb{Q}[\text{Fr}] \otimes \mathbb{R}$  as the identity map.

The field  $\mathbb{C}$  has only two automorphisms of finite order: the identity map and complex conjugation. The identity on  $\mathbb{C}$  is not positive definite, else  $0 < \text{tr}(i \cdot i) = \text{tr}(-1) = -1 \text{tr}(1)$ , which contradicts that  $\text{tr}(1) = \text{tr}(1 \cdot 1) > 0$ . Hence,  $(\cdot)^\dagger$  must act on the complex factors as conjugation.

Now given any homomorphism of commutative  $\mathbb{Q}$ -algebras  $\rho : \mathbb{Q}[\text{Fr}] \rightarrow \mathbb{C}$ .

Then  $\rho \otimes 1 : \mathbb{Q}[\text{Fr}] \otimes \mathbb{R} \rightarrow \mathbb{C} \otimes_{\mathbb{Q}} \mathbb{R}$  is  $\mathbb{R}$  linear, so for any  $a \in \mathbb{Q}[\text{Fr}]$

$$\begin{aligned} \rho(a^\dagger) \otimes 1 &= (\rho \otimes 1)(a^\dagger \otimes 1) = (\rho \otimes 1)((a \otimes 1)^\dagger) = (\rho \otimes 1)(\overline{a \otimes 1}) \\ &= \overline{(\rho \otimes 1)(a \otimes 1)} = \overline{\rho(a) \otimes 1} = \overline{\rho(a)} \otimes 1 \end{aligned}$$

where  $\overline{a \otimes 1}$  denote complex conjugation in every coordinate of  $a \otimes 1 = (a_1, \dots, a_j) \in \mathbb{Q}[\text{Fr}] \otimes \mathbb{R}$ .

So, by flatness of the  $\mathbb{Q}$  module  $\mathbb{Q}[\text{Fr}]$  we have  $\rho(a^\dagger) = \overline{\rho(a)}$ .

Let  $\mu \in \mathbb{Q}[x]$  be the unique polynomial with leading coefficient 1 that generates the kernel of  $\mathbb{Q}[x] \rightarrow \mathbb{Q}[\text{Fr}], x \mapsto \text{Fr}$ . Then the map  $\mathbb{Q}[x]/(\mu) \rightarrow \mathbb{Q}[\text{Fr}], x + (\mu) \mapsto \text{Fr}$  is an isomorphism.

Let  $\alpha \in \mathbb{C}$  be a root of  $\mu$ . The ring-homomorphism  $\psi : \mathbb{Q}[x] \rightarrow \mathbb{C}, f \mapsto f(\alpha)$  factors as  $\mathbb{Q}[x] \rightarrow \mathbb{Q}[x]/(\mu) \xrightarrow{x+(\mu) \mapsto \alpha} \mathbb{C}$ . So, we obtain a ring-homomorphism  $\rho : \mathbb{Q}[\text{Fr}] \rightarrow \mathbb{C}$  sending  $\text{Fr}$  to  $\alpha$ . This yields  $|\alpha|^2 = \overline{\alpha} \cdot \alpha = \overline{\rho(\text{Fr})} \rho(\text{Fr}) = \rho(\text{Fr}^\dagger) \rho(\text{Fr}) = \rho(\text{Fr}^\dagger \circ \text{Fr}) \stackrel{\text{Claim 4}}{=} \rho(q) = q$ .

Now let  $l$  be a prime  $l \neq \text{char}(k)$ . Then the minimal polynomial  $\tilde{\mu}$  of  $V_l(\text{Fr}) \in \text{End}_{\mathbb{Q}}(V_l(J_k))$  divides  $\mu$ , because  $\mu(V_l(\text{Fr})) \stackrel{(15)}{=} V_l(\mu(\text{Fr})) = V_l(0) = 0$ . Hence, all roots of  $\tilde{\mu}$  are roots of  $\mu$  and

therefore have absolute value  $\sqrt{q}$ . But the characteristic polynomial of  $V_l(\text{Fr})$  has the same roots as  $\tilde{\mu}$ , so claim 5 follows by theorem 1.22.

Equation (31) in conjunction with the Riemann hypothesis give the Hesse-Weil bound:

$$|\#C(\mathbb{F}_{q^n} - (q^n + 1))| = \left| \sum_{i=1}^{2g} \alpha_i^n \right| \leq \sum_{i=1}^{2g} |\alpha_i|^n = 2g(\sqrt{q})^n.$$

The identity  $\ln(1 - t) = -\sum_{n=1}^{\infty} \frac{t^n}{n}$  implies that

$$\begin{aligned} \ln\left(\frac{\prod_{i=1}^{2g}(1 - \alpha_i x)}{(1 - x)(1 - qx)}\right) &= -\ln(1 - x) + \sum_{i=1}^{2g} \ln(1 - x\alpha_i) - \ln(1 - qx) \\ &= \sum_{n=1}^{\infty} \left(\frac{x^n}{n}\right) - \sum_{i=1}^{2g} \left(\sum_{n=1}^{\infty} \frac{x^n \alpha_i^n}{n}\right) + \sum_{n=1}^{\infty} \left(\frac{(qx)^n}{n}\right) \\ &= \sum_{n=1}^{\infty} \left(\left(1 - \sum_{i=1}^{2g} \alpha_i^n + q^n\right) \frac{x^n}{n}\right) = \sum_{n=1}^{\infty} \left(\#C(\mathbb{F}_{q^n}) \frac{x^n}{n}\right), \end{aligned}$$

where we used equation (31) for the last equality. This proves the rationality of the zeta function. Moreover,  $\prod_{i=1}^{2g} (1 - \alpha_i x) = x^{2g} \prod_{i=1}^{2g} (\frac{1}{x} - \alpha_i) = x^{2g} P(\frac{1}{x})$  has integer coefficients, because  $P \in \mathbb{Z}[x]$  by theorem 1.22.

**Claim 6:** The map  $1 - \text{Fr}^n : J_k \rightarrow J_k$  is an étale morphism. Since  $k$  is algebraically closed it suffices to prove that  $1 - \text{Fr}^n$  induces an isomorphism on tangent spaces for all  $k$ -valued points. But we have already seen that  $\text{Fr}^n$  induces the zero map on tangent spaces, hence  $1 - \text{Fr}^n$  is the identity on tangent spaces and claim 6 follows.

In particular,  $1 - \text{Fr}^n$  is an isogeny by theorem 1.4 and by equation (1)  $h^0(\ker(1 - \text{Fr}^n), \mathcal{O}_{\ker(1 - \text{Fr}^n)}) = \deg(1 - \text{Fr}^n)$ . Now by claim 6 the fiber  $\ker(1 - \text{Fr}^n)$  is reduced and finite over the algebraically closed field  $k$ , so  $\#\ker(1 - \text{Fr}^n)(k) = h^0(\ker(1 - \text{Fr}^n), \mathcal{O}_{\ker(1 - \text{Fr}^n)})$ . All in all, we obtain

$$\#\{x \in J_k(k) : \text{Fr}^n(x) = x\} = \#\ker(1 - \text{Fr}^n)(k) = h^0(\ker(1 - \text{Fr}^n), \mathcal{O}_{\ker(1 - \text{Fr}^n)}) = \deg(1 - \text{Fr}^n).$$

Note that claim 2 and claim 3 can be analogously be proven for the absolute Frobenius  $F_J : J \rightarrow J$  and its base change  $\text{Fr} = F_J \times 1_k : J_k = J \times_{\mathbb{F}_q} k \rightarrow J_k$ . So, applying equation (30) to the variety  $J_k = J \times_{\mathbb{F}_q} k$  shows that  $\#J(\mathbb{F}_{q^n}) = \#\{x \in J_k(k) : \text{Fr}^n(x) = x\}$ .

Now  $\#J(\mathbb{F}_{q^n}) = \#J_{\mathbb{F}_{q^n}}(\mathbb{F}_{q^n})$  and the latter equals  $\#\text{Pic}^0(C_{\mathbb{F}_{q^n}})$  whenever  $C_{\mathbb{F}_{q^n}}$  has an  $\mathbb{F}_{q^n}$ -valued point by equation (7) and the discussion in section 2.7 b) because  $J_{\mathbb{F}_{q^n}} = J \times_{\mathbb{F}_q} \mathbb{F}_{q^n}$  is the Jacobian variety of the curve  $C_{\mathbb{F}_{q^n}}$  over  $\mathbb{F}_{q^n}$ .

Let  $P_{\text{Fr}^n}$  be the characteristic polynomial of  $\text{Fr}^n$ . By theorem 1.22 the roots of  $P_{\text{Fr}^n}$  are  $\alpha_1^n, \dots, \alpha_{2g}^n$ . Further, by definition of  $P_{\text{Fr}^n}$  we have  $P_{\text{Fr}^n}(1) = \deg(1 - \text{Fr}^n)$ .

All in all, for  $n$  big enough, i.e. such that  $C(\mathbb{F}_{q^n}) \neq \emptyset$ ,

$$\#\text{Pic}^0(C_{\mathbb{F}_{q^n}}) = \#J_{\mathbb{F}_{q^n}}(\mathbb{F}_{q^n}) = \#\{x \in J_k(k) : \text{Fr}^n(x) = x\} = \deg(1 - \text{Fr}^n) = P_{\text{Fr}^n}(1) = \prod_{i=1}^{2g} (1 - \alpha_i^n).$$

This prove equation (27) and therefore completes the proof.  $\square$

**Example 3.2** (Elliptic Curves). Suppose the genus of  $C$  is equal to one. Then the Hesse-Weil bound gives us that  $\#C(\mathbb{F}_q) = 1 - (\alpha_1 + \alpha_2) + q$  and by the Riemann-Hypothesis  $|\alpha_1 + \alpha_2| \leq 2\sqrt{q}$ . Therefore,  $\#C(\mathbb{F}_q) \geq 1 - 2\sqrt{q} + q = (\sqrt{q} - 1)^2$ . Hence  $C$  will admit an  $\mathbb{F}_q$  valued point, i.e.  $C$  is an elliptic curve, see remark 2.4.

## References

- [1] T. Stacks project authors, “The stacks project.” <https://stacks.math.columbia.edu>, 2023.

- [2] J. S. Milne, *Algebraic geometry*. Allied Publishers, 2012.
- [3] R. Vakil, “The rising sea: Foundations of algebraic geometry,” *preprint*, 2017.
- [4] G. van der Geer and B. Moonen, “Abelian varieties,” *Book in preparation*, 2007.
- [5] D. Mumford, C. P. Ramanujam, and J. I. Manin, *Abelian varieties*, vol. 5. Oxford university press Oxford, 1974.
- [6] J. S. Milne, “Abelian varieties,” *Arithmetic geometry*, pp. 103–150, 1986.
- [7] S. Bosch, *Algebraic geometry and commutative algebra*. Springer, 2013.
- [8] R. Hartshorne, *Algebraic geometry*, vol. 52. Springer Science & Business Media, 2013.
- [9] S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron models*, vol. 21. Springer Science & Business Media, 2012.
- [10] J. S. Milne, *Algebraic number theory*. JS Milne, 2008.
- [11] S. Lang, *Abelian varieties*. Dover Publications, 2019.
- [12] A. Grothendieck, “Éléments de géométrie algébrique: Iii. étude cohomologique des faisceaux cohérents, première partie,” *Publications Mathématiques de l’IHÉS*, vol. 11, pp. 5–167, 1961.
- [13] N. M. Katz and B. Mazur, “Arithmetic moduli of elliptic curves.(am-108), volume 108,” in *Arithmetic Moduli of Elliptic Curves.(AM-108), Volume 108*, Princeton University Press, 2016.
- [14] A. Grothendieck, “Technique de descente et théorèmes d’existence en géométrie algébrique. i. généralités. descente par morphismes fidèlement plats,” *Séminaire Bourbaki*, vol. 5, pp. 299–327, 1959.
- [15] W. Fulton, *Intersection theory*, vol. 2. Springer Science & Business Media, 2013.