Title
Some results on arithmetic aspects of K3 surfaces and abelian varieties

Author
Gao, Anningzhe

Publication Date
2021

Peer reviewed|Thesis/dissertation

Some results on arithmetic aspects of K3 surfaces and abelian varieties

by

Anningzhe Gao

A dissertation submitted in partial satisfaction of the

requirements for the degree of

Doctor of Philosophy

in

Mathematics

in the

Graduate Division

of the

University of California, Berkeley

Committee in charge:

Professor Martin Olsson, Chair
Professor Richard Borcherds
Associate Professor Ori Ganor

Spring 2021

Some results on arithmetic aspects of K3 surfaces and abelian varieties

Abstract

Some results on arithmetic aspects of K3 surfaces and abelian varieties

by

Anningzhe Gao

Doctor of Philosophy in Mathematics

University of California, Berkeley

Professor Martin Olsson, Chair

The thesis is divided into three parts. We consider the essential dimension of algebraic stacks, and compute the essential dimension of moduli stack of polarized K3 surfaces in part 1. In part 2 we concentrate on the period index problems. More precisely, we show that if C is an algebraic curve of genus 1 over a field k of characteristic 0 then the index of C, defined to be the greatest common divisor of the degrees of its closed points, is equal to the index of the Brauer class defined by the $\mathbb{G}_m$-gerbe given by the Picard stack of degree 0 line bundles on C. We also relate this number to the essential dimension. In the last part we give a new proof of the finiteness of abelian varieties over finite fields using the Tate conjecture. This result was first proved by Zarhin.

Contents

Acknowledgments

I would like to thank my advisor, Martin Olsson. He introduced me these interesting topics and encouraged me when I had lots of difficulties. He shared his ideas on my problems and helped me check the details. His mathematical style really influenced me a lot and I hope to continue learning from him.

I would like to thank Max Lieblich for helpful discussions. I also got lots of help from Angelo Vistoli, in particular he gave the idea of the proof for the essential dimension of the moduli stack of polarized K3 surfaces of degree 2.

My family gave me lots of support during my tough time. I'm grateful for their help.

I received support from Lehmer Fellowship during Spring 2020.

Chapter 1

Introduction

The thesis is divided into three parts: In part 1 we consider the essential dimension of algebraic stacks, in part 2 we consider the period index problem of abelian varieties and in part 3 we consider the finiteness of abelian varieties over finite fields.

1.1 Essential dimension of algebraic stacks

The essential dimension was first proposed by Buhler and Reichstein in [6], who defined the essential dimension of an algebraic group. Then in [30] Merkurjev generalized it to any functors from the category of field extensions to the category of sets. We will recall the basic properties of essential dimension in part 1 and compute the essential dimension of the moduli stack of polarized K3 surfaces.

Roughly speaking, the essential dimension of an algebraic object is the minimal number of parameters needed to describe it. In the following discussion we will use k to denote a given base field. Given an object defined over a field extension K of k, one can ask whether this object can be defined over some subfield of K, in particular, we might hope to have a minimal subfield K' of K over which the object can be defined. It turns out, however, that considering the minimal field does not lead to the good definition. Rather, one should consider the minimal transcendental degree of a field of definition (see [38, Section 1] for discussion). Let $Field/k$ be the category of field extensions of k. Given a functor $F : Field/k \to Set$, and an object $\eta \in F(K)$ for some field extension K, we may consider the smallest transcendence degree over k of a subfield over which η is defined. This is called the *essential dimension* of the object, denoted by $ed_k(\eta)$. Taking the supremum over all pairs (K, η) we get the essential dimension $ed_k F$ of the functor F.

For an algebraic stack $\mathcal{X}/k$, define the functor $F_{\mathcal{X}} : Field/k \to Set$ by sending

a field extension K/k to the isomorphism classes of objects in the category $\mathcal{X}(K)$. The essential dimension of the algebraic stack is defined as the essential dimension of the functor $F_{\mathcal{X}}$, and we use $ed_k\mathcal{X}$ instead of $ed_k F_{\mathcal{X}}$ to denote it.

To motivate why we consider algebraic stacks, consider the following example from [3, Proposition 8.3]. Assume the characteristic of k is 0, and consider the moduli stack of elliptic curves over k. It is known that any elliptic curve can be defined by a Weierstrass equation $Y^2 = X^3 + aX + b$ for some $a, b \in k$. Therefore the curve is defined over $\mathbb{Q}(a, b) \subset k$. This implies that the essential dimension of the moduli stack of the elliptic curves is less than or equal to 2. Combining with the genericity theorem (see [3, Theorem 4.1]) the essential dimension of the moduli stack of elliptic curves is 2. This may at first seem counter intuition: The moduli stack is of dimension 1 and the essential dimension of a scheme or a space is the same as its usual dimension. The stacky nature of the moduli stack introduces a difference between the usual dimension and the essential dimension. We will discuss this in more detail later. Hence to get interesting results, we need to consider algebraic stacks.

We will concentrate on the essential dimension of algebraic stacks in this part, in particular Deligne-Mumford stacks. Brosnan, Reichstein and Vistoli developed many aspects of the theory for algebraic stacks in [3]. In particular, they proved the genericity theorem of the essential dimension of Deligne-Mumford stacks, which is the most important tool in our computation. They also discussed the essential dimension of some gerbes. In [10, Section 1], the following conjecture is proposed:

Conjecture 1.1.1. ([10]) Let k be a field of characteristic 0 and $\eta \in Br(k)$ be a Brauer class. Let n be the index of η. Let $n = p_1^{r_1}...p_s^{r_s}$ is the prime decomposition of n, and let $\mathcal{X} \to \mathrm{Spec}(k)$ be the μ_n-gerbe corresponding to the Brauer class η. Then we have

$$ed_k\mathcal{X} = p_1^{r_1} + p_2^{r_2} + ... + p_s^{r_s} - s + 1$$

The conjecture has been proved in the case when n is a power of a single prime ([3, Theorem 5.4]) and when $n = 6$ ([10, Theorem 1.3]).

The main result we will show is:

Theorem 1.1.2. ([15, Theorem 1.1 and Theorem 1.2]) Let k be an algebraically closed field. Let $\mathcal{M}_d$ be the moduli stack of polarized K3 surfaces of degree d over k. Then

(1) If k is of characteristic 0, the essential dimension of $\mathcal{M}_d$ is 20 when $d = 2$ and 19 if $d \geq 4$.

(2) If k is of characteristic p for some $p > 22$, then the essential dimension of $\mathcal{M}_d$ is 19 when $d > 2$.

In Chapter 2 we recall the basic properties of the essential dimension of algebraic stacks. In Chapter 3 we give the proof of Theorem 1.1.2. The proof is based on the genericity theorem (Theorem 2.3.2). It says that for an integral Deligne-Mumford stack, the essential dimension of the stack is determined by the usual dimension of the stack and the essential dimension of the generic gerbe. In Chapter 3 we will show that the moduli stack $\mathcal{M}_d$ is generically a scheme when $d > 2$, then by the genericity theorem the essential dimension of $\mathcal{M}_d$ is the same as its usual dimension. When $d = 2$ we will show that the stack is generically a trivial $\mathbb{Z}/2$ gerbe, then we apply the genericity theorem again to prove the theorem.

1.2 The period-index problem

In this part we consider the period index problem for elliptic curves. The classical paper about the period index problem is [26], and there are also several results in [9] and [29].

Let A be an abelian variety over k. An *A-torsor* is a pair (T, f), where T is a non-empty k-scheme and $f : T \times A \to T$ is a morphism, such that the following conditions hold:

(1) The following diagrams commute:

$$\begin{array}{ccc} T \times A \times A & \xrightarrow{f\times 1} & T \times A \\ {\scriptstyle 1\times m}\downarrow & & \downarrow{\scriptstyle f} \\ T \times A & \xrightarrow{\quad f \quad} & T \end{array}$$

$$\begin{array}{ccc} T & \xrightarrow{1\times\epsilon} & T \times A \\ {\scriptstyle id}\downarrow & \swarrow{\scriptstyle f} & \\ T & & \end{array}$$

Here $m : A \times A \to A$ is the addition morphism and $\epsilon : \mathrm{Spec}(k) \to A$ is the unit of A.

(2) The morphism

$$T \times A \to T \times T$$
$$(t, a) \to (t, ta)$$

is an isomorphism.

It is well known that the isomorphism classes of torsors are classified by the first cohomology group.

Theorem 1.2.1. ([19, Chapter 3, Remark 3.5.4], [35, Corollary 12.1.5]) Let A be an abelian variety over some field k, then there is a bijection

$$\{Isomorphism\ classes\ of\ A\text{-}torsors\ over\ k\} \leftrightarrow H^1(k, A)$$

Given a torsor T of an abelian variety A over k, the *period* of T, denoted by $per(T)$, is the order of the cohomology class $[T]$ in the first cohomology group $H^1(k, A)$. The *index* $I(T)$ of T, is defined to be the greatest common divisor of the degrees of closed points of T. We have the relation between these two numbers $per(T)|I(T)|per(T)^{2g}$, where g is the dimension of the abelian variety A. Details can be found in the first two sections of [9].

We also need the definition of gerbes.

Definition 1.2.2. ([27, Definition 3.15]) Given an algebraic stack $\mathcal{X}$, an algebraic space X and a morphism $\pi : \mathcal{X} \to X$. We say $\mathcal{X}$ is a *gerbe* over X if the two morphisms $\pi : \mathcal{X} \to X$ and $\Delta : \mathcal{X} \to \mathcal{X} \times_X \mathcal{X}$ are both epimorphims.

Let G be a sheaf of abelian group over k. A *gerbe banded by* G, sometimes referred to as a *G-gerbe*, is a gerbe $\mathcal{X}$ over k equipped with an isomorphism $G_{\mathcal{X}} \simeq \mathcal{I}_{\mathcal{X}}$ between $G \times \mathcal{X}$ and the inertia stack of $\mathcal{X}$. Concretely this means that for every object $\eta \in \mathcal{X}(S)$ over a k-scheme S we are given an isomorphism $Aut_S(\eta) \simeq G_S$ and these isomorphisms are appropriately functorial. A G-gerbe is *trivial* if it is equivalent to the classifying stack B_kG. Similar to the isomorphism classes of torsors, we have the following theorem:

Theorem 1.2.3. ([19, Chapter 4, Theorem 3.4.2], [35, Theorem 12.2.8]) Let X be an algebraic space over k, G is a sheaf of abelian groups. Then there is a bijection

$$\{Isomorphism\ classes\ of\ G\text{-}gerbes\ over\ X\} \leftrightarrow H^2(X, G)$$

We are interested in the case of dimension 1. Let E be an elliptic curve and let C be an E-torsor. Let $\mathcal{P}ic^0_{C/k}$ be the moduli stack of degree 0 line bundles on C, and let $\mathbf{Pic}^0_C$ be the Jacobian of C. Then $\mathcal{P}ic^0_C$ is a $\mathbb{G}_m$-gerbe over $\mathbf{Pic}^0_C$, and, using the canonical isomorphism $E \simeq \mathbf{Pic}^0_C$, we can view this as a $\mathbb{G}_m$-gerbe over E. Restricting to the function field K of E we obtain an element of the Brauer group Br(K). However we know that the set of isomorphism classes of $\mathbb{G}_m$-gerbes over Spec(K) is just $H^2(K, \mathbb{G}_m)$, and the latter one is just the Brauer group $Br(K)$ of K.

We define a new constant $i(C)$ to be the index of the Brauer class $\mathcal{P}ic^0_{C/k} \to \mathrm{Spec}(K)$ in $Br(K)$, called *generic index*. The main result of this part is the following:

Theorem 1.2.4. ([16, Theorem 1.1]) With the notations defined as above, we have

$$i(C) = I(C)$$

The reason we consider $i(C)$ is the following: Similar to the case of Deligne-Mumford stacks, we also have the genericity theorem of $\mathbb{G}_m$-gerbes. The Picard stack $\mathcal{P}ic^0_{C/k}$ is a $\mathbb{G}_m$-gerbe over the Picard variety $\mathbf{Pic}^0_{C/k}$, and the generic index is just the index of the generic gerbe in the Brauer group $H^2(k(\mathbf{Pic}^0_{C/k}), \mathbb{G}_m)$. Combined with the Conjecture 1.1.1, we can see the result is related to the essential dimension of $\mathcal{P}ic^0_{C/k}$. We will discuss this in Chapter 5.

1.3 The finiteness of abelian varieties

Let A be an abelian variety over k with $\dim A = g$. Choose l a prime number with $l \neq p$. We know that if $(p, n) = 1$, the morphism $n : A \to A$ is a separable isogeny of degree n^{2g}, denote $A[n] = Ker(n : A \to A)$, then $A[n](\bar{k}) \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$. The Tate module is defined as

$$T_l(A) = \varprojlim_n A[l^n](\bar{k})$$

In [42, Section 1], Tate proved the following famous theorem

Theorem 1.3.1 (Tate)**.** Let $k = \mathbb{F}_q$ be a finite field where q is a power of a prime p. Let A, B be two abelian varieties over k. Let $G = Gal(\bar{k}/k)$ be the absolute Galois group of k. If l is a prime and $l \neq p$, then we have the isomorphism

$$\mathrm{Hom}_{AV}(A, B) \otimes \mathbb{Z}_l \cong \mathrm{Hom}_{\mathbb{Z}_l[G]}(T_l(A), T_l(B))$$

Here T_l is the Tate module of an abelian variety.

The key ingredient in the proof is the following result:

Key Ingredient. Fix an integer d, a prime l and an abelian variety A over k. Then the number of isomorphism classes of abelian varieties which admits a polarization of degree d^2 and an isogeny $B \to A$ of degree l^n for some n is finite.

In fact, a stronger statement is true. Namely, for a given dimension g there are only finitely many abelian varieties of dimension g over a given finite field. In part 3, we will show this stronger statement is, in fact, implied by the Tate conjecture.

Theorem 1.3.2. Let k be a finite field. The Tate conjecture of abelian varieties over k implies that there are only finitely many abelian varieties of dimension g over k.

This result is first proved by Zarhin [46, Theorem 4.1]. We will give a different approach to this result.

Part I

The essential dimension of algebraic stacks

Chapter 2

Essential dimension and algebraic stacks

In this chapter we review the definitions and facts we need in our discussion.

2.1 The essential dimension of a functor

We refer to the survey article [1] for basic material of the essential dimension. Let k be a field. We use $Field/k$ to denote the category of field extensions of k with morphisms the obvious inclusions and Set the category of sets. Given a functor

$$F : Field/k \to Set$$

for an element $\eta \in F(K)$ for some field extension K/k, we say an intermediate field $k \subseteqq L \subseteqq K$ a $defining\ field$ of η if there is an element $\eta' \in F(L)$ such that $\eta'|_K \in F(K)$ is just η under the inclusion. The *essential dimension* of η, which is denoted by $ed_k\eta$, is defined by

$$ed_k\eta = min_L tr.deg(L/k)$$

where L runs over all the defining field of η. The *essential dimension* of the functor F, which is denoted by ed_kF, is defined by

$$ed_kF = max_{\eta \in F(K)} ed_k\eta$$

for all field extension K/k and all elements in $F(K)$.

From the definition we can see that the essential dimension of a functor can be infinity.

Here are some interesting examples:

Example 2.1.1. Let G be a group variety over k. Define a functor F:

$$\begin{aligned} F :& Field/k \to Set \\ & K/k \to H^1(K, G_K) \end{aligned}$$

sending K to the set of isomorphism classes of G-torsors over K. In this case we usually denote the essential dimension of F by $ed_k G$. This is a numerical invariant of the group variety G. This invariant gives us the information about how many parameter we need to describe a torsor of the group variety.

Example 2.1.2. Given an integral variety X/k, consider the following functor:

$$\begin{aligned} F :& Field/k \to Set \\ & K/k \to X(K) \end{aligned}$$

We can compute the essential dimension of F in this case. For any field extension K/k, an element in $\eta \in X(K)$ is just a morphism

$$\mathrm{Spec}(K) \to X$$

but any morphism from a point to a scheme can be factored through some point on X, i.e. it can be factored through

$$\mathrm{Spec}(K) \to \mathrm{Spec}(\kappa(x)) \to X$$

for some point $x \in X$. Then we have

$$ed_k \eta = tr.deg(\kappa(x)/k)$$

So we have

$$ed_k F \leq max_{x \in X} tr.deg(\kappa(x)/k) = \mathrm{dim} X$$

On the other hand, the generic point of X has essential dimension $\mathrm{dim} X$. So we have

$$ed_k F = \mathrm{dim} X$$

For an integral algebraic space X, we can always find a stratification of it and each strata is a scheme. So by definition if we define a functor F as above, we still have

$$ed_k F = \mathrm{dim} X$$

so there is no much interest for algebraic varieties or algebraic spaces. The situation is much more interesting for algebraic stacks.

