ssdnm
środowiskowe
studia doktoranckie
z nauk matematycznych

Tomasz Lenarcik

Uniwersytet Jagielloński

Abelian varieties and Jacobians of curves over finite fields

Praca semestralna nr 2

(semestr zimowy 2010/11)

Opiekun pracy: Wojciech Gajda

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI

UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY

ABELIAN VARIETIES AND JACOBIANS OF CURVES OVER FINITE FIELDS

TOMASZ LENARCIK

Abstract. This article is a brief survey covering some fundamental theorems in the theory of abelian varieties. Basic examples of Jacobian varieties defined over finite fields serve as motivation to develop the theory in positive characteristic.

Our main goal is to collect a bunch of tools which should allow us to analyze the classical proof (following Tate's original paper) of the famous Tate's conjecture concerning the image of the natural map

$$\mathbb{Z}_l \otimes_{\mathbb{Z}} \mathrm{Hom}(X, Y) \longrightarrow \mathrm{Hom}_{\mathbb{Z}_l}(T_l(X), T_l(Y))$$

where X and Y are abelian varieties defined over a finite field k_0, and l is a prime number different from the characteristic of k_0.

Contents

1. Introduction

1.1. **Background.** An *abelian variety* is by definition a complete algebraic variety equipped with a group structure where the addition law and inverse map are given by morphisms in the adequate category. Here, by *complete variety* we mean an integral scheme, proper over algebraically closed field k. ([1]) It turns out, ([2]) that completeness combined with existence of the group law already implies that any abelian variety is projective. For the purpose of this paper the algebraically closed field k of characteristic p (possibly $p > 0$) has been chosen once and for all; in particular "variety" will always mean "variety over k" and the same applies to morphisms.

If we speak about abelian varieties, "a morphism" always means a morphism of varieties which is a group homomorphism at the same time. One can show, ([3]) that the condition of preserving the neutral element is already sufficient for an arbitrary morphism of varieties, i.e., not necessarily a group homomorphism, to commute with the group law. In particular, the inverse map is always a group homomorphism, which is tantamount to the fact that every abelian variety is necessarily a commutative group. For this reason, we will consequently use the additive notation for the group law.

Given an arbitrary abelian variety X the only immediate examples of endomorphisms are the "multiplication by n" maps defined for any $n \in \mathbb{Z}$. We will usually denote them by n_X, or we will even drop the subscript unless it leads to a confusion. We will see, that n_X is surjective. This automatically implies that n_X is generically finite, but one may also verify (using translations) that it is in fact a finite map. Furthermore, the degree of n_X equals n^{2g} where $g := \dim X$. ([4])

Example. A fundamental example to look at is a *complex torus*, i.e. an analytic variety defined as the quotient of $\mathbb{C}^g$ by some sublattice $\Lambda \subset \mathbb{C}^g$ of rank $2g$. It is easily seen to be a compact manifold with a natural group structure induced from $\mathbb{C}^g$. Note, that all the properties we have mentioned so far are very easy to verify in this context.

By elementary properties of complex Lie groups, one can verify that in fact every abelian variety over $\mathbb{C}$ is biholomorphic to some complex torus. On the other hand, surprisingly, there exist complex tori which are non algebraic, i.e. which are not biholomorphic to any (complex) abelian variety. Note, that this problem does not occur in dimension one (elliptic curves), since there is one to one correspondence between compact Riemann surfaces and smooth complete (projective) curves.

We are not going to go deeper into this interesting subject, but let us at least recall the following important result:

Theorem 1.1.1. *Let Λ be a lattice in $\mathbb{C}^g$ (of rank $2g$). The complex torus $\mathbb{C}^g$ is an abelian variety if and only if there exists a positive definite Hermitian*

[1] Let us recall, that "separated and of finite type over k" is already contained in the definition of *properness*.

[2] See Corollary 2.2.4.

[3] See Corollaries 2.1.2 and 2.1.3.

[4] See Corollary 2.3.2.

form on $\mathbb{C}^g \times \mathbb{C}^g$ *whose imaginary part takes integer values when restricted to* $\Lambda \times \Lambda$.

Proof. See Hindry and Silverman [5, Ch. A.5].

1.2. **Tate module.** The endomorphisms $(l^i)_X$, with $i \geq 1$ and l a prime number different from p, will be of particular importance. Since $p \nmid \deg(l^i)_X = l^{2ig}$, such a morphism is always separable. In particular, the number of points in a fiber is generically equal to $\deg(l^i)_X$. Since we are dealing with a group homomorphism, all fibers are bijective to the kernel of $(l^i)_X$, which we will consequently denote by X_{l^i}, and so they all have the same number of element equal to l^{2ig}. The following construction will be in the center of our interests.

Definition (Tate module)**.** The abelian groups X_{l^i}, with $i \geq 1$, form the inverse system

$$\ldots \xleftarrow{l_X} X_{l^{i-1}} \xleftarrow{l_X} X_{l^i} \xleftarrow{l_X} X_{l^{i+1}} \xleftarrow{l_X} \ldots \tag{1}$$

with each X_{l^i} viewed as an $\mathbb{Z}/l^i$-module. ([5]) This gives rise to a $\mathbb{Z}_l$-module structure on the limit of (1), which is usually denoted by $T_l(X)$ and it is called the *Tate module* of X.

Remark. Since $(\mathbb{Z}/l^i)^{2g}$ is the only abelian group of rank l^{2ig} which is anihilated by l^i, then $X_{l^i} \simeq (\mathbb{Z}/l^i)^{2g}$. Furthermore, the isomorphisms can be chosen to fit into the commutative diagram

$$\begin{array}{ccccccccc}
\ldots & \xleftarrow{l_X} & X_{l^{i-1}} & \xleftarrow{l_X} & X_{l^i} & \xleftarrow{l_X} & X_{l^{i+1}} & \xleftarrow{l_X} & \ldots \\
 & & \simeq\downarrow & & \simeq\downarrow & & \simeq\downarrow & & \\
\ldots & \longleftarrow & (\mathbb{Z}/l^{i-1})^{2g} & \longleftarrow & (\mathbb{Z}/l^i)^{2g} & \longleftarrow & (\mathbb{Z}/l^{i+1})^{2g} & \longleftarrow & \ldots
\end{array}$$

It follows, that abstractly $T_l(X) \simeq (\mathbb{Z}_l)^{2g}$.

Continuing the above notation, let Y be another abelian variety and let $f : X \longrightarrow Y$ be a morphism of abelian varieties. Since clearly $l_Y \circ f = f \circ l_X$ and $f(X_{l^i}) \subset Y_{l^i}$, it follows that f induces a $\mathbb{Z}_l$-linear map $T_l(f) : T_l(X) \longrightarrow T_l(Y)$. A straightforward verification shows, that this construction gives rise to a functor from the category of abelian varieties into the category of $\mathbb{Z}_l$-modules. We have the following result:

Theorem 1.2.1. *For any pair of abelian varieties* X *and* Y, $\mathrm{Hom}(X, Y)$ *is a finitely generated free abelian group, and the natural map*

$$\mathbb{Z}_l \otimes_{\mathbb{Z}} \mathrm{Hom}(X, Y) \longrightarrow \mathrm{Hom}_{\mathbb{Z}_l}(T_l(X), T_l(Y)) \tag{2}$$

induced by $T_l : \mathrm{Hom}(X, Y) \longrightarrow \mathrm{Hom}_{\mathbb{Z}_l}(T_l(X), T_l(Y))$ *(*l *any prime* $\neq \mathrm{char}\, k$*) is injective.*

Proof. See Mumford [7, §19 Thm. 3, p. 176].

[5] It makes sense, since each X_{l^i} is anihilated by l^i.

Example. A similar type of representations, can be achieved for complex tori by means of complex analysis. Let us look closer at a simple example of the elliptic curve $E/\mathbb{C}$ given as the quotient $E = \mathbb{C}/\Lambda$ with $\Lambda = \mathbb{Z} \oplus \mathbb{Z}\lambda$, and let $f : E \longrightarrow E$ be a holomorphic map such that $f(0) = 0$. Since the natural map $\pi : \mathbb{C} \longrightarrow E$ is a covering and $\mathbb{C}$ is simply connected, there exists a unique map $g : \mathbb{C} \longrightarrow \mathbb{C}$ such that the diagram

$$\begin{array}{ccc} \mathbb{C} & \overset{g}{\longrightarrow} & \mathbb{C} \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi} \\ \mathbb{C}/\Lambda & \xrightarrow{f} & \mathbb{C}/\Lambda \end{array}$$

is commutative. Pick any $\mu \in \Lambda$. Then the function

$$z \longmapsto g(z + \mu) - g(z)$$

is continuous and takes values in Λ, which is a discrete set, hence it must be constant. This shows, that the derivative $\partial g/\partial z$ is periodic with respect to Λ and so it must be constant by Liouville's theorem. It follows that $g : \mathbb{C} \longrightarrow \mathbb{C}$ is a linear function (recall that $g(0) = 0$), so $g(z) = \theta z$ for some $\theta \in \mathbb{C}$. Since we clearly have $g(\Lambda) \subset \Lambda$, then in fact $\theta \in \Lambda$ and $\theta\Lambda \subset \Lambda$. This defines a faithful representation

$$\mathrm{End}(E) \longrightarrow \mathrm{End}(\mathbb{Z}^2).$$

In particular θ is always a zero of a monic, quadratic polynomial. This shows, that either $\mathrm{End}(E) = \mathbb{Z}$ or $\mathrm{End}(E)$ is an order in a quadratic number field.

Let us now return to the main theme. Speaking of the Tate's module it seems natural to ask about the image of (2). In fact, this paper is devoted to answer this question in case of varieties which are defined over finite fields. However, before going into the details, let us first recall the notion of the *field of definition*.

Definition 1.2.2. We say that an variety X is defined over a field $k_0 \subset k$, if there exists a scheme X_0 over k_0 and an isomorphism (of schemes over k)

$$X \simeq X_0 \times_{k_0} k. \quad (6)$$

If furthermore, X is an abelian variety then the term "is defined over k_0" also means that the morphisms determining the group structure on X, i.e., the group law, inversion map and the identity element, are induced (by pulling back) by morphisms of the form

$$X_0 \times_{k_0} X_0 \longrightarrow X_0, \quad X_0 \longrightarrow X_0, \quad \mathrm{Spec}\, k_0 \longrightarrow X_0. \quad (7)$$

Instead of "morphism defined over k_0", we will often write "k_0-morphism" for brevity. The same convention applies to other objects which can be defined over smaller field, e.g., "k_0-line bundles".

Remark. Suppose X is defined over k_0. Then it can also be defined over any larger subfield of k. Note, that if X is of finite type over k (and abelian varieties are), then k_0 can be chosen to be of finite type over the prime field.

---

[6] We will consequently use this abbreviation to denote $X \times_{\mathrm{Spec}\, k_0} \mathrm{Spec}\, k$.

[7] Probably a better way to express the same is to use the notion of *group schemes*, which we tried to avoid here. See Mumford [7, §11] for more details on this subject.

Remark. The statement "X is defined over k_0" will always mean that the object we are interested in is X_0 rather than X, which is only seen to be the result of a base extension. Think of X_0 as being fixed once and for all, for only then the notion of $\overline{k}_0$-rational points and the action of Galois group $\mathrm{Gal}(\overline{k}_0/k_0)$ is well defined.

As we have already mentioned every abelian variety is automatically projective. ([8]) It particular, one may also think of X, (defined over k_0), as a subvariety of a projective space over k given by homogeneous equations with coefficients in k_0.

Remark. Suppose that X is an abelian variety defined over k_0. Since the set $X(k_0)$ of k_0-rational points is mapped to itself by every k_0-morphism and the group structure on X is given by k_0-morphisms, then $X(k_0)$ forms a subgroup of X. We can not resist mentioning the following beautiful theorem first proved by Louis Mordell, but only for elliptic curves over $\mathbb{Q}$, and then generalized by André Weil to the higher dimensional case:

Theorem 1.2.3 (Mordell-Weil-Lang)**.** *If the abelian variety X is defined over a finitely generated field k_0, then the group $X(k_0)$ is finitely generated.*

Proof. See Mumford [7, Appendix II].

1.3. **Statement of the main theorem.** We can now return to describing the image of (2). Suppose that k_0 is a field of definition of both X and Y. In particular, the zero elements are k_0-rational, and so are the elements in the fibers ([9])

$$X_{l^i} = (l^i)_X^{-1}(0), \qquad Y_{l^i} = (l^i)_Y^{-1}(0).$$

Since furthermore, the fibers are stable under Galois conjugations, there is a natural (discrete) action of $G := \mathrm{Gal}(\overline{k}_0/k_0)$ on X_{l^i} and Y_{l^i}, which commutes with the "multiplication by l" map. This gives rise to a continuous Galois action on both $T_l(X)$ and $T_l(Y)$. ([10]) For any subgroup $H \subset G$ we may now consider the subset

$$\mathrm{Hom}_{\mathbb{Z}_l[H]}(T_l(X), T_l(Y)) \subset \mathrm{Hom}_{\mathbb{Z}_l}(T_l(X), T_l(Y))$$

consisting of $\mathbb{Z}_l[H]$-morphisms, i.e. $\mathbb{Z}_l$-homomorphisms $\varphi : T_l(X) \longrightarrow T_l(Y)$, such that $\sigma \circ \varphi = \varphi \circ \sigma$ for any $\sigma \in H$, or equivalently, the H-invariant elements $\varphi \in \mathrm{Hom}_{\mathbb{Z}_l}(T_l(X), T_l(Y))$, provided that we let $\sigma \in G$ act on φ by the formula $\sigma.\varphi = \sigma \circ \varphi \circ \sigma^{-1}$.

