Lecture Notes in Mathematics 1680

Ke-Zheng Li Frans Oort

# Moduli of Supersingular Abelian Varieties

Springer

Ke-Zheng Li Frans Oort

# Moduli of Supersingular Abelian Varieties

Springer

Authors

Ke-Zheng Li
Graduate School of Academia Sinica
Department of Mathematics
P.O. Box 3908
Beijing 100039, China
e-mail: kzli@math07.math.ac.cn

Frans Oort
Mathematisch Instituut
Budapestlaan 6
NL-3508 TA Utrecht, The Netherlands
e-mail: oort@math.ruu.nl

Cataloging-in-Publication Data applied for

**Die Deutsche Bibliothek - CIP-Einheitsaufnahme**

**Li, Ke-Zheng:**
**Moduli of supersingular Abelian varieties / Ke-Zheng Li ; Frans Oort. - Berlin ; Heidelberg ; New York ; Barcelona ; Budapest ; Hong Kong ; London ; Milan ; Paris ; Santa Clara ; Singapore ; Tokyo : Springer, 1998**
**(Lecture notes in mathematics ; Vol. 1680)**
**ISBN 3-540-63923-3**

Mathematics Subject Classification (1991):
14K10, 14G15, 14L05, 14L15, 14D20, 14D22, 11G10, 11G15, 11R29

ISSN 0075-8434
ISBN 3-540-63923-3 Springer-Verlag Berlin Heidelberg New York



Typesetting: Camera-ready TEX output by the author
SPIN: 10553445 46/3143-543210 - Printed on acid-free paper

# Contents

# 0. Introduction

## 0.1. Moduli of supersingular abelian varieties.

In this book we consider polarized abelian varieties over a field $K$ of characteristic $p$. In positive characteristic abelian varieties naturally have an extra structure (not present in characteristic zero), given by properties of the subgroup scheme of "points" of $p$-power order.

Let us first explain briefly the main results, and then give more details. An elliptic curve $E$ in characteristic $p$ is called *supersingular* if it has no geometric points of order equal to $p$, i.e. let $E$ be defined over a field $K \supset \mathbb{F}_p$, let $k$ be an algebraically closed field containing $K$, then

$$E \text{ is supersingular} \overset{\text{def}}{\iff} \quad E[p](k) = 0$$

(some notation necessary to understand the contents of this introduction will be gathered together in 0.6 below). An abelian variety $X$ in positive characteristic is called *supersingular* if it is geometrically isogenous to a product of supersingular elliptic curves, or in other words: if $X$ is defined over $K \supset \mathbb{F}_p$, the dimension of $X$ equals $g$, and $k$ is an algebraically closed field containing $K$, then

$$X \text{ is supersingular} \overset{\text{def}}{\iff} X \otimes k \sim E^g,$$

where $E$ is a supersingular elliptic curve over $k$ and "$\sim$" denotes isogeny equivalence (there are many other characterizations and properties, see 0.6 below).

Given $g \in \mathbb{Z}_{>0}$, a prime number $p$, and $d \in \mathbb{Z}_{>0}$, we denote by $\mathcal{A}_{g,d} \otimes \mathbb{F}_p$ the moduli space of all $(X, \lambda)$, where $X$ is an abelian variety of dimension $g$ with a polarization $\lambda$ of degree $d^2$, in characteristic $p$. We write

$$\mathcal{S}_{g,d} \subset \mathcal{A}_{g,d} \otimes \mathbb{F}_p \tag{0.1.1}$$

for the subset corresponding to all cases where $X$ is supersingular, called the *supersingular locus* (in fact this is a closed algebraic subset).

One of the main results in this book is:

- *The dimension of* $\mathcal{S}_{g,1}$ *equals* $[g^2/4]$ (the integral part of $g^2/4$), and
- $$\#\{\text{irreducible components of } \mathcal{S}_{g,1}\} = \begin{cases} H_g(p,1) & \text{if } g \text{ is odd,} \\ H_g(1,p) & \text{if } g \text{ is even.} \end{cases}$$

## 0.2. The supersingular locus in the moduli of abelian varieties.

A reader might wonder why these objects are studied, why they seem to be interesting.

In characteristic $p$ the structure of the $p$-power torsion of an abelian variety is a canonical, extra structure (not present in this form in characteristic zero). Like abelian varieties can degenerate, also the "$p$-structure" can "degenerate". One can consider "ordinary abelian varieties" (those which have the maximal possible number of points of order $p$) as giving moduli points to the "interior" of the moduli space, while one could consider "degeneration" of the $p$-structure (while the abelian variety stays an abelian variety) as approaching to some kind of boundary. For example think of a variable elliptic curve in characteristic $p$, and put your fingers on the geometric points of order $p$; you feel that these come together when you specialize to a supersingular elliptic curve. This gives a fine structure on these moduli spaces which turn out to be of great help in understanding such moduli spaces (also the ones in characteristic zero). It turns out that the supersingular abelian varieties should be considered as the ones where the $p$-structure is most degenerated (analogous to the "cusps at infinity" in the boundary). For this reason these spaces $\mathcal{S}_{g,d}$ are interesting.