2.2 The essential dimension of algebraic stacks

We refer to [35] and [44] for more details of algebraic stacks. Let S be a scheme. We denote Aff_S the category of affine schemes over S. A stack over S is a stack over Aff_S. That is, a fibered category over Aff_S satisfying the Definition 4.6 of [44].

Definition 2.2.1. ([35, Definition 8.1.4]) A stack $\mathcal{X}$ over a scheme S is called an *algebraic stack* if it satisfies the following two conditions:

(1) The diagonal

$$\mathcal{X} \to \mathcal{X} \times_S \mathcal{X}$$

is representable, separated and quasi-compact.

(2) There is an algebraic space X and a morphism $X \to \mathcal{X}$ which is surjective and smooth.

Now let the base scheme S be $\mathrm{Spec}(k)$ for some field k, and $\mathcal{X} \to \mathrm{Spec}(k)$ an algebraic stack over k. Consider the functor

$$\begin{aligned} F_{\mathcal{X}} : &Field/k \to Set \\ &K/k \to \{Isomorphism\ classes\ of\ objects\ in\ \mathcal{X}(K)\} \end{aligned}$$

The essential dimension of $\mathcal{X}$ is just the essential dimension of this functor $F_{\mathcal{X}}$. Usually we use $ed_k\mathcal{X}$ instead of $ed_k F_{\mathcal{X}}$ to denote the essential dimension of an algebraic stack.

This is a natural generalization of the case of algebraic varieties or spaces. Unlike the previous two cases, the essential dimension of algebraic stacks can be really complicated. We consider the following examples.

Example 2.2.2. Let G be a smooth algebraic group, and $\mathcal{X} = BG$ the classifying stack of G. In this case we know that the set of K points of the classifying stack is just the set of isomorphism classes of torsors of G. So $ed_k BG = ed_k G$, as we defined in Example 2.1.1. We refer to [3] for more results on classifying stacks.

Example 2.2.3. ([3, Theorem 1.8]) Assume the base field k has characteristic 0. Let $\mathcal{M}_{g,n}$ be the moduli stack of n pointed curves with genus g. Then we have

$$ed_k\mathcal{M}_{0,0} = ed_k\mathcal{M}_{1,1} = 2$$

$$ed_k\mathcal{M}_{0,1} = ed_k\mathcal{M}_{0,2} = 0$$

$$ed_k\mathcal{M}_{1,0} = +\infty$$

$$ed_k\mathcal{M}_{2,0} = 5$$

otherwise we have

$$ed_k\mathcal{M}_{g,n} = 3g - 3 + n$$

We can see from these examples that the essential dimension of algebraic stacks are usually complicated, it can even be infinity.

We need some basic facts about the essential dimension of algebraic stacks.

Proposition 2.2.4. ([3, Propositon 2.12]) Let $\mathcal{X}/k$ be an algebraic stack over k and K/k a field extension. Then we have

$$ed_K\mathcal{X}_K \leq ed_k\mathcal{X}$$

Proof. Let L/K be a field extension, then we have the map $\mathcal{X}_K(L) \to \mathcal{X}(L)$ is an equivalence. Pick some element $\xi \in \mathcal{X}_K(L)$, and suppose M/k is a field of definition of $\xi \in \mathcal{X}_K(L) \cong \mathcal{X}(L)$. Then any field containing M and K will be a defining field of $\xi \in \mathcal{X}_K(L)$ (as an object in $Field/K$). So we may pick some composition field N of M and K and we can see that $tr.deg(N/K) \leq tr.deg(M/k)$, hence we have $ed_K(\xi) \leq ed_k(\xi)$, hence

$$ed_K\mathcal{X}_K \leq ed_k\mathcal{X}$$

□

Proposition 2.2.5. ([3, Proposition 2.24]) Let $\mathcal{X}$ and $\mathcal{Y}$ be two algebraic stacks, then we have

$$ed_k(\mathcal{X} \times_k \mathcal{Y}) \leq ed_k\mathcal{X} + ed_k\mathcal{Y}$$

Proof. This is almost by definition. We refer to [27, Chapter 2, 2.2.2] the construction of fiber products of fiber categories. Let K/k be a field extension. Pick an object (η, ξ) in $(\mathcal{X} \times_k \mathcal{Y})(K)$, then we may choose $k \subseteqq F \subseteqq K$ to be a defining field of η with $tr.deg(F/k) \leq ed_k\mathcal{X}$ and $k \subseteqq L \subseteqq K$ to be a defining field of ξ with $tr.deg(L/k) \leq ed_k\mathcal{Y}$. Then any composition field of F and L is a defining field of (η, ξ). So we must have $ed_k(\eta, \xi) \leq ed_k\mathcal{X} + ed_k\mathcal{Y}$. Since this is true for all elements, so we have

$$ed_k(\mathcal{X} \times_k \mathcal{Y}) \leq ed_k\mathcal{X} + ed_k\mathcal{Y}$$

□

Remark 2.2.6. The equality doesn't hold in general. For example, if $\mathcal{X} \cong B\mu_2$ and $\mathcal{Y} \cong B\mu_3$, the base field k is algebraically closed, then we have

$$ed_kB\mu_2 = 1,\ ed_kB\mu_3 = 1$$

while

$$ed_k(B\mu_2 \times_k B\mu_3) = ed_kB\mu_6 = 1$$

2.3 The genericity theorem

In this section we will introduce the genericity theorem proved in [3, Theorem 4.1] and generalized in [5, Theorem 6.1]. An algebraic stack $\mathcal{X}$ is called a Deligne-Mumford stack, if in the condition (2) of Definition 2.2.1, we can find an algebraic space X and a morphism $X \to \mathcal{X}$ which is *etale* and surjective. We will use *DM stack* instead of *Deligne-Mumford stack* in the thesis. Now suppose we have a DM stack $\mathcal{X}$. The inertia stack of $\mathcal{X}$ is $\mathcal{X} \times_{\mathcal{X}\times\mathcal{X}} \mathcal{X}$, we use $\mathcal{I}_{\mathcal{X}}$ to denote it. We say the DM stack $\mathcal{X}$ admits finite inertia if the canonical morphism

$$\mathcal{I}_{\mathcal{X}} \to \mathcal{X}$$

is finite.

Definition 2.3.1. ([35, Definition 11.1.1]) Let $\mathcal{X}$ be an algebraic stack, X an algebraic space with a morphism $\pi : \mathcal{X} \to X$. We say X is a *coarse moduli space* of $\mathcal{X}$ with respect to the morphism π if the following two conditions are satisfied:

(1) For all algebraically closed field K, the morphism π induces a bijection of points $|\pi| : |\mathcal{X}(K)| \to |X(K)|$. Here for an algebraic stack $\mathcal{X}$ and a field K, $|\mathcal{X}(K)|$ means the set of isomorphism classes in $\mathcal{X}(K)$.

(2) π is universal for all morphisms from $\mathcal{X}$ to an algebraic space. That is if there is another algebraic space Z and a morphism $g : \mathcal{X} \to Z$ then there is a morphism $f : X \to Z$ such that $g = f\pi$.

By the Keel-Mori theorem (see [11] for the statement and the proof), if $\mathcal{X}$ is a DM stack locally of finite type over k with finite inertia $\mathcal{I}_{\mathcal{X}}$, then $\mathcal{X}$ admits a coarse moduli space. Now we can state the genericity theorem:

Theorem 2.3.2. ([3, Theorem 4.1], [5, Theorem 6.1]) Let $\mathcal{X}$ be a smooth integral tame connected DM stack locally of finite type. Let $\mathcal{U}$ be any open substack of $\mathcal{X}$ with finite inertia, and by Keel-Mori theorem, $\mathcal{U}$ admits a coarse moduli space U. Denote the function field of U to be K, and $\mathcal{U}_K = \mathcal{U} \times_U \mathrm{Spec}(K)$. Then we have

$$ed_k\mathcal{X} = \mathrm{dim}U + ed_K\mathcal{U}_K$$

Remark 2.3.3. In [3, Theorem 4.1], the theorem is proved in the case when the base field k is of characteristic 0. In [5, Theorem 6.1], the authors proved a general statement for positive characteristic base field and the algebraic stack $\mathcal{X}$ is integral and smooth (not necessarily with fintie inertia). Also a proposition they used in that paper is incorrect, but they gave a correct version in [4, Theorem 1.2]. Please check these papers for details.

We have two direct corollaries.

Corollary 2.3.4. Let $\mathcal{X}$ be a DM stack satisfying the properties needed in Theorem 2.3.2. For any open substack $\mathcal{U}$ of $\mathcal{X}$, we have

$$ed_k\mathcal{X} = ed_k\mathcal{U}$$

Corollary 2.3.5. Let $\mathcal{X}$ be a DM stack satisfying the properties needed in Theorem 2.3.2. If the generic point has a trivial automorphism group, then

$$ed_k\mathcal{X} = \dim X$$

Example 2.3.6. The tameness here is really important. We can consider the following example: Set $G = \mathbb{Z}/p^r\mathbb{Z}$ for some odd prime p. Then by Lemma 3 in [40] we can construct a smooth curve X over $\mathbb{F}_p$ with a smooth G fixed point. Set $\mathcal{X} = [X/G]$. Then $\mathcal{X}$ is a smooth DM integral stack locally of finite type over $\mathbb{F}_p$. But it is obvious that

$$ed_{\mathbb{F}_p}\mathcal{X} \geq ed_{\mathbb{F}_p}\mathbb{Z}/p^r\mathbb{Z}$$

And Ledet conjectured in [28, Remark in page 4] that

$$ed_{\mathbb{F}_p}\mathbb{Z}/p^r\mathbb{Z} = r$$

So if the conjecture holds, we can see that the essential dimension of $\mathcal{X}$ can never be controlled by its generic point.

A naive question is the following: Give a DM stack $\pi : \mathcal{X} \to X$ which is a smooth map, and $\mathcal{X}$ is smooth integral tame, X is integral and regular, then for any point $x \in X$, we have a stack $\mathcal{X}_s$, then we may ask how the essential dimensions of this family of stacks change. Or more precisely, does the function

$$f(x) = ed_{k(x)}\mathcal{X}_x$$

have some good properties? The following example shows that this function is not locally constant.

Example 2.3.7. Consider the affine line C over $\mathbb{F}_p$, where p is a prime. Choose some q a prime number such that $q|p-1$ but $q^2 \nmid p-1$, for example $p = 29, q = 7$. Then consider the trivial gerbe $\mathcal{X} = X \times B(\mathbb{Z}/q^r\mathbb{Z})$ for some $r > 1$. We need to use [14, Theorem 4.1]. We can see the essential dimension $ed_{k(\eta)}\mathcal{X}_\eta = q^{r-1}$. Then suppose the function defined above is locally constant, then there exists an open subset $U \subsetneqq C$ such that for any $u \in U$, we always have

$$ed_{k(u)}\mathcal{X}_u = q^{r-1}$$

Let's prove this cannot happen. From elementary number theory we can always find an integer t such that $q^r|p^t-1$. Suppose $C-U=\{x_1,x_2,...,x_n\}$, we set

$$N=max_{1\leq i\leq n}deg(k(x_i)/\mathbb{F}_p)$$

We may choose an irreducible polynomial $f(x)$ of degree tN in $\mathbb{F}_p[x]$. Then the canonical quotient morphism $\mathbb{F}_p[x]\to\mathbb{F}_p[x]/f(x)=F$ gives us a natural closed point

$$x:\mathrm{Spec}(F)\to C$$

and the image of x must be in U. Then we have $k(x)\cong\mathbb{F}_{p^{tN}}$. And we have $ed_{k(x)}\mathcal{X}_x$ is just the essential dimension of the constant groups scheme over F. But then by Theorem 4.1 of [14], we can see that $ed_{k(x)}\mathcal{X}_x\leq q$ (here we cannot apply the theorem directly but at least the inequality holds). Which is a contradiction.

2.4 The essential dimension of gerbes

We can see that to compute the essential dimension of a DM stack $\mathcal{X}$, by Theorem 2.3.2 we just need to consider the generic gerbe of it (lots of stacks coming from moduli problems satisfy the conditions we need in Theorem 2.3.2). Then we need to consider the essential dimension of gerbes.

Definition 2.4.1. ([27, Definition 3.15]) Given an algebraic stack $\mathcal{X}$, an algebraic space X and a morphism $\pi:\mathcal{X}\to X$. We say $\mathcal{X}$ is a *gerbe* over X if the two morphisms $\pi:\mathcal{X}\to X$ and $\Delta:\mathcal{X}\to\mathcal{X}\times_X\mathcal{X}$ are both epimorphisms.

Remark 2.4.2. This is a formal definition. There is another concrete explanation. Since we will mostly consider gerbes over fields, so we just give this description in this case, for details, please check [35, Chapter 12]. Let $\mathcal{X}$ be a stack over a field k. We say $\mathcal{X}\to\mathrm{Spec}(k)$ is a gerbe over $\mathrm{Spec}(k)$ if the following conditions are satisfied:

(1) There exists a field extension k'/k such that $\mathcal{X}(k')$ is non-empty.

(2) Given an affine scheme S over k and two objects $\eta,\xi\in\mathcal{X}(S)$, there exists a fppf cover $\{S_i\to S\}$ such that the pullback η_{S_i} and ξ_{S_i} are isomorphic in $\mathcal{X}(S_i)$.

We call $\mathcal{X}$ is a *trivial* gerbe (or *neutral* gerbe) over $\mathrm{Spec}(k)$ if $\mathcal{X}(k)$ is non-empty.

Let G be a sheaf of abelian group over k. $\mathcal{X}$ is a gerbe over k. $\mathcal{X}$ is called a gerbe *banded* by G, or simply a G-gerbe, if for any affine scheme S and any object $\eta\in\mathcal{X}(S)$, we have an isomorphism $G_S\cong Aut_s(\eta)$ compatible with pullbacks, here $Aut_S(\eta)$ is the group scheme of automorphisms of η over S. A G-gerbe is trivial if and only if it is equivalent to the classifying stack B_kG.

The following theorem is well known.

Theorem 2.4.3. ([19, Chapter 4, Theorem 3.4.2], [35, Theorem 12.2.8]) Let X be a algebraic space over k, G is a sheaf of abelian groups. Then there is a bijection

$$\{Isomorphism\ classes\ of\ G\text{-}gerbes\ over\ X\} \leftrightarrow H^2(X, G)$$

We will concentrate on μ_n-gerbes and $\mathbb{G}_m$-gerbes. As the previous theorem shows they are just $H^2(k, \mu_n)$ and $H^2(k, \mathbb{G}_m)$. We know that $H^2(k, \mathbb{G}_m)$ is canonically isomorphic to the Brauer group $Br(k)$ of k, the equivalent classes of central simple algebras over k. By Wedderburn's theorem, any central simple algebra over k is isomorphic to a matrix algebra $M_n(D)$ for some division algebra D. For any Brauer class $\alpha \in Br(k)$, there is a matrix algebra $M_n(D)$ representing α, the *index* of α, denote it by $ind(\alpha)$, is defined as the square root of the dimension of D, i.e. $\sqrt{\dim_k(D)}$. Also the *period* of α, denote it by $per(\alpha)$, is defined to be the order of α in $Br(k)$. For details of the Brauer group over fields we refer to [18].

For future use we need an explicit way from a cohomology class to a central simple algebra. The construction is as follows: Given a cohomology class $\alpha \in H^2(k, \mathbb{G}_m)$, this is represented by some cycle, that is a map

$$f : G \times G \to \bar{k}^*$$

satisfying the relation:

$$f(\sigma, \tau\nu)f(\tau, \nu) = f(\sigma\tau, \nu)\nu(f(\sigma, \tau))$$

Here G is the absolute Galois group of k. Choose some finite Galois extension k'/k such that $\alpha_{k'}$ is trivial in $H^2(k', \mathbb{G}_m)$, and write $G' = Gal(k'/k)$ the Galois group. Then α is equivalent to a map

$$f : G' \times G' \to k'^*$$

satisfying the same relation. Now we can construct an algebra as follows: Let A be a k' vector space with basis labeled by G', i.e. A is a vector space spanned by x_σ for $\sigma \in G'$. We equip A with the following product rules:

$$x_\sigma x_\tau = x_{\sigma\tau} f(\sigma, \tau)$$

$$cx_\sigma = x_\sigma \sigma(c)$$

We can show this is a central simple algebra, so we get a Brauer class represented by A. We will need this construction in Chapter 4.

There is an short exact sequence of group schemes:

$$1 \to \mu_n \to \mathbb{G}_m \xrightarrow{\times n} \mathbb{G}_m \to 1$$

which induces a morphism:

$$H^2(k, \mu_n) \to H^2(k, \mathbb{G}_m)[n]$$

So we can see that $H^2(k, \mu_n)$ corresponds to n torsion elements of the Brauer group.

Now we need a technical theorem.