Now, any morphism $f : X \longrightarrow Y$ takes points of finite order in X into the points of finite order in Y. Since both sets are $\overline{k}_0$-rational and dense in X and Y respectively, ([11]) it follows that f is already defined over $\overline{k}_0$,

[8] This is sometimes called "embedding theorem of Lefschetz"; see also Theorem 2.2.5 for more precise result.

[9] This is because the maps $(l^n)_X$, $(l^n)_Y$ are finite and they are defined over k_0 as well. The problem reduces to the simple fact that a finite-dimensional local algebra over an algebraically closed filed remains local after extending the base field.

[10] Let us recall, that the group $\mathrm{Gal}(\overline{k}_0/k_0)$ is equipped with the *Krull topology*. This is the same as compact-open topology if one consider $\overline{k}_0$ as a discrete topological space.

[11] See Observation 2.6.5.

([12]) and so it is defined over some finite extension k_1/k_0. It follows that $\sigma f(x) = f(\sigma x)$ for any $\overline{k}_0$-rational point $x \in X$ and any $\sigma \in \mathrm{Gal}(\overline{k}_0/k_1)$. Hence, if we denote the set of morphisms which are defined over k_1 by $\mathrm{Hom}_{k_1}(X,Y)$, then

$$\mathrm{Hom}(X,Y) = \bigcup_{\substack{k_1/k_0 \text{ finite} \\ \text{extension}}} \mathrm{Hom}_{k_1}(X,Y), \tag{3}$$

and the natural homomorphism (2) restricts to

$$\mathbb{Z}_l \otimes \mathrm{Hom}_{k_1}(X,Y) \longrightarrow \mathrm{Hom}_{\mathbb{Z}_l}(T_l(X), T_l(Y))^{\mathrm{Gal}(\overline{k}_0/k_1)}.$$

From now on, for the sake of simplicity, we will only consider those morphisms which are defined over k_0. Note, that it does not change our perspective at all. In fact, by Theorem 1.2.1 the left-hand-side of (3) is a finitely generated abelian group, so the sum is actually finite. It follows, that in the worst case we can always replace k_0 by some finite extension to get $\mathrm{Hom}(X,Y) = \mathrm{Hom}_{k_0}(X,Y)$. The main goal of this paper is to prove the following

Theorem 1.3.1 (Tate)**.** *Suppose that the abelian variety is defined over a finite field k_0. Then the homomorphism*

$$\mathbb{Z}_l \otimes \mathrm{Hom}_{k_0}(X,Y) \longrightarrow \mathrm{Hom}_{\mathbb{Z}_l}(T_l(X), T_l(Y))^{\mathrm{Gal}(\overline{k}_0/k_0)}. \tag{4}$$

is already bijective.

Remark. This theorem was first proved by John Tate in [10], where he also conjectured that the statement may also be true for number fields. It seemed very reasonable, since such a result had been already known for elliptic curves. The problem was eventually solved by Gerd Faltings in 1983 in his famous paper [2].

Currently, we know that the theorem holds for any field of finite type over the prime field. The Faltings' proof works for function fields as well if $\mathrm{char}\, k = 0$. The case of positive characteristic was solved by Yurij Zahin. A simple proof of this last case was also found by Moret-Bailly in 1983.

In the following sections we are going to present the original proof of Tate (cf. [10]), enhanced with some additional refinements due to C. P. Ramanujam (see Mumford [7, Appendix I]).

2. Abelian varieties

The goal of this section, is to provide the reader with a minimal background and collect some fundamental facts about abelian varieties which we will need later in the proof of Tate's theorem (see Theorem 1.3.1). With a few exceptions, we will only state theorems without proving them. However, we will always try to give appropriate clues to help the reader find the

[12] To see this, just verify the following simple fact: Let L/K be any field extension and let $A := L[X_1, \ldots, X_n]/I$ be an L-algebra where I is generated by some polynomials with coefficients in K. Suppose that the set $\{x_i\} \subset k^n$ is such that for any $f \in A$ the identity $f(x_i) = 0$, for all i, implies $f \in I$. Then, given $g \in A$ with $g(x_i) \in k$, for all i, one can represent g by a polynomial with coefficients in k.

proofs in the literature. Our main references are Mumford [7], Hindry and Silverman [5].

2.1. **Morphisms and commutativity.** We will now verify some of the properties which were pointed out in the introduction. First, we will prove that any regular map between abelian varieties is a composition of group homomorphism and a translation. Then, we conclude that an abelian variety is necessarily a commutative group. Finally, we will observe that in the category of abelian varieties the product and coproduct can be modeled by the same variety. Let us start by proving: ([13])

Lemma 2.1.1 (rigidity/constancy lemma)**.** *Let X be a complete variety, Y and Z varieties, and $f : X \times Y \longrightarrow Z$ a morphism such that for some $y_0 \in Y$, $f(X \times \{y_0\})$ is a single point z_0 in Z. Then there is a morphism $g : Y \longrightarrow Z$ such that if $p_2 : X \times Y \longrightarrow Y$ is the projection, $f = g \circ p_2$.*

Proof. Choose any $x_0 \in X$ and let us define $g : Y \longrightarrow Z$ by $g(y) = f(x_0, y)$. We are now going to verify that $f = g \circ p_2$ on some nonempty open subset of $X \times Y$. Note, that this will actually show, that the equality holds on $X \times Y$. ([14])

Let U be any affine neighborhood of z_0, and set $F = Z \setminus U$. Since X is complete, then $G = p_2(f^{-1}(F))$ is a closed subset of Y, and $y_0 \notin Y$. Furthermore, for any $y \notin G$ the image of the complete variety $f(X \times \{y\})$ is contained in the affine variety U, hence it must be a single point. ([15]) In particular, for such y one has the equality

$$f(x, y) = f(x_0, y) = g(p_2(x, y))$$

which shows, that f and $g \circ p_2$ agree on $p_2^{-1}(Y \setminus G)$. □

Corollary 2.1.2. *If X and Y are abelian varieties and $f : X \longrightarrow Y$ is any morphism, then $f = \tau_y \circ h$ where h is a homomorphism of X into Y, $y \in Y$ and τ_y denotes the "translation by y" map. We will make use of this notion later in this paper.*

Proof. By composing f with a suitably chosen translation, we reduce to the case when f sends the neutral element of X to the neutral element of Y. We are now going to verify that this is already a group homomorphism. To this end, let us define a morphism of varieties

$$\varphi : X \times X \ni (x, y) \longmapsto f(xy)f(y)^{-1}f(x)^{-1} \in X.$$

If we show, that φ maps $X \times X$ to a single point then we are done. But X is a complete variety, and since $\varphi(X \times \{e\}) = \{e\}$ and also $\varphi(\{e\} \times X) = \{e\}$, this shows by Lemma 2.1.1 that φ neither depends on the first nor on the second argument, and so it is a constant map. □

[13] See also Mumford [7, p. 43], Hindry and Silverman [5, Lem. A.7.1.1], or Bombieri and Gubler [1, Lem. 8.2.6]

[14] The set on which the two morphisms agrees is closed because Z is separated, and every open subset of $X \times Y$ is dense since $X \times Y$ is irreducible.

[15] This is because the variety $V := f(X \times \{y\})$ is both affine and complete. If $\dim V > 0$, then the projective closure of V would contain points at infinity, which is impossible since V is complete. For moclosure However, if $\dim f(X \times \{y\}) > 0$, then the re details, see Bombieri and Gubler [1, A.6.15 as well as A.10.18].

Corollary 2.1.3. *If X is an abelian variety, then X is a commutative group.*

Proof. A group is commutative if and only if the inverse map is a group homomorphism. But the inverse map is a morphism of abelian varieties which sends the neutral element to itself, so by Corollary 2.1.2 it is a group homomorphism. □

The following fact is a consequence of the commutativity of abelian varieties The verification is left to the reader.

Observation 2.1.4. *The diagram*

$$X \longrightarrow X \times Y \longleftarrow Y$$

with the arrows given by $x \longmapsto (x, 0)$ and $y \longmapsto (0, y)$ respectively, is the coproduct in the category of abelian varieties.

Corollary 2.1.5. *Let $X_1, \ldots, X_r$ be abelian varieties. Then, there is a natural isomorphisms of groups*

$$\operatorname{End}(X_1 \times \ldots \times X_r) \simeq \bigoplus_{i,j=1}^{r} \operatorname{Hom}(X_i, X_j). \tag{5}$$

Furthermore, if all X_i's are all defined over k_0, then so is their product. It follows, that the correspondence remains correct if we restrict both sides to morphisms defined over k_0.

Proof. A standard consequence of Observation 2.1.4.

Remark. Note, that the the right-hand-side group in (5) has a natural ring structure. More precisely, this is a ring of $r \times r$ matrices filled in with adequate morphisms of abelian varieties. Clearly (5) becomes ring isomorphism in this setup.

With a help of this simple tools, we can already perform the first reduction of Theorem 1.3.1. This is summarized in the following

Corollary 2.1.6. *Suppose that we already know, that the conclusion of Theorem 1.3.1 is true with $X = Y$. Then it holds true in general.*

Proof. Let $G = \operatorname{Gal}(\overline{k}_0/k_0)$, and suppose that we already know that

$$\mathbb{Z}_l \otimes_{\mathbb{Z}} \operatorname{End}_{k_0}(X \times Y) \simeq \operatorname{End}_{\mathbb{Z}_l[G]}(T_l(X \times Y)) \tag{6}$$

Since clearly $T_l(X \times Y) \simeq T_l(X) \times T_l(Y)$ and G acts diagonally on this module, then by Corollary 2.1.5 both sides of (6) decomposes

$$\begin{aligned}
\mathbb{Z}_l \otimes_{\mathbb{Z}} \operatorname{End}_{k_0}(X) &\simeq \operatorname{End}_{\mathbb{Z}_l[G]}(T_l(X)) \\
\mathbb{Z}_l \otimes_{\mathbb{Z}} \operatorname{Hom}_{k_0}(X, Y) &\simeq \operatorname{Hom}_{\mathbb{Z}_l[G]}(T_l(X), T_l(Y)) \\
\mathbb{Z}_l \otimes_{\mathbb{Z}} \operatorname{Hom}_{k_0}(Y, X) &\simeq \operatorname{Hom}_{\mathbb{Z}_l[G]}(T_l(Y), T_l(X)) \\
\mathbb{Z}_l \otimes_{\mathbb{Z}} \operatorname{End}_{k_0}(Y) &\simeq \operatorname{End}_{\mathbb{Z}_l[G]}(T_l(Y))
\end{aligned}$$

and the result follows. □

2.2. **Existence of ample line bundles.** We are now going to review some unique properties of line bundles on abelian varieties. Unfortunately, the proofs of the most interesting results are out of the scope of this paper. We want to show that every abelian variety admits an ample line bundle, or equivalently it is can be embedded into projective space. The following theorem is of fundamental importance.

Theorem 2.2.1. *Let X be any variety, Y an abelian variety, and $f, g, h : X \longrightarrow Y$ morphisms. Then for all $L \in \mathrm{Pic}(Y)$, we have*

$$(f+g+h)^*L \otimes f^*L \otimes g^*L \otimes h^*L \simeq (f+g)^*L \otimes (g+h)^*L \otimes (h+f)^*L$$

Proof. See Mumford [7, §5, Corollary 2, p. 58], or Hindry and Silverman [5, Corollary A.7.2.4].

Let us recall (see Corollary 2.1.2) that we denote the "translation by x" map by τ_x. As a consequence of Theorem 2.2.1 we get:

Corollary 2.2.2 (Theorem of the square)**.** *Let X be an abelian variety. For all line bundles L and $x, y \in X$*

$$\tau_{x+y}^*L \otimes L \simeq \tau_x^*L \otimes \tau_y^*L.$$

Proof. Just apply Theorem 2.2.1 with $f \equiv x$, $g \equiv y$ and $h = 1_X$. □

Definition. Given any line bundle L on X, we associate with it the following map

$$\phi_L : X \ni x \longmapsto \text{isom. class of } \tau_x^*L \otimes L^{-1} \in \mathrm{Pic}(X). \tag{7}$$

which by Corollary 2.2.2 is a group homomorphism. Let us denote by $K(L)$ the kernel of ϕ_L.

We are now going to characterize the ampleness of a line bundle L associated to an effective divisor in terms of $K(L)$.

Theorem 2.2.3. *Let D be an effective divisor on an abelian variety X and let $L = L(D)$ be the associated line bundle. The following conditions are equivalent.*

1. *The subgroup $H = \{x \in X : \tau_x^*(D) = D\}$ of X is finite (equality of divisors, not only divisor classes).*
2. *$K(L)$ is finite.*
3. *The linear system $|2D|$ has no base points, and defines a finite morphism $X \longrightarrow \mathbb{P}^N$.*
4. *L is ample on X.*

Proof. See Mumford [7, §6, Application 1, p. 60]

Using the above result, we can now prove that every abelian variety is projective.