It turns out that the supersingular locus is quite different from other subsets defined by this kind of fine structures. The geometry of these spaces is very rich, it has certain geometric properties, but also a number theoretic flavor. Moreover, part of the structure of these spaces can be studied by purely algebraic methods which make some results even better accessible. We expect that while the supersingular locus is highly reducible (for $g$ and $p$ large), it might be true that the other loci (e.g. the ones given by Newton polygons which are not supersingular) can very well be irreducible. All this would give a strong approach to geometric, arithmetic and number theoretic study of moduli spaces of abelian varieties. For these reason we would like to understand the supersingular locus in itself very well. In this book we study various properties of these spaces. However, we leave aside how they are attached to the other interesting loci in the moduli space.

## 0.3. Polarizations, isogeny correspondences.

**Why polarizations?** We comment on some technical aspects of this work. First of all one should keep in mind that there is a difference between elliptic curves on the one hand (abelian varieties of dimension one), and abelian varieties of higher dimensions on the other hand. An abelian variety comes naturally with a rational point, the zero point. In the case of $g = 1$ this defines a divisor. For this reason every abelian variety of dimension one has a natural principal polarization; we can speak of moduli spaces of elliptic curves, meaning abelian varieties of dimension one with this natural (unique) principal polarization. However there are abelian varieties (of any dimension $g > 1$) which do *not* admit a principal polarization (this phenomenon occurs in all characteristics). And, when there is a principal polarization, it need not be unique (if $g > 1$); actually this is one of the main tools in the present study (we shall deal with all kind of mutually different principal

polarizations on an abelian variety like $E^g$). When considering higher dimensions, it turns out that there is no good notion of moduli spaces of abelian varieties (without considering a polarization). For example, if one takes over the complex numbers the set of isomorphism classes of all abelian surfaces, there is no reasonable, natural geometric structure on this set (dividing out the equivalence relation, one might obtain non-Hausdorff spaces, this is a very classical topic, already known more than a century). Hence it is natural to consider *polarized* abelian varieties, when studying the cases with $g > 1$.

**Isogenies.** One can consider isogeny correspondences (Hecke correspondences) between components of moduli spaces. In characteristic zero, for an abelian variety $X$ there are only a finite number of isogenies $X \to Y$ of a given degree, and this, in a certain way, simplifies the study of such correspondences. However in positive characteristic such correspondences (still well-defined) in general are not finite-to-finite; this accounts for several interesting and difficult aspects. For example it turns out that all of the components of the moduli space of polarized abelian varieties of dimension $g$ over any field have the same dimension ($g(g+1)/2$ in fact), isogeny correspondences blow-up and down, but leave the dimension of the total spaces the same; miraculously the same holds for subsets defined by the $p$-rank. However components of the supersingular locus $\mathcal{S}_g = \bigcup_d \mathcal{S}_{g,d}$ can have different dimensions (when $g \geq 3$), in fact numbers between $[g^2/4]$ and $g(g-1)/2$ show up. This accounts for truly deep and difficult problems when studying certain closed subsets of the moduli space of polarized abelian varieties in positive characteristic. We shall deal with some of these questions.

### 0.4. PFTQs and parameter spaces of supersingular abelian varieties.

**Flag type quotients.** Here is the basic idea how to describe components of $\mathcal{S}_g$. Almost by definition, a supersingular abelian variety comes from $E^g$ via an isogeny $E^g \to X$. This isogeny can be chosen to be purely inseparable, and in that case the group scheme $\ker(E^g \to X) \subset E^g$ is a repeated extension of the simple finite group scheme $\alpha_p$. The basic idea is to describe the supersingular locus via all possibilities of such finite subgroup schemes of $E^g$. A hint what should be done is given by the fact that a "general" supersingular abelian variety canonically is the quotient of $E^g$ via an isogeny of degree $p^{g(g-1)/2}$. Naturally this leads to the notion of *flag type quotients*.