Theorem 2.4.4. ([5, Theorem 4.1]) Assume the base field has characteristic 0. Let $d > 1$ be an integer. Let $\alpha \in H^2(k, \mu_d)$ be a cohomology class and $\beta \in H^2(k, \mathbb{G}_m)$ be its image under the above map. Let $\mathcal{X}$ be the μ_d-gerbe associated to α and $\mathcal{Y}$ the $\mathbb{G}_m$-gerbe associated to β, then we have

$$ed_k\mathcal{X} = ed_k\mathcal{Y} + 1$$

In Conjecture 1.1.1 it is conjectured that the essential dimension of μ_n-gerbes is closed related to the index of its associated Brauer class. The conjecture has been proved in the case when the index is a prime power.

Theorem 2.4.5. ([3, Theorem 5.4]) Let $\mathcal{X}$ be a gerbe over k banded by μ_{p^n} for some prime p. Then we have

$$ed_k\mathcal{X} = ind[\mathcal{X}]$$

where $[\mathcal{X}]$ means the Brauer class of $\mathcal{X}$ in $Br(k)$.

With these preparations we can prove:

Theorem 2.4.6. Let X be a smooth integral variety over some field k of characteristic 0. Let $\mathcal{X} \to X$ be a $\mathbb{G}_m$-gerbe. Denote K the function field of X, then we have

$$ed_k\mathcal{X} = \dim X + ed_K\mathcal{X}_K$$

Here $\mathcal{X}_K$ means the base change of $\mathcal{X}$ along the generic point $\mathrm{Spec}(K) \to X$.

Proof. Since X is smooth, the canonical inclusion $\mathrm{Spec}(K) \to X$ induces an injection $H^2(X, \mathbb{G}_m) \to H^2(K, \mathbb{G}_m)$, which implies that $H^2(X, \mathbb{G}_m)$ is torsion. So the cohomology class $[\mathcal{X}] \in H^2(X, \mathbb{G}_m)$ lies in the image of $H^2(X, \mu_n) \to H^2(X, \mathbb{G}_m)$ for some n. Write $\mathcal{Y} \to X$ the μ_n-gerbe such that its image in $H^2(X, \mathbb{G}_m)$ is just $[\mathcal{X}]$. Then we have

$$\begin{aligned} ed_k\mathcal{X} &= max_{p\in X}\{ed_{k(p)}\mathcal{X}_p + tr.deg(k(p))\} \\ &= max_{p\in X}\{ed_{k(p)}\mathcal{Y}_p + tr.deg(k(p))\} - 1 \\ &= \dim X + ed_K\mathcal{Y}_K - 1 \\ &= \dim X + ed_K\mathcal{X}_K \end{aligned}$$

where $k(p)$ is the residue field of $p \in X$ and $\mathcal{X}_p$ is the restriction of $\mathcal{X}$ to p, similar for $\mathcal{Y}_p$. The first equality is by definition, the second is by Theorem 2.4.4, the third is by Theorem 2.3.2, the last is again by Theorem 2.4.4. □

This implies for $\mathbb{G}_m$-gerbes over smooth varieties, we still have the genericity theorem. This fact is known to experts, for example see [39, Chapter 2].

We also have a small lemma.

Lemma 2.4.7. Given a $\mathbb{G}_m$-gerbe $\mathcal{X}$ over some field k of characteristic 0, then we have $ed_k\mathcal{X} = 0$ if and only if $\mathcal{X}$ is the trivial gerbe.

Proof. If $\mathcal{X}$ is the trivial gerbe then obivously we have $ed_k\mathcal{X} = ed_k\mathbb{G}_m = 0$. Let's prove the other direction. Suppose $ed_k\mathcal{X} = 0$. Let $\mathcal{Y}$ be a μ_d-gerbe for some d and $[\mathcal{Y}]$ maps to $[\mathcal{X}]$ in $H^2(k, \mathbb{G}_m)$. By Theorem 2.4.4, we have $ed_k\mathcal{Y} = 1$. Write

$$ind[\mathcal{Y}] = p_1^{r_1}...p_k^{r_k}$$

the prime decomposition of the index of $[\mathcal{Y}]$. Then we have

$$ed_k\mathcal{Y} \geq p_1^{r_1}$$

by Theorem 2.4.5. Hence we must have $r_1 = 0$. This is true for all prime factors, so we have $\mathcal{X}$ is the trivial gerbe. □

Chapter 3

Essential dimension of moduli stack of polarized K3 surfaces

In this chapter we will discuss the essential dimension of the moduli stack of K3 surfaces. The proof of $d = 2$ case was given by Angelo Vistoli through an email with the author. The material in this chapter is more or less the same as [15].

3.1 The case when $d = 2$

A K3 surface X over k is a smooth proper variety over k with trivial canonical line bundle and $H^1(X, \mathcal{O}_X) = 0$. For a line bundle L on X, L is called *primitive* if there exists no line bundle M on X such that $L = M^{\otimes d}$ for some $d > 1$. A *polarized K3 surface of degree d* is a pair (X, L) with X a K3 surface and L a primitive ample line bundle with $L^2 = d$. Note here d must be an even number.

We will omit the details for the moduli stack (space) of polarized K3 surfaces of degree d, for details, see [23] and [41].

We use $\mathcal{M}_d$ to denote the moduli stack of polarized K3 surfaces with degree d. We have

Theorem 3.1.1. ([41, Theorem 4.3.3]) The moduli stack $\mathcal{M}_d$ is a connected smooth DM stack with finite inertia locally of finite type.

So we have a coarse moduli space M_d. It is integral of dimension 19, but it is not smooth.

Next we consider the case when $d = 2$. We first list some properties of polarized K3 surfaces (X, L) with degree 2 as an example here.

Example 3.1.2. Given a polarized K3 surface (X, L) with $(L^2) = 2$. Then we know that the global sections of L give a double cover $\pi : X \to \mathbf{P}^2$, and π is ramified along a smooth curve $C \subsetneqq \mathbf{P}^2$ of degree 6. And we know that a general curve of degree 6 in $\mathbf{P}^2$ has trivial automorphism group. Then by the standard description of double covers we know that a general polarized K3 surface (X, L) of degree 2 has automorphism group $\mathbb{Z}/2\mathbb{Z}$. So we know that in this case if we denote the field of rational functions of M_2 by K, then the fiber product $\mathcal{M}_{2,K} = \mathcal{M}_2 \times_{M_2} \mathrm{Spec}(K)$ is a $\mathbb{Z}/2\mathbb{Z}$ gerbe over K.

With the previous example and Theorem 2.3.2 we see to find the essential dimension of $\mathcal{M}_2$ over k we just need to consider the essential dimension of $\mathcal{M}_{2,K}$ over K, then by Theorem 2.4.5 we just need to find the index of the class of $[\mathcal{M}_{2,K}]$ in $Br(K)$.

Theorem 3.1.3. ([15, Theorem 3.2]) The gerbe $\mathcal{M}_{2,K}$ is a trivial gerbe, so it has index 1, hence $ed_k\mathcal{M}_2 = 20$.

Proof. From Example 3.3.4 we know that the moduli space M_2 is just the quotient of the space of smooth curves of degree 6 in $\mathbf{P}^2$ by the PGL_3 action. So there exists a Brauer-Severi surface P over K and a degree 6 curve $C \subsetneqq P$ such that the generic gerbe is just the stack of the double covers $Y \to P$ which ramified over C. To prove the gerbe is trivial it suffices to show $\mathcal{M}_{2,K}(K)$ is non-empty. But by the description of double covers we just need to find a square root of $\mathcal{O}(C)$. Then since $\mathbf{Pic}(P) \cong \mathbb{Z}$, we just need to find a line bundle of degree 3. But the inverse of the canonical line bundle has degree 3, so the gerbe is trivial, we finish the proof. □

This gives the answer in the case of $d = 2$.

3.2 The case when $d > 2$

Next we consider the case when the degree is greater than 2. We first assume $k = \mathbb{C}$. We need a technical lemma.

Lemma 3.2.1. Let $\mathcal{X}$ be a smooth connected DM stack with finite inertia locally of finite type over k. If there exists a k point x on $\mathcal{X}$ such that the automorphism group G_x is trivial, then there exists an open dense substack $\mathcal{U}$ of $\mathcal{X}$ such that for any point on $\mathcal{U}$, it will have trivial automorphism group, hence the generic point has trivial automorphism group.

Proof. The automorphism group G_x is the pull-back

$$G_x = \mathrm{Spec}(k) \times_{\mathcal{X}} \mathcal{I}_{\mathcal{X}}$$

where $\mathcal{I}_{\mathcal{X}}$ is the inertia stack of $\mathcal{X}$. We pick some etale cover $U \to \mathcal{X}$ of $\mathcal{X}$, then we have U is smooth. Then there exists a k point u on U such that the composition

$$u \to U \to \mathcal{X}$$

is just the given k point (here we use the fact that k is algebraically closed). We may choose an affine connected open neighborhood of u, also denoted by U. Write

$$G_U = U \times_{\mathcal{X}} \mathcal{I}_{\mathcal{X}}$$

Since $\mathcal{I}_{\mathcal{X}}$ is finite over $\mathcal{X}$, by definition G_U is also an affine scheme over k. Also we know for any dense open subset of U its image in $\mathcal{X}$ will be a dense open set. So we just need to prove that there exist an open dense subscheme W of U such that for any point of W the fiber is just $\mathrm{Spec}(k)$.

Let's denote the morphism $G_U \to U$ by π, and the point with trivial automorphism group by x. Write $G_U = \mathrm{Spec}(B)$, $U = \mathrm{Spec}(A)$, the maximal ideal corresponding to x by $\mathfrak{m}$, then we have $B/\mathfrak{m}B \cong k$. Consider the sheaf associated to B on U, we call it $\mathcal{F}$. Then $\mathcal{F}$ is coherent. We have

$$\dim \mathcal{F}_x \otimes \mathcal{O}_{U,x}/\mathfrak{m}_x = 1$$

But by [21, Ex. 5.8] on page 125, the function

$$\phi(u) = \dim \mathcal{F}_u \otimes \mathcal{O}_{U,u}/\mathfrak{m}_u$$

is an upper semi-continuous function. Since the fiber over any point is non-empty, so

$$W = \{u \in U | \phi(u) = 1\}$$

is an open subscheme of U. Since U is integral, W is dense.

By the same exercise, since U is integral, so on W, $\mathcal{F}_W$ is a line bundle. Then we may choose an open subscheme of W (just shrink W, so we still use W to denote it) such that on it we have $\mathcal{F}_W \cong \mathcal{O}_W$. Then on this subset, it is obvious that every point has fiber $\mathrm{Spec}(k)$. This dense open subscheme satisfies the properties we want. □

By the above lemma, since $\mathcal{M}_d$ satisfies all the property we need, if we find a polarized K3 surface with a trivial automorphism group, then the generic point must have trivial automorphism group. But we know there must exist a polarized K3 surface with Picard number 1 of any degree, then by the following theorem, we can get our result.

Theorem 3.2.2. ([23, Corollary 12.2.12]) If X is a complex projective K3 surface with $\mathbf{Pic}(X) = \mathbb{Z}H$ and $(H^2) > 2$, then $Aut(X) = id$.

For proof, see [23, Corollary 12.2.12].

Combine this theorem and the above technical lemma and Theorem 2.3.2, we can see that if the base field is the field of complex numbers, then the theorem is true. For the general case, we know that $\mathcal{M}_d$ is defined over $\mathbb{Q}$. By [3, Proposition 2.14] we have

$$ed_{\bar{\mathbb{Q}}}\mathcal{M}_{d,\bar{\mathbb{Q}}} = ed_k\mathcal{M}_{d,k} = ed_{\mathbb{C}}\mathcal{M}_{d,\mathbb{C}}$$

So we have:

Theorem 3.2.3. Let k be an algebraically closed field of characteristic 0. The essential dimension of $\mathcal{M}_d$ is 19 when $d > 2$.

3.3 The case of positive characteristic

By [3, Proposition 2.14] , we may assume that the base field $k = \bar{\mathbb{F}}_p$ for some p prime. We will consider the moduli stack of polarized K3 surfaces when the base field is of (large) positive characteristic in this section. Actually we will only consider the K3 surfaces over $\mathbb{F}$, the algebraic closure of $\mathbb{F}_p$ for some prime $p \geq 23$ and $p \nmid d$. The idea is to apply the deformation theory of K3 surfaces and the result we got above. We first collect some results we need.

Recall that actually to compute the essential dimension of some DM stack with finite inertia actually we just need to consider the general case, so it suffices to consider the ordinary K3 surfaces. It suffices to find one point in the stack with trivial automorphism group, so let's concentrate on the K3 surfaces with height 1 and Picard number 20. Over $\mathbb{C}$, K3 surfaces with Picard number 20 can be classified by the transcendental lattices, which have rank 2. More precisely, let S_p denote the set of positive definite even lattices with rank 2 such that the discriminant is a non-zero square mod p. Given any positive definite, oriented even lattice M of rank 2, there exists a unique complex K3 surface X_M with its transcendental lattice is just M. Such X is defined over $\bar{\mathbb{Q}}$. The reduction of X over $\mathbb{F}$ is a K3 surface with Picard number 20 (for details see the discussion in [25, Section 3]). This gives us a morphism from the set S_p to the set of isomorphism classes of K3 surfaces with Picard number 20 over $\mathbb{F}$. We have the following:

Theorem 3.3.1. ([25, Theorem 3.7]) The morphism defined above is a bijection.

For an ordinary K3 surface over $\mathbb{F}$ with Picard number 20, it has a unique Neron-Severi preserved lifting, which is just the canonical lifting [34, Definition 1.9]. We have the following theorem comparing the automorphism group of the K3 surface itself and the Neron-Severi preserved lifting.

Theorem 3.3.2. ([24, Theorem 3.7]) Let X be a weakly tame K3 surface over $\mathbb{F}$, then there exists a Neron-Severi group preserving lifting $\mathfrak{X}/W$, where W is the Witt vector of $\mathbb{F}$, such that the reduction map $Aut(\mathfrak{X} \otimes K) \to Aut(X)$ is an isomorphism.

For the proof and the definition of *weakly tame*, we refer to [24, Theorem 3.7]. Recall that if $p > 22$, then every K3 surface of finite height is weakly tame. And by the standard argument we can show that in this case $Aut(\mathfrak{X} \otimes \mathbb{C}) \cong Aut(X)$ and $NS(\mathfrak{X} \otimes \mathbb{C}) \cong NS(X)$ canonically.

Now let's return to the polarized case. Given the moduli stack $\mathcal{M}_d$ of polarized K3 surfaces over $\mathbb{F}$, let's assume the degree of the polarization is greater than 2. By Lemma 3.2.1, if we can find a point on $\mathcal{M}_d$ with trivial automorphism group, we can show the generic point has trivial automorphism group.

We next need to use the theory of period domain. We suggest [23, Chapter 6] for the basic facts and properties. We have the following theorem:

Theorem 3.3.3. We fix the ground field to be $\mathbb{C}$. In the moduli stack $\mathcal{M}_d$, the set of K3 surfaces with Picard number 20 and the discriminant of the transcendental lattice is a non-zero square mod p form a dense subset of $\mathcal{M}_d(\mathbb{C})$.

Before we start our proof, let's first recall some basic results about the period domain. Set the lattice $\Lambda_d = \mathbb{Z}(-d) \oplus U^{\oplus 2} \oplus E_8(-1)^{\oplus 2}$ and $(-,-)$ the quadratic form on it, where U is the hyperbolic lattice and E_8 is the lattice associated to the Dynkin diagram E_8. This is the lattice orthogonal to the lattice generated by the ample line bundle of degree d we choose in the standard K3 lattice, see [23, Chapter 6].

So we have the period domain of marked polarized K3 surfaces with degree d, which we denoted by D_d. D_d is a subset of $\mathbb{P}(\Lambda_{d,\mathbb{C}})$. The group of orthogonal matrix O_d has a natural action on D_d, and we know that the coarse moduli space M_d is just an open subset of the quasi-projective variety D_d/O_d. So to prove the above theorem, we just need show the points on D_d corresponding to the mark polarized K3 surfaces with transcendental lattice having discriminant a non-zero square mod p is dense in D_d. But since D_d is diffeomorphic to the set of oriented planes in $\Lambda_d \otimes \mathbb{R}$ such that the restriction of the quadratic form on the plane is positive definite ([23, Proposition 6.1.5]), and the set of positive definite planes is an open subset of the set of all planes, we just need to prove the following theorem. For simplicity, we call

the property of a lattice *with discriminant a non-zero square mod p* just property R.

Theorem 3.3.4. The set of rationally generated planes in $\Lambda_d \otimes \mathbb{R}$ satisfying property R forms a dense subset of the grassmannian $Gr(2, \Lambda_d \otimes \mathbb{R})$.

Proof. Choose an open subset of $Gr(2, \Lambda_d \otimes \mathbb{R})$. We first choose a rationally generated plane $H \in U$. And we notice that actually to check property R, it suffices to check the discriminant of a *rational basis* of $H \cap \Lambda_d$. The reason is that the discriminant of such basis only differ with the discriminant of the integral basis by a square, so if the discriminant of a rational basis is a non-zero square mod p, the same is true for the integral basis. Also, when we write $\frac{1}{N} \in \mathbb{Z}/p$ for some $p \nmid N$, we just mean the inverse of N in $\mathbb{Z}/p$.

