Computing abelian varieties over finite fields

Stefano Marseglia

Academic dissertation for the Degree of Doctor of Philosophy in Mathematics at Stockholm University to be publicly defended on Friday 8 June 2018 at 13.00 in sal 14, hus 5, Kräftriket, Roslagsvägen 101.

Abstract

In this thesis we address the problem of developing effective algorithms to compute isomorphism classes of polarized abelian varieties over a finite field and of fractional ideals of an order in a finite product of number fields.

There are well-known methods to efficiently compute the classes of invertible ideals of an order in a number field, but not much has previously been known about non-invertible ideals. In Paper I we produce algorithms to compute representatives of all ideal classes of an order in a finite product of number fields. We also extend a theorem of Latimer and MacDuffee about conjugacy classes of integral matrices.

There are equivalences established by Deligne and Centeleghe-Stix between the category of abelian varieties over a finite field and the category of finitely generated free abelian groups with an endomorphism satisfying some easy-to-state axioms, which in certain cases can be described in terms of fractional ideals of orders in finite products of number fields. In Paper II we use this method to produce an algorithm that computes the isomorphism classes of abelian varieties in an isogeny class determined by an ordinary square-free q-Weil polynomial or by a square-free p-Weil polynomial with no real roots (where p denotes a prime and q is a power of a prime). In the ordinary case we also produce an algorithm that computes the polarizations up to isomorphism and the automorphism groups of the polarized abelian varieties. If the polarization is principal, we can compute a period matrix of the canonical lift of the abelian variety.

In Paper III we extend the description of the second paper to the case when the Weil polynomial is a power of a square-free polynomial which fulfills the same requirements as in Paper II.

In Paper IV we use the results of the second and third papers to study questions related to base-field extension of the abelian varieties over finite fields.

Keywords: *abelian varieties, finite fields, period matrices, ideal classes, orders, number fields, integral matrices.*

Stockholm 2018
http://urn.kb.se/resolve?urn=urn:nbn:se:su:diva-154874

ISBN 978-91-7797-274-7
ISBN 978-91-7797-275-4

Department of Mathematics

Stockholm University, 106 91 Stockholm

COMPUTING ABELIAN VARIETIES OVER FINITE FIELDS

Stefano Marseglia

Stockholm
University

Computing abelian varieties over finite fields

Stefano Marseglia

ISBN print 978-91-7797-274-7
ISBN PDF 978-91-7797-275-4

Printed in Sweden by Universitetsservice US-AB, Stockholm 2018
Distributor: Department of Mathematics, Stockholm University

Abstract

In this thesis we address the problem of developing effective algorithms to compute isomorphism classes of polarized abelian varieties over a finite field and of fractional ideals of an order in a finite product of number fields.

There are well-known methods to efficiently compute the classes of invertible ideals of an order in a number field, but not much has previously been known about non-invertible ideals. In Paper I we produce algorithms to compute representatives of all ideal classes of an order in a finite product of number fields. We also extend a theorem of Latimer and MacDuffee about conjugacy classes of integral matrices.

There are equivalences established by Deligne and Centeleghe-Stix between the category of abelian varieties over a finite field and the category of finitely generated free abelian groups with an endomorphism satisfying some easy-to-state axioms, which in certain cases can be described in terms of fractional ideals of orders in finite products of number fields. In Paper II we use this method to produce an algorithm that computes the isomorphism classes of abelian varieties in an isogeny class determined by an ordinary square-free q-Weil polynomial or by a square-free p-Weil polynomial with no real roots (where p denotes a prime and q is a power of a prime). In the ordinary case we also produce an algorithm that computes the polarizations up to isomorphism and the automorphism groups of the polarized abelian varieties. If the polarization is principal, we can compute a period matrix of the canonical lift of the abelian variety.

In Paper III we extend the description of the second paper to the case when the Weil polynomial is a power of a square-free polynomial which fulfills the same requirements as in Paper II.

In Paper IV we use the results of the second and third papers to study questions related to base-field extension of the abelian varieties over finite fields.