For $g = 2$ a flag type quotient consists of

$$E^2 = X_1 \to E^2/\alpha_p \cong X_0. \tag{0.4.1}$$

Here we see that locally on the components of $\mathcal{S}_2$ the structure is given by varying $\alpha_p$ inside $E^2$, which is the same as giving a parameter on $\mathbf{P}^1$; in fact every component of $\mathcal{S}_2$ turns out to be a rational curve; the non-uniqueness of flag type quotients for some abelian surfaces gives rise to singularities of $\mathcal{S}_{2,1}$ which are transversal crossings of regular branches. For $g = 3$ a flag type quotient consists of

$$E^3 = X_2 \to E^3/(\alpha_p)^2 \cong X_1 \to X_1/\alpha_p \cong X_0. \tag{0.4.2}$$

In most cases, for a given $X_0$ such a sequence is unique, however for some cases it is not, and this causes the effect of singularities (in fact, of quite a bad type) on the components of $\mathcal{S}_{3,1}$. In general a flag type quotient, abbreviated by *FTQ*, for a supersingular abelian variety $X_0$ of dimension $g$ is a sequence

$$E^g = X_{g-1} \to \cdots \to X_i/(\alpha_p)^i \cong X_{i-1} \to \cdots \to X_1 \to X_0, \tag{0.4.3}$$

where $E$ is a supersingular elliptic curve (which, for $g \geq 2$ can be chosen once and for all).

**Polarized flag type quotients.** In order to obtain components of $\mathcal{S}_g$ we have to put a polarization on the $X_0$ in consideration. This can be done by choosing a polarization on $E^g$, of degree $d^2 \cdot p^{g(g-1)}$ in fact, which descends via the flag type quotient (0.4.3) to a polarization $\lambda_0$ of degree $d^2$ on $X_0$. Then in (0.4.3) each $X_i$ is equipped with a polarization of the appropriate degree, such that they form a descending chain of polarizations. Such a sequence is called a *polarized flag type quotient*, abbreviated *PFTQ*, for $(X_0, \lambda_0)$. The moduli space $P$ of PFTQs exists, and there is a surjective morphism

$$\Psi : P \quad \twoheadrightarrow \quad \mathcal{S}_g \subset \mathcal{A}_g. \tag{0.4.4}$$

As we have already mentioned earlier, also for the polarized case, for "general" polarized supersingular abelian varieties a PFTQ is unique. However the phenomenon that for special cases it is not unique causes that the morphism $\Psi$ is blowing down, for $g \geq 3$, certain subsets of this parameter space $P$ to subsets of $\mathcal{S}_g$. For $g \geq 4$ this turns out to be rather bad: it might blow down a whole component of $P$ to a proper closed subset of a component of $\mathcal{S}_g$ (this even happens above $\mathcal{S}_{g,1}$); we call such a component of $P$ a "garbage component". The existence of these was for a long time the obstacle to describe all components of $\mathcal{S}_{g,1}$ in the case when $g \geq 4$. One of the main points of the present work is the (rather technical) definition of a "rigid PFTQ". This notion singles out a Zariski open subset $P' \subset P$, on which the map

$$\Psi : P' \quad \to \quad \mathcal{S}_g \tag{0.4.5}$$

is indeed *finite to one and surjective* (for example the closure of $P'$ in $P$ does not contain any of the garbage components). For a general principally polarized supersingular abelian variety its (canonical) polarized flag type quotient is automatically rigid. As is usual in moduli theory, once a good moduli-theoretic description is given, one can proceed. In fact we show that any component of $P'$ maps finite to one onto a (non-empty open set of a) component of $\mathcal{S}_g$, and any component of the latter one can be obtained in precisely one way along this line. Once we have arrived this point, it is clear how to proceed:

- *compute the dimension of every component of $P'$; this turns out to be equal to $[g^2/4]$ above $\mathcal{S}_{g,1}$, and*
- *compute the number of isomorphism classes of polarizations with the required properties on $E^g$ in order to describe the number of components of $\mathcal{S}_{g,d}$.*
- For $d = 1$, the case of principally polarized supersingular abelian varieties, this amounts to considering all polarizations

$$\eta : E^g \to (E^g)^t, \quad \text{with} \quad \ker(\eta) = E^g[F^{g-1}],$$

where $F$ is the Frobenius morphism of $E^g$.

- For $g$ odd this amounts to the same as the number of equivalence classes of principal polarizations on $E^g$, which is known to be equal to the class number $H_g(p,1)$, hence this is the number of geometrically irreducible components of $\mathcal{S}_{g,1}$. For $g$ even we obtain the class number $H_g(1,p)$ as the number of components.

### 0.5. Strategy for proving the main properties of the moduli of rigid PFTQs.

It seems natural to consider for a given $g$ and for a given $0 \leq m \leq g-1$ a moduli space $\mathcal{V}_m$ of polarized, rigid, partial flags

$$E^g \cong Y_{g-1} \to \cdots \to Y_{m+1} \to Y_m. \tag{0.5.1}$$

In this way we obtain a sequence of spaces and "truncation maps"

$$\mathcal{V}_0 \to \cdots \to \mathcal{V}_{g-2} \to \mathcal{V}_{g-1} = \{\text{one point}\}, \tag{0.5.2}$$

where $\mathcal{V}_m$ $(0 \leq m \leq g-1)$ is the moduli of sequences (0.5.1), and in particular $\mathcal{V}_0$ is the moduli of PFTQs.