Assume $H \cap \Lambda_d$ is rationally generated by ω_1, ω_2 in Λ_d. We first need to do some reductions:

Step 1. We may assume $(\omega_1, \omega_1) \neq 0$ in $\mathbb{Z}/p$. If not, we can consider the element $\delta \in \Lambda_d$ satisfying $(\delta, \delta) = -2$. Of course δ in not in H. Then consider the plane H' generated by $(\omega_1 + \frac{1}{N}\delta, \omega_2)$. For N large enough, H' is in U. And

$$(\omega_1 + \frac{1}{N}\delta, \omega_1 + \frac{1}{N}\delta) = (\omega_1, \omega_1) + \frac{2}{N}(\omega_1, \delta) + \frac{1}{N^2}(\delta, \delta)$$

since $(\delta, \delta) \neq 0 \in \mathbb{Z}/p$, there must exist some N such that $(\omega_1, \omega_1) + \frac{2}{N}(\omega_1, \delta) + \frac{1}{N^2}(\delta, \delta) \neq 0$ in $\mathbb{Z}/p$. We we can replace H by H' to assume that $(\omega_1, \omega_1) \neq 0$ in $\mathbb{Z}/p$.

Step 2. We may assume $disc(\omega_1, \omega_2)$ is non-zero mod p. Consider H' generated by $(\omega_1, \omega_2 + \frac{1}{N}\delta)$ with any $(\delta, \delta) \neq 0$ in $\mathbb{Z}/p$. Then we have $disc(\omega_1, \omega_2 + \frac{1}{N}\delta) = ((\omega_1, \omega_1)(\omega_2, \omega_2) - (\omega_1, \omega_2)^2) + \frac{2}{N}((\omega_1, \omega_1)(\omega_2, \delta) - (\omega_1, \delta)(\omega_1, \omega_2)) + \frac{1}{N^2}((\omega_1, \omega_1)(\delta, \delta) - (\omega_1, \delta)^2)$. By the same reason, we just need to find some δ such that the leading coefficient $(\omega_1, \omega_1)(\delta, \delta) - (\omega_1, \delta)^2$ is non-zero in $\mathbb{Z}/p$. We prove the existence of such δ by contradiction. Assume for any $(\delta, \delta) \neq 0$ in $\mathbb{Z}/p$, we have $(\omega_1, \omega_1)(\delta, \delta) - (\omega_1, \delta)^2$ is zero in $\mathbb{Z}/p$. Since Λ_d contains $E_8(-1)$, so we can find δ_1, δ_2, with $(\delta_1, \delta_2) = 0$ and $(\delta_i, \delta_i) = -2$ for $i = 1, 2$. We have

$$(\omega_1, \omega_1)(\delta_i, \delta_i) - (\omega_1, \delta_i)^2$$

is zero for both i, and $(\omega_1, \omega_1)(\delta_1 + \delta_2, \delta_1 + \delta_2) - (\omega_1, \delta_1 + \delta_2)^2$ is zero, we may conclude

$$(\omega_1, \omega_1)(\delta_1, \delta_2) = (\omega_1, \delta_1)(\omega_1, \delta_2)$$

in $\mathbb{Z}/p$. But $(\delta_1, \delta_2) = 0$, so we may assume $(\omega_1, \delta_1) = 0$ in $\mathbb{Z}/p$. But then

$$(\omega_1, \omega_1)(\delta_1, \delta_1) - (\omega_1, \delta_1)^2 \equiv (\omega_1, \omega_1)(\delta_1, \delta_1)$$

which is non-zero, which is a contradiction. By replacing H by H', we may assume the discriminant is non-zero.

Step 3. We may assume there exists a $\eta \in \Lambda_d$ orthogonal to H and (η, η) is non-zero in $\mathbb{Z}/p$. From the previous two steps, we may assume H is rationally generated by ω_1, ω_2 with $(\omega_i, \omega_i) \neq 0$ in $\mathbb{Z}/p$ for $i = 1, 2$ and $(\omega_1, \omega_2) = 0$ (just by diagonalizing the matrix). Pick any $\delta \in \Lambda_d$, we have

$$\delta - \frac{(\omega_1, \delta)}{(\omega_1, \omega_1)}\omega_1 - \frac{(\omega_2, \delta)}{(\omega_2, \omega_2)}\omega_2$$

is orthogonal to H. And

$$(\delta - \frac{(\omega_1, \delta)}{(\omega_1, \omega_1)}\omega_1 - \frac{(\omega_2, \delta)}{(\omega_2, \omega_2)}\omega_2, \delta - \frac{(\omega_1, \delta)}{(\omega_1, \omega_1)}\omega_1 - \frac{(\omega_2, \delta)}{(\omega_2, \omega_2)}\omega_2)$$

$$= (\delta, \delta) - \frac{(\omega_1, \delta)^2}{(\omega_1, \omega_1)} - \frac{(\omega_2, \delta)^2}{(\omega_2, \omega_2)}$$

If for some δ the above number is non-zero in $\mathbb{Z}/p$, we are done. If not, let's choose a η orthogonal to H, also let's assume η is primitive. Then H' defined by $(\omega_1, \omega_2 + \frac{1}{N}\eta)$ also satisfies the assumption we made in step 1 and step 2. If for this plane, we also have every δ orthogonal to H' has $(\delta, \delta) \equiv 0$, then we have

$$(\delta, \delta) - \frac{(\omega_1, \delta)^2}{(\omega_1, \omega_1)} - \frac{(\omega_2 + \frac{1}{N}\eta, \delta)^2}{(\omega_2, \omega_2)}$$

is zero in $\mathbb{Z}/p$. Comparing with the previous equation we get

$$(\eta, \delta) \equiv 0$$

for any δ. But this makes η is divided by p in Λ_d, which is a contradiction to the primitivity of η. So by replacing H by H' we may assume there is a η orthogonal to H with $(\eta, \eta) \neq 0$ in $\mathbb{Z}/p$.

Step 4. We finish the proof in this step. So far we have a plane $H \in U$ rationally generated by ω_1, ω_2 with $(\omega_i, \omega_i) \neq 0$ in $\mathbb{Z}/p$ and $(\omega_1, \omega_2) = 0$. Set $A = disc(\omega_1, \omega_2)$. Then $A \neq 0$ in $\mathbb{Z}/p$ under the reduction of step 2. If A is already a square, we are done. If not, by step 3, we choose η orthogonal to H and $(\eta, \eta) \neq 0$ in $\mathbb{Z}/p$. Consider H' generated by $\omega_1, \omega_2 + \frac{1}{N}\eta$ for large enough N. Then

$$disc(\omega_1, \omega_2 + \frac{1}{N}\eta) = A + \frac{1}{N^2}(\omega_1, \omega_1)(\eta, \eta)$$

Denote $B = -(\omega_1, \omega_1)(\eta, \eta)$, then B is non-zero in $\mathbb{Z}/p$. And

$$disc(\omega_1, \omega_2 + \frac{1}{N}\eta) = A - By^2$$

Here y is the inverse of N mod p and can be 0, which means $H = H'$. We just need to show for some y, $A - By^2$ is a square mod p. We separate the problem into 2 cases:
(1) If B is a square mod p, consider the set $S = \{0, 1, 2, ..., \frac{p-1}{2}\}$. Then for any $y_1, y_2 \in S$, $A - By_1^2 \neq A - By_2^2$ mod p unless $y_1 = y_2$. But $A - By^2$ cannot be 0 in $\mathbb{Z}/p$ since A is not a square. But we only have $\frac{p-1}{2}$ non-squares mod p, and S contains $\frac{p+1}{2}$ elements. So there must be some y that makes $A - By^2$ a non-zero square.
(2) If B is not a square, then A/B is a square. We prove by contradiction. If for any y, $A - By^2$ is zero or not a square mod p, then for any y, $\frac{A}{B} - y^2$ is a square (maybe 0), hence $1 - y^2$ is a square for any y. The following is a little tricky: We notice -1 cannot be a square, or $y^2 - 1$ is a square then by induction every element in $\mathbb{Z}/p$ is a square, which is not true. Then 2 cannot be a square, otherwise $1 - 2 = -1$ is a square. Then $-2 = -1 \times 2$ is a square. So $1 - (-2) = 3$ is a square. On the other hand, $\frac{1}{y^2} - 1$ is a square for any $y \neq 0$, in particular $-2 - 1 = -3$ is a square, this makes $-1 = \frac{-3}{3}$ is a square, which is a contradiction. We finish the proof. □

So by the above theorem, and Theorem 3.2.2, we can find a polarized K3 surface over $\mathbb{C}$ with trivial automorphism group such that the transcendental lattice T is in S_p. It's reduction is a polarized K3 surface (X, L) over $\mathbb{F}$. Then from Theorem 3.3.1 and 3.3.2, we can conclude that $Aut(X, L) = \{id\}$. Then by Lemma 3.2.1, we can conclude that the generic object of $\mathcal{M}_d$ in characteristic p case also has trivial automorphism group if $d > 2$.

In [13, Theorem 2.1], it is proved that if $p > 11$, then every automorphism of a K3 surface with finite order is tame. In particular, that implies in this case the moduli stack $\mathcal{M}_d$ is tame, so apply Theorem 2.3.2, we have

Theorem 3.3.5. Assume k is an algebraically closed field of characteristic p for $p \geq 23$. Then the essential dimension of $\mathcal{M}_d$ with $d > 2$ and $p \nmid d$ is 19.

Part II

The period-index problem of elliptic curves

Chapter 4

Period-index problem of elliptic curves

In this chapter we consider the period-index problem of elliptic curves. We will see in the next chapter how this topic is related to the essential dimension of algebraic stacks. We refer to [9] for details.

4.1 The general setting of period-index problem

In the general case, fix a base field k, and we denote $G = Gal(k^{sep}/k)$ the absolute Galois group. Let M be a G module, write $\eta \in H^i(k, M)$ a cohomology class of M. The *period* of η, which is denoted by $per(\eta)$, is the order of η in $H^i(k, M)$. A field extension l/k is called a *splitting field* of η, if the restriction $\eta|_l$ is trivial in $H^i(l, M)$. The *index* of η, denote it by $I(\eta)$, is defined as the greatest common divisor of the degrees of finite splitting fields of η. The basic properties of $per(\eta)$ and $I(\eta)$ are collected in the following:

Proposition 4.1.1. ([9, Proposition 9]) Let $\eta \in H^i(k, M)$ be a cohomology class for some $i > 0$.

(1) $per(\eta)$ divides $I(\eta)$ and they have the same prime factors.

(2) If l/k is a field extension with degree prime to $per(\eta)$, then we have $per(\eta) = per(\eta|_l)$ and $I(\eta) = I(\eta|_l)$.

A natural way to relate an abelian variety to Galois cohomology theory is the theory about the torsors. Let A be an abelian variety over k. An *A-torsor* is a pair (T, f), where T is a non-empty k-scheme and $f : T \times A \to T$ is a morphism, such that the following conditions hold:

(1) The following diagrams commute:

$$\begin{array}{ccc} T \times A \times A & \xrightarrow{f\times 1} & T \times A \\ {\scriptstyle 1\times m}\downarrow & & \downarrow{\scriptstyle f} \\ T \times A & \xrightarrow{\quad f \quad} & T \end{array}$$

$$\begin{array}{ccc} T & \xrightarrow{1\times\epsilon} & T \times A \\ {\scriptstyle id}\downarrow & \swarrow_{f} & \\ T & & \end{array}$$

Here $m : A \times A \to A$ is the addition morphism and $\epsilon : \mathrm{Spec}(k) \to A$ is the unit of A.

(2) The morphism

$$T \times A \to T \times T$$
$$(t, a) \to (t, ta)$$

is an isomorphism.

Similar to gerbes banded by some group scheme, we also have a similar description of torsors.

Theorem 4.1.2. ([19, Chapter 3, Remark 3.5.4], [35, Corollary 12.1.5]) Let A be an abelian variety over some field k, then there is a bijection

$$\{\textit{isomorphism classes of } A\textit{-torsors over } k\} \leftrightarrow H^1(k, A)$$

We give a concrete construction here for future use. Given an abelian variety A over k, T is a torsor of A. By the condition (2) of torsors, we can see that after we pass to the separated closure k^{sep}, $T_{k^{sep}}$ is isomorphic to $A_{k^{sep}}$. We choose an isomorphism $\tau : T_{k^{sep}} \to A_{k^{sep}}$. Fix any k^{sep} point t on $T_{k^{sep}}$, then for any $\sigma \in G(= Gal(k^{sep}/k))$, there is a unique element $\sigma(t) - t$ in $A(k^{sep})$ such that $f(t, (\sigma(t) - t)) = \sigma(t)$. Then we have a map $g : G \to A(k^{sep})$. It is straightforward to check this is a cocycle, which is the cohomology class in $H^1(k, A)$ representing this torsor.

Now for any torsor T of A we can associate a cohomology class $[T] \in H^1(k, A)$. So we can define its index and period as above. We use $per(T)$ and $I(T)$ to denote them. In this special case we have a better relation between them.

Theorem 4.1.3. ([9, Corollary 11]) Let A be an abelian variety of dimension g over k, T is a torsor of A, then we have

$$per(T)|I(T)|per(T)^{2g}$$

Before we prove it, we need a lemma.

Lemma 4.1.4. ([9, Proposition 10]) Let M be a finite G module with n elements, and $\eta \in H^1(k, M)$ a cohomology class, then we always have

$$I(\eta)|n$$

Proof. Let $\xi : G \to M$ be the 1 cocycle representing the cohomology class. Define H to be the subset of G consists of elements $\sigma \in G$ with $\xi(\sigma) = 0$. We can check H is a subgroup (not necessarily normal). Then we have an injection of sets

$$\phi : G/H \to M$$

Let l be the fixed field of H by Galois theory, then we can see that l is a splitting field of η. This proves the lemma. □

Now we go back to the proof of the theorem. We have the Kummer sequence (see [32, Example 7.9])

$$1 \to A(l)/nA(l) \to H^1(l, A[n]) \to H^1(l, A)[n] \to 1$$

for any number n and field extension l/k. Pick n here to be the period of T, then the cohomology class of T lies in $H^1(k, A)[n]$. By the exact sequence to split T it suffices to split its lift $\xi \in H^1(k, A[n])$. So we have $I(T)|I(\xi)$. But we have $A[n]$ is a finite module with n^{2g} elements. Then by the previous lemma we have

$$I(T)|I(\xi)|per(T)^{2g}$$

4.2 Picard stacks of curves with genus 1

In this section we will consider elliptic curves. In the previous section we can see if E is an elliptic curve over k, C is a torsor of E (We use C instead of T cause C stands for *curves*), then we always have

$$per(C)|I(C)|per(C)^2$$

We first introduce a new invariant of C. In the rest of the chapter we will assume the characteristic of the base field k is 0. The reason why we don't consider the positive characteristic case is because we need to apply Theorem 2.4.6. In the proof of the theorem if the base field is of positive characteristic, then we don't have the tameness of the DM stack $\mathcal{Y}$.

Definition 4.2.1. Let C be a curve of genus 1. Then its Picard variety $\mathbf{Pic}^0_{C/k}$ is an elliptic curve. We use E to denote it. Then C is a torsor of E ($C \cong \mathbf{Pic}^1_{C/k}$ and the latter has a natural action of E). The Picard stack, the moduli stack of line bundles on C with degree 0, we use $\mathcal{P}ic^0_{C/k}$ to denote it, has a natural morphism

$$\mathcal{P}ic^0_{C/k} \to \mathbf{Pic}^0_{C/k}$$

makes $\mathcal{P}ic^0_{C/k}$ a $\mathbb{G}_m$-gerbe over $\mathbf{Pic}^0_{C/k}$. Write K the function field of E. Restrict to the generic point we have a $\mathbb{G}_m$-gerbe

$$\mathcal{P}ic^0_{C/k}|_K \to \mathrm{Spec}(K)$$

this corresponds to a Brauer class in $Br(K)$. We define $i(C)$ to be the index of this Brauer class.

In some references the authors call this number $i(C)$ the index of the $\mathbb{G}_m$-gerbe $\mathcal{P}ic^0_{C/k}$. We first consider the $\mathbb{G}_m$-gerbe $\mathcal{P}ic^0_{C/k}$. One easy observation is that when C admits a k rational point, then it is a trivial E torsor, and in that case since we have the Poincare bundle on $C \times \mathbf{Pic}^0_{C/k}$, so $\mathcal{P}ic^0_{C/k}$ is a trivial $\mathbb{G}_m$-gerbe. The converse is also true.

Theorem 4.2.2. ([20, Section 10.1.7]) Let E/k be an elliptic curve over some field k with characteristic 0 and C is a torsor of E. Then C is a trivial torsor if and only if $\mathcal{P}ic^0_{C/k}$ is a trivial $\mathbb{G}_m$-gerbe over E.

We summarize the basic facts of these three values in the following lemma.