Sammanfattning

I denna avhandling försöker vi utveckla en effektiv algoritm för att beräkna isomorfiklasser av polariserade abelska varieteter över en ändlig kropp och av fraktionsideal till en talring i en ändlig produkt av talkroppar.

Det finns väletablerade metoder för att effektivt beräkna klasserna av inverterbara ideal till en talring i en talkropp, men inte så mycket har tidigare varit känt när det gäller fallet med icke-inverterbara ideal. I Artikel I skapar vi algoritmer för att beräkna representanter till alla idealklasser till en talring i en ändlig produkt av talkroppar. Vi generaliserar också en sats av Latimer och MacDuffee om konjugatklasser av matriser med heltalskoefficienter.

Det finns ekvivalenser som skapats av Deligne och Centeleghe-Stix mellan kategorin av abelska varieteter över ett ändlig kropp och kategorin av ändligtgenererade fria abelska grupper med en endomorfi som uppfyller ett antal lättformulerade axiom som i vissa fall kan beskrivas i termer av fraktionsideal till talringar i ändliga produkter av talkroppar. I Artikel II använder vi denna metod för att skapa en algoritm som beräknar isomorfiklasserna av abelska varieteter i en isogeniklass bestämd av ett ordinärt kvadratfritt q-Weilpolynom eller bestämd av ett kvadratfritt p-Weilpolynom utan reella rötter (där p är ett primtal och q är en primtalspotens). I det ordinära fallet så skapar vi också en algoritm som beräknar polariseringar upp till isomorfi och även automorfigruppen till de polariserade abelska varieteterna. Om det är fråga om en huvudpolarisering så beräknar vi också en periodmatris till den kanoniska lyftningen av den abelska varieteten.

I Artikel III utvidgar vi beskrivningen från Artikel II till fallet när Weilpolynomet är en potens av ett kvadratfritt polynom (och där det kvadratfria polynomet har samma restriktioner som i Artikel II).

I Artikel IV använder vi resultaten från Artikel II och III för att studera frågor om baskroppsutvidningar av abelska varieteter över ändliga kroppar.

List of Papers

The following papers, referred to in the text by their Roman numerals, are included in this thesis.

PAPER I: **Computing the ideal class monoid of an order**
Stefano Marseglia

PAPER II: **Computing square-free polarized abelian varieties over finite fields**
Stefano Marseglia

PAPER III: **Computing abelian varieties over finite fields isogenous to a power**
Stefano Marseglia

PAPER IV: **Computing base extensions of ordinary abelian varieties over a finite field**
Stefano Marseglia

Contents

Acknowledgements

First and foremost I would like to express my gratitude to my supervisor Jonas Bergström. The full list of reasons for which I am thankful to Jonas won't fit in one single page, so, with my heart burdened by this constrain, I thank him for his joy and enthusiasm, for his knowledge and for his wisdom. I have learned a lot from him and his example has made me grow both as a mathematician and as a person. I'll never forget the excitement that we shared while staring at the screen, waiting to see if the results of our computations matched our expectations and I apologize for all the Italian swear words that I taught him when the output was not the desired one.

I would also like to thank the current and former members of the Algebra group for creating a stimulating atmosphere where learning and doing mathematics is a very pleasant and fun job.

I am grateful to all the present and former members of the department for making it a lovely place where to work. Their professionalism made the job easier and their warmth and caring made the department feel like a big family.

I have been very fortunate for all the friends that I found in Stockholm, inside the department, at the klättercenter, in Lappis, and...well...everywhere in the city. You made the last years great fun! I'll never forget all the moments we have shared together. A big hug goes to my friends back in Italy and around the world, both in the mathematical world and outside, for being the living proof that distance cannot break real friendship.

Finally, I want to thank my family and in particular my parents Lello and Maru: you started all of this by instilling in me determination, ambition, curiosity and, with the help of a couple of great teachers, love for science. Thanks for all the love and encouragement during the difficult times and also for helping to celebrate when those were over.