This idea has to be refined. The heart of the proof of the main result on $\mathcal{S}_{g,1}$ uses complete induction from $g-2$ to $g$, by constructing moduli spaces which combine a partial flag $Y_{g-1} \to \cdots \to Y_m$ for genus $g$, with a complete flag for genus $g-2$, related in some way, with extra properties, which ensure that the incomplete flag can be completed; this is a tricky condition (see condition d) in 11.3). For example consider the explicit condition for the case $g = 4$ (see 9.7). The moduli spaces thus obtained fit into a sequence of morphisms; each turns out to be a smooth epimorphism of relative dimension one. Once this is proved the main result follows.

One may note the different behavior between $\mathcal{S}_{g,1}$ for odd $g$ on the one hand, and the same for even $g$ on the other hand. This is reflected in the fact that we consider polarizations of $E^g$ whose kernel is $E[F^{g-1}]$. For

$$g-1 = 2m \quad \text{we have} \quad E[F^{g-1}] = E^g[p^m],$$

and such a polarization equals $p^m$ times a principal polarization. For

$$g-1 = 1+2m \quad \text{we have} \quad E[F^{g-1}] = E^g[p^m F],$$

which gives polarizations with a different type of behavior. Also the difference is found back in the proof (which works by induction from $g-2$ to $g$).

There is one more technical point we would like to mention. Let $G$ be the formal group (in this case also the $p$-divisible group) of a supersingular elliptic curve $E$. A principal polarization on $E^g$ gives a quasi-polarization on $G^g$. It turns out that any two principal polarizations on $E^g$ give equivalent quasi-polarizations on $G^g$ (a kind of global-local property). This simplifies the description of the components of

the moduli of rigid PFTQs, and the class numbers involved describe the number of components of $\mathcal{S}_{g,1}$.

For further discussions of technical points, of examples, of other results, we refer to the main text.

### 0.6. Some definitions used in the introduction.

In this section we collect some definitions and explain some of the terminology used in the introduction. We shall write $K$ for a field and $k$ for an algebraically closed field, we usually assume $K \subset k$. A term like "geometrically integral" will mean "integral after $\otimes_K k$".

**Definition**: An *abelian variety* defined over $K$ is a complete group variety over $K$, i.e. a $K$-group scheme which is proper over $K$ and geometrically integral. Note that for an abelian variety the group law is commutative.

An *abelian scheme* $X \to S$ is an $S$-group scheme which is smooth and proper over $S$ such that all fibres are abelian varieties. (For general references see [53] or [56].)

**Definition**: An *elliptic curve* over a field $K$ is an abelian variety over $K$ of dimension one.

Note that the following properties are equivalent:

i) $E$ is an elliptic curve over $K$, isomorphisms are isomorphisms of group varieties.

ii) $E$ is an elliptic curve over $K$, isomorphisms are isomorphisms of varieties, preserving the point zero.

iii) $E$ is a an algebraic curve smooth and proper over $K$, geometrically connected, of genus 1, with a given $K$-rational point $0 \in E(K)$; isomorphisms are isomorphisms of algebraic curves, preserving the point 0.

iv) $E \subset \mathbb{P}^2_K$ is a projective, plane curve of degree 3, smooth over $K$, with a given point $0 \in E(K)$; isomorphisms are given by projective isomorphisms preserving the point 0.

v) $E \subset \mathbb{P}^2_K$ is given by the equation

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

with $a_i \in K$, with the discriminant non-zero (we do not write it down here), where the point zero on the curve is given by $(0 : 1 : 0)$; isomorphisms are given by projective isomorphisms preserving the point zero.

For an additive abelian group $A$ and an integer $n$ we write $A[n]$ for the kernel of $\times n : A \to A$. For a commutative group scheme $G$ we write

$$G[n] = \ker(n\cdot\mathrm{id}_G : G \to G),$$

considered as a subgroup scheme of $G$. Note that we have

$$G[n](k) = G(k)[n]$$

if $G$ is a group scheme over some subfield of $k$.

If $G$ is a group scheme over a field $K$ of characteristic $p > 0$, we have the *relative Frobenius homomorphism* $F_{G/K} : G \to G^{(p)}$ (see 2.3), and we write $G[F] = \ker(F_{G/K})$.

A finite surjective homomorphism $X \to Y$ between abelian schemes over $S$ is called an *isogeny*. If there exists an isogeny $\phi : X \to Y$, then we say $X$ is *isogenous* to $Y$, denoted by $X \sim Y$. It turns out that $\sim$ is an equivalence relation: since $n = \deg(\phi)$ annihilates $\ker(\phi)$, we have $\ker(\phi) \subset X[n]$, hence there exists an isogeny $\psi : Y \to X$ such that $\psi \circ \phi = n \cdot \mathrm{id}_X$, in particular $Y \sim X$.