Lemma 4.2.3. The numbers $per(C),\ i(C),\ I(C)$ have the following relations:

$$per(C)|i(C)$$
$$i(C)|I(C)$$

Proof. The inclusion $Br(E) \to Br(K)$ is injective (see [32, Example 3.2.22]), so we can see that $per(C) = per(\mathcal{P}ic^0_{C/k}|_K)$, hence we always have $per(C)|i(C)$. Also we know that suppose C is a torsor splitting over some finite field extension L with

degree d, then we know C admits a L point, so $\mathcal{P}ic^0_{C_L/L}$ is a trivial gerbe over E_L, hence $K \otimes_k L$ is a splitting field of the Brauer class $\mathcal{P}ic^0_{C/k}|_K$, so $i(C)|L$, which implies $i(C)|I(C)$. □

In Chapter 5 we will consider the relation between the essential dimension of the Picard stack $\mathcal{P}ic^0_{C/k}$ and the index of C. The purpose of this chapter is to consider the period and the index. The question is whether we always have $per(C) = I(C)$? This is true in some cases which we list below:

Theorem 4.2.4. ([29, Theorem 1]) Let E is an elliptic curve over k and C is a torsor of it. If we have $Br(k) = 0$, then we have

$$per(C) = I(C)$$

Theorem 4.2.5. ([29, Theorem 3]) Let E is an elliptic curve over a *p-adic* field, C is a torsor of E, then we have

$$per(C) = I(C)$$

Remark 4.2.6. We can see that this period-index problem can be considered for any abelian varieties. Please see [26] and [9] for more details.

However, this is not true in general. The following example is given by Cassels [7].

Example 4.2.7. Let E be the elliptic curve given by

$$X^2 = Y^2 - T^2$$

$$Z^2 = Y^2 + T^2$$

for any m, n, l, we have a torsor $C_{m,n,l}$ defined by

$$mnX^2 = nlY^2 - T^2$$

$$mlX^2 = nlY^2 + T^2$$

Using the construction we given (from torsors to $H^1(k, E)$) we can see that $per(C_{m,n,l}) = 2$ for any m, n, l. And in [7] it shows that for infinitely many (m, n, l), $I(C_{m,n,l}) = 4$, for example $(m, n, l) = (3, 1, -11)$

We will consider this problem by using $\mathcal{P}ic^0_{C/k}$. First we need some preparations.

4.3 Canonical decomposition of $Br(E)$

We give the following geometric interpretation of the $Br(E)$. The decomposition is well known but the author didn't find references for this theorem, so we give a proof here.

Theorem 4.3.1. Given an elliptic curve E. We have a canonical decomposition

$$\pi : Br(k) \oplus H^1(k, E) \to Br(E)$$

defined as below: For any $\mathcal{G} \in Br(k)$ and torsor C of E

$$\pi(\mathcal{G}, C) = f^*\mathcal{G} + \mathcal{P}ic^0_{C/k}$$

where $f : E \to \mathrm{Spec}(k)$ is the structure morphism.

Proof. This is a direct consequence of the Leray spectral sequence of the morphism $f : E \to \mathrm{Spec}(k)$. We first show that π is an injection. Suppose $\pi(f^*\mathcal{G} + \mathcal{P}ic^0_{C/k}) = 0 \in Br(E)$, then $f^*\mathcal{G} + \mathcal{P}ic^0_{C/k}$ restricts to the identity of E is a trivial gerbe, but the restriction of $\mathcal{P}ic^0_{C/k}$ to the identity is always trivial since we always have the structure sheaf, so $\mathcal{G} = 0 \in Br(k)$. Now $\mathcal{P}ic^0_{C/k}$ is a trivial gerbe over E then by Theorem 4.2.2 we must have C is a trivial torsor. So π is injective.

For surjectivity, we have the exact sequence

$$0 \to Br(k) \to Br(E) \to H^1(k, E) \to 0$$

induced by the Leray spectral sequence, and the Picard stack $\mathcal{P}ic^0_{C/k} \in Br(E)$ maps to $C \in H^1(k, E)$. So for any $\mathcal{X}$ a $\mathbb{G}_m$-gerbe over E, define $C \in H^1(k, E)$ to be the image of $\mathcal{X}$. Then we have $\mathcal{X} - \mathcal{P}ic^0_{C/k}$ maps to 0 under the morphism $Br(E) \to H^1(k, E)$. So $\mathcal{X} - \mathcal{P}ic^0_{C/k} = f^*\mathcal{G}$ for some $\mathcal{G} \in Br(k)$. This proves the surjectivity. □

4.4 2-torsion elements of $Br(E)$

We need to following useful description of the 2-torsion elements in $Br(E)$ for an elliptic curve E given in [8]. For any field L, two elements $a, b \in L^*$, we use the notation $< a, b > \in Br(L)$ to denote the quaternion algebra generated by $1, i, j, ij$ with relations

$$i^2 = a, j^2 = b, ij = -ji$$

We first set up the notations. Let E/k be an elliptic curve over some field k with characteristic 0, and suppose that the 2-torsion points of E are defined over k. We

use σ, τ, ω to denote the three non-trivial 2-torsion points of E, e the identity point of E. We denote $f_{\sigma,\sigma}$ the rational function on E with double zeroes at σ, double poles at e. Moreover, if we denote $\mathcal{O}_{E,e}$ the local ring at the point e, and π an uniformizer of it, then we need $\pi^2 f_{\sigma,\sigma} \in \mathcal{O}_{E,p}/\pi\mathcal{O}_{E,p}$ a square in k^*. We can define $f_{\tau,\tau}, f_{\omega,\omega}$ similarly. In the case when the elliptic curve is given by

$$y^2 = (x-a)(x-b)(x-c)$$

the three non-trivial 2-torsion points are $(a,0),(b,0),(c,0)$, and in this case we can set $f_{\sigma,\sigma} = x-a$, $f_{\tau,\tau} = x-b$, $f_{\omega,\omega} = x-c$.

Theorem 4.4.1. ([8, Theorem 3.6]) With the notations defined as above. All elements in $H^1(k,E)[2] \subseteq Br(E)[2] \subseteq Br(K)[2]$ can be written in the form:

$$< f_{\sigma,\sigma}, r > \otimes < f_{\tau,\tau}, s >$$

Also all biquaternion algebras of this form arise from some torsors. And such a biquaternion algebra is trivial if and only if it is similar to one of the following three types:

(a) $< f_{\sigma,\sigma}, u-b > \otimes < f_{\tau,\tau}, u-a >$ where u is the x coordinate of some points in $E(k)$ with $u \neq a, u \neq b$.

(b) $< f_{\sigma,\sigma}, a-b > \otimes < f_{\tau,\tau}, (a-b)(a-c) >$

(c) $< f_{\sigma,\sigma}, (b-a)(b-c) > \otimes < f_{\tau,\tau}, b-a >$

With these tools, we can begin our discussion.

4.5 A computation of $I(C)$ for 2-torsion elements in $Br(E)$

In this section we will discuss $I(C)$ in details. We will first fix our field to be k of characteristic 0. We assume the elliptic curves we consider admits full 2-torsion points, that is $E[2]$ are all k rational points. So the elliptic curve can be written as:

$$y^2 = x(x-a)(x-b)$$

and K its functional field, e the identity point. We fix the following notations:

$$f_{\sigma,\sigma} = x-a$$

$$f_{\tau,\tau} = x-b$$

The general theory about the case when $I(C) = 2$

By Theorem 4.4.1, elements in $Br(K)$ come from $\mathcal{P}ic^0_{C/k}$ with $per(C) = 2$ if and only if it can be represented as:

$$< f_{\sigma,\sigma}, M > \otimes < f_{\tau,\tau}, N >$$

for some $A, B \in k$. Denote C the torsor corresponding to this Brauer class. We will describe the case when $I(C) = 2$.

We need some computation on elliptic curves. We suppose $I(C) = 2$, and that means C admits a closed points with degree 2, say $C(k(\sqrt{\alpha}))$ is not empty for some α non-square in k. Set $G_\alpha = Gal(k(\sqrt{\alpha})/k)$, and g the only non-trivial element. So $[C] \in H^1(k, E)$ is represented by a 1 cocycle

$$\begin{aligned} \theta : & g \to p_g \\ & 1 \to e \end{aligned}$$

for some point $p_g \in E(k(\sqrt{\alpha}))$. The case when p_g is a 2-torsion point on E is easy to control, so we assume $2p_g \neq e$. Since θ is a cocycle, we must have $p_g + gp_g = e$, so we must have $p_g = (A, \sqrt{A(A-a)(A-b)})$ and $\alpha/A(A-a)(A-b)$ is a square for some $A \in k$. We use m to denote $p_g/2$ (choose either one). By the standard calculation we have $m = (x_m, y_m)$ where

$$x_m = A + \sqrt{(A-a)(A-b)} + \sqrt{A(A-a)} + \sqrt{A(A-b)}$$

$$y_m = (x_m^2 - ab)/2\sqrt{A}$$

So we can see that if we set $L := k(x_m, y_m) = k(\sqrt{A}, \sqrt{A-a}, \sqrt{A-b})$, then we have the following three cases, $[L : k] = 2, 4$ or 8. The first two cases are really similar to the last one, so we only discuss the case when $[L : k] = 8$:

If $[L : k] = 8$. Then we consider the following three elements in $Gal(L/k)$:

$$\begin{aligned} g : & \sqrt{A} \to -\sqrt{A} \\ & \sqrt{A-b} \to \sqrt{A-b} \\ & \sqrt{A-a} \to \sqrt{A-a} \end{aligned}$$

$$\begin{aligned} \beta : & \sqrt{A} \to -\sqrt{A} \\ & \sqrt{A-b} \to -\sqrt{A-b} \\ & \sqrt{A-a} \to \sqrt{A-a} \end{aligned}$$

$$\begin{aligned}\gamma :&\sqrt{A} \to -\sqrt{A}\\ &\sqrt{A-b} \to \sqrt{A-b}\\ &\sqrt{A-a} \to -\sqrt{A-a}\end{aligned}$$

Then g, β, γ are generators of $Gal(L/k)$ and β, γ fix the field $k(\sqrt{\alpha})$. By definition, the following two cocycles are same:

$$\begin{aligned}\eta_1 :&g \to p_g\\ &\beta \to e\\ &\gamma \to e\end{aligned}$$

$$\begin{aligned}\eta_2 :&g \to p_g + gm - m\\ &\beta \to e + \beta m - m\\ &\gamma \to e + \gamma m - m\end{aligned}$$

We can see that η_1 is just θ under the obvious restriction. Also η_2 can be regarded as elements in $H^1(k, E[2])$. Since the action of $Gal(\bar{k}/k)$ on $E[2]$ is trivial, η_1 is just a group homomorphism, and the kernel is generated by $g + \gamma + \beta$. Denote $F = k(\sqrt{A(A-a)}, \sqrt{A(A-b)})$. Define $\mu, \nu \in Gal(F/k)$ where μ sends $\sqrt{A(A-a)}$ to $-\sqrt{A(A-a)}$ and ν sends $\sqrt{A(A-b)}$ to $-\sqrt{A(A-b)}$. We can see that $g+\gamma = \mu$ and $g+\beta = \nu$ in $Gal(k(\sqrt{A(A-a)}, \sqrt{A(A-b)})/k)$. We have $e+(g+\gamma)m-m = \sigma$ and $e + (g + \beta)m - m = \tau$ by direct calculation. So define:

$$\begin{aligned}\eta :&\mu \to \sigma\\ &\nu \to \tau\end{aligned}$$

We can see that η and γ are the same if we restricts to $H^1(Gal(L/k), E)$. So $[C] \in H^1(k, E)$ is also represented by η. That means, the Brauer class

$$< f_{x_\sigma,\sigma}, M > \otimes < f_{\tau,\tau}, N >$$

has index 2 if and only if it is isomorphic to

$$< f_{\sigma,\sigma}, A(A-a) > \otimes < f_{\tau,\tau}, A(A-b) >$$

and the splitting field is $k(\sqrt{A(A-a)(A-b)})$. The cases when $[L:k]=2,4$ are the same. From Mordell-Weil theorem we know that $E(k)/2E(k)$ is a finite set. By the exact sequence

$$E(k)/2E(k) \to H^1(k, E[2]) \to H^1(k, E)[2] \to 0$$

There is a finite set of pairs of integers $P = \{(\beta_1, \gamma_1), ..., (\beta_n, \gamma_n)\}$ with elements in $k^*/(k^*)^2 \times k^*/(k^*)^2$ such that

$$< f_{\sigma,\sigma}, M > \otimes < f_{\tau,\tau}, N > \cong < f_{\sigma,\sigma}, M' > \otimes < f_{\tau,\tau}, N' >$$

if and only if $(MM', NN') \in P$ (Since everything is in $k^*/(k^*)^2 \times k^*/(k^*)^2$ so $M/M' = MM'$). So we have

Theorem 4.5.1. Let E/k be an elliptic curve over k with characteristic 0. Given some element

$$< f_{\sigma,\sigma}, M > \otimes < f_{\tau,\tau}, N >$$

coming from some torsor C of E. Let $P = \{(\beta_1, \gamma_1), ..., (\beta_n, \gamma_n)\}$ be the set of pairs of integers coming from $E(k)/2E(k)$. Then $I(C) = 2$ if and only C is not trivial and for some $A \in k$, we have $(MA(A-a), NA(A-b)) \in P$, or the Brauer class of $\mathcal{P}ic^0_{C/k}|_K$ is isomorphic to $< f_{\sigma,\sigma}, A >$, $< f_{\tau,\tau}, A >$ or $< f_{\omega,\omega}, A >$ for some $A \in k$.

The theorem seems hard to control, but we will see in the next section that in specific cases it is really clear.

A concrete examples for the elliptic curve $y^2 = x(x^2-1)$

In this part we concentrate on the elliptic curve E defined by

$$y^2 = x(x^2-1)$$

over $k = \mathbb{Q}$. The discussion in this part can be easily generalized. It is easy to see that all 2 torsion points are defined over k and they are all k points of E. So by Theorem 4.4.1,

$$< f_{\sigma,\sigma}, M > \otimes < f_{\tau,\tau}, N >$$

is trivial if and only if $(M, N) = (1,1), (1,-1), (2,2), (2,-2)$ in $k^*/(k^*)^2 \times k^*/(k^*)^2$. Suppose we have some torsor C with $\mathcal{P}ic^0_{C/k}|_K$ is represented by

$$< f_{\sigma,\sigma}, M > \otimes < f_{\tau,\tau}, N >$$

Denote $P = \{(1,1),(1,-1),(2,2),(2,-2)\}$. Then by Theorem 4.5.1 we know that $I(C) = 2$ if and only there exists some $A \in k$ such that $(MA(A-1), N(A+1)) \in P$. Let $(MA(A-1), NA(A+1)) = (1,1)$ in $k^*/(k^*)^2 \times k^*/(k^*)^2$. Then we have equations:

$$A(A-1) = Mx^2$$

$$A(A+1) = Ny^2$$

for some $x, y \in k$. Take the sum we have $2A^2 = Mx^2 + Ny^2$. This is the same as $< 2M, 2N >= 1 \in Br(k)$. On the other hand, suppose we have $< 2M, 2N >= 1$, this means there exists some rational numbers $x, y \in k$ such that $Mx^2 + Ny^2 = 2z^2$. Take $r = (Ny^2 - Mx^2)/2$. Define

$$A = \frac{s^2}{r}$$

We can see that A satisfies equations:

$$A(A-1) = Mx^2s^2/r^2$$

$$A(A+1) = Ny^2s^2/r^2$$

so $(A(A-1), A(A+1)) = (M, N)$ in $k^*/(k^*)^2 \times k^*/(k^*)^2$. We can check other three cases similarly. So we have proved:

Theorem 4.5.2. Let $E/\mathbb{Q}$ be the elliptic curve defined by

$$y^2 = x(x^2 - 1)$$

then the Brauer class

$$< f_{\sigma,\sigma}, M > \otimes < f_{\tau,\tau}, N >$$

has index 2 if and only if it is non-trivial and at least one of the following quaternion algebras

$$< M, N >, < M, -N >, < 2M, 2N >, < 2M, -2N >$$

splits.

Remark 4.5.3. The theorem can be generalized to any elliptic curves directly. Set E/k defined by $y^2 = x(x-a)(x-b)$. If we denote $P = \{(\beta_1, \gamma_1), ..., (\beta_n, \gamma_n)\}$ as usual, then we can see that

$$< f_{\sigma,\sigma}, M > \otimes < f_{\tau,\tau}, N >$$

has index at most 2 if and only if one of the following quaternion algebras:

$$< -(a-b)bM\beta_i, (a-b)aN\gamma_i >$$

for $1 \leq i \leq n$ is trivial.

Remark 4.5.4. The integers M, N are not symmetric since for example we have $< f_{\tau,\tau}, -1 >$ is trivial while $< f_{\sigma,\sigma}, -1 >$ is not.