Introduction

In this thesis we address the problem of developing an effective algorithm to compute isomorphism classes of polarized abelian varieties over a finite field $\mathbb{F}_q$ and their automorphisms, where q is a power of a prime number p. Our results are presented in the form of four papers, a summary of which can be found at the end of this introduction. These results are implemented in a series of algorithms in Magma [BCP97] which are available on the webpage of the author.

In general, abelian varieties have a very rich algebraic structure due to the fact that their set of points forms a group. In dimension greater than one it is difficult to find equations describing abelian varieties as subvarieties of a projective space. Even if we don't have equations to work with, it is often possible to attach some "concrete" object to an abelian variety. For example, an abelian variety over $\mathbb{C}$ of dimension g is isomorphic to $\mathbb{C}^g/L$, where L is a full lattice of rank $2g$. The lattice L encodes the algebraic properties of A, which then can be studied with multi-linear algebra techniques. When we move from $\mathbb{C}$ to the wilder realm of positive characteristic, it is not possible to functorially attach a lattice of rank $2g$ to the whole category of abelian varieties. This is a consequence, as Serre pointed out, of the existence of objects such as supersingular elliptic curves, whose endomorphism algebras are quaternion algebras and hence do not admit a 2-dimensional representation.

Nevertheless, when our field of definition is a finite field we can restrict our attention to a subcategory and obtain similar results to the ones over the complex numbers. Deligne [Del69] proved that there is an equivalence between the category of ordinary abelian varieties over $\mathbb{F}_q$ and the category of finitely generated free $\mathbb{Z}$-modules satisfying certain easy-to-state axioms. Howe then described, in the article [How95], the dual variety and polarizations in Deligne's category. Deligne's equivalence has recently been extended in [CS15] by Centeleghe and Stix to a larger subcategory, but Howe's description of polarizations does not apply.

In order to count the isomorphism classes of abelian varieties over $\mathbb{F}_q$, we first fix an isogeny class, which by Honda-Tate theory corresponds to fixing a conjugacy class of Frobenius and hence a q-Weil polynomial h, see [Tat66]

and [Hon68]. Under some assumptions on h, we can reduce our computation to determining the isomorphism classes of fractional ideals of an order R in a product of number fields. The main issue is that the order R does not need to be maximal and hence there might be non-invertible ideal classes. If there are effective algorithms to compute the group of classes of invertible fractional ideals, not much is known about the non-invertible ones and the monoid that they form. In this thesis we will first study a computationally easier problem, namely the computation of the weak equivalence class monoid, and then we will describe how to effectively construct a complete set of representatives of the isomorphism classes of fractional ideals of the order, which also returns the isomorphism classes of the abelian varieties in the isogeny class. If the isogeny class is ordinary we also describe, in this ideal theoretic setting, the dual of a variety, the polarizations and the automorphisms of a polarized abelian variety.

Apart from giving concrete examples to test conjectures, counting isomorphism classes of principally polarized abelian varieties of dimension g over a finite field with their automorphisms groups gives cohomological information about the corresponding moduli space $\mathcal{A}_g$. Using the close relation between the moduli space $\mathcal{M}_g$ of curves of genus g and $\mathcal{A}_g$ for $g = 1,2,3$ it is possible to produce these data using the equations of the curves, see for example [BFvdG14]. But, by using this approach, it is not possible to get complete information for higher g, hence the need to develop a new method to directly count the abelian varieties. Furthermore, our point counts on $\mathcal{A}_g$ over finite fields shed light on the stratification of such moduli spaces with respect to invariants like the Newton polygons and the p-rank, which are far from being understood in their totality.

The goal of this introduction is to give an overview of the basic theory of abelian varieties. The reader should be advised that this does not intend to be a comprehensive overview of the subject, but a summary of the prerequisites necessary to understand the objects that are going to be studied in the papers.

The introduction is structured as follows. In Section 1 we recall the notion of abelian variety over any field k and their basic properties. In Sections 2 and 3 we focus respectively on the cases $k = \mathbb{C}$ and k with positive characteristic, in particular $k = \mathbb{F}_q$. Finally in Section 4 we give a brief overview of the results contained in the papers. The material in Sections 1, 2 and 3 is adapted from the licentiate thesis [Mar16].