For an abelian scheme $X \to S$ there is a *dual* abelian scheme $X^t \to S$. A *polarization* on $X \to S$ is by definition an $S$-isogeny $\lambda : X \to X^t$ which on every geometric fibre is given by an ample divisor (see [56, Definition 6.3]). A polarization is called *principal* if it is an isomorphism.

Here is a way to construct abelian varieties which do not admit a principal polarization. Choose an integer $g \in \mathbb{Z}_{\geq 2}$, choose a field $k$ and an abelian variety $X$ over $k$ such that $\mathrm{End}(X) \cong \mathbb{Z}$ (for every characteristic such abelian varieties exist). If $X$ does not admit a principal polarization we are done. If $X$ does admit a principal polarization, choose an integer $n \in \mathbb{Z}_{\geq 2}$ prime to $\mathrm{char}(k)$, and a cyclic subgroup $N \subset X$ of order $n$; then $Y := X/N$ does not admit a principal polarization. This can be seen as follows: there does exist an isogeny $Y^t \to X^t$ with kernel cyclic of order $n$, a principal polarization on $Y$ would give

$$h := (X \to X/N = Y \cong Y^t \to Y^t/N = X^t \cong X) \in \mathrm{End}(X) \cong \mathbb{Z};$$

if $h = m \cdot \mathrm{id}_X$, then on the one hand $\ker(h) \cong (\mathbb{Z}/m\mathbb{Z})^{2g}$; on the other hand $\ker(h)$ is an extension of $\mathbb{Z}/n\mathbb{Z}$ by $\mathbb{Z}/n\mathbb{Z}$, and we obtain a contradiction with $g \geq 2$.

In positive characteristic one easily constructs examples (even over $\bar{\mathbb{F}}_p$) of abelian varieties which do not admit a separable polarization.

For the definition and existence of the moduli spaces

$$\mathcal{A}_{g,d,n} \to \mathrm{Spec}(\mathbb{Z}[1/n])$$

we refer to [56, 7.2].

**Definition**: Let $X$ be an abelian variety over $K \supset \bar{\mathbb{F}}_p$. Then there exists an integer $f = f(X)$, called the *p-rank* of $X$, such that

$$X[p](k) \cong (\mathbb{Z}/p\mathbb{Z})^f.$$

Note that $0 \leq f \leq g = \dim(X)$. An abelian variety $X$ is called *ordinary* if its $p$-rank is maximal, i.e.

$$X \text{ is ordinary} \iff X[p](k) \cong (\mathbb{Z}/p\mathbb{Z})^{\dim(X)}.$$

If $X$ and $Y$ are isogenous to each other then $f(X) = f(Y)$.

An elliptic curve in positive characteristic is called *supersingular* if it is not ordinary, i.e. if it does not contain a point of order $p$.

Over an algebraically closed field $k \supset \mathbf{F}_p$ there are, up to isomorphism, exactly three group schemes whose structure ring has rank $p$ over $k$:

$$\mu_p, \qquad \alpha_p, \qquad \mathbf{Z}/p\mathbf{Z}.$$

Moreover when $G$ is a finite group scheme over $K$ then $G \cong \alpha_p$ if and only if $G \otimes k \cong \alpha_p$.

An ordinary abelian variety $X$ in characteristic $p$ is characterized by:

$$X \text{ is ordinary } \iff X[p] \otimes k \cong (\mu_p)^{\dim(X)} \times (\mathbf{Z}/p\mathbf{Z})^{\dim(X)}.$$

We see that an elliptic curve $E$ is supersingular (when defined over a field of characteristic $p$) if and only if $E[F] \cong \alpha_p$.

**Complex multiplications and supersingularity.** We give some more information, which might explain the terminology "supersingular".

Let $X$ be an abelian variety of dimension $g$. If $\mathrm{End}^0(X) = \mathrm{End}(X) \otimes \mathbf{Q}$ contains a commutative semi-simple algebra of rank $2g$ over $\mathbf{Q}$, then we say $X$ has "*sufficiently many complex multiplications (smCM)*".

Let us explain first the case of elliptic curves. In characteristic zero, say over the field $\mathbf{C}$ of complex numbers, an elliptic curve $E$ either has the property $\mathrm{End}(E) = \mathbf{Z}$ (and we say "$E$ has no complex multiplications"), or $\mathbf{Z} \subset \mathrm{End}(E)$ is a proper inclusion (and we say "$E$ has complex multiplications", or CM in short). It is known classically that an elliptic curve with CM can be defined over a finite extension of $\mathbf{Q}$ (i.e. over a number field); classically the $j$-invariant in this case was called a "singular $j$-invariant"; in this case $\mathrm{End}(E)$ is an order in an imaginary quadratic field.