From the theorem we can give infinitely many torsors C of E with $per(C) = 2$ but $I(C) = 4$ concretely. For example, we pick $(M, N) = (-1, 7)$, then we can see in this case the index is 4. This generalizes Cassel's construction [7].

Another example of $per(C) < I(C)$

In this part we give another example.

We set $k = \mathbb{Q}(t_1, t_2, t_3, t_4)$. Here actually $\mathbb{Q}$ can be replaced by any field of char 0. We define an elliptic curve E/k by

$$y^2 = x(x - t_1)(x - t_2)$$

By Theorem 4.4.1, the central simple algebra

$$A =< f_{\sigma,\sigma}, t_3 > \otimes < f_{\tau,\tau}, t_4 >$$

comes from some torsor C. We have $per(C) = 2$. Now we have the following:

Theorem 4.5.5. The central simple algebra A has index 4 in $Br(K)$.

Proof. By [18, Theorem 1.5.5], A has degree 4 if and only if the equation

$$f_{\sigma,\sigma}u^2 + t_3v^2 - t_3f_{\sigma,\sigma}w^2 = f_{\tau,\tau}r^2 + t_4s^2 - t_4f_{\tau,\tau}p^2$$

has no non-trivial solutions. Now we have $f_{\sigma,\sigma} = x$, $f_{\tau,\tau} = x - t_1$, and we know $K \cong k(x)[y]/(y^2 - x(x - t_1)(x - t_2))$, so every element in K can be written in the form $fy + g$ where f, g are rational functions of x. Then we write every element in the equation in the explicit form, the equation is the same as the following two equations:

$$xu_1u_2 + t_3v_1v_2 - t_3xw_1w_2 = (x - t_1)r_1r_2 + t_4s_1s_2 - t_4(x - t_1)p_1p_2$$

$$\begin{aligned} x(u_1^2x(x-t_1)(x-t_2)+u_2^2)+t_3(v_1^2x(x-t_1)(x-t_2)+v_2^2)-t_3x(w_1^2x(x-t_1)(x-t_2)+w_2^2) \\ = (x - t_1)(r_1^2x(x - t_1)(x - t_2) + r_2^2) + t_4(s_1^2x(x - t_1)(x - t_2) + s_2^2) \\ -t_4(x - t_1)(p_1^2x(x - t_1)(x - t_2) + p_2^2) \end{aligned}$$

We may assume that all things appear in the equation are polynomials of x. We will use infinite descend to get a contradiction. For simplicity, we will use the same

notations when we consider things modulo some element. In the following proof, we will concentrate on the second equation, cause the first one will be satisfied automatically. Suppose we have a non-trivial solution, we may assume that the sum of their degrees (as polynomials in $k[x]$) is minimal.

Let $x = 0$, we have

$$t_3 v_2^2 = -t_1 r_2^2 + t_4 s_2^2 + t_4 t_1 p_2^2$$

Here v_2, r_2, s_2, p_2 means their values at $x = 0$, same for the following discussion. We show that this equation has only trivial solution, in other words, we must have

$$x | v_2, r_2, s_2, p_2$$

in the original equation.

Assume this is not true. Since v_2, r_2, s_2, p_2 are rational functions in t_1, t_2, t_3, t_4, we can regarded them as polynomials in t_4 and coefficients in $\mathbb{Q}(t_1, t_2, t_3)$. We may also assume not all of them are divided by t_4. If $t_4 \nmid v_2$ *or* r_2, then set $t_4 = 0$ we will see that $-t_1 t_3$ will be a square in $\mathbb{Q}(t_1, t_2, t_3)$, which is not true. So $t_4 | v_2, r_2$. Write $v_2 = t_4 v_2', r_2 = t_4 r_2'$, we have

$$t_3 t_4 v_2'^2 = -t_1 t_4 r_2'^2 + s_2^2 + t_1 p_2^2$$

By our assumption one of s_2, p_2 cannot be divided by t_4, this implies t_1 is a square in $\mathbb{Q}(t_1, t_2, t_3)$, which cannot happen. So we have $x | v_2, r_2, s_2, p_2$ in the original equation.

Write $v_2 = x v_2', r_2 = x r_2', s_2 = x s_2' p_2 = x p_2'$. We have

$$\begin{aligned}(u_1^2 x(x-t_1)(x-t_2) + u_2^2) + t_3(v_1^2(x-t_1)(x-t_2) + x v_2'^2) - t_3(w_1^2 x(x-t_1)(x-t_2) + w_2^2)\\ = (x-t_1)(r_1^2(x-t_1)(x-t_2) + x r_2'^2) + t_4(s_1^2(x-t_1)(x-t_2) + x s_2'^2)\\ -t_4(x-t_1)(p_1^2(x-t_1)(x-t_2) + x p_2'^2)\end{aligned}$$

We let $x = 0$, then we have

$$u_2^2 + t_3 t_1 t_2 v_1^2 - t_3 w_2^2 = -t_1^2 t_2 r_1^2 + t_1 t_2 t_4 s_1^2 + t_1^2 t_2 t_4 p_1^2$$

Same as before we will show that this equation will only have trivial solution, which means

$$x | u_2, v_1, w_2, r_1, s_1, p_1$$

in the original one. We can consider $u_2, v_1, w_2, r_1, s_1, p_1$ are polynomials in t_4 with coefficients in $\mathbb{Q}(t_1, t_2, t_3)$, and not all of them are divided by t_4. If one of u_2, v_1, w_2, r_1 is not divided by t_4, by letting $t_4 = 0$, we have

$$u_2^2 + t_1 t_2 t_3 v_1^2 - t_3 w_2^2 = -t_1^2 t_2 r_1^2$$

where $u_2, v_1, w_2, r_1 \in \mathbb{Q}(t_1, t_2, t_3)$ and not all of them are zeroes. Then we may consider them as polynomials in t_3 and coefficients in $\mathbb{Q}(t_1, t_2)$. Similar as before we may assume not all of are divided by t_3. If t_3 doesn't divide one of u_2, r_1, modulo t_3 will lead to $-t_2$ is a square in $\mathbb{Q}(t_1, t_2)$, which is a contradiction. So $t_3|u_2, r_1$. Divide t_3 and since t_3 doesn't divide one of v_1, w_2, this leads to $t_1 t_2$ a square in $\mathbb{Q}(t_1, t_2)$, which is a contradiction. So we must have

$$t_4|u_2, v_1, w_2, r_1$$

Divide t_4 since $t_4 \nmid s_1$ or $t_4 \nmid p_1$, this implies t_1 is a square in $\mathbb{Q}(t_1, t_2, t_3)$, which is a contradiction. So we must have

$$x|u_2, v_1, w_2, r_1, s_1, p_1$$

Write $u_2 = xu_2', v_1 = xv_1', w_2 = xw_2', r_1 = xr_1', s_1 = xs_1', p_1 = xp_1'$, we have

$$(u_1^2(x-t_1)(x-t_2)+xu_2'^2)+t_3(v_1'^2x(x-t_1)(x-t_2)+v_2'^2)-t_3(w_1^2(x-t_1)(x-t_2)+xw_2'^2)$$

$$= (x-t_1)(r_1'^2x(x-t_1)(x-t_2)+r_2'^2)+t_4(s_1'^2x(x-t_1)(x-t_2)+s_2'^2)$$
$$-t_4(x-t_1)(p_1'^2x(x-t_1)(x-t_2)+p_2'^2)$$

The following argument is really the same. We can conclude that $x|u_1, w_1$. Write $u_1 = xu_1', w_1 = xw_1'$, then

$$u_1', u_2', v_1', v_2', w_1', w_2', r_1', r_2', s_1', s_2', p_1', p_2'$$

form a new solution of the original equation with smaller degree in x, which is a contradiction. So we can see that

$$A =< f_{\sigma,\sigma}, t_3 > \otimes < f_{\tau,\tau}, t_4 >$$

is a division algebra, hence $i(C) = 4$. □

Chapter 5

The relation between two indices and the essential dimension of $\mathcal{P}ic^0_{C/k}$

In this chapter we will concentrate on the relation between the two indices and the essential dimension of Picard stacks. Through this chapter the base field will be of characteristic 0.

We first show that

Theorem 5.0.1. Let C be an algebraic curve of genus 1. We always have

$$i(C) = I(C)$$

Then we have the result about the essential dimension of $\mathcal{P}ic^0_{C/k}$. By Theorem 2.4.6 we have:

Lemma 5.0.2. Let C be a curve of genus 1 over k, let K be the function field of $\mathbf{Pic}^0_{C/k}$, then we have

$$ed_k\mathcal{P}ic^0_{C/k} = 1 + ed_K\mathcal{P}ic^0_{C/k}|_K$$

The restriction $\mathcal{P}ic^0_{C/k}|_K$ is a $\mathbb{G}_m$ gerbe over $\mathrm{Spec}(K)$. From Conjecture 1.1.1 we can see that its essential dimension is closed related to its index, so it reasonable to consider $i(C)$. Our purpose in this chapter is to prove $i(C) = I(C)$, so we can see that the essential dimension problem and the period-index problem are closed related. However, we have an easy corollary.

Corollary 5.0.3. We have

$$ed_k\mathcal{P}ic^0_{C/k} = 1$$

if and only if C is a trivial torsor.

Proof. This is a direct consequence of Lemma 5.0.2 and Lemma 2.4.7 □

We need some preparations.

5.1 Fourier-Mukai transforms

We need the basic properties of Fourier-Mukai transforms in this part, so we give a brief introduction. We refer to [22] for details. Let X, Y be two projective smooth varieties over k, $D^b(X), D^b(Y)$ the derived category of coherent sheaves on X, Y.

Definition 5.1.1. ([36, Chapter 1]) Let X, Y be two smooth projective varieties over k. $P \in D^b(X \times Y)$ an object in the derived category of coherent sheaves on $X \times Y$. Denote $p : X \times Y \to X$ and $q : X \times Y \to Y$ the two projections. The *Fourier-Mukai transform* with *kernel* P is defined as follows:

$$\begin{aligned}\Phi_P :& D^b(X) \to D^b(Y)\\ & F \to Rq_*(p^*F \otimes P)\end{aligned}$$

We can see that the Fourier-Mukai transform gives a morphism of derived categories. The following theorem gives an answer to the other direction:

Theorem 5.1.2. ([36, Theorem 3.2.1]) Let X, Y be two smooth projective varieties over k. Let $F : D^b(X) \to D^b(Y)$ a triangulated equivalence between them. Then F is isomorphic to a Fourier-Mukai transform Φ_P for some kernel $P \in D^b(X \times Y)$, and P is unique up to isomorphism.

This theorem is really powerful. It gives us a concrete way to describe the equivalences between derived categories of smooth projective varieties. Orlov's result is more general where he doesn't require F to be an equivalence but with other weaker conditions. See [36, Theorem 3.2.1] for more details.

Remark 5.1.3. The projectivity of X, Y is essential here. If we want to consider proper smooth varieties, then we need to use differential graded categories, see [43] for details.

We concentrate on the Fourier-Mukai transform between abelian varieties.

Theorem 5.1.4. ([33], [22, Theorem 9.19]) Let A be an abelian variety over k of dimension g and $\widehat{A}$ its dual abelian variety. Let P be the Poincare line bundle on $A \times \widehat{A}$. Then the Fourier-Mukai transform with kernel $P \in D^b(X \times Y)$

$$\Phi_P : D^b(\widehat{A}) \to D^b(A)$$

is an equivalence. Moreover, the composition

$$D^b(\widehat{A}) \xrightarrow{\Phi_P} D^b(A) \xrightarrow{\Phi_P} D^b(\widehat{A})$$

is isomorphic to $\hat{\iota}^*[-g]$, here $\hat{\iota} : \widehat{A} \to \widehat{A}$ is the inverse of the dual abelian variety.

With this we can prove the following lemma. The author didn't find the references but this lemma is well known to experts. We give a proof here, there are also some discussions in Bhatt's note [2, Lemma 18.1].

Lemma 5.1.5. Let A be an abelian variety over an algebraically closed field k of dimension g, $\widehat{A}$ its dual abelian variety. Choose $x \in \widehat{A}(k)$ a point and $M_x \in \mathbf{Pic}^0(A)$ the corresponding line bundle. If $F \in D^b(A)$, there is a canonical isomophism

$$R\Gamma(A, F \otimes M_x) \cong \Phi_P(F)|_x$$

Similarly, for some $G \in D^b(\widehat{A})$, there is a canonical isomorphism

$$R\Gamma(\widehat{A}, \Phi_P(G) \otimes M_x) \cong G[-g]|_x$$

Proof. By taking $G = \Phi_P(F)$ then with the above theorem we can see that the second statement is the same as the first one. We have the fiber diagram

$$\begin{array}{ccc} A \times x & \xrightarrow{\iota} & A \times \widehat{A} \\ \downarrow{\scriptstyle p'} & & \downarrow{\scriptstyle p} \\ x & \xrightarrow{\iota'} & \widehat{A} \end{array}$$

Then by the flat base change theorem, we have

$$\Phi_P(F)|_x \cong \iota'^* R p_*(q^* F \otimes P) \cong R p'_*(\iota^*(q^* F \otimes P)) \cong R\Gamma(A, F \otimes M_x)$$

□

Remark 5.1.6. Take x to be the identity in the second statement we have

$$R\Gamma(A, \Phi_P(G)) \cong G[-g]_e$$

which we have

$$\chi(\Phi_P(G)) = (-1)^g rk(G)$$

Here χ is the Euler characteristic and $rk(G)$ is the rank of G.

5.2 The relation between $I(C)$ and $i(C)$

From Theorem 5.0.2 we have the following theorem if the Conjecture 1.1.1 holds

Theorem 5.2.1. Assume Conjecture 1.1.1 holds. Let C/k be a curve over k with genus 1. Write

$$i(C) = p_1^{r_1} p_2^{r_2} ... p_s^{r_s}$$

the prime decomposition. Then we have

$$ed_k \mathcal{P}ic^0_{C/k} = p_1^{r_1} + ... + p_s^{r_s} - s + 1$$

Since the Conjecture 1.1.1 has been proved in the case when $s = 1$, so the previous theorem is always true in this case.

Usually the value $i(C)$ is not so easy to control but $I(C)$ is easy to estimate in particular when the curve is given by some functions. So it's reasonable to consider the relation between them. Actually we have:

Theorem 5.2.2. Let C be a curve of genus 1 over a field k of characteristic 0. Then we always have

$$i(C) = I(C)$$

Proof. We have seen that $i(C) \leq I(C)$, so we just need to show the other direction. Recall we use E to denote the Picard variety $\mathbf{Pic}^0_{C/k}$ and K its function field. Since $\mathcal{P}ic^0_{C/k}|_K \in Br(K)$ has index $i(C)$, so there is a finite field extension L/K of degree $i(C)$ such that $\mathcal{P}ic^0_{C/k}|_L \in Br(L)$ is trivial. Then there is a projective smooth curve D with a commutative diagram

$$\begin{array}{ccc} \mathrm{Spec}(L) & \longrightarrow & \mathrm{Spec}(K) \\ \downarrow & & \downarrow \\ D & \longrightarrow & E \end{array}$$

See [21, Chapter 1, Corollary 6.12] for details. We use $\pi : D \to C$ to denote the morphism, and we can see that this is finite flat. Since the image of $\mathcal{P}ic^0_{C/k} \in Br(E)$ is 0 under the composition of morphisms

$$Br(E) \to Br(D) \to Br(L)$$

and the morphism $Br(D) \to Br(L)$ is injective, so we can see the fiber product

$$\mathcal{P}ic^0_{C/k} \times_E D \to D$$

is a trivial $\mathbb{G}_m$-gerbe. This implies $\mathcal{P}ic^0_{C/k}(D)$ is non-empty. From the definition of Picard stacks, there is a universal line bundle V on $D \times C$. Let $p : D \times C \to C$ be the projection, we claim that

$$deg(Rp_*V) = -i(C)$$

To prove it, since the degree doesn't change under the field extension, so we may assume k is algebraic closed. Then C is isomorphic to E. Denote $q : D \times C \to D$ the first projection and P the Poincare line bundle on $C \times E$. We have that

$$V \cong q^*M \otimes (\pi \times 1)^*P$$

for some line bundle on D. Write $p' : E \times C \to C$ and $q' : E \times C \to E$ the two projections. Now by the flat base change and projection formula we have

$$\begin{aligned} Rp_*V &\cong Rp_*(q^*M \otimes (\pi \times 1)^*P) \\ &\cong Rp'_*R(\pi \times 1)_*(q^*M \otimes (\pi \times 1)^*P) \\ &\cong Rp'_*(R(\pi \times 1)_*q^*M \otimes P) \\ &\cong Rp'_*(q'^*\pi_*M \otimes P) \\ &\cong \Phi_P(\pi_*M) \end{aligned}$$

where the third equality is given by the projection formula and the fourth is given by the flat base change. Since $\pi : D \to E$ is flat and finite of degree $i(C)$, we have $rk(\pi_*M) = i(C)$. Then by Lemma 5.1.5, we have

$$\chi(Rp_*V) = \chi(\Phi_P(M)) = rk(\pi_*M) = -i(C)$$

hence we have

$$deg(Rp_*V) = \chi(Rp_*V) = -i(C)$$

by the Riemann-Roch theorem.