We made the choice of not discussing the theory of orders and fractional ideals in this introduction since we give a complete and self-contained overview in the beginning of Paper I.

1 Abelian Varieties

Notation

Let k' be an extension of a field k. For an algebraic variety V over k we denote by $V(k')$ the set of points of V defined over k' and by $V_{k'}$ the base field extension $V \otimes_k k'$ of V to k'. We write $\bar{k}$ for the algebraic closure of k.

1.1 Basic definitions

In this section we recall the definitions and the basic properties of abelian varieties which are the main object of interest of this thesis. Even if we perform our computations over finite fields, the general theory is presented over an arbitrary field k. Unless otherwise specified, we will follow [CS86, J.S. Milne, Abelian Varieties, Chapter V] and we refer to it for the proofs.

Definition 1.1. *A* group variety *over a field k is a variety V together with morphisms*

$$m : V \times V \to V \text{ and } i : V \to V,$$

and a point $\varepsilon \in V(k)$ such that the structure on $V(\bar{k})$ defined by m and i is that of a group with multiplication induced by m, inverse by i and identity element ε.

Equivalently, we can say that the quadruple (V, m, i, ε) is a group object in the category of varieties over k.

For every geometric point $a \in V(\bar{k})$, the projection $V_{\bar{k}} \times V_{\bar{k}} \to V_{\bar{k}}$ induces an isomorphism $V_{\bar{k}} \times \{a\} \simeq V_{\bar{k}}$. We define the *translation t_a by a* as the composition

$$V_{\bar{k}} \simeq V_{\bar{k}} \times \{a\} \subset V_{\bar{k}} \times V_{\bar{k}} \xrightarrow{m} V_{\bar{k}}.$$

On points t_a acts as $P \mapsto m(P, a)$. In particular if $a \in V(k)$ then t_a maps V into V.

For any variety the non-singular locus U is open and non-empty, see [Har77, Theorem 5.3]. For a group variety V the translates of $U_{\bar{k}}$ cover $V_{\bar{k}}$, hence every group variety is non-singular.

Definition 1.2. *A connected and complete group variety is called an* abelian variety.

In the next proposition we will sum up some interesting properties of abelian varieties.

Proposition 1.3. *Let A be any abelian variety. Then*

- *every morphism $f : A \to B$ of abelian varieties is the composite of a homomorphism $h : A \to B$ with a translation t_b, where $b = -f(0) \in B(k)$;*
- *the group law on A is commutative;*
- *for every group scheme G, every rational map $g : G \dashrightarrow A$ is the composite of a homomorphism $h' : G \to A$ with a translation t_a, where $a = -g(0) \in A(k)$;*
- *A is projective.*

Example 1.4. *An abelian variety of dimension one is the same as an* elliptic curve *E, that is, a smooth projective plane curve of degree 3 together with a chosen point. It is easy to describe elliptic curves embedded in a projective space in terms of equations. For example, if the characteristic of k is not 2 or 3 then E inside $\mathbb{P}^2 = \operatorname{Proj} k[x,y]$ is given by an equation of the form*

$$zy^2 = x^3 + axz^2 + bz^3,$$

for some $a, b \in k$ such that $4a^3 + 27b^2 \neq 0$ with marked point $(0:1:0)$. In this case it is possible to give explicit formulas for the addition of two points. The theory of elliptic curves is very rich and many results about them can be generalized to the higher dimensional case, but they will have a much more abstract flavor, since in general it is hard to find equations describing an abelian variety.

1.2 Isogenies

Among all morphisms between abelian varieties, the so-called isogenies play a special role since they allow us to split each abelian variety into a product of simple objects, see Corollary 1.18. In particular, over a finite field, we can classify and enumerate up to isogeny all abelian varieties of a given dimension, as we explain in Section 3.