In positive characteristic there are more possibilities. Suppose $\mathbf{F}_p \subset K$, let $k$ be an algebraically closed field containing $K$, and let $E$ be an elliptic curve over $K$. Then one of the following three properties holds:

i) $\mathrm{End}(E \otimes k) = \mathbf{Z}$. In this case $E$ cannot be defined over a finite field. Equivalently: its $j$-invariant is transcendental over $\mathbf{F}_p$. In this case $E$ is ordinary.

ii) $\mathrm{End}(E \otimes k)$ is an algebra of rank 2 over $\mathbf{Z}$. In this case $\mathrm{End}(E)$ is an order in an imaginary quadratic field in which $p$ is split and $E$ (or its $j$-value) is called *singular*. Also in this case $E$ is ordinary, and it can be defined over a finite field.

iii) $\mathrm{End}(E \otimes k)$ is an algebra of rank 4 over $\mathbf{Z}$. In this case its endomorphism algebra $\mathrm{End}^0(E \otimes k) := \mathrm{End}(E \otimes k) \otimes \mathbf{Q}$ is a central simple algebra of degree 4 over $\mathbf{Q}$ ramified exactly at $\infty$ and at $p$. Moreover $E[p](k) = 0$, and $j(E) \in \mathbf{F}_{p^2}$, and $E$ (or its $j$-value) is called *supersingular*.

A little warning: it might happen for an elliptic curve $E$ defined over a field $K$ that $\mathrm{End}(E)$ has rank two over $\mathbf{Z}$, and $\mathrm{End}(E \otimes k)$ has rank four over $\mathbf{Z}$. In that case, $\mathrm{char}(K) = p > 0$, and $\mathrm{End}(E)$ is an order in an imaginary quadratic number field in which $p$ does not split.

For every $p$ there exists a supersingular elliptic curve over $\mathbb{F}_p$. The number $h_p$ of isomorphism classes of supersingular elliptic curves (over $k$, say over $\bar{\mathbb{F}}_p$) is finite, this number is a classical invariant (we will come back to this, see 9.1). Any two supersingular elliptic curves over $\bar{\mathbb{F}}_p$ are isogenous to each other.

**Supersingular abelian varieties.** For abelian varieties of arbitrary dimension over $K \supset \mathbb{F}_p$ there are many possibilities for the structure of the $p$-torsion subgroup scheme, and for $\mathrm{End}(X)$. If $\mathrm{End}(X)$ is larger than $\mathbb{Z}$ one could say "$X$ has complex multiplications" (but in general we *don't*), the rank of $\mathrm{End}(X)$ over $\mathbb{Z}$ can have several values. An abelian variety $X$ of dimension $g$ is supersingular if and only if $\mathrm{End}(X \otimes k)$ is of rank $(2g)^2$ over $\mathbb{Z}$.

We remark that in higher dimension (over $K \supset \mathbb{F}_p$) there are showing up some complexities (or, if you like, some extra interesting features), not present for elliptic curves:

- If $\dim(X) \leq 2$ and $X[p](k) = 0$ then $X$ is supersingular, however,
- for every $g \geq 3$ there is an abelian variety $X$ of dimension $g$ with $X[p](k) = 0$ which is not supersingular.
- As Tate showed (see [97]), any abelian variety $X$ defined over a finite field has sufficiently many complex multiplications. However the converse is not quite true, as Grothendieck showed (see [66]): an abelian variety $X$ with smCM is isogenous to an abelian variety defined over a finite extension of the prime field (but $X$ need not be defined over a finite field in the case of finite characteristic, see Appendix A.3 for more details). In particular:
- For every $g \geq 2$ there exist positive dimensional non-trivial families of supersingular abelian varieties, in other words: in these cases there exist supersingular abelian varieties not defined over a finite field, but they are isogenous to an abelian variety defined over a finite field, e.g. to $E^g$, where $E$ is a supersingular elliptic curve .
- In fact, for integers $g \geq 2$ and $f$ with $0 \leq f \leq g-2$ there exist abelian varieties in characteristic $p > 0$ of dimension $g$, with $p$-rank equal to $f$, which have smCM, but which cannot be defined over a finite field.

**Newton polygons** (not used in this book). Using Dieudonné-Manin theory one can define for every abelian variety (of dimension $g$) in characteristic $p$ its *Newton polygon* (NP). This is a polygon which starts at $(0,0)$, ends at $(2g,g)$, which is lower convex, and has break points with integral coordinates. Moreover for the slope $\lambda$ of every side of this polygon we have $0 \leq \lambda \leq 1$. In fact ordinary abelian varieties are characterized by the fact that the NP has $g$ slopes equal to 0, and $g$ slopes equal to 1. Supersingular abelian varieties turn out to be characterized by the fact that all $2g$ slopes are equal to $1/2$. Any other of these Newton Polygons is between these two. We see that from this point of view the ordinary abelian varieties are the most general ones, and the supersingular ones, studied in this book, are the most particular ones.

N.B. *We should mention results previously obtained, we should acknowledge contributions to this topic made in the past. In order not to overburden this short*

*introduction, this will be done in the Appendix of this book, where we give a historical survey of (part of) this topic.*

**Convention.** In the text we use the section numbers to index definitions, theorems, remarks etc., for example Lemma 6.1 means the lemma in 6.1.