Corollary 2.2.4. *Every abelian variety admits an ample line bundle. In particular, an abelian variety is always projective.*

Proof. Let X be an abelian variety and let U be an open affine neighborhood of $0 \in X$. We will verify, that the divisor $D = \sum_{i=1}^{r} D_i$, where D_i's are irreducible components of $X \setminus U$, satisfies condition (1) of Theorem 2.2.3. Let us observe that the set

$$H = \{x \in X : \tau_x^*(D) = D\} = \bigcap_{y \in D} (\tau_y)^{-1}(D)$$

is a closed subset of X. ([16]) Note furthermore, that for any $x \in H$, U is stable for τ_x, i.e. $x + U \subset U$. Since $0 \in H$, then in particular $H \subset U$. But U is affine and H is complete, so H must be finite. □

One can give more precise statement concerning the existence of embedding into projective space. The following fact will play a very important role in the proof of the Tate's Theorem.

Theorem 2.2.5 (Lefschetz)**.** *For any ample line bundle L on an abelian variety X, L^n is very ample, if $n \geq 3$.*

Proof. See Mumford [7, §17, Thm. on page 163].

2.3. **The $\mathrm{Pic}^0(X)$ group.** We are now going to look closer at the map

$$\mathrm{Pic}(X) \ni L \longmapsto \phi_L \in \mathrm{Hom}(X, \mathrm{Pic}(X))$$

induced by (7). This is clearly seen to be a group homomorphism. We denote its kernel by $\mathrm{Pic}^0(X)$, i.e.,

$$\mathrm{Pic}^0(X) = \{L \in \mathrm{Pic}(X) : \tau_x^* L \simeq L \text{ for all } x \in X\}.$$

Using Corollary 2.2.2 we can see that the image of $\phi_L : X \longrightarrow \mathrm{Pic}(X)$ is always contained in $\mathrm{Pic}^0(X)$. Indeed, for any $x, y \in X$

$$\tau_x^*(\tau_y^* L \otimes L^{-1}) \otimes (\tau_y^* L \otimes L^{-1})^{-1} \simeq \tau_{x+y}^* L \otimes \tau_x^* L^{-1} \otimes \tau_y^* L^{-1} \otimes L \simeq 0.$$

Let us summarize the above observations by writing down the following exact sequence

$$0 \longrightarrow \mathrm{Pic}^0(X) \longrightarrow \mathrm{Pic}(X) \xrightarrow{L \longmapsto \phi_L} \mathrm{Hom}(X, \mathrm{Pic}^0(X))$$

Define the Nèron-Severi group:

$$\mathrm{NS}(X) := \mathrm{Pic}(X)/\mathrm{Pic}^0(X).$$

This is clearly a subgroup of $\mathrm{Hom}(X, \mathrm{Pic}^0(X))$ and we will also see in a moment that it is torsion free. But first, let us verify the following

Proposition 2.3.1 (Mumford's formula)**.** *Let L be a line bundle on an abelian variety X. Then for any $n \in \mathbb{Z}$*

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

In particular, for any line bundle such that $L \simeq (-1)_X^* L$ we get $n_X^* L \simeq L^{n^2}$.

Definition. A line bundle satisfying $L \simeq (-1)_X^* L$ will be called *symmetric*. Note that the set of symmetric classes forms a subgroup of $\mathrm{Pic}(X)$.

[16] In fact, it is even a subgroup but we will not need it.

Proof of Proposition 2.3.1. The statement is obvious for $n = -1, 0, 1$. By Theorem 2.2.1 applied to $f = n_X$, $g = 1_X$ and $h = (-1)_X$ we get

$$n_X^* L^2 \otimes L \otimes (-1)_X^* L \simeq (n+1)_X^* L \otimes (n-1)_X^* L \tag{8}$$

and the result follows by induction on n (in both directions). □

Corollary 2.3.2. *The map n_X is surjective for any $n \neq 0$ and furthermore $\deg n_X = n^{2g}$ where $g = \dim X$. In particular, n_X is separable if $p \nmid n$.*

Proof. The first assertion follows directly from Proposition 2.3.1. Namely, for any ample line bundle L the formula (8) implies that $n_X^* L$ is again ample. On the other hand, $n_X^* L$ is both ample and trivial on $\operatorname{Ker} n_X$, which is a closed subset of a complete variety, so it follows that $\dim \operatorname{Ker} n_X = 0$. By the dimension formula $\dim \operatorname{Im} n_X + \dim \operatorname{Ker} X = \dim X$, so eventually $\operatorname{Im} n_X = \dim X$, which shows that n_X is surjective.

To prove the second assertion we will need the following simple fact from the intersection theory.

Lemma. *Let X and Y be normal projective varieties of dimension g, and let $f : X \longrightarrow Y$ be a finite morphism. Let $D_1, \ldots, D_g$ be divisors on Y. Then*

$$(f^* D_1, \ldots, f^* D_g)_X = (\deg f) \cdot (D_1, \ldots, D_g)_Y.$$

Proof. For a sketch of the proof see for example Hindry and Silverman [5, Thm. A.2.3.2 and also Exercise A.2.10].

To finish the argument, let D be the divisor associated to a symmetric ample line bundle L. ([17]) Let us verify

$$\begin{aligned} \deg(n_X) \cdot (D, \ldots, D) &= (n_X^* D, \ldots, n_X^* D) && \text{by the Lemma} \\ &= (n^2 D, \ldots, n^2 D) && \text{by Proposition 2.3.1} \\ &= n^{2g} \cdot (D, \ldots, D) \end{aligned}$$

Since D is ample, $(D, \ldots, D) > 0$ and the result follows. □

Corollary 2.3.3. *The group $\mathrm{NS}(X)$ is torsion free.*

Proof. Suppose that $L^n \in \mathrm{Pic}^0(X)$ for some $n \in \mathbb{Z}$. Then for any $x \in X$

$$\phi_L(nx) = n\phi_L(x) = \phi_{L^n}(x) = 0.$$

But n_X is surjective, so $\phi_L \equiv 0$. □

Before moving further, let us recall another fundamental fact, which is

Theorem 2.3.4 (seesaw theorem)**.** *Let X be a complete variety, Y any variety and L a line bundle on $X \times Y$. Then the set*

$$Y_1 = \{y \in Y : L|_{X \times \{y\}} \text{ is trivial on } X \times \{y\}\}$$

is closed in Y, and if on $X \times Y_1$, $p_2 : X \times Y_1 \longrightarrow Y_1$ is the projection, then $L\,|_{X \times Y_1} \simeq p_2^*(M)$ for some line bundle M on Y_1. In particular, if $Y_1 = Y$ and for some y_0 the restriction of L to the slice $X \times \{y_0\}$ is trivial, then L is trivial.

[17] For any ample line bundle L, $L \otimes (-1)_X^* L$ is both symmetric and ample.

Proof. See Mumford [7, §5, Corollary 6, p. 54], or Hindry and Silverman [5, Lemma A.7.2.3].

Corollary 2.3.5. *Let X be an abelian variety, L a line bundle on X. Then*

$$L \in \mathrm{Pic}^0(X) \iff \tau_x^* L \otimes L^{-1} \simeq 0 \text{ for all } x \iff m^* L \simeq p_1^* L \otimes p_2^* L$$

where $m : X \times X \longrightarrow X$ denotes the addition map, and $p_1, p_2 : X \times X \longrightarrow X$ are the corresponding projections.

Proof. Let $M := m^* L \otimes p_1^* L^{-1} \otimes p_2^* L^{-1}$. By Theorem 2.3.4, M is trivial if and only if $M|_{X \times \{x\}} \simeq \tau_x^* L \times L^{-1}$ is trivial for any $x \in X$ and $M|_{\{0\} \times X}$ is trivial, which is always the case by the same isomorphism. □

Corollary 2.3.6. *Let X be a variety, Y an abelian variety, $f, g : X \longrightarrow Y$ morphisms. Then for any $L \in \mathrm{Pic}^0(Y)$*

$$(f+g)^* L \simeq f^* L \otimes g^* L.$$

In particular $n_Y^* L \simeq L^n$ for any $n \in \mathbb{Z}$.

Proof. By Lemma 2.3.5, $m^* L \otimes \simeq p_1^* L \otimes p_2^* L$. Pulling this identity back by $(f, g) : X \longrightarrow Y \times Y$ yields the equation. The second assertion follows by induction on n. □

Corollary 2.3.7. *If $L \in \mathrm{Pic}^0(X)$ is symmetric, then $L^2 \simeq 0$.*

Proof. By Corollary 2.3.6 and symmetry $L^{-1} \simeq (-1)_X^* L \simeq L$. □

Theorem 2.3.4 can be also used to proof the following

Proposition 2.3.8. *$K(L)$ is a Zariski-closed subgroup of X.*

Proof. Let $m : X \times X \longrightarrow X$ denote the addition map and $p_1 : X \times X \longrightarrow X$ the first projection. Consider a line bundle $m^* L \otimes p_1^* L^{-1}$ on $X \times X$, then

$$y \in K(L) \iff T_y^* L \otimes L^{-1} \simeq 0 \iff m^* L \otimes p_1^* L^{-1} \,|_{X \times \{y\}} \simeq 0$$

so $K(L)$ is closed by Theorem 2.3.4. □

2.4. **Riemann forms.** Only for the purpose of this section we introduce the notation $\widehat{X} := \mathrm{Pic}^0(X)$. We do it for purely notational reasons, but is is worth mentioning that $\widehat{X}$ usually denotes the *dual variety*. This is an abelian variety which is naturally isomorphic to $\mathrm{Pic}^0(X)$ as a group. We are not going to go deeper into this subject, since we will only use the abstract group structure of $\widehat{X}$.

Given an ample line bundle L on X, we are going to construct a non-degenerated skew-symmetric bilinear form

$$e^L : T_l(X) \times T_l(X) \longrightarrow M_l$$

where M_l stands for the limit of the inverse system

$$\ldots \xleftarrow{(-)^l} \mu_{l^{i-1}} \xleftarrow{(-)^l} \mu_{l^i} \xleftarrow{(-)^l} \mu_{l^{i+1}} \xleftarrow{(-)^l} \ldots$$

with $k \supset \mu_{l^i} :=$ the group of l^i-th roots of unity. Let us first define a map

$$\overline{e}_n : X_n \times (\widehat{X})_n \longrightarrow \mu_n \tag{9}$$

To this end, take any $\lambda \in (\widehat{X})_n$ and let D be the associated divisor. By Corollary 2.3.6 we have $\lambda^n \simeq 0$ as well as $n_X^* \lambda \simeq 0$. It follows that there

exist rational functions f, g on X with $(f) = nD$ and also $(g) = n_X^{-1}D$. Since furthermore $(f \circ n_X) = n \cdot n_X^{-1}D = (g^n)$, the fact that X is complete implies that for some constant $c \in k$, we have $g^n = c(f \circ n_X)$. In particular, for any $x \in X_n$

$$\left(\frac{g(y)}{g(x+y)}\right)^n = \frac{cf(ny)}{cf(nx+ny)} \equiv 1, \qquad \text{for all } y \in X.$$

It follows that the function $y \mapsto g(y)/g(y+x)$ is constant and equals an n-th root of unity. This allows us to define

$$\overline{e}_n(x, \lambda) := \frac{g(y)}{g(x+y)} \quad \text{(with any } y\text{)}$$

One then verifies the following

Theorem 2.4.1. *If $p \nmid n$ then the map (9) is a perfect pairing. Let m be another integer coprime to the characteristic and $x \in X_{mn}$, $\lambda \in (\widehat{X})_{mn}$. Then*

$$\overline{e}_n(mx, m\lambda) = (\overline{e}_{mn}(x, \lambda))^m$$

Proof. For the proof of the first statement see Mumford [7, §6, Prop. 6 and Thm. 4, as well as §20 Lemma on page 184]. For the second one see Mumford [7, §20, Prop. on page 185].

Now take any prime $l \neq p$. By Theorem 2.4.1, we have the following identity for any $i \geq 0$

$$\overline{e}_{l^i}(lx, l\lambda) = \overline{e}_{l^{i+1}}(x, \lambda)^l, \quad \text{for all } x \in X_{l^{i+1}}, \lambda \in (\widehat{X})_{l^{i+1}}.$$

This says, that the mapping

$$e_l : T_l(X) \times T_l(\widehat{X}) \ni ((x_i), (\lambda_i)) \longmapsto (\overline{e}_{l^i}(x_i, y_i)) \in M_l$$

is well defined. Also by Theorem 2.4.1, we can see that e_l is a non-degenerated bilinear form. Finally, we can define the *Riemann form* associated with a line bundle.

Definition 2.4.2. s For any line bundle L on X let us define

$$e^L : T_l(X) \times T_l(X) \ni (x, \lambda) \longmapsto e_l(x, T_l(\phi_L)(y)) \in M_l.$$

By the above discussion this is easily seen to be a bilinear form, which is also non-degenerated as long as L is ample. ([18])

Among many other important properties of the Riemann form we will particularly need the following three.

Theorem 2.4.3. *The Riemann form e^L of any line bundle L is skew-symmetric.*

Proof. See Mumford [7, §20, Thm 1, p. 186].

Proposition 2.4.4. *If $f : X \longrightarrow Y$ is a morphism of abelian varieties and L a line bundle on Y, we have*

$$e^{f^*L}(x, y) = e^L(T_l(f)(x), T_l(f)(y)), \quad \textit{for all } x, y \in T_l(X).$$

[18] Note, that $T(\phi_L)(y)$ for some $y \in T_l(X) \setminus 0$ implies that $K(L)$ is infinite, which would contradict the ampleness of L.