Proposition 1.5. *Let $f : A \to B$ be a homomorphism of abelian varieties. The following are equivalent:*

1. *f is surjective and $\dim(A) = \dim(B)$;*
2. *$\ker(f)$ is a finite group scheme and $\dim(A) = \dim(B)$;*
3. *f is finite, flat and surjective.*

Definition 1.6. *A homomorphism $f : A \to B$ satisfying the conditions of 1.5 is called an* isogeny. *The* degree *of an isogeny is the degree of the function field extension $[k(A) : k(B)]$.*

Equivalently we can define the degree of an isogeny as the rank of its kernel as a group scheme. Observe that the composition of two isogenies is an isogeny and the degree is multiplicative with respect to composition.

Let n be a non-zero integer and consider the homomorphism multiplication by n, $[n]_A : A \to A$. Write $A[n] := \ker([n]_A)$.

Proposition 1.7. *The homomorphism $[n]_A$ is an isogeny. If $g = \dim(A)$ then $\deg([n]_A) = n^{2g}$.*

Proposition 1.8. *If $f : A \to B$ is an isogeny of degree d, then there exists an isogeny $g : B \to A$ such that $g \circ f = [d]_A$ and $f \circ g = [d]_B$.*

1.3 Dual abelian varieties and polarizations

For an abelian variety A we denote with $\mathrm{Pic}(A)$ the group of isomorphism classes of invertible sheaves on A with multiplication given by the tensor product. We will denote with $m : A \times A \to A$ (resp. p and q) the multiplication (resp. the projection on the first and second factor). An invertible sheaf on $A \times A$ can be considered as a family of invertible sheaves on the first factor A parametrized by the second factor A.

Let $\mathcal{L}$ be an invertible sheaf on A. It is an important fact that the map

$$\varphi_{\mathcal{L}} : A(k) \to \mathrm{Pic}(A) \qquad a \mapsto t_a^* \mathcal{L} \otimes \mathcal{L}^{-1}$$

is a homomorphism. Define

$$K_{\mathcal{L}} = \left\{ a \in A : \text{ the restriction of } m^* \mathcal{L} \otimes q^* \mathcal{L}^{-1} \text{ to } \{a\} \times A \text{ is trivial} \right\}.$$

Note that $K_{\mathcal{L}}$ is a reduced sub-scheme of A. After some obvious identifications we find that

$$K_{\mathcal{L}}(k) = \{ a \in A(k) : t_a^* \mathcal{L} \simeq \mathcal{L} \}.$$

Observe that the definition of $K_{\mathcal{L}}$ commutes with change of base field.

Proposition 1.9. *For an invertible sheaf $\mathcal{L}$ on A, the following conditions are equivalent:*

1. $K_{\mathcal{L}} = A$
2. $t_a^* \mathcal{L} \simeq \mathcal{L}$ *on* $A_{\bar{k}}$ *for every* $a \in A(\bar{k})$
3. $m^* \mathcal{L} \simeq p^* \mathcal{L} \otimes q^* \mathcal{L}$.

We define $\mathrm{Pic}^0(A)$ as the subgroup of $\mathrm{Pic}(A)$ consisting of isomorphism classes of invertible sheaves satisfying one of the equivalent conditions of 1.9.

Definition 1.10. *Let A and $A^\vee$ be abelian varieties and $\mathcal{P}$ an invertible sheaf on $A \times A^\vee$. We call $A^\vee$ the* dual *abelian variety of A and $\mathcal{P}$ the* Poincaré *sheaf if:*

1. *$\mathcal{P}|_{\{0\}\times A^\vee}$ is trivial and $\mathcal{P}|_{A\times\{a\}}$ lies in $\mathrm{Pic}^0(A_{k(a)})$ for all $a \in A^\vee$;*
2. *for every (finite) k-scheme T and invertible sheaf $\mathcal{L}$ on $A \times T$ such that $\mathcal{L}|_{\{0\}\times T}$ is trivial and $\mathcal{L}|_{A\times\{t\}}$ lies in $\mathrm{Pic}^0(A_{k(t)})$ for all $t \in T$, there is a unique morphism $f : T \to A^\vee$ such that $(1 \times f)^*\mathcal{P} \simeq \mathcal{L}$.*

It follows immediately from the definition that if the pair $(A^\vee, \mathcal{P})$ exists, then it is unique up to a unique isomorphism and that the formation of the dual abelian variety commutes with change of base field. Moreover, one can prove that $A^{\vee\vee} = A$. The proof of the existence of the dual abelian variety together with $\mathcal{P}$ is rather involved and we refer to [Mum08]. For us, it will suffice to think of it as an abelian variety of the same dimension as A such that $A^\vee(\bar{k}) = \mathrm{Pic}^0(A_{\bar{k}})$.