**Acknowledgements.**

We wish to thank especially T. Ekedahl, K. Feng, T. Ibukiyama, A.J. de Jong, T. Katsura, W.C. Winnie Li, A. Ogus, and many other colleagues for valuable discussions, suggestions, and their patience in listening to our supersingular expositions.

The first author wishes to thank the constant support of National Science Foundation Committee (NSFC) of China and the support of Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO) of The Netherlands, also wishes to thank the University of Utrecht for the hospitality and the stimulating environment of mathematical research. In 1991 the first author was invited by Prof. T. Oda and Prof. M. Miyanishi to visit Japan, and gave a special talk on the result of this text in the annual meeting of the Mathematical Society of Japan (MSJ). This enabled him to discuss with several specialists on this topic. He also wishes to thank MSJ, Tohoku University and Osaka University for their support and hospitality.

The second author wishes to thank T. Oda and T. Katsura for many years of growing results on this topic.

The main material for this book originated several years ago, and we feel we should apologize that the publication was somewhat slow.

# 1. Supersingular abelian varieties

Throughout this book we will denote by $p$ a prime number, which is fixed unless otherwise specified. We denote by $K$ a field of characteristic $p$ and by $k$ an algebraically closed field containing $K$. For any $K$-scheme $X$ and any field extension $K' \supset K$, we will denote $X \times_{\mathrm{Spec}(K)} \mathrm{Spec}(K')$ simply by $X \otimes_K K'$, or even $X \otimes K'$ if there is no confusion.

In this chapter every scheme is defined over some $K$, unless otherwise specified.

## 1.1. Supersingular elliptic curves.

Let $E$ be an elliptic curve over $K$. Then either $E$ has a geometric point of order exactly $p$ and $E$ is called *ordinary*, or $E$ has no geometric point of order $p$ and $E$ is called *supersingular*.

It is well known that the number of isomorphism classes of supersingular elliptic curves over $k$ is finite (the number is roughly $p/12$ and $\leq [p/12]+2$, cf. [23, Corollary IV.4.23], see (9.1.4) for an exact formula), and any two supersingular elliptic curves over $k$ are isogenous (i.e., there exists a finite-to-one morphism from one to the other, cf. [9, p. 252]).

## 1.2. Endomorphism algebra of supersingular elliptic curves.

For every prime number $p$ there exists an elliptic curve $E$ over the prime field $\mathbf{F}_p$ such that its relative Frobenius

$$F : E \to E^{(p)} \cong E \tag{1.2.1}$$

satisfies

$$F^2 + p = 0 \tag{1.2.2}$$

(cf. [97, pp. 139-140], [98, p. 96], [100, Theorem 4.1.5]). For the rest of this book we fix a choice of such an $E$ over $\mathbf{F}_p$ for each $p$. Note that $E$ has the property

$$\mathrm{rank}_{\mathbf{Z}}(\mathrm{End}(E)) = 2 \tag{1.2.3}$$

and

$$\mathcal{O} := \mathrm{End}(E \otimes \mathbf{F}_{p^2}) = \mathrm{End}(E \otimes k) \tag{1.2.4}$$

has rank 4 over $\mathbf{Z}$; it is a maximal order in the quaternion algebra

$$B := \mathrm{End}^0(E \otimes k) = \mathrm{End}(E \otimes k) \otimes \mathbf{Q} \cong Q_{\infty,p} \tag{1.2.5}$$

which is split at every prime number $l \neq p$ (see [9, p.199]).

### 1.3. $p$-divisible groups and duality.

Fix a base scheme $S$. For a commutative group scheme $\pi : G \to S$ and any positive integer $n$, we will denote

$$G[n] := \ker(n_G : G \to G) \tag{1.3.1}$$

where $n_G = n \cdot \mathrm{id}_G$ is the multiplication by $n$.

If $\pi$ is flat and finite, we denote by $G^D$ the Cartier dual of $G$ over $S$, i.e. the structure $O_S$-algebra of $G^D$ is isomorphic to $\mathcal{H}om_{O_S}(\pi_* O_G, O_S)$, the dual Hopf algebra of $\pi_* O_G$ over $O_S$ (cf. e.g. [64, I.2]).

Let $\mathfrak{C}_S^1$ be the category of flat finite commutative group schemes over $S$ whose ranks are powers of $p$. Let $\mathfrak{C}_S$ be the category of formal inductive limits in $\mathfrak{C}_S^1$:

$$G = \varinjlim_n G_n \tag{1.3.2}$$

satisfying

a) $G_n = G_{n+1}[p^n]$ for each $n$.

Such a $G$ is called a *commutative formal group*, and it is called a *p-divisible group* if in addition that

b) $p_G$ is an epimorphism.