However for curves of genus 1 we have

$$deg(det(Rp_*V)^{-1}) = -deg(Rp_*V) = i(C)$$

So we get a line bundle of degree $i(C)$ on the curve C. Then by the definition of $I(C)$ we get $I(C)|i(C)$, which proves the other direction. We finish the proof. □

With this theorem and curves given by equations we can estimate the essential dimension of its Picard stack easily.

Remark 5.2.3. By a really similar idea we can see for any torsor T of an abelian varietiy of dimension g we always have

$$I(T)|i(T)g!$$

The question whether $I(T) = i(T)g!$ seems unknown.

Part III

The Tate conjecture and finiteness of abelian varieties over finite fields

Chapter 6

Tate conjecture and finiteness of abelian varieties over finite fields

6.1 Introduction

Through the chapter, k is a finite field of characteristic p and $\bar{k}$ means the algebraic closure of k.

In this chapter we will prove the following theorem.

Theorem 6.1.1. The Tate conjecture of abelian varieties over k implies that there are only finitely many abelian varieties of dimension g over k.

This result is first proved by Zarhin in [46, Theorem 4.1]. We will give a different approach to this result.

Notations: We will use k to represent a finite field of characteristic p, $\bar{k}$ its algebraic closure, $G = Gal(\bar{k}/k)$ the absolute Galois group. σ is the Frobenius element. For a projective variety X over k, we use π_X to denote the Frobenius morphism of X.

6.2 Some basic facts about abelian varieties

In this section we recall the Tate module of an abelian variety and the p-divisible group.

Let A be an abelian variety over k with $\dim A = g$. Choose l a prime number with $l \neq p$. We know that if $(p, n) = 1$, the morphism $n : A \to A$ is a separable isogeny of degree n^{2g}, denote $A[n] = Ker(n : A \to A)$, then $A[n](\bar{k}) \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$.

The Tate module is defined as

$$T_l(A) = \varprojlim_n A[l^n](\bar{k})$$

We know $T_l(A) \cong \mathbb{Z}_l^{2g}$ non-canonically. The Galois group G acts on $T_l(A)$ in a natural way. This action is continuous, since the Frobenius is a topological generator of G, so the action of σ determines the action of G. The Frobenius morphism $\pi_A : A \to A$ is a morphism in $\mathrm{Hom}_{AV}(A, A)$, and the image of π_A under the natural morphism

$$\mathrm{Hom}_{AV}(A, A) \otimes \mathbb{Z}_l \to \mathrm{Hom}_{\mathbb{Z}_l[G]}(T_l(A), T_l(A))$$

is σ.

In [42, Section 1], Tate proved the following famous theorem

Theorem 6.2.1 (Tate)**.** Let $k = \mathbb{F}_q$ be a finite field where q is a power of a prime p. Let A, B be two abelian varieties over k. Let $G = Gal(\bar{k}/k)$ be the absolute Galois group of k. If l is a prime and $l \neq p$, then we have the isomorphism

$$\mathrm{Hom}_{AV}(A, B) \otimes \mathbb{Z}_l \cong \mathrm{Hom}_{\mathbb{Z}_l[G]}(T_l(A), T_l(B))$$

Here T_l is the Tate module of an abelian variety.

For π_A, we define a function $P_{\pi_A}(n) = deg(n - \pi_A)$, then P_{π_A} is a polynomial of degree $2g$ with $\mathbb{Z}$ coefficients. It is the same as the characteristic polynomial of σ on $V_l(A) = T_l(A) \otimes \mathbb{Q}_l$. In particular the characteristic polynomial of σ on $V_l(A)$ is independent of l. We will use several properties of the characteristic polynomials, we refer to [17, Chapter 16] for details.

In the case if $l = p$, since now $p : A \to A$ is not separate, things are a little different. We use the p-divisible group in this case. It is defined as

$$A[p^\infty] = \varinjlim_n A[p^n]$$

To introduce the Tate p-conjecture, we need to use the definitions and properties of Dieudonne ring and Dieudonne modules, for details, see [45, Chapter 1] and [37, Section 23].

Let D_k be the Dieudonne ring of k, it is a non-commutative associative $W(k)-$algebra ($W(k)$ is the ring of Witt vectors) with two generators F, V satisfying the following conditions:

$$FV = VF = p$$

$$F(c) = \phi(c)F$$

$$cV = V\phi(c)$$

for any $c \in W(k)$. Here ϕ is the automorphism of $W(k)$ induced by the automorphism $x \to x^p$ on k. So if $k = \mathbb{F}_p$, then D_k is commutative.

By the standard procedure (see [37, Section 23]) we can associate $A[p^\infty]$ with a D_k module $M(A)$. It is a free $W(k)$ module of rank $2g$. Its D_k action is uniquely determined by the action of F (or V), then Tate proved

Theorem 6.2.2 (Tate)**.** For two abelian varieties A, B over k, with the above notations, we have a natural isomorphism

$$\mathrm{Hom}_{AV}(A, B) \otimes \mathbb{Z}_p \cong \mathrm{Hom}_{D_k}(M(B), M(A))$$

This theorem can be found in [45, Page 4]. In particular, we have

$$\mathrm{Hom}_{AV}(A, A) \cong \mathrm{Hom}_{D_k}(M(A), M(A))$$

In this case, if we denote σ_A is image of π_A (The Frobenius morphism of A) under this isomorphism, then $\sigma_A = F^m$ if $k = \mathbb{F}_{p^m}$. And the character polynomial of σ_A is just P_{π_A}.

6.3 The finiteness of isogeny classes

In this section we will prove that there are finitely many isogeny classes of abelian varieties over k of dimension g. We first recall the isogeny theorem.

Theorem 6.3.1. ([42, Section 3, Theorem 1]) Given two abelian varieties A, B over k, then

$$\begin{aligned} &A \text{ and } B \text{ are isogenous} \\ \iff\ & P_{\pi_A} = P_{\pi_B} \\ \iff\ & T_l(A) \otimes \mathbb{Q}_l \cong T_l(B) \otimes \mathbb{Q}_l \text{ as } \mathbb{Q}_l[G] \text{ modules} \end{aligned}$$

So to consider the isogeny classes we just need to consider the characteristic polynomials of the Frobenius. But we have the following big theorem.

Theorem 6.3.2. (Weil Conjecture, see [12, Theorem 1.6]) Let A be an abelian variety over k with dimension g, then P_{π_A} is a monic polynomial with coefficients in $\mathbb{Z}$ with degree $2g$, and if α is a root of P_{π_A}, then for any Galois embedding $\eta : \bar{\mathbb{Q}} \to \bar{\mathbb{Q}}$ over $\mathbb{Q}$, we have $|\eta(\alpha)| = \sqrt{q}$, here q is the number of elements in k.

With these two theorems, we can state

Corollary 6.3.3. There are only finitely many isogeny classes of abelian varieties over k of dimension g.

Proof. By Theorem 6.3.1, it suffices to prove there are only finitely many characteristic polynomials. Suppose $k = \mathbb{F}_q$. If

$$P(x) = \Sigma_{i=0}^{2g} a_i x^{2g-i}$$

is the characteristic polynomial of some abelian variety, and $\alpha_1, \alpha_2, ..., \alpha_{2g}$ are roots of $P(x)$, then by Theorem 6.3.2, $|\alpha_i| \leq \sqrt{q}$, so we have

$$\begin{aligned} |a_s| &= |\Sigma_{1 \leq i_1 < i_2 < ... < i_s \leq 2g} \alpha_{i_1} ... \alpha_{i_s}| \\ &\leq \Sigma_{1 \leq i_1 < i_2 < ... < i_s \leq 2g} |\alpha_{i_1} ... \alpha_{i_s}| \\ &\leq \Sigma_{1 \leq i_1 < i_2 < ... < i_s \leq 2g} \sqrt{q}^s \\ &\leq M \sqrt{q}^s \end{aligned}$$

for some M. So we know all a_i are bounded by some number which only depends on the field k and the dimension g. But we know all a_i are integers, so we only have finitely many choices, so there are only finitely many polynomials can be the characteristic polynomial of some abelian varieties. So there are only finitely many isogeny classes. □

So to prove there are finitely many isomorphism classes it suffices to show that every isogeny class of abelian varieties only contains finitely many isomorphism classes.

6.4 Some calculus of the Tate module

In this section we fix an abelian variety A over k of dimension g. π_A will denote the Frobenius morphism of A, P_{π_A} is its characteristic polynomial. Let $\mathcal{C}$ be the isogeny class containing A. We will also use π_A to denote the element in $\mathrm{Hom}_{\mathbb{Z}_l[G]}(T_l(A), T_l(A))$ under the Tate's isomorphism, which can be regarded as a $2g \times 2g$ matrix with element in $\mathbb{Z}_l$.

The main proposition of this section is:

Proposition 6.4.1. With the above data, there exists a positive integer N which only depends on A (we will see from the proof N only depends on $\mathcal{C}$), such that for any $B \in \mathcal{C}$ and $l > N$, $T_l(B) \cong T_l(A)$ as $\mathbb{Z}_l[G]$ modules, and for $l < N$, the set $\{T_l(B) | B \in \mathcal{C}\}$ (consider as $\mathbb{Z}_l[G]$ modules) is a finite set (we include the case $l = char\ k$, in which case we consider Dieudonne modules as in Section 6.2).

Before the proof, we first notice that we must have $T_l(A) \otimes \mathbb{Q}_l \cong T_l(B) \otimes \mathbb{Q}_l$ as $\mathbb{Q}_l[G]$ modules. As we discussed, the G action on the Tate module is uniquely determined by the action of the Frobenius. So we can see $T_l(A) \cong T_l(B)$ as $\mathbb{Z}_l[G]$ modules if and only if π_A and π_B are conjugate by some matrix in $GL_{2g}(\mathbb{Z}_l)$ (not $GL_{2g}(\mathbb{Q}_l)$, they already conjugate by some matrix in $GL_{2g}(\mathbb{Q}_l)$ by Tate's isogeny theorem).

We separated the proof into two parts, consists of the following two lemmas. They are all purely linear algebra things.

Lemma 6.4.2. There exists a positive N such that for any abelian variety B which is isogenous to A, and $l > N$, we can find basis of $T_l(B)$ and $T_l(A)$ such that the matrices of π_A and π_B will be the same.

Proof. We know A is isogenous to $A_1^{b_1} \times A_2^{b_2} \times ... \times A_s^{b_s}$ where all A_i are simple, non-isogenous with each other. We know for a simple abelian variety A_i, the characteristic polynomial $P_{\pi_{A_i}}$ of the Frobenius is a power of an irreducible polynomial, so $P_{\pi_{A_i^{b_i}}}$ is also a power of an irreducible polynomial. The characteristic polynomials $P_{\pi_{A_i^{b_i}}}$ should be coprime with each other, let $K_i = \Pi_{j \neq i} P_{\pi_{A_j^{b_j}}}$. Then by Bezout's theorem, there exists $g_i \in \mathbb{Q}[x]$ such that

$$\Sigma_{i=1}^{s} g_i(x) K_i(x) = 1$$

Then choose N_0 be a positive number such that if $l > N_0$, then all $g_i(x) \in \mathbb{Z}_l[x]$ (i.e. l doesn't divide any denominators in g_i). And denote $M_i = K_i(\pi) T_l(A)$. Then since all $g_i \in \mathbb{Z}_l[x]$, so if $l > N_0$, $T_l(A) = \oplus M_i$. And this N_0 only depends on the chosen isogeny class $\mathcal{C}$. On each M_i, the characteristic polynomial of π_A is $P_{\pi_{A_i^{b_i}}}$, which is a power of an irreducible polynomial. Then we will concentrate on one M_1, i.e. we just assume $M_1 = T_l(A)$, and we can see the similar procedure can be applied to all $2 \leq i \leq s$ and prove the lemma in the general case.

We know π_A is an invertible matrix with coefficients in $\mathbb{Z}_l$. Let $\{\alpha_1, ..., \alpha_t\}$ be the roots of P_{π_A}, then we have $P_{\pi_A} = ((x - \alpha_1)...(x - \alpha_t))^e$ for some e and $Q(x) = \Pi_{i=1}^{t}(x - \alpha_i) \in \mathbb{Z}[x]$ is irreducible. Then we define

$$P_i(x) = \Pi_{j \neq i}(x - \alpha_j)$$

for $1 \leq i \leq k$. Since they don't have common factors, so we may choose $h_i(x) \in \bar{\mathbb{Q}}[x]$ such that

$$\Sigma h_i P_i = 1$$

Choose N_1 such that if $l > N_1$, then we have $h_i \in \bar{\mathbb{Z}}_l[x]$. Then we can see for any $v \in T_l(A)$, $v = \Sigma h_i(\pi_A)P_i(\pi_A)v$. Also it is easy to check

$$L_i = P_i(\pi_A)T_l(A)$$

lies in α_i-eigenspace (consider this over $\bar{\mathbb{Z}}_l$). Let $\bar{L_i}$ be the $\bar{\mathbb{Z}}_l$ linear expansion of L_i in $T_l(A) \otimes \bar{\mathbb{Z}}_l$. Since every eigenspace of different eigenvalues are linearly independent, so we have

$$T_l(A) \otimes \bar{\mathbb{Z}}_l = \oplus \bar{L_i}$$

Define $D = \Pi_{i \neq j}(\alpha_i - \alpha_j)^2$, then $D \in \mathbb{Z}$. We pick $u_1, ..., u_e$ to be an integral basis of $\bar{L_1}$ over $\bar{\mathbb{Z}}_l$, such that $u_1, ..., u_e$ can be represented by $u_i = P_1(\pi_A)(w_i)$ for $w_1, ..., w_e$ in $T_l(A)$ (This is true by linear algebra and the definition of $\bar{L_1}$). Define $v_i = \Sigma P_j(\pi_A)(w_i)$. Then we have $v_i \in T_l(A)$. We prove if $l > max(N_0, N_1, |D|)$, then

$$\{v_1, \pi_A(v_1), ..., \pi_A^{t-1}(v_1), v_2, ..., \pi_A^{t-1}(v_2), ..., v_e, ..., \pi_A^{t-1}(v_e)\}$$

is an integral basis of $T_l(A)$. Since $v = \Sigma h_i(\pi_A)P_i(\pi_A)v$, so it suffices to show $P_i(\pi_A)(v)$ can be represented over $\bar{\mathbb{Z}}_l$ by these elements. From the Galois theory $P_i(x) = \phi(P_1(x))$ for some $\phi \in Gal(\bar{\mathbb{Q}}_l/\mathbb{Q}_l)$. By definition of w_i,

$$P_1(\pi_A)(v) = \Sigma \beta_j P_1(\pi_A)(w_j)$$

for some $\beta_j \in \bar{\mathbb{Z}}_l$, so we have

$$P_i(\pi_A)(v) = \Sigma \phi(\beta_j) P_i(\pi_A)(w_j)$$

Then we just need to show $P_i(\pi_A)(w_j)$ can be represented over $\bar{\mathbb{Z}}_l$ by these elements. This is solved by considering the system linear equations:

$$v_1 = \Sigma P_i(\pi_A)(w_1)$$

$$\pi_A(v_1) = \Sigma \alpha_i P_i(\pi_A)(w_1)$$

$$....$$

$$\pi_A^{t-1}(v_1) = \Sigma \alpha_i^{t-1} P_i(\pi_A)(w_1)$$

Then the matrix of this system of linear equations has determinant D, so by definition of l and the Crammer's rule, $P_i(\pi_A)(w_j)$ can be represented over $\bar{\mathbb{Z}}_l$ by these elements. So

$$\{v_1, \pi_A(v_1), ..., \pi_A^{t-1}(v_1), v_2, ..., \pi_A^{t-1}(v_2), ..., v_e, ..., \pi_A^{t-1}(v_e)\}$$

is an integral basis of $T_l(A)$ (Here we only proved every element can be represented integrally by these elements. But we have te elements here and $te = 2g = \dim T_l(A) \otimes \mathbb{Q}_l$, so they must form a basis). And the matrix of π_A under this basis is uniquely determined by P_{π_A}, just denote this matrix by C. So if we set $N = max(N_0, N_1, |D|)$, then for $l > N$, we can choose a basis as above such that the Frobenius acts on $T_l(A)$ is represented by the matrix C. But this is independent of A, so we can do the same thing for B, so the matrices of π_A and π_B are the same. For the general case, we can find N_i for each M_i, they are all only depend on P_{π_A}, so just choose $N = max(N_0, N_1, ..., N_s)$, then from the above procedure, we can choose basis such that π_A and π_B have the same matrix when $l > N$. We proved the lemma.

□

Lemma 6.4.3. With N defined as above, for $l < N$, the set $\{T_l(B) | B \in \mathcal{C}\}$ (consider as $\mathbb{Z}_l[G]$ modules) is a finite set (we include the case $l = char\ k$, in which case we consider Dieudonne modules as in section 2).