Let $f : A \to B$ be a homomorphism of abelian varieties and let $\mathcal{P}_B$ be the Poincaré sheaf on $B \times B^\vee$. The invertible sheaf $(f \times 1)^*\mathcal{P}_B$ on $A \times B^\vee$ gives rise to a homomorphism $f^\vee : B^\vee \to A^\vee$ such that $(1 \times f^\vee)^*\mathcal{P}_A \simeq (f \times 1)^*\mathcal{P}_B$. On points, $f^\vee$ is simply the map $\mathrm{Pic}^0(B) \to \mathrm{Pic}^0(A)$ sending the class of an invertible sheaf to its inverse image.

Theorem 1.11. *Let $f : A \to B$ be an isogeny with kernel N. The exact sequence*

$$0 \to N \to A \to B \to 0$$

gives rise to a dual exact sequence

$$0 \to N^\vee \to B^\vee \to A^\vee \to 0,$$

where $N^\vee$ is the Cartier dual of the group scheme N.

Definition 1.12. *A* polarization λ *on an abelian variety A is an isogeny $\lambda : A \to A^\vee$ such that $\lambda_{\bar{k}} = \varphi_{\mathcal{L}}$ for some ample invertible sheaf $\mathcal{L}$ on $A_{\bar{k}}$, where $\varphi_{\mathcal{L}}$ is the map $A(k) \to \mathrm{Pic}(A)$ defined by $a \mapsto t_a^*\mathcal{L} \otimes \mathcal{L}^{-1}$. The* degree *of a polarization is its degree as an isogeny. A pair (A, λ) is called a* polarized abelian variety *and when we talk about morphisms between them we require the obvious compatibility of the polarizations. If λ has degree 1, that is, λ is an isomorphism, then λ is called* principal.

Roughly speaking, a polarization of A encodes information about how A embeds into a projective space. This data is more explicit in the case $k = \mathbb{C}$, see Section 2.

Let the *Néron-Severi group* $\mathrm{NS}(A)$ of A be the quotient $\mathrm{Pic}(A)/\mathrm{Pic}^0(A)$. Observe that the map $\mathcal{L} \mapsto \varphi_{\mathcal{L}}$ defines an injection $\mathrm{NS}(A) \hookrightarrow \mathrm{Hom}(A, A^\vee)$. Assume that λ is a polarization, that k is perfect and put $G = \mathrm{Gal}(\bar{k}/k)$. There need not be an invertible sheaf $\mathcal{L}$ on A such that $\lambda = \varphi_{\mathcal{L}}$, but we know that there exists an $\mathcal{L}$ on $A_{\bar{k}}$ such that $\lambda_{\bar{k}} = \varphi_{\mathcal{L}}$. Observe that $\lambda_{\bar{k}}$ is fixed by the action of G on $\mathrm{Hom}(A_{\bar{k}}, A^\vee_{\bar{k}})$, but this does not mean that the class of $\mathcal{L}$ lifts to $\mathrm{Pic}(A)$. Indeed we have a sequence of Galois cohomology groups

$$0 \to A^\vee(k) \to \mathrm{Pic}(A) \to \mathrm{NS}(A_{\bar{k}})^G \to H^1(G, A^\vee(\bar{k}))$$

and the obstruction in $H^1(G, A^\vee(\bar{k}))$ might be non-zero. However, if k is finite then it is possible to prove that $H^1(G, A^\vee(\bar{k})) = 0$ and therefore $\lambda = \varphi_{\mathcal{L}}$.

Example 1.13. *Let E be an elliptic curve over k. We have that $E \simeq E^\vee$ and there exists a unique principal polarization up to isomorphism.*

1.4 Endomorphisms

Let A and B be abelian variety over the field k. If f and g are homomorphisms from A to B then we can define a morphism

$$f + g = m_B \circ (f, g) : A \xrightarrow{(f,g)} B \times_k B \xrightarrow{m_B} B.$$

This shows that $\mathrm{Hom}_k(A, B)$ has the structure of an abelian group and that $\mathrm{End}_k(A)$ has a ring structure with composition as multiplication.

If $n \in \mathbb{Z}$ and $f \in \mathrm{Hom}_k(A, B)$ then $n \circ f = [n]_B \circ f = f \circ [n]_A$. If $n \neq 0$ then $[n]_A$ is an isogeny and it is in particular surjective. This implies that $\mathrm{Hom}_k(A, B)$ is torsion-free. We define

$$\mathrm{Hom}^0_k(A, B) = \mathrm{Hom}_k(A, B) \otimes_{\mathbb{Z}} \mathbb{Q} \text{ and } \mathrm{End}^0_k(A) = \mathrm{End}_k(A) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

The $\mathbb{Q}$-algebra $\mathrm{End}^0_k(A)$ is called the *endomorphism algebra* of A. Observe that every isogeny $f : A \to B$ becomes invertible in $\mathrm{Hom}^0_k(A, B)$.

Theorem 1.14 (Poincaré Splitting Theorem)**.** *Let A be an abelian variety over a field k. If $B \subset A$ is an abelian sub-variety then there exists an abelian sub-variety $C \subset A$ such that the homomorphism $f : B \times C \to A$ given by $(x, y) \mapsto x + y$ is an isogeny.*

Definition 1.15. *An abelian variety A over the field k is* simple *if it does not have non-trivial sub-varieties, that is, if $B \subset A$ is a sub-variety, then $B = 0$ or $B = A$.*

Remark 1.16. *Let $f : A \to B$ be a homomorphism between abelian varieties. If A and B are simple then f is either zero or an isogeny.*

Let k' be a field extension of k. An abelian variety defined over k and which is simple over k need not be simple also over k'.

Example 1.17. *Let q be a power of a prime number and let a be an integer such that $|a| < 2\sqrt{q}$ and coprime with q. Take an elliptic curve E over $\mathbb{F}_{q^2}$ in the isogeny class determined by the polynomial $x^2 + ax + q^2$, see Section 3 for the definition. Let A be the Weil restriction $\mathrm{Res}(\mathbb{F}_{q^2}/\mathbb{F}_q, E)$ of E to $\mathbb{F}_q$. By our assumptions on a, we see that the characteristic polynomial of Frobenius $x^4 + ax^2 + q$ of A is irreducible. Hence A is simple over $\mathbb{F}_q$, but it is isogenous to $E \times E^{(q)}$ over $\mathbb{F}_{q^2}$, where $E^{(q)}$ is the $\mathbb{F}_q$-conjugate of E.*

Corollary 1.18. *Every non-zero abelian variety A over k is isogenous to a product of simple abelian varieties over k. More precisely, there exist k-simple abelian varieties $B_1, \ldots, B_r$, pairwise non-isogenous, and positive integers m_i, such that*

$$A \sim_k B_1^{m_1} \times \ldots \times B_r^{m_r}.$$

This decomposition is unique up to permutation of the indices.

1.5 The Rosati involution

Fix a polarization λ on A. Since λ is an isogeny $\lambda : A \to A^\vee$ it has an inverse in $\mathrm{Hom}^0(A^\vee, A)$.

Definition 1.19. *The* Rosati involution *on* $\mathrm{End}^0(A)$ *corresponding to* λ *is*

$$\alpha \mapsto \alpha^\dagger := \lambda^{-1} \circ \alpha^\vee \circ \lambda.$$

Theorem 1.20. *The bilinear form*

$$\mathrm{End}^0(A) \times \mathrm{End}^0(A) \to \mathbb{Q} \qquad (\alpha, \beta) \mapsto \mathrm{Tr}(\alpha \circ \beta^\dagger)$