Condition b) is equivalent to that the homomorphism $G_{n+1} \to G_n$ induced by $p_G$ is an epimorphism for each $n$, in this case we have induced monomorphisms $G_n^D \hookrightarrow G_{n+1}^D$ and we denote

$$G^t = \varinjlim_n G_n^D, \tag{1.3.3}$$

called the *Serre dual* of $G$.

An *isogeny* of $p$-divisible groups is an epimorphism with finite kernel. If there is an isogeny from $G$ to $G'$, then we say $G$ and $G'$ are *isogenous* to each other, denoted by $G \sim G'$.

### 1.4. The formal isogeny type of an abelian variety.

For an abelian scheme $X$ over $S$ we define:

$$\varphi_p X := \varinjlim_i (X[p^i]). \tag{1.4.1}$$

(Sometimes this is denoted by $X[p^\infty]$.) This is a $p$-divisible group, called the *Barsotti-Tate group* of $X$.

Denote by $X^t$ the dual abelian scheme of $X$. Clearly we have $\varphi_p(X^t) \cong (\varphi_p X)^t$ (see (1.3.3) and [56, III.15]).

Over an algebraically closed field $k$, the $p$-divisible groups have been classified up to isogeny by the Dieudonné-Manin theory. For the case of Barsotti-Tate groups we have:

$$\varphi_p X \sim \sum_i (G_{m_i,n_i} \oplus G_{n_i,m_i}) \bigoplus G_{1,1}^{\oplus s} \bigoplus (G_{1,0} \oplus G_{0,1})^{\oplus f} \qquad (m_i > n_i > 0,\ \text{g.c.d.}(m_i, n_i) = 1); \tag{1.4.2}$$

here $G_{m,n}$ is a simple $p$-divisible group over $k$ (see [48, p.37]) which has the following properties: $\dim_k \mathrm{Lie}(G_{m,n}) = m$ and $\dim_k \mathrm{Lie}(G^t_{m,n}) = n$ (cf. (2.1)). Such a decomposition (up to isogeny) is called a *formal isogeny type*. (The symmetry in (1.4.2) is called the "Manin symmetry condition".) We say that this formal isogeny type is

$$\textbf{supersingular} \text{ iff } \varphi_p X \sim G_{1,1}^{\oplus g}$$

where $g = \dim(X)$. In general, an abelian variety $X$ over $K$ is called *supersingular* if $\varphi_p(X \otimes_K k)$ is supersingular.

**Convention:** The $p$-divisible group $G_{m,n}$ is defined over $\mathbb{F}_p$, however for any field extension $\mathbb{F}_p \subset K$ we shall write $G_{m,n}$ instead of $G_{m,n} \otimes K$. The same for $\alpha_p$, $\mu_p$, $\mathbb{G}_a$, $\mathbb{G}_m$, in case no confusion can arise.

### 1.5. The $a$-number.

For a commutative group scheme $X$ over a field $K$ we define

$$a(X) = \dim_K \mathrm{Hom}(\alpha_p, X). \tag{1.5.1}$$

If $K \subset K'$ then

$$\dim_K \mathrm{Hom}(\alpha_p, X) = \dim_{K'} \mathrm{Hom}(\alpha_p, X \otimes K'), \tag{1.5.2}$$

i.e. the $a$-number does not depend on the field we are working over. Furthermore, there is a smallest subgroup scheme $A(X) \subset X$ containing all of the images of $\alpha_p \to X$; note that its rank is $p^{a(X)}$ (see 2.5).

### 1.6. A characterization of supersingularity.

Supersingular abelian varieties are distinguished from other abelian varieties by the following property. For any formal isogeny type which is not supersingular, there exists a simple abelian variety over $k$ having this formal isogeny type (cf. [44, p.47]). However for supersingular formal isogeny types with $g \geq 2$ the situation is different:

**Fact.** *Let $X$ be an abelian variety of dimension $g \geq 2$. Then*
*i) $X$ is supersingular if and only if $X \otimes k \sim E^g \otimes k$, thus:*

$$\varphi_p(X \otimes k) \sim G_{1,1}^g \iff X \otimes k \sim E^g \otimes k;$$

ii) $$a(X) = g \iff X \otimes k \cong E^g \otimes k.$$

The first statement can be found in [67, Theorem 4.2]. For the second statement one uses [69, Theorem 2]: we see that $a(X) = g$ iff $X \otimes k$ is isomorphic to a product $E_1 \times ... \times E_g$ of supersingular elliptic curves over $k$; by a theorem due to Deligne (using a calculation by Eichler) and to Ogus (cf. [62, Theorem 6.2] and [95, Theorem 3.5]), we know that for any $g \geq 2$ and any supersingular elliptic curves $E_1, ..., E_{2g}$ over $k$,

$$E_1 \times ... \times E_g \cong E_{g+1} \times ... \times E_{2g}. \tag{1.6.1}$$