Proof. We use the same idea and notations as in Lemma 6.4.2. We collect them here.
Let $P_{\pi_A} = \Pi_{i=1}^s P_{\pi_{A_i^{b_i}}}$ where $P_{\pi_{A_i^{b_i}}}$ is a power of an irreducible polynomial. Set $K_i = \Pi_{j \neq i} P_{\pi_{A_j^{b_j}}}$ for $1 \leq i \leq s$, then these $K_i(x)$ don't have common factors. So we have $g_i(x) \in \mathbb{Q}[x]$ such that

$$\Sigma_{i=1}^s g_i(x) K_i(x) = 1$$

Fix some $l < N$. Define $M_i = K_i(\pi_A) T_l(A)$. If we set s_1 to be the smallest integer such that $l^{s_1} g_i(x) \in \mathbb{Z}_l[x]$, then we have

$$l^{s_1} T_l(A) \subseteq \oplus M_i \subseteq T_l(A)$$

Notice that this s_1 only depends on P_{π_A} and l. Then π_A acts on M_i, and its characteristic polynomial is just $P_{\pi_{A_i^{b_i}}}$. Write $P_{\pi_{A_i^{b_i}}} = (\Pi_{j=1}^{r_i}(x - \alpha_{ij}))^{e_i}$. Define

$$P_{ij} = \Pi_{n \neq j}(x - \alpha_{in})$$

for $1 \leq i \leq s$ and $1 \leq j \leq r_i$. Then by Bezout's theorem, we may find $h_{ij} \in \bar{\mathbb{Q}}[x]$ such that

$$\Sigma_{j=1}^{r_i} h_{ij} P_{ij} = 1$$

Define

$$L_{ij} = P_{ij}(\pi_A) M_i$$

and $\bar{L_{ij}}$ be the $\bar{\mathbb{Z}}_l$ expansion of L_{ij} in $T_l(A) \otimes \bar{\mathbb{Z}}_l$. Then $\bar{L_{ij}}$ is a free module of rank e_i. Choose $\{w_{i1}, ..., w_{ie_i}\}$ such that $P_{i1}(\pi_A)(w_{ij})$ $1 \leq j \leq e_i$ is an integral basis of L_{i1}. Define

$$v_{ij} = \Sigma_{n=1}^{r_i} P_{in}(\pi_A)(w_{ij}),\ 1 \leq i \leq s,\ 1 \leq j \leq e_1$$

Define N_i to be the submodule of M_1 generated by

$$\{v_{i1}, \pi_A(v_{i1}), ..., \pi_A^{r_i-1}(v_{i1}), ..., v_{ie_i}, ..., \pi_A^{r_i-1}(v_{ie_i})\}$$

Let $D = (\Pi_{i=1}^t \Pi_{1 \leq j,k \leq r_i}(\alpha_{ij} - \alpha_{ik}))^{2(e_1+e_2+...+e_s)}$, and choose s_2 to be the smallest number such that

$$l_{s_2} h_{ij} \in \mathbb{Z}_l[x], \frac{l^s}{D} \in \mathbb{Z}$$

Then similar to the proof in Lemma 6.4.2 we can see

$$l^{s_2}(\oplus M_i) \subseteq \oplus N_i \subseteq \oplus M_i$$

Then we have

$$\oplus N_i \subseteq T_l(A) \subseteq l^{-s_1-s_2} \oplus N_i$$

Note that the matrix of π_A on $\oplus N_i$ is only determined by P_{π_A} in the chosen basis. Also the action of π_A on $T_l(A)$ is induced from $l^{-s_1-s_2}(\oplus N_i)$. But $(l^{-s_1-s_2}(\oplus N_i))/(\oplus N_i)$ is a finite set, so we proved the finiteness of $\{T_l(B)|B \in \mathcal{C}\}$ if $l \neq p$.

The $l = p$ case is similar as we can see we can do the similar calculus for $W(k)$ module $M(A)$ with the action $\pi_A = L^m$ if $k = \mathbb{F}_{p^m}$. Then we can see that the set of $M(A)$ with the action of π_A is finite, but for fixed π_A, there are only finitely many choices of L since they must be semi-simple. So we have the set of $M(A)$ with D_k action is a finite set. □

By Proposition 6.4.1, to prove the finiteness of isomorphism classes of abelian varieties, it suffices to show for a fixed abelian variety A of dimension g, the set

$$\{B|B \textit{ is an abelian variety, } T_l(B) \cong T_l(A) \textit{ as } \mathbb{Z}_l[G] \textit{ modules for all prime } l\}$$

is a finite set. Here we include the case $l = p$, which we consider the D_k module $M(A)$. We will show this in the next section.

6.5 Proof of the main theorem

In this section, we will show the set in the previous section

$$\{B|B \textit{ is an abelian variety, } T_l(B) \cong T_l(A) \textit{ as } \mathbb{Z}_l[G] \textit{ modules for all prime } l\}$$

is finite with the fixed A.

Lemma 6.5.1. For a prime $l \neq p$, if $T_l(A) \cong T_l(B)$ as a $\mathbb{Z}_l[G]$ module, then there exists an isogeny $\pi : B \to A$ with $(deg\pi, l) = 1$.

Proof. From the Tate conjecture, we have the following isomorphism

$$\mathrm{Hom}_{AV}(B, A) \cong \mathrm{Hom}_{\mathbb{Z}_l[G]}(T_l(B), T_l(A))$$

If $\sigma : T_l(B) \to T_l(A)$ the isomorphism, then since $\mathbb{Z}$ is dense in $\mathbb{Z}_l$, so we may find an isogeny $\pi : B \to A$ such that the image of π is close to σ. So the image of π is also an isomorphism. Then set $N = Ker(\pi)$, so we have the exact sequence

$$0 \to T_l(B) \to T_l(A) \to N_l \to 0$$

here N_l means the sylow l group of N, see [17, Proposition 10.6]. Since π induces isomorphism between Tate modules, so we must have $N_l = \{0\}$, so $(deg\pi, l) = 1$. □

Lemma 6.5.2. The same holds for $l = p$ case.

Proof. The proof is really similar, the exact sequence is

$$0 \to N_p \to B[p^\infty] \to A[p^\infty] \to 0$$

see [17, p. 10.17] □

We can conclude the previous two lemmas into one property:

Proposition 6.5.3. Fix an abelian variety A. If there exists an abelian variety B such that $T_l(B) \cong T_l(A)$ for $l \neq p$ and $M(B) \cong M(A)$ as D_k modules, then for any prime l, we have an isogeny $\pi_l : B \to A$ such that $deg(\pi)$ is coprime to l.

We need a technique lemma.

Lemma 6.5.4. Assume there exists two abelian varieties A and B and two isogenies $\pi_1 : B \to A$ and $\pi_2 : B \to A$. If we have two integers m_1, m_2 such that $(m_1, m_2) = 1$ and $(m_1, deg\pi_1) = (m_2, deg\pi_2) = 1$, then we have an isogeny $\pi : B \to A$ such that $(deg\pi, m_1 m_2) = 1$.

Proof. Set $\pi = m_2\pi_1 + m_1\pi_2$. First we show π is an isogeny. Pick some $l \mid m_1$, then consider the image of π in $\mathrm{Hom}_{\mathbb{Z}_l[G]}(T_l(B), T_l(A))$ under the Tate isomorphism. We can see by condition $m_2\pi_1$ under this isomorphism induces an isomorphism since $(m_2 deg\pi_1, l) = 1$, and π and $m_2\pi_1$ are differ by l times some homomorphism, so we have π is an isomorphisms of Tate modules, so π is an isogeny.

If $(deg\pi, m_1m_2) \neq 1$, then there exists some $x \in Ker(\pi) \cap B[m_1m_2]$. Then by replacing x by some multiple, we may assume there exists some prime factor l of m_1m_2, just say a prime factor of m_1 (the case of m_2 is the same), such that $x \neq 0$, $lx = 0$ and $x \in Ker(\pi)$. But then we have

$$0 = \pi(x) = m_2\pi_1(x) + m_1\pi_2(x) = m_2\pi_1(x)$$

so $x \in Ker(m_2\pi_1)$, so $x \in Ker(m_2\pi_1) \cap B[l] = \{0\}$, which is a contradiction. So this π satisfies our requirements. □

Now we come to the next lemma.

Lemma 6.5.5. Fix an abelian variety A. If there exists an abelian variety B such that $T_l(B) \cong T_l(A)$ for $l \neq p$ and $M(B) \cong M(A)$ as D_k modules, then B is a direct component of $A \times A$. Here direct component means we have an abelian variety C such that $B \times C \cong A \times A$

Proof. Choose any isogeny $\pi_1 : B \to A$, then by Lemma 6.5.4, Prop 6.5.3 and the induction procedure, we may find an isogeny π_2 such that $(deg\pi_1, deg\pi_2) = 1$, then we have an embedding

$$g : B \to A \times A$$

$$b \to (\pi_1(b), \pi_2(b))$$

Then we may find isogenies $\phi_1 : A \to B$ and $\phi_2 : A \to B$ such that

$$\phi_1\pi_1 = deg\pi_1$$

$$\phi_2\pi_2 = deg\pi_2$$

Since $(deg\pi_1, deg\pi_2) = 1$, so there exists $s, t \in \mathbb{Z}$ such that $sdeg\pi_1 + tdeg\pi_2 = 1$. Define

$$f : A \times A \to B$$

$$(a_1, a_2) \to s\phi_1(a_1) + t\phi_2(a_2)$$

Then we have $fg = 1_B$, so B is a direct factor of $A \times A$. □

Now we can finish our proof.

Theorem 6.5.6. There are only finitely abelian varieties of dimension g over k.

Proof. By [31, Theorem 18.7], for a fixed abelian variety, there are only finitely many direct components, then the theorem follows from Corollary 6.3.3, Prop 6.4.1 and Lemma 6.5.5. □

Bibliography

[1] Grégory Berhuy and Giordano Favi. "Essential dimension: a functorial point of view (after A. Merkurjev)". In: *Doc. Math* 8.106 (2003), pp. 279–330.

[2] Bhargav Bhatt. *Topics in algebraic geometry 1 - abelian varieties*.

[3] Patrick Brosnan, Zinovy Reichstein, and Angelo Vistoli. "Essential dimension and algebraic stacks". In: *arXiv preprint math/0701903* (2007).

[4] Patrick Brosnan, Zinovy Reichstein, and Angelo Vistoli. "Essential dimension in mixed characteristic". In: *arXiv preprint arXiv:1801.02245* (2018).

[5] Patrick Brosnan et al. "Essential dimension of moduli of curves and other algebraic stacks". In: *arXiv preprint arXiv:0907.0924* (2009).

[6] Joe Buhler and Zinovy Reichstein. "On the essential dimension of a finite group". In: *Compositio Mathematica* 106.2 (1997), pp. 159–179.

[7] JWS Cassels. "Arithmetic on Curves of Genus 1 (V). Two Counter-Examples". In: *Journal of the London Mathematical Society* 1.1 (1963), pp. 244–248.

[8] V Chernousov and V Guletskiı. "2-torsion of the Brauer group of an elliptic curve: generators and relations". In: *Conference on Quadratic Forms*. 2001, p. 85.

[9] Pete L Clark. "The period-index problem in WC-groups II: abelian varieties". In: *arXiv preprint math/0406135* (2004).

[10] Jean-Louis Colliot-Thelene, Nikita Karpenko, and Alexander Merkurjev. "Rational surfaces and canonical dimension of PGL6". In: *St Petersburg Mathematical Journal* (2008).

[11] Brian Conrad. *Keel–Mori theorem via stacks*. 2005.

[12] Pierre Deligne. "La conjecture de Weil. I". In: *Publications Mathématiques de l'Institut des Hautes Études Scientifiques* 43.1 (1974), pp. 273–307.

[13] Igor V Dolgachev and JongHae Keum. "Finite groups of symplectic automorphisms of K3 surfaces in positive characteristic". In: *Annals of mathematics* (2009), pp. 269–313.

[14] Mathieu Florence. "On the essential dimension of cyclic p-groups". In: *Inventiones mathematicae* 171.1 (2008), pp. 175–189.

[15] Anningzhe Gao. "Essential dimension of the moduli stack of polarized K3 surfaces". In: *Proceedings of the American Mathematical Society* (2020).

[16] Anningzhe Gao. "The period-index problem for elliptic curves and the essential dimension of Picard stacks". In: *arXiv preprint arXiv:2002.11814* (2020).

[17] Gerard van der Geer and Ben Moonen. *Abelian varieties*.

[18] Philippe Gille and Tamás Szamuely. *Central simple algebras and Galois cohomology*. Vol. 165. Cambridge University Press, 2017.

[19] Jean Giraud. *Cohomologie non abélienne*. Vol. 4. Springer, 1971.

[20] Günter Harder. "Lectures on algebraic geometry II". In: *Aspects of Mathematics* 39 (2008).

[21] Robin Hartshorne. *Algebraic geometry*. Vol. 52. Springer Science & Business Media, 2013.

[22] Daniel Huybrechts. *Fourier-Mukai transforms in algebraic geometry*. Oxford University Press on Demand, 2006.

[23] Daniel Huybrechts. *Lectures on K3 surfaces*. Vol. 158. Cambridge University Press, 2016.

[24] Junmyeong Jang. "A Lifting of an Automorphism of a K3 Surface over Odd Characteristic". In: *International Mathematics Research Notices* 2017.6 (2016), pp. 1787–1804.

[25] Junmyeong Jang. "Neron-Severi group preserving lifting of K3 surfaces and applications". In: *arXiv preprint arXiv:1306.1596* (2013).

[26] Serge Lang and John Tate. "Principal homogeneous spaces over abelian varieties". In: *American Journal of Mathematics* 80.3 (1958), pp. 659–684.

[27] Gérard Laumon and Laurent Moret-Bailly. *Champs algébriques*. Vol. 39. Springer, 2018.

[28] Arne Ledet. "On the essential dimension of p-groups". In: *Galois theory and modular forms*. Springer, 2004, pp. 159–172.

[29] Stephen Lichtenbaum. "The period-index problem for elliptic curves". In: *American Journal of Mathematics* 90.4 (1968), pp. 1209–1223.

[30] Alexander S Merkurjev. "Essential dimension". In: *Contemporary Mathematics* 493 (2009), p. 299.

[31] James S Milne. "Abelian varieties". In: *Arithmetic geometry*. Springer, 1986, pp. 103–150.

[32] James S Milne and James S Milne. *Etale cohomology (PMS-33)*. 33. Princeton university press, 1980.

[33] Shigeru Mukai. "Duality between D (X) and with its application to Picard sheaves". In: *Nagoya Mathematical Journal* 81 (1981), pp. 153–175.

[34] Niels O Nygaard. "The Tate conjecture for ordinary K3 surfaces over finite fields". In: *Inventiones mathematicae* 74.2 (1983), pp. 213–237.

[35] Martin Olsson. *Algebraic spaces and stacks*. Vol. 62. American Mathematical Soc., 2016.

[36] Dmitri Olegovich Orlov. "Derived categories of coherent sheaves and equivalences between them". In: *Russian Mathematical Surveys* 58.3 (2003), p. 511.

[37] Richard Pink. "Finite group schemes". In: *Notes de Cours http://www. math. ethz. ch/pink/FiniteGroupSchemes. html* (2004).

[38] Zinovy Reichstein. "Essential dimension". In: *Proceedings of the International Congress of Mathematicians 2010 (ICM 2010) (In 4 Volumes) Vol. I: Plenary Lectures and Ceremonies Vols. II–IV: Invited Lectures*. World Scientific. 2010, pp. 162–188.

[39] Zinovy Reichstein and Angelo Vistoli. "A genericity theorem for algebraic stacks and essential dimension of hypersurfaces". In: *arXiv preprint arXiv:1103.1611* (2011).

[40] Zinovy Reichstein and Angelo Vistoli. "Essential dimension of finite groups in prime characteristic". In: *Comptes Rendus Mathematique* 356.5 (2018), pp. 463–467.

[41] Jordan Rizov. "Moduli stacks of polarized K3 surfaces in mixed characteristic". In: *arXiv preprint math/0506120* (2005).

[42] John Tate. "Endomorphisms of abelian varieties over finite fields". In: *Inventiones mathematicae* 2.2 (1966), pp. 134–144.

[43] Bertrand Toën. "The homotopy theory of dg-categories and derived Morita theory". In: *Inventiones mathematicae* 167.3 (2007), pp. 615–667.

[44] Angelo Vistoli. "Notes on Grothendieck topologies, fibered categories and descent theory". In: *arXiv preprint math/0412512* (2004).

[45] William C Waterhouse and JS Milne. "Abelian varieties over finite fields". PhD thesis. Harvard University, 1968.

[46] Yuri Zarhin. "Endomorphisms of abelian varieties and points of finite order in characteristic p". In: *Mathematical notes of the Academy of Science of the USSR* 21 (1977), pp. 415–419.