Proof. See Mumford [7, §20, eq. II, p. 187].

Proposition 2.4.5. *If X is an abelian variety defined over k_0 and L is a k_0-bundle, then for any $\sigma \in \mathrm{Gal}(\overline{k}_0/k_0)$*

$$e^L(\sigma x, \sigma y) = \sigma e^L(x, y), \quad \text{for all } x, y \in T_l(X).$$

The Galois action on the right-hand-side is given by ([19])

$$M_l \ni (\xi_i)_i \longmapsto (\sigma(\xi_i))_i \in M_l.$$

Proof. The proof is exactly the same as in the case of Weil pairing for elliptic curves. For the latter see Silverman [8, Ch. III, Prop. 8.1(d)].

2.5. **Dividing by a finite subgroup.** Given a variety X (not necessarily abelian) and a group of automorphisms $G \subset \mathrm{Aut}(X)$ acting on X, we would like to have some natural structure of variety on the set of orbits, which we will denote by X/G. It is not always the case, but we have the following result, which will be sufficient for our needs.

Theorem 2.5.1. *Let X be an algebraic variety, and G a finite group of automorphisms of X. Suppose that for any $x \in X$, the orbit G_x of x is contained in an affine open subset of X. Then there is a pair (Y, π), where Y is a variety and $\pi : X \longrightarrow Y$ a morphism, satisfying the following conditions:*

(i) as a topological space, (Y, π) is the quotient of X for the G-action,
(ii) if $\pi_*(\mathcal{O}_X)^G$ denotes the subsheaf of G-invariants of $\pi_*(\mathcal{O}_X)$ for the action of G on $\pi_*(\mathcal{O}_X)$ deduced from (i), the natural homomorphism $\mathcal{O}_Y \longrightarrow \pi_*(\mathcal{O}_X)^G$ is an isomorphism.

The pair (Y, π) is determined up to isomorphism by these conditions. The morphism π is finite, surjective and separable. Y is affine if X is affine.

If further G acts freely on X (that is, if $gx \neq x$ for any $x \in X$ and any $g \in G$ with $g \neq e$), then π is an étale morphism.

Remark. Since an abelian variety is always projective (see Corollary 2.2.4), the assumption concerning the existence of open affine subset containing G_x is trivially satisfied, because the orbit G_x is a finite set.

Sketch of the proof. First, construct a locally ringed space according to (i) and (ii). Our goal now is to verify that this space is in fact it is a variety. The assumption about the orbits allows us to reduce to the affine case. Then one uses the following algebraic fact: ([20])

Lemma 2.5.2 (Hilbert)**.** *Let A be an integral domain that is a finitely generated k-algebra. Let G be a finite group that acts on A as a k-algebra. Then the fixed subalgebra*

$$A^G = \{a \in A : g(a) = a \text{ for all } g \in G\}$$

is again a finitely generated k-algebra.

For more details refer to Mumford [7, §7, Thm. on page 66], or Hindry and Silverman [5, Thm. A.8.3.1].

[19] Recall that we defined $M_l := \lim_i \mu_{l^i}$.
[20] See Hindry and Silverman [5, Prop. A.8.3.2].

Suppose that we are working with an abelian variety which is defined over k_0. Then we will also need the following stronger result, which gives us some control on the field definition of the quotient variety.

Theorem 2.5.3. *Let X be an abelian variety defined over k_0. Let us consider a finite subgroup $K \subset X(k_1)$ acting on X by translations, with with k_1/k_0 a finite Galois extension. Suppose furthermore that K is stable under the action of $\mathrm{Gal}(k_1/k_0)$. Then the quotient X/K can be defined over k_0.*

Proof. See Mumford [7, Appendix I, Lem. 2, p. 244].

Observation 2.5.4. *Suppose that the quotient $\pi : X \longrightarrow X/G$ exists. Then any morphism $f : X \longrightarrow Y$ with $f \circ g = f$, for $g \in G$, factorizes uniquely $f = \lambda \circ \pi$ where $\lambda : X/G \longrightarrow Y$. If furthermore X, X/G, π, Y and f are all defined over some perfect field k_0, then so is λ.*

Sketch of the proof. First, use the properties (i) and (ii) indicated in the statement of Theorem 2.5.1 to see, that such a λ exists and furthermore it is unique. For the second assertion use the fact that f and π are defined over k_0 to see, that λ is invariant under the action of $\mathrm{Gal}(\overline{k}_0/k_0)$. Now, since k_0 is perfect, λ is also defined over k_0.

Corollary 2.5.5. *With the hypothesis of Theorem 2.5.3, suppose furthermore that k_0 is perfect. Then X/K is an abelian variety defined over k_0.*

Proof. We already know, that X/K is defined over k_0 as a variety, but we still need to verify that the group structure can be also defined over k_0. Let $m : X \times X \longrightarrow X$ denote the addition map and $\pi : X \longrightarrow X/K$. Since $\mathrm{Ker}(\pi \circ m)$ contains $K \times K = \mathrm{Ker}(\pi \times \pi)$, $(\pi \circ m)$ factorizes as $\pi \circ m = \overline{m} \circ (\pi \times \pi)$ for some $\overline{m} : X/K \times X/K \longrightarrow X/K$. Then $\overline{m}$ is defined over k_0 by Observation 2.5.4. A similar argument can be used to prove that the inverse map is defined over k_0. □

Remark 2.5.6. We already now that the map $n_X : X \longrightarrow X$ is surjective and has a finite kernel $K := X_n$, which is isomorphic to $(\mathbb{Z}/n)^{2g}$, at least if $p \nmid n$. Furthermore, K acts on X freely by translations. By Theorem 2.5.1, the set X/K has a structure of a smooth variety and by Observation 2.5.4 there exists a bijective morphism $\lambda : X/K \longrightarrow X$ with $n_X = \lambda \circ \pi$. Note, that is of a great importance to know if λ is an isomorphism. Indeed, for suppose that we are given a morphism $f : X \longrightarrow Y$ with finite kernel anihilated by n, i.e. $\mathrm{Ker}\, f \subset K$. Then, we naturally expect that it factorizes trough n_X. But it seems that there is no simple way to prove this unless we now that $\lambda : X/K \simeq X$ and use Observation 2.5.4. Note however, that bijectivity of λ implies $\deg \lambda = 1$, which shows that λ is birational. Now, one can use the following result to see that this is in fact an isomorphism.

Lemma. *A rational map from a smooth variety to an abelian variety is a morphism.*

Proof. See Bombieri and Gubler [1, Cor. 8.2.22].

Theorem 2.5.7. ([21]) *Suppose that $\pi : X \longrightarrow X'$ is a surjective morphism of abelian varieties and $\dim X = \dim X'$. Let $f : X \longrightarrow Y$ be another*

[21] See also Mumford [7, §7, Thm 4, p. 72] for another formulation.

morphism with $\operatorname{Ker}\pi \subset \operatorname{Ker} f$. *Then, there exist* $\lambda : X' \longrightarrow Y$ *such that* $f = \lambda \circ \pi$. *If furthermore all the objects are defined over a perfect field* k_0, *then so is* λ.

Proof. Just mimic the argument presented in Remark 2.5.6. For the second part, note that thanks to the assumption that k_0 is perfect we may also assume that $\operatorname{Ker}(\pi) \subset X(k_1)$ for some finite Galois extension k_1/k_0, so we can use both Theorem 2.5.3 and Observation 2.5.4 to conclude that λ is defined over k_0. The details are left to the reader.

Definition. A surjective morphism $f : X \longrightarrow Y$ with finite kernel is called an *isogeny*. We say that X and Y are *isogenous* if there exists an isogeny from X to Y. It turns out, that it is an equivalence relation. Clearly, "isogenous" implies "equal dimension".

Theorem 2.5.8. *Given an isogeny* $f : X \longrightarrow Y$ *with* $\deg f = n$ *one can find another isogeny* $g : Y \longrightarrow X$ *such that* $g \circ f = n_X$ *and also* $f \circ g = n_Y$. *If furthermore* f *is defined over perfect field* k_0, *then so is* g.

Proof. The existence of g with $g \circ f = n_X$ follows from Theorem 2.5.7. But then $f \circ g = n_X$ too. Indeed, for all $y \in Y$, $y = f(x)$ for some x. Therefore

$$f(g(y)) = f(g(f(x))) = f(nx) = nf(x) = ny.$$

The assertion concerning the field of definition is clear. □

We are now going to use the above results to perform another reduction of Theorem 1.3.1. Let us prove

Lemma 2.5.9. *In the notation of Theorem 1.3.1, let* C *be the cokernel of the map*

$$\mathbb{Z}_l \otimes_{\mathbb{Z}} \operatorname{Hom}_{k_0}(X, Y) \longrightarrow \operatorname{Hom}_{\mathbb{Z}_l[G]}(T_l(X), T_l(Y)).$$

Then C *is a free* $\mathbb{Z}_l$*-module.*

Proof. Tensoring the exact sequence with $\mathbb{F}_l$ ([22]) one gets

$$0 = \operatorname{Tor}_1^{\mathbb{Z}_l}(M, \mathbb{F}_l) \longrightarrow \operatorname{Tor}_1^{\mathbb{Z}_l}(C, \mathbb{F}_l) \longrightarrow M'/lM' \longrightarrow M/lM \tag{10}$$

where M' and M stand for $\mathbb{Z}_l \otimes_{\mathbb{Z}} \operatorname{Hom}_{k_0}(X, Y)$ and $\operatorname{Hom}_{\mathbb{Z}_l[G]}(T_l(X), T_l(Y))$, respectively. Note, that $\operatorname{Tor}_1^{\mathbb{Z}_l}(M, \mathbb{F}_l) = 0$ because M is free. ([23])

Suppose that we already verified that the map $M'/lM' \longrightarrow M/lM$ is injective. Then, by exactness of (10) we get $\operatorname{Tor}_1^{\mathbb{Z}_l}(C, \mathbb{F}_l) = 0$. Since $\mathbb{Z}_l$ is a local ring with residual field equal to $\mathbb{F}_l$ and C is finitely generated, this already shows that C is a free $\mathbb{Z}_l$-module. ([24])

Now we only need to check that $M'/lM' \longrightarrow M/lM$ is injective. To this end, suppose that $T_l(\varphi) \in lM$ for some $\varphi \in \operatorname{Hom}_{k_0}(X, Y)$. ([25]) It follows that $\varphi(X_l) \subset lY_l = 0$, so by Theorem 2.5.7 ($k_0$ is perfect because it is finite) there exists $\psi \in \operatorname{Hom}_{k_0}(X, Y)$ with $\varphi = \psi \circ l_X = l_Y \circ \psi$ so indeed $\varphi \in lM'$. □

[22] The structure of $\mathbb{Z}_l$-module on $\mathbb{F}_l$ is given by the natural mapping $\mathbb{Z}_l \longrightarrow \mathbb{Z}_l/l\mathbb{Z}_l = \mathbb{F}_l$.

[23] It is a submodule of $\mathbb{Z}_l \otimes_{\mathbb{Z}} \operatorname{Hom}(X, Y)$, which is a free $\mathbb{Z}_l$-module of finite rank (see Theorem 1.2.1) and $\mathbb{Z}_l$ is a principal ideal domain.

[24] This is a corollary from Nakayama's lemma.

[25] Observe that in fact $M'/lM' = \operatorname{Hom}(X, Y)/l \operatorname{Hom}(X, Y)$ so we do not really need to consider $\varphi \in \mathbb{Z}_l \otimes \operatorname{Hom}(X, Y)$.

Definition. For any abelian variety X let $V_l(X) := \mathbb{Q}_l \otimes_{\mathbb{Z}_l} T_l(X)$.

Corollary 2.5.10. *To prove Theorem 1.3.1 it is enough to verify that the homomorphism*

$$\mathbb{Q}_l \otimes_{\mathbb{Z}} \mathrm{End}_{k_0}(X) \longrightarrow \mathrm{End}_{\mathbb{Q}_l[G]}(V_l(X)) \tag{11}$$

is surjective for any abelian variety X defined over k_0 and $l \neq p = \mathrm{char}\, k_0$.

Proof. First, use Corollary 2.1.6 to reduce to the case $X = Y$. Then, in the notation of Lemma 2.5.9 observe that the cokernel of (11) equals $\mathbb{Q}_l \otimes_{\mathbb{Z}_l} C$. Since C is free $\mathbb{Z}_l$-module, $\mathbb{Q}_l \otimes_{\mathbb{Z}_l} C = 0 \iff C = 0$. □

2.6. **Poincaré complete reducibility.** Motivated by Corollary 2.5.10 we will now be interested in the properties of the ring $\mathrm{End}_{k_0}(X)$, or more precisely the $\mathbb{Q}$-algebra $\mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}_{k_0}(X)$. As we have seen in the previous section, most of the results which give us the possibility to control the field of definition rely on the fact that the field of definition is perfect. So let us agree, that for the purpose of this paragraph, the field of definition will always be perfect.

Definition. We say that an abelian variety X defined over k_0 is *k_0-simple* if it does not contain any nontrivial abelian k_0-subvariety; X is *simple* if it is k-simple.

Lemma 2.6.1. *If X is k_0-simple, then $\mathbb{Q} \otimes \mathrm{End}_{k_0}(X)$ is a division algebra.*

Proof. Suppose that $f : X \longrightarrow X$ is k_0-endomorphism. Then, its image is k_0-abelian subvariety, so by the assumption it is either X or a single point, in which case f the zero element of $\mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}_{k_0}(X)$. On the other hand, if f is surjective, then it is an isogeny so by Theorem 2.5.8 there exists a k_0-isogeny $g : X \longrightarrow X$ such that $g \circ f = f \circ g = n_X$, which shows that f is invertible in $\mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}_{k_0}(X)$. □

Theorem 2.6.2 (Poincaré complete reducibility theorem)**.** *If X is abelian variety and Y is an abelian subvariety there is an abelian variety Z such that $Y \cap Z$ is finite and $Y + Z = X$. In other words, X is isogenous $Y \times Z$. If furthermore X is defined over k_0 and Y is a k_0-subvariety then Z can be chosen to be a k_0-variety.*

Proof. See Mumford [7, §19, Thm. 1, p. 173 and also Appendix I, argument on page 255]. □

Corollary 2.6.3. *Any abelian variety X defined over k_0 is k_0-isogenous to a product*

$$X_1^{n_1} \times \ldots \times X_k^{n_k}$$

with some positive n_i and mutually nonisogenous k_0-simple varieties X_i. Furthermore, the pairs (X_i, n_i) are uniquely determined by X.

Corollary 2.6.4. *Suppose that X is an abelian variety defined over k_0. Then the algebra*

$$End^0_{k_0}(X) := \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}_{k_0}(X)$$

is a semisimple ring. Furthermore $K \otimes_{\mathbb{Z}} \mathrm{End}_{k_0}(X)$ is a semisimple K-algebra for any field extension $K/\mathbb{Q}$.

Proof. The first assertion is a consequence of Corollary 2.6.3 and the properties of morphisms between products of abelian varieties. ([26]) The latter is a general property of finite-dimensional semisimple algebras (see Theorem A.4.2). □

Finally, we give a simple result concerning the topology of the set of l-torsion points.

Observation 2.6.5. *For any prime number $l \neq p$, the set*

$$X_{l^\infty} = \{x \in X : l^n x = 0 \text{ for some } n \geq 0\}$$

is dense in X.

Sketch of the proof. Consider the closure of X_{l^∞} which is a subgroup of X. Let Y be the connected component of zero. Now suppose that $\dim Y < \dim X$ and use Poincaré reducibility theorem to achieve the contradiction. Further details are left to the reader.

2.7. **Frobenius endomorphism.** For the purpose of this section suppose that $X \simeq X_0 \times_{k_0} k$ is defined over a finite field k_0. Let $\sigma \in \mathrm{Gal}(\overline{k}_0/k_0) =: G$ be the corresponding Frobenius automorphism. Since G acts continuously on $T_l(X)$ and the cyclic subgroup generated by σ is dense in G, then

$$\mathrm{End}_{\mathbb{Q}_l[G]}(V_l(X)) = \mathrm{End}_{\mathbb{Q}_l[\sigma]}(V_l(X)).$$

Let $\pi \in \mathrm{End}_{k_0}(X)$ denote the lift of the Frobenius endomorphism associated to the scheme X_0. Observe, that the action of π on $T_l(X)$ is virtually the same as the action of σ and π has the advantage of being a true morphism of abelian varieties, whereas σ is only an automorphism of $\overline{k}_0$. So if we view $V_l(X)$ as an E_l-module, $E_l := \mathbb{Q}_l \otimes_{\mathbb{Z}} \mathrm{End}_{k_0}(X)$, by the natural homomorphism

$$\mathbb{Q}_l \otimes_{\mathbb{Z}} \mathrm{End}_{k_0}(X) \longrightarrow \mathrm{End}_{\mathbb{Q}_l}(V_l(X)),$$

and let F_l denote the $\mathbb{Q}_l$-subalgebra of E_l generated by π, then clearly

$$\mathrm{End}_{F_l}(V_l(X)) = \mathrm{End}_{\mathbb{Q}_l[\sigma]}(V_l(X)).$$

We now have the following

Observation 2.7.1. *The algebra $F_l \subset E_l$ is semisimple.*

Proof. Since F_l is commutative, then we only need to verify that it is nilpotent-free (see Corollary A.2.5). Note, that F_l is contained in the center of semisimple ring E_l. By structural theorems ([27]) this center is isomorphic to a product of fields, so it is clearly nilpotent-free. □

Remark 2.7.2. The proof does not actually depend on l, so by the same argument one can prove that the subalgebra $F \subset \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}_{k_0}(X)$ generated by π is semisimple.

In order to prove Theorem 1.3.1, note the first important consequence of E_l being semisimple:

[26] See Corollary 2.1.5 for more details on products and Theorem A.2.3 for properties of matrices with coefficients in division rings.

[27] See Theorem A.2.4).

Lemma 2.7.3. *In the above notation, let $V_l = V_l(X)$. Since F_l is contained in the center of E_l we have*

$$E_l \longrightarrow \mathrm{End}_{F_l} V_l \text{ is surjective } \iff F_l \longrightarrow \mathrm{End}_{E_l} V_l \text{ is surjective.}$$

Proof. First, we will prove implication "$\Longleftarrow$". Let us denote $D := \mathrm{End}_{E_l} V$. Since E_l is semisimple, then by Jacobson-Chevalley Density Theorem ([28]) E_l acts densely on V_l considered as a D-module. Furthermore, V_l is also finitely generated as a D-module, so in fact

$$E_l \longrightarrow \mathrm{End}_D V_l \subset \mathrm{End}_{F_l} V_l$$

is surjective, and the inclusion becomes equality if we use the assumption, that $F_l \longrightarrow D$ is also surjective. Note, that since F_l is also semisimple, the same argument remains valid for the other implication. □

2.8. **Further consequences of semisimplicity.** We continue the notation of the previous section. Let us recall that by Theorem 1.2.1 we already now that the natural homomorphism

$$\mathrm{End}(X) \longrightarrow \mathrm{End}_{\mathbb{Z}_l}(T_l(X))$$

is injective. Since $T_l(X) \simeq (\mathbb{Z}_l)^{2g}$, $\mathrm{End}(X)$ is a free $\mathbb{Z}$-module of finite rank. ([29]) It shows, that every element of $\mathrm{End}(X)$, so in particular the Frobenius morphism, is anihilated by a monic polynomial with integer coefficients, namely its characteristic polynomial.

We have seen that $F = \mathbb{Q}[\pi]$ is a semisimple commutative ring (see Remark 2.7.2. It follows ([30]) that F is isomorphic to a product of fields

$$F \simeq K_1 \times \ldots \times K_r \tag{12}$$

with $K_i/\mathbb{Q}$ finite. On the other hand, there is a surjective homomorphism

$$\mathbb{Q}[T] \ni f(T) \longmapsto f(\pi) \in F$$

with kernel generated by some monic $f \in \mathbb{Z}[T]$. ([31]) Clearly $F \simeq \mathbb{Q}[T]/(f)$ and semisimplicity of F is tantamount to the fact that f does not contain a multiple factor. More precisely, if $f = P_1 \cdots P_r$ with P_i monic and irreducible, then all P_i are distinct and also $\mathbb{Q}[T]/(P_i) \simeq K_i$, possibly after permuting indexes.

Now let V be any finite F-module. The identity (12) gives rise to a decomposition of V into a direct sum of F-modules

$$V \simeq V_1 \oplus \ldots \oplus V_r$$

with F acting coordinatewise. Hence, each V_i can be viewed as a K_i-vector space with $\dim_{K_i} V_i = n_i$ and it can be further decomposed into a product

$$V_i = V_{i,1} \oplus \ldots \oplus V_{i,n_i}$$

of one dimensional K_i-subspaces. Clearly, all $V_{i,1}, \ldots, V_{i,n_i}$ are mutually isomorphic simple F-modules. Furthermore, the characteristic polynomial corresponding to the action of π restricted to $V_{i,j}$ equals P_i, so in particular $V_{i,j}$ and $V_{i',j'}$ are not isomorphic as F-modules provided that $i \neq i'$.

[28] See Theorem A.3.3 and also Corollary A.3.4.

[29] In fact it is at most $4g^2$.

[30] See Corollary A.2.5.

[31] This is necessarily a divisor of the characteristic polynomial.

Combining this data for all $i = 1, \dots, r$ we can see, that the characteristic polynomial P of π acting on V equals

$$P = P_1^{n_1} \cdots P_r^{n_r}.$$

In particular, it provides complete information about possible decompositions of V into simple F-modules.

Lemma 2.8.1. *With the above notation, let P be the characteristic polynomial of the Frobenius endomorphism π and let*

$$P = P_1^{n_1} \cdots P_r^{n_r}$$

be the decomposition over $\mathbb{Q}$ into irreducible factors. Then

$$\dim_{\mathbb{Q}_l} \mathrm{End}_{F_l} V_l = \sum_{i=1}^{r} n_i^2 \deg P_i.$$

In particular, the left-hand-side entity does not depend on l.

Proof. Let $P_i = Q_{i,1} \cdots Q_{i,k_i}$ with irreducible $Q_{i,j} \in \mathbb{Z}_l[T]$. Since the polynomials P_i were already irreducible over $\mathbb{Q}$, then $Q_{i,j}$ are pairwise distinct. From the above discussion one can see, that

$$\dim_{\mathbb{Q}_l} \mathrm{End}_{F_l} V_l = \sum_{i=1}^{r} \sum_{j=1}^{k_i} n_i^2 \deg Q_{i,j} = \sum_{i=1}^{r} n_i^2 \deg P_i.$$

□

Remark 2.8.2. With a little more effort, one can generalize the above calculation to the case of two vector spaces. Namely, given a pair of semisimple operators $\pi_1 \in \mathrm{End}_k(V_1)$ and $\pi_2 \in \mathrm{End}_k(V_2)$ one can equip both V_1 and V_2 with a structure of semisimple $k[T]$-module through the ring homomorphisms $k[T] \longrightarrow \mathrm{End}_k(V_i)$, $T \longmapsto \pi_i$ with $i = 1, 2$. Let us denote by P_1 and P_2 the characteristic polynomials of π_1 and π_2 respectively. We have

$$\dim_k \mathrm{Hom}_{k[T]}(V_1, V_2) = \sum_P v_P(P_1) v_P(P_2) \deg P =: r(P_1, P_2), \quad ([32])$$

where the sum runs over all irreducible polynomials and v_P stands for the P-valuation, i.e. $v_P(Q) =$ "the multiplicity of P in the prime decomposition of polynomial Q".

Corollary 2.8.3. *To prove Theorem 1.3.1 one only needs to verify, that for any abelian variety X the homomorphism*

$$\rho : E_l \longrightarrow \mathrm{End}_{F_l} V_l$$

is surjective for at least one l.

Proof. Recall, that ρ is injective. Hence, the statement "ρ is surjective" is equivalent to "domain and codomain have euqal $\mathbb{Q}_l$-dimensions". Since

$$\dim_{\mathbb{Q}_l} E_l = \mathrm{rank}_{\mathbb{Z}} \mathrm{End}(X)$$

and also (by Lemma 2.8.1) the dimension of $\mathrm{End}_{F_l} V_l$ does not depend on l, the claim follows. □

[32] We will use this definition in the statement of Theorem 4.2.1.

Lemma 2.8.4. *There exists a prime number l, such that F_l is isomorphic to a product of copies of $\mathbb{Q}_l$.*

Proof. As we already have seen that

$$F = \mathbb{Q}[\pi] \simeq K_1 \times \ldots \times K_r,$$

with $K_i/\mathbb{Q}$ finite. Let K be a normal extension of $\mathbb{Q}$ which contains all K_i's. Since $K/\mathbb{Q}$ is Galois, then $K \simeq \mathbb{Q}[x]/(f)$ where $f \in \mathbb{Q}[x]$ is an irreducible polynomial, which splits completely in K. Clearly, the following statements are equivalent:

(13) f has a root in $\mathbb{Q}_l \iff \mathbb{Q}_l$ contains K as a subfield $\iff$
f splits completely in $\mathbb{Q}_l \iff \mathbb{Q}_l \otimes_{\mathbb{Q}} K \simeq \mathbb{Q}_l \times \ldots \times \mathbb{Q}_l$.

Note, that the last isomorphism is given by the evaluation at the roots of the polynomial f. It follows, that if any of the above statements is true, then the group $\mathrm{Gal}(K/\mathbb{Q})$ operates on $\mathbb{Q}_l \otimes_{\mathbb{Q}} K$ by permuting the coordinates of the product transitively. Since $K_i \subset K$ is a field of invariants for some subgroup $H \subset \mathrm{Gal}(K/\mathbb{Q})$, then also $\mathbb{Q}_l \otimes_{\mathbb{Q}} K_i \subset \mathbb{Q}_l \otimes_{\mathbb{Q}} K$ is an algebra of invariants under the induced action of H. By the description of this action given above, one can easily see, that $\mathbb{Q}_l \otimes_{\mathbb{Q}} K_i$ must be isomorphic to a product of copies of $\mathbb{Q}_l$.

So we only need to verify that "f has a root in $\mathbb{Q}_l$" holds for some l. Without loosing generality we may assume, that the polynomial f is monic and has integral coefficients. Let Δ be its discriminant, and suppose $l \nmid \Delta$. If f happened to have a root in $\mathbb{F}_l$, then this root would be simple, so by Hensel's lemma it would give rise to a root in $\mathbb{Q}_l$, and we are done. Eventually we only need to show, that for infinitely many ([33]) primes l the polynomial f has a root in $\mathbb{F}_l$. This is left as an exercise for the reader. □

2.9. **Riemann-Roch and the vanishing theorem.** At the end of this section we review a few results concerning the Euler characteristic of a line bundle.

Definition. Given a line bundle L ([34]) on a projective variety X we define its *Euler characteristic* to be

$$\chi(L) = \sum_{i=0}^{\infty} (-1)^i \dim_k H^i(X, L).$$

Note, that $\dim_k H^i(X, L) < \infty$ for all i, since X is projective, ([35]) and also $H^i(X, L) = 0$ for $i > \dim X$ by the Grothendieck Vanishing Theorem. ([36])

Theorem 2.9.1. *Let $f : X \longrightarrow Y$ be an isogeny of abelian varieties. Then for any line bundle L on Y*

$$\chi(f^*(L)) = (\deg f)\chi(L).$$

Proof. See Mumford [7, §11, Thm. 2, p. 121] where this statement is proved in much more general context.

[33] So that we can avoid the discriminant

[34] More generally, any one can take any coherent sheaf of $\mathcal{O}_X$-modules.

[35] See Hartshorne [4, Ch. III, Thm. 5.2].

[36] See Hartshorne [4, Ch. III, Thm. 2.7]

Theorem 2.9.2 (Riemann-Roch)**.** *For all line bundles L on X, if $L = L(D)$, we have*

$$\chi(L) = \frac{(D^g)}{g!}, \quad \chi(L)^2 = \deg \phi_L,$$

where (D^g) is the g-fold self intersection number of D.

Proof. See Mumford [7, §16, p. 150].

Corollary 2.9.3. *Let L be a line bundle on X. Then*

$$\chi(L^n) = n^g \chi(L).$$

Theorem 2.9.4 (vanishing theorem)**.** *If for a line bundle L on X, $K(L)$ is finite, there is a unique integer $i = i(L)$, $0 \leq i(L) \leq g = \dim X$, such that $H^j(X, L) = 0$ for $j \neq i$ and $H^i(X, L) \neq 0$. Further, $i(L^{-1}) = g - i(L)$.*

Proof. See Mumford [7, §16, p. 150].

Corollary 2.9.5. *If L is very ample, then $H^0(X, L) = \chi(L)$.*

Proof. Since L is very ample, $H^0(X, L) \neq 0$. Then use Theorem 2.9.4. □

Corollary 2.9.6. *Let k_0 be a finite field. For a given $d > 0$, there are only finitely many k_0-isomorphism classes of abelian varieties which are defined over k_0 and admit an ample line bundle with Euler characteristic equal to d.*

Proof. Suppose that X is defined over k_0 and L is an ample k_0-line bundle with $\chi(L) = d$. By Theorem 2.2.5 the line bundle L_i^3 is very ample and $\chi(L_i^3) = 3^g \chi(L_i) = 3^g d$ (by Corollary 2.9.3). By Corollary 2.9.5 and Theorem 2.9.2, X can be embedded into $\mathbb{P}^{3^g d-1}$ as a k_0-subvariety of degree $(g!)\chi(L_i) = (g!)3^g d$. Since k_0 is finite, there are only finitely many such varieties. ([37]) □

We will also need the following result.

Theorem 2.9.7. *If L is a line bundle on an abelian variety X and $n \in \mathbb{Z}$, then $L \simeq M^n$ for some line bundle M if and only if $X_n \subset K(L)$.*

Proof. See Mumford [7, §23, Thm 3, p. 231].

3. Examples of abelian varieties

3.1. **CM-varieties.** As we have pointed out, not every complex torus $\mathbb{C}^g/\Lambda$ is an abelian variety. This is controlled by the existence of a positive defined Hermitian form whose imaginary part takes integral values when restricted to the lattice Λ (see Theorem 1.1.1). This imaginary part is the *Riemann form* (it is always nondegenerated and skew-symmetric).

Example. Assume, that $C = \mathbb{C}/\Lambda$ with $\Lambda = \mathbb{Z}\lambda_1 \oplus \mathbb{Z}\lambda_2$ and $\Im(\lambda_1/\lambda_2) > 0$. Considering $\mathbb{C}$ as a 2-dimensional real space, let us define $E : \mathbb{C} \times \mathbb{C} \longrightarrow \mathbb{R}$ by the formula

$$z_1 \wedge z_2 = E(z_1, z_2)\lambda_1 \wedge \lambda_2$$

[37] This can be shown in many different ways. In particular, there is an elementary argument using only Bézout Theorem.

By the properties of determinant, this form is easily seen to be alternating and non-degenerate. Furthermore $E(\Lambda,\Lambda)\subset\mathbb{Z}$ and $E(iz_1,iz_2)=E(z_1,z_2)$ because the "multiplication by i" is area-preserving. This shows that

$$H:\mathbb{C}\times\mathbb{C}\ni(z_1,z_2)\longrightarrow E(iz_1,z_2)+iE(z_1,z_2)\in\mathbb{C}$$

is a Hermitian form with properties of a Riemann form.

Next, we will present another class of complex tori for which it is possible to write down a Riemann form explicitly.

Definition. A CM-*field* is a totally imaginary quadratic extension K of a totally real number field K^+. In particular, any CM-field admits a unique nontrivial automorphism in $\mathrm{Gal}(K/K^+)$, which will be denoted by $x\longmapsto\widetilde{x}$. Examples of CM-fields are provided by imaginary quadratic number fields and cyclotomic fields.

Let K be a CM-field. By definition $K=K^+(\xi)$ for some $\xi\in\mathbb{C}$ satisfying a quadratic equation $a\xi^2+b\xi+c=0$ with $a,b,c\in K^+$. Since K is an imaginary extension of K^+, $4ac-b^2>0$ is a totally positive element of K^+ and also $K=K^+(\sqrt{b^2-4ac})$. Replacing ξ with $\sqrt{b^2-4ac}$ we may therefore assume that $-\xi^2\in K^+$ is totally positive and $\widetilde{\xi}=-\xi$. Also, replacing ξ with its positive multiplicity we may assume that $\xi\in\mathcal{O}_K$.

Let $2g:=[K:\mathbb{Q}]$ and $\varphi_1,\overline{\varphi}_1,\ldots,\varphi_g,\overline{\varphi}_g$ denote the set of all complex embeddings $K\longrightarrow\mathbb{C}$. Without loosing generality we may assume that $\Im\varphi_i(\xi)>0$ for any i. Now, define

$$\varphi:K\ni x\longmapsto(\varphi_1(x),\ldots,\varphi_g(x))\in\mathbb{C}^g.$$

Given any ideal $I\subset K$ ([38]) we have that $\varphi(I):=\Lambda\subset\mathbb{C}^g$ is a lattice of rank $2g$. In particular, $X:=\mathbb{C}^g/\Lambda$ is a complex torus. Consider the $\mathbb{R}$-bilinear alternating form

$$E(z,w):=\sum_{j=1}^{g}\varphi_i(\xi)(\overline{z}_jw_j-z_j\overline{w}_j).$$

Clearly $E(iz,iw)=E(z,w)$ and he assumptions on ξ imply that $E(iz,w)$ is positively defined. It follows that $H(z,w):=E(iz,w)+iE(z,w)$ is a positively defined Hermitian form. Since furthermore ([39])

$$\begin{aligned}E(\varphi(x),\varphi(y))&=\sum_{j=1}^{g}\varphi_i(\xi)(\overline{\varphi_j}(x)\varphi_j(y)-\varphi_j(x)\overline{\varphi_j}(y))\\&=\sum_{j=1}^{g}\varphi_i(\xi)\varphi_j(\widetilde{x})\varphi_j(y)+\overline{\varphi_i}(\xi)\overline{\varphi_j}(\widetilde{x})\overline{\varphi_j}(y)=\mathrm{Tr}(\xi\widetilde{x}y),\end{aligned}$$

then $E(\Lambda,\Lambda)\in\mathbb{Z}$, ([40]) which shows that E is a Riemann form. Also note that any element x of the multiplier ring ([41])

$$(I:I)=\{x\in K:xI\subset I\}$$

[38] Here, "ideal" is a fractional ideal of K.

[39] Note that $\widetilde{\xi}=-\xi$.

[40] Because all $\widetilde{x},y,\xi$ are algebraic integers.

[41] This is always an order in K, so in particular a subgroup of rank $2g$.

gives rise to an endomorphism of $\mathbb{C}^g$

$$\mathbb{C}^g \ni (z_i) \longmapsto (\varphi(x)z_i) \in \mathbb{C}^g,$$

which preserves Λ. This shows, that we have actually defined an injective homomorphism $(I : I) \longrightarrow \mathrm{End}(X)$ which lifts to

$$K \longrightarrow \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}(X).$$

In this situation, X is said to admit complex multiplications by K.

3.2. **Jacobians of curves.** The fundamental examples of an abelian varieties, are elliptic curves. Indeed, using the classical Riemann-Roch theorem one may easily verify that any complete curve of genus 1, C say, admits a group structure given by morphisms. This makes C into an abelian variety (see Silverman [8, III 2]). Furthermore, as an abstract group variety C is isomorphic to $\mathrm{Pic}^0(C)$. In particular $\mathrm{Pic}^0(C)$ is naturally equipped with a structure of a variety. In general, we have the following

Theorem 3.2.1. *Let C be a smooth projective curve of genus $g \geq 1$. There exists an abelian variety* $\mathrm{Jac}(C)$*, called* Jacobian *of C, and an injection $j : C \longrightarrow \mathrm{Jac}(C)$, called the* Jacobian embedding *of C, with the following properties:*

(i) Extend j linearly to divisors on C. Then j induces a group isomorphism between $\mathrm{Pic}^0(C)$ *and* $\mathrm{Jac}(C)$*.*

(ii) For each $r \geq 0$, define a subvariety $W_r \subset \mathrm{Jac}(C)$ by

$$W_r = \underbrace{j(C) + \ldots + j(C)}_{r \text{ copies}}, \quad W_0 = \{0\}$$

Then

$$\dim(W_r) = \min\{r, g\} \quad \textit{and} \quad W_g = \mathrm{Jac}(C).$$

In particular, $\dim(Jac(C)) = g$*.*

(iii) Let $\Theta = W_{g-1}$. Then Θ is an irreducible ample divisor on $\mathrm{Jac}(C)$*.*

Remark. The idea of the proof is due to Chow. ([42]) It is described in details by Hindry and Silverman [5, A.8]. There is also a similar (older) construction by Weil, which technically is a little bit more complicated.

Sketch of the proof, Theorem 3.2.1. Take any sufficiently large n ([43]) and consider the variety ([44])

$$\mathrm{Sym}^n C := \underbrace{C \times \ldots \times C}_{n \text{ times}} / S_n$$

with the symmetric group S_n acting by permuting the coordinates. Clearly, there is a natural correspondence between points of $\mathrm{Sym}^n C$ and the set of effective divisors of degree n on C. If $D \in \mathrm{Sym}^n C$, then one may verify that the linear system $|D|$ is a subvariety of $\mathrm{Sym}^n C$, which is isomorphic to $\mathbb{P}^{n-g}$ by the Riemann-Roch Theorem. Let us define

$$J := \{\text{linear systems of degree } n \text{ on } C\}$$

[42] Actually, Chow completed the argument of Weil.

[43] By the Riemann-Roch Theorem $n \geq 2g - 1$ will do.

[44] To see that this is a variety use for example Theorem 2.5.1.

and also

$$\pi : \mathrm{Sym}^n \ni D \longmapsto |D| \in J.$$

Thanks to the fact that the fibers of π are all isomorphic to $\mathbb{P}^{n-g}$ it is now possible to check that J can be given a natural structure of algebraic variety such that π is a surjective morphism. In particular, the dimension formula yields

$$\dim(J) = \dim \mathrm{Sym}^n C - \dim \mathbb{P}^{n-q} = n - (n-g) = g.$$

Next, we will define a group law on J. Suppose for simplicity, that C has a k-rational point P_0. Let $D_0 = n(P_0)$ and set

$$m : J \times J \ni (|D_1|, |D_2|) \longmapsto |D_1 + D_2 - D_0| \in J.$$

This is in fact a morphism and it is easily seen to define a group law on J. Finally, let

$$j : C \ni P \longmapsto |(P) + (n-1)(P_0)| \in J.$$

Using the group structure introduced on J, we can extend j linearly to get a homomorphism

$$j : \mathrm{Pic}^0(C) \ni \text{class of } D \longmapsto |D + D_0| \in J$$

which turns out to be a group isomorphism. For more details of this construction we refer the reader to Hindry and Silverman [5, A.8.1 and Appendix A.8.3].

Remark. It is not automatically clear that jacobians of curves actually give rise to nontrivial examples of abelian varieties. In particular, it may happen that a jacobian variety of a curve is isomorphic to a product of elliptic curves. However, using some techniques connected with Tate's theorem (see Theorem 1.3.1 and also Theorems 4.2.1 and 4.2.2) and the characteristic polynomial of the Frobenius morphism, one may actually check if a given jacobian is isogenous to a product of lower dimensional abelian varieties (i.e., is a simple abelian variety). For some results of this kind see for example Stoll [9], where the author verifies interesting properties of the jacobian varieties associated to the following curves: ([45])

$$(14)\quad y^2 = 1960641x^6 - 14210996x^5 - 149332238x^4 + 1238887722x^3 + 2145729513x^2 - 23268170226x + 49641176809$$

$$(15)\quad y^2 = 72029x^6 + 94774x^5 - 24415528x^4 - 97717622x^3 + 2258016816x^2 + 16063224440x + 27181336900$$

From Mordell-Weil Theorem (see Theorem 1.2.3) we already now, that the group of $\mathbb{Q}$-rational points on every jacobian variety is finitely generated. It turns out, that in the case of (14) and (15) the rank is at least 19. Later, Stoll found a curve of genus 2 with Mordell-Weil rank ≥ 20, but the result was not published. The example is

$$y^2 = 3250391x^6 + 33094338x^5 - 536952605x^4 - 4958284752x^3 + 20719669525x^2 + 215672449542x + 344282132601.$$

[45] These curves are of genus 2.

The jacobian varieties corresponding to these curves are simple.

4. The Theorem of Tate

In this section we finish the proof of Theorem 1.3.1 and we present some of its important consequences.

4.1. **End of the proof.** Let us recall that by the results presented so far, especially Lemma 2.7.3 and Corollary 2.8.3, we reduced the proof of Theorem 1.3.1 to the following statement:

Proposition 4.1.1. *In the notation of Lemma 2.7.3 if the prime number l is chosen so that $F_l \simeq \mathbb{Q}_l \times \ldots \times \mathbb{Q}_l$ (note that by Lemma 2.8.4 such a number always exists), then the natural homomorphism*

$$F_l \longrightarrow \mathrm{End}_{E_l} V_l \tag{16}$$

is surjective.

Remark. Since from now on we will work with only one l, we are going to drop the subscripts in F_l, E_l and V_l for brevity.

Remark. Since $E \longrightarrow \mathrm{End}_F V$ and (16) are injective, we can harmlessly identify both E and F with their images in $\mathrm{End}\, V$. Clearly (16) is surjective if and only if F equals the comutant of E.

Let X be an abelian variety defined over the finite field k_0. Chose an ample k_0-line bundle L on X. Consider the Riemann form e^L associated to L (see Definition 2.4.2), which extends naturally to

$$e^L : V_l(X) \times V_l(X) \longrightarrow \mathbb{Q}_l \otimes M_l$$

We observe that the conclusion of Proposition 4.1.1 is a fairly simple consequence of the following

Lemma 4.1.2. *Let W be an F-stable maximal isotropic subspace of V. Then there exists an element $u \in E$, such that $uV = W$.*

Suppose for a moment, that we already proved it, and pick any F-stable maximal isotropic subspace $W \subset V$; in particular $\dim_{\mathbb{Q}_l} W = g$. Then we claim, that W is also D-stable. Indeed, by Lemma 4.1.2 there exists some $u \in E$ with $uV = W$. We now have

$$DW = DuV = uDV \subset uV = W,$$

and the claim follows. We will now verify by descending induction on the dimension of W, that the same statement remains correct for any isotropic subspace, so in particular any F-stable one dimensional subspace is also D-stable.

Let $W \subset V$ be F-stable and isotropic, but not maximal, i.e. $W \subsetneq W^\perp$. By the properties of Riemann form (see Proposition 2.4.5) we can see that also $W^\perp$ is also F-stable, and so it is a semisimple F-module. So there exists a decomposition

$$W^\perp = W \oplus \sum_{i=1}^{s} L_i$$

with L_i simple. Recall, that $F \simeq \mathbb{Q}_l \times \ldots \times \mathbb{Q}_l$, r times. It follows, that every simple F-module is isomorphic to $\mathbb{Q}_l$, and so all L_i are one dimensional, hence isotropic. Since furthermore $\dim W + \dim W^\perp = \dim V$, then $\dim W^\perp - \dim W \geq 2$, i.e. $s \geq 2$. By the induction hypothesis the (isotropic) subspaces $W + L_i \subset V$ are D-stable. But $W = \bigcap_{i=1}^{s}(W + L_i)$, since $s \geq 2$, so W is also D-stable.

Proof of Proposition 4.1.1. The decomposition of F into product of $\mathbb{Q}_l$'s induces a decomposition $V \simeq V_1 \times \ldots \times V_r$ with F acting coordinatewise. The isotropic subspace W generated by the vector

$$v = (0, \ldots, v_i, \ldots, 0) \in V_1 \times \ldots \times V_i \times \ldots \times V_r$$

is easily seen to be F-stable, so it is also D-stable by the above claim. Consider the action of D restricted to any V_i. This shows that any one dimensional subspace of V_i is D-stable. But this is only possible when D acts on V_i by scalar multiplication, so indeed D is contained in the image of F. □

Proof of Lemma 4.1.2. With the above notation, let $T = T_l(X)$ and for any positive integer i define

$$T^i = (T \cap W) + l^i T \subset T$$

and also K^i = the image of T under the natural projection $T \longrightarrow X_{l^i}$. Consider the diagram

$$\begin{array}{ccc} T & \longrightarrow & X_{l_i} \\ \simeq\downarrow & & \downarrow\simeq \\ (\mathbb{Z}_l)^{2g} & \longrightarrow & (\mathbb{Z}/l^i)^{2g} \end{array}$$

Since $W \cap T \subset T$ is a pure sublattice of rank g, it follows that K^i is a subgroup of X_{l^i} of both rank and index equal to l^{ig}. Furthermore, since W is F-stable, then so is K^i. The main consequence of this observation is that varieties of the form $Y^i = X/K^i$ are all defined over k_0 (see Theorem 2.5.3).

We want to construct $u \in E$ such that $uV = W$. Since it is already quite difficult to write down any nontrivial endomorphism (i.e. not contained in F), even without assuming any further properties, the idea is to use morphisms between X and Y^i. There is at least one natural choice, namely the projection map $\pi_i : X \longrightarrow Y^i$, but also $K^i \subset X_{l^i} = \mathrm{Ker}(l^i)_X$ so by the fundamental property of quotient variety, the map $(l^i)_X$ factors as $(l^i)_X = \lambda_i \circ \pi_i$ for some $\lambda_i : Y^i \longrightarrow X$. Since

$$l^{2ig} = \deg(l^i)_X = (\deg \lambda_i)(\deg \pi_i) \quad \text{and} \quad \deg \pi_i = l^{ig}$$

then also $\deg \lambda_i = l^{ig}$. Next, we determine the image of

$$T(\lambda_i) : T_l(Y^i) \longrightarrow T.$$

Since T_l is a functor then from equality $\lambda_i \circ \pi_i = (l^i)_X$ one gets

$$(T_l(\lambda_i) \circ T_l(\pi_i))(T) = T((l^i)_X)(T) = l^i T$$

and clearly $l^iT \subset T_l(\lambda_i)(T_l(Y^i))$. Note furthermore that

$$\begin{aligned}
\pi_i \circ \lambda_i \circ \pi_i = \pi_i \circ (l^i)_X = (l^i)_Y \circ \pi_i \Longrightarrow \quad & \text{(because } \pi_i \text{ is surjective)} \\
\pi_i \circ \lambda_i = (l^i)_Y \Longrightarrow \quad & \\
(l^i)_Y^{-1}(0) = \lambda_i^{-1}(\pi_i^{-1}(0)) \Longrightarrow \quad & \text{(because } \pi_i \text{ is surjective)} \\
\lambda_i((Y^i)_{l^i}) = \pi_i^{-1}(0) = K^i. &
\end{aligned}$$

Hence, for any $w \in W \cap T$ there exists $v \in T_l(Y^i)$ with

$$\lambda_i v - w \in l^iT \subset T_l(\lambda_i)(T_l(Y^i))$$

which already shows that $T^i \subset T_l(\lambda_i)(T_l(Y^i))$. By the same argument one verifies the other inclusion, so eventually

$$T_l(\lambda_i)(T_l(Y^i)) = T^i. \tag{17}$$

This looks promising due to the fact that $\bigcap T^i = T \cap W$, but still, we need to construct an endomorphism which we do not have yet. What we are missing are clearly nontrivial morphisms between Y^i's, and they seem even more difficult to find. We will now show how to do that.

Suppose for a moment that we managed to prove, that there are only finitely many k_0-isomorphism classes among Y^i's. Then, there exists a positive integer n together with k_0-isomorphisms $v_i : Y^n \simeq Y^i$ for infinitely many $i \geq n$. Let us denote the set of these "good" indexes by I and for any $i \in I$ define $u_i = l^{-ng}\lambda_i v_i \widetilde{\lambda}_n \in E$ where $\widetilde{\lambda}_n : X \longrightarrow Y^n$ is an isogeny such that $\widetilde{\lambda}_n \circ \lambda = (l^{ng})_X$ and also $\lambda_n \circ \widetilde{\lambda} = (l^{ng})_Y$ (see Theorem 2.5.8). Let us verify

$$\begin{aligned}
u_iT^n &= l^{-ng}\, T_l(\lambda_i \circ v_i \circ \widetilde{\lambda}_n)(T^n) \\
&= l^{-ng}\, T_l(\lambda_i \circ v_i \circ \widetilde{\lambda}_n \circ \lambda_n)(T_l(Y^n)) && \text{by (17)} \\
&= T_l(\lambda_i \circ v_i)(T_l(Y^n)) \\
&= T_l(\lambda_i)(T_l(Y^i)) \\
&= T^i && \text{by (17)}
\end{aligned}$$

so in fact $u_iT^n \subset T^n$, which shows that each u_i is belongs to the compact set $\mathrm{End}_{\mathbb{Z}_l}(T^n)$. Therefore, restricting to a subsequence and taking into account that E is closed, ([46]) we may assume that $u_i \to u$ for some $u \in E$. Now, for any $x \in T^n$, $T^i \ni u_i(x) \to u(x)$. Since all T^i are closed, it follows that $u(x) \in \bigcap_{i\in I} T^i = T \cap W$. ([47]) But T^n already contains a basis of V and $T \cap W$ contains a basis of W so in the end $uV = W$.

It remains to verify that there are only finitely many k_0-isomorphism classes among Y^i's. By Corollary 2.9.6 it is enough to construct an ample k_0-line bundle L_i on each Y^i with Euler characteristic bounded by some constant not depending on i. To construct L_i with desired properties first note, that λ_i^*L (recall, that L was chosen at the beginning of the proof) is an ample k_0-line bundle on Y^i with

$$\chi(\lambda_i^*L) = (\deg \lambda_i)\chi(L) = l^{ig}d, \quad \text{where } d = \chi(L).$$

[46] This is because E is a subspace of finite-dimensional $\mathbb{Q}_l$-vector space.

[47] This is a general topological fact.

To eliminate the dependence on i in the above formula we will find a line bundle $\widetilde{L}$, such that $\widetilde{L}^{l_i} \simeq \lambda_i^* L$. By Theorem 2.9.7, the existence of such a bundle is equivalent to the condition $(Y^i)_{l^i} \subset K(\lambda_i^* L)$. We are going to verify the latter in a moment, but for now suppose that we have already done it, i.e. assume that the line bundle $\widetilde{L}$ exists. Things are looking better, since

$$l^{ig} d = \chi(\lambda_i^* L) = \chi(\widetilde{L}^{l^i}) = (l^i)^g \chi(\widetilde{L}) \Longrightarrow \chi(\widetilde{L}) = d,$$

but unfortunately we do not know if $\widetilde{L}$ can be defined over k_0. However, we may always assume that it is defined over $\overline{k}_0$, and so over some finite extension k_1/k_0. Now, for any $\sigma \in \mathrm{Gal}(k_1/k_0)$ let us consider the morphism (of schemes)

$$\sigma := 1_{Y_0} \times \operatorname{Spec} \sigma : Y_0 \times_{k_0} \overline{k}_0 \longrightarrow Y_0 \times_{k_0} \overline{k}_0.$$

with Y_0 chosen so that $Y^i = Y_0 \times_{k_0} k$. Due to the fact that booth L and λ are defined over k_0 we have

$$(\sigma^* \widetilde{L})^{l^i} \simeq \sigma^*(\widetilde{L}^{l^i}) \simeq \sigma^* \lambda^* L \simeq \lambda^* \sigma^* L \simeq \lambda^* L \simeq \widetilde{L}^{l^i},$$

provided that the last σ denotes the corresponding morphism on X. Since the Néron-Severi group $\mathrm{NS}(Y^i)$ is torsion free (see Corollary 2.3.3), it follows that $\sigma^* \widetilde{L} \otimes \widetilde{L}^{-1} \in \mathrm{Pic}^0(Y)$. Eventually, let us define $L_i := \widetilde{L} \otimes [-1]^* \widetilde{L}$. Then, $\chi(L_i) = 2d$, both L_i and $\sigma^* L_i \otimes L_i^{-1}$ are symmetric and also $\sigma^* L_i \otimes L_i^{-1} \in \mathrm{Pic}^0(Y^i)$, which shows that $\sigma^* L_i \simeq L_i$ by Corollary 2.3.7. To conclude that L_i can be defined over k_0 we now use the following

Lemma 4.1.3. *Let Y be a complete variety defined over k_0 with a k_0-rational point, k_1 a Galois extension of k_0 and M a line bundle on Y defined over k_1 such that for every $\sigma \in \mathrm{Gal}(k_1/k_0)$, $\sigma^*(L) \simeq L$ with σ understood as above. Then L can be defined over k_0.*

Proof. See Mumford [7, Appendix I, Lem. 4, p. 246].

Finally, let us verify that

$$Y_{l^i} \subset K(\lambda_i^* L). \tag{18}$$

By properties of Riemann forms for any $x, y \in T_l(Y^i)$ one has

$$\begin{aligned} e_l(x, \phi_{\lambda_i^* L}(y)) &= e^{\lambda_i^* L}(x, y) \\ &= e^L(T_l(\lambda_i)(x), T_l(\lambda_i)(y)) && \text{by Proposition 2.4.4} \\ &\in e^L(T^i, T^i) \\ &= e^L(l^i T, T \cap W + l^i T) \subset l^i M_l && \text{since } W \text{ is isotropic} \end{aligned}$$

So in particular $\overline{e}_{l^i}(x, \phi_{\lambda_i^*}(y)) \equiv 1$ for all $x, y \in (Y^i)_{l^i}$. Since $\overline{e}_{l^i}$ is non-degenerate, $\phi_{\lambda_i^*}(y) = 0$ for any $y \in (Y^i)_{l^i}$, which proves (18). □

4.2. **Some applications.** The following theorems can be derived from Tate's Theorem. Proofs can be found in Mumford [7] and Tate [10].

Theorem 4.2.1. *Let X and Y be abelian varieties over a finite field k_0, and let P_X and P_Y be the characteristic polynomials of their Frobenius endomorphisms relative to k_0. Then*

(a) *With r defined as in Remark 2.8.2 we have*

$$\operatorname{rank}(\operatorname{Hom}_{k_0}(X,Y) = r(P_X, P_Y).$$

(b) *The following statements are equivalent:*
  (b1) *Y is k_0-isogenous to an abelian subvariety of X defined over k_0.*
  (b2) *$V_l(Y)$ is G-isomorphic to G-subspace of $V_l(X)$ for some l.*
  (b3) *P_Y divides P_X.*

(c) *The following statements are equivalent:*
  (c1) *X and Y are k_0-isogenous.*
  (c2) *$P_X = P_Y$.*
  (c3) *The zeta functions of X and Y are the same.*
  (c4) *X and Y have the same number of k_1-rational points for every finite extension k_1 of k_0.*

Proof. See Tate [10] or Mumford [7, Appendix I, Thm. 2].

Theorem 4.2.2. *Let X be an abelian variety of dimension g defined over a finite field k_0. Let π be the Frobenius endomorphism of X relative to k_0 and P its characteristic polynomial. We then have the following statements.*

(a) *The algebra $F = \mathbb{Q}[\pi]$ is the center of the semisimple algebra $E = \mathbb{Q} \otimes \operatorname{End}_{k_0}(X)$.*

(b) *$\mathbb{Q} \otimes \operatorname{End}_{k_0}(X)$ contains a semisimple $\mathbb{Q}$-algebra of rank $2g$ which is maximal commutative.*

(c) *The following statements are equivalent:*
  (c1) *$[E : \mathbb{Q}] = 2g$,*
  (c2) *P has no multiple roots.*
  (c3) *$E = F$.*
  (c4) *E is commutative.*

(d) *The following statements are equivalent:*
  (d1) *$[E : \mathbb{Q}] = (2g)^2$.*
  (d2) *P is a power of a linear polynomial.*
  (d3) *$F = \mathbb{Q}$.*
  (d4) *E is isomorphic to the algebra of g by g matrices over the quaternion division algebra D_p over $\mathbb{Q}$ ($p = \operatorname{char} k_0$) which splits at all primes $l \neq p, \infty$.*
  (d5) *X is k-isogenous to the g-th power of a super-singular elliptic curve, all of whose endomorphisms are defined over k_0.*

(e) *X is k_0-isogenous to a power of a k_0-simple abelian variety if and only if P is a power of $\mathbb{Q}$-irreducible polynomial. When this is the case, E is a central simple algebra over F which splits at all finite primes v of F not dividing p, but does not split any real prime of F.*

Proof. See Tate [10] or Mumford [7, Appendix I, Thm. 3].

Appendix A. Semisimple rings and density theorem

This section is a brief review of fundamental facts on semisimple rings. Here, we assume that a ring R has an identity and is not necessarily commutative. By R-module we always mean a left R-module, i.e., to give a

structure of R-module on M is equivalent to give a ring homomorphism

$$R \longrightarrow \mathrm{End}(M).$$

A.1. **Semisimple modules.**

Definition A.1.1. An R-module M is called a *simple (or irreducible) R-module* if $M \neq 0$, and M contains no R-submodules other than (0) and M.

An R-module M is called *semisimple (or completely reducible)* if every R-submodule of M is an R-module direct summand of M. This is equivalent to say that any exact sequence of the form

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

splits.

Theorem A.1.2. *For an R-module M, the following conditions are equivalent:*

(1) M is semisimple
(2) M is the direct sum of a family of simple R-modules
(3) M is the sum of a family of simple submodules

Proof. See Lam [6, Thm. 2.4].

A.2. **Semisimple rings.**

Theorem A.2.1. *For a ring R, the following statements are equivalent:*

(1) All short exact sequences of R-modules split.
(2) All R-modules are semisimple.
(3) All finitely generated R-modules are semisimple.
(4) All cyclic R-modules are semisimple.
(5) The left regular R-module ${}_RR$ is semisimple. ([48])

Proof. See Lam [6, Thm 2.5].

Definition A.2.2. A ring R is said to be (left) semisimple if any of the conditions from Theorem A.2.1 holds.

Theorem A.2.3. *Let D be a division ring, and let $R = M_n(D)$. Then*

(1) R is simple, left semisimple, left artinian and left noetherian.
(2) R has (up to isomorphism) a unique left simple module V. R acts faithfully on V, and ${}_RR \simeq nV$ as R-modules.
(3) The endomorphism ring $\mathrm{End}_R(V)$, is isomorphic to D^{op}.

Proof. See [6, Thm. 3.3].

Remark. From Theorem A.2.1 we see, that a finite product of semisimple rings is again a semisimple ring. Combining this with Theorem A.2.3 allows us to construct many of examples of semisimple rings. Namely, for any division rings $D_1, \ldots, D_r$ and positive integers $n_1, \ldots, n_r$, the ring

$$R = M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r) \tag{19}$$

is semisimple. The following result shows, that there are no other examples.

[48]Here, *the left regular R-module ${}_RR$* stands for R considered as R-module with the structure given by left multiplication.

Theorem A.2.4 (Wedderburn-Artin)**.** *Let R be any left semisimple ring. Then Any (left) semisimple ring R is of the form* (19) *for suitable division rings $D_1, \ldots, D_r$ and positive $n_1, \ldots, n_r$. The number r is uniquely determined, as are the pairs $(n_1, D_1), \ldots, (n_r, D_r)$ (up to a permutation). There are exactly r mutually nonisomorphic left simple modules over R, namely $M_{n_1}(D_1), \ldots, M_{n_r}(D_r)$ considered as R-modules in the only natural way.*

Proof. See [6, Thm. 3.5].

Corollary A.2.5. *If R is a commutative ring, then the following statements are equivalent:*

(1) R is semisimple
(2) R is a product of fields
(3) R is artinian and has no nilpotent elements

Proof. The equivalence (1) $\iff$ (2) follows from Theorem A.2.3 and Theorem A.2.4, and the implication (2)$\Longrightarrow$(3) is trivial. To see, that (3)$\Longrightarrow$(2) is also true, recall that an artinian ring is necessarily noetherian and of Krull dimension 0, i.e. every prime ideal is minimal and maximal at the same time. In particular, there are only finitely many prime ideals in R. Let us denote these ideals by $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$. Since all $\mathfrak{p}_i$ are maximal, by Chinese Reminder Theorem there is an isomorphism

$$R/\mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_n \simeq R/\mathfrak{p}_1 \times \ldots \times R/\mathfrak{p}_n$$

but the intersection $\mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_n = \mathrm{nil}(R)$ is zero, and again from maximality of $\mathfrak{p}_i$ one concludes, that every ring $R/\mathfrak{p}_i$ is in fact a field. □

A.3. **Density Theorem.** Let R, k be two rings and suppose that M is an (R, k)-bimodule. Let us also denote $E = \mathrm{End}_k(M)$.

Definition A.3.1. We say, that R *acts densely* on a k-module M if for any $f \in E$ and $x_1, \ldots, x_n \in M$, there exists $r \in R$ such that

$$rx_i = f(x_i), \text{ for each } i = 1, \ldots, n.$$

Remark. If one considers M as a topological space with the discrete topology, then there is a natural topology on E, given by the subbase ([49])

$$U(x_1, \ldots, x_n; y_1, \ldots, y_n) = \{f \in E : f(x_i) = y_i\}, \quad x_i, y_i \in M.$$

Since M is (R, k)-bimodule, the image of R in $\mathrm{End}(M)$ is contained in E. In this setup, it can be seen that R acts densely on M if and only if R maps to a dense subset of E.

Lemma A.3.2. *Use the notation introduced above. Suppose that M is a semisimple R-module and put $k = \mathrm{End}_R(M)$. Then any R-submodule $N \subset M$ is also an E-submodule.* ([50])

Proof. There exists an element $u \in E$, such that $uN = N$ and $uM \subset N$. Indeed, since M is R-semisimple, N is a direct summand of M and u can be obtained as the projection on N followed by inclusion $N \longrightarrow M$. We now have

$$EN = EuN = uEN \subset uM = N,$$

[49] Note, that this is a special case of the compact-open topology.
[50] And of course conversely, since R maps into $E \subset \mathrm{End}(M)$.

which finishes the proof. □

Theorem A.3.3 (Jacobson-Chevalley)**.** ([51]) *Let R be a ring and M a semisimple R-module. Then, for $k = \mathrm{End}_R(M)$, R acts densely on M viewed as a k-module.*

Proof. Take any $f \in E = \mathrm{End}_k(M)$, $x_1, \ldots, x_n \in M$ and let us define

$$\widetilde{M} = M^n, \quad \widetilde{k} = \mathrm{End}_R(\widetilde{M}) = \mathrm{End}_R(M^n) = \mathbb{M}_n(\mathrm{End}_R(M)) = \mathbb{M}_n(k)$$
$$\widetilde{f} : \widetilde{M} \ni (y_1, \ldots, y_n) \longmapsto (f(y_1), \ldots, f(y_n)) \in \widetilde{M}.$$

Now $\widetilde{M}$ is again a semisimple R-module, and it is a matter of straightforward verification to see that $\widetilde{f} \in \mathrm{End}_{\widetilde{k}}(\widetilde{M})$. Consider the cyclic R-submodule $N \subset \widetilde{M}$, generated by vector $x = (x_1, \ldots, x_n)$. By Lemma A.3.2, N is invariant under the action $End_{\widetilde{k}}(\widetilde{M})$, so in particular $\widetilde{f}(x) \in N$. It follows, that for some $r \in R$, $\widetilde{f}(x) = rx$. □

Corollary A.3.4. ([52]) *In the above notation, suppose furthermore that M is finitely generated as a k-module. Then the natural map $\rho : R \longrightarrow E$ is onto.*

Proof. Let $x_1, \ldots, x_n$ be the generators of M viewed as k-module. By Theorem A.3.3 given any $f \in E$, there exists an element $r \in R$, such that $f(x_i) = rx_i$ for $i = 1, \ldots, n$. Since both f and "multiplication by r" map are k-linear, and they agree on a set of k-generators, they must be equal. □

A.4. **Semisimplicity under scalar extension.**

Definition A.4.1. Let R be a semisimple finite k-algebra. One verifies easily, ([53]) that the center of R is isomorphic to a product of fields

$$C_1 \times \ldots \times C_n$$

where each C_i is an algebraic extension of k. The k-algebra R is said to be *separable* if all these fields are separable extensions of k.

Remark. In particular every semisimple $\mathbb{Q}$-algebra is separable.

Theorem A.4.2. *If R is semisimple, separable k-algebra, then $K \otimes_k R$ is a semisimple K-algebra for any field extension.*

Proof. See [3, Prop. 3.8, pp. 89].

Corollary A.4.3. *If R is a semisimple $\mathbb{Q}$-algebra, then the $\mathbb{Q}_l$-algebra $\mathbb{Q}_l \otimes_{\mathbb{Q}} R$ is semisimple.*

---

[51] See also Lam [6, Thm 11.16].
[52] See also [6, Cor. 11.17].
[53] Use Theorem A.2.4 for example.

References

[1] E. Bombieri and W. Gubler. *Heights in Diphantine Geometry*. Cambridge University Press, 2006.

[2] G. Faltings. Endlichkeitssätze für abelsche varietäten über zahlkörpern. *Inventiones Mathematicae*, 73(3):349–366, 1983.

[3] B. Farb and R. K. Dennis. *Noncommutative algebra*, volume 144 of *Graduate texts in mathematics*. Springer, 1993.

[4] R. Hartshorne. *Algebraic geometry*, volume 53 of *Graduate texts in mathematics*. Springer, 1977.

[5] M. Hindry and J. H. Silverman. *Diophantine Geometry – An Introduction*, volume 201 of *Graduate texts in mathematics*. Springer, 2000.

[6] T. Y. Lam. *A First Course in Noncommutative Rings*, volume 131 of *Graduate texts in mathematics*. Springer, 1991.

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

[8] J. H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate texts in mathematics*. Springer, 2009.

[9] M. Stoll. Two simple 2-dimensional abelian varieties over $\mathbb{Q}$ with mordell-weil group of rank at least 19. *C. R. Acad. Sci. Paris*, 321 (10):1341–1345, 1995.

[10] J. Tate. Endomorphisms of abelian varieties over finite fields. *Inventiones Mathematicae*, 2(2):134–144, 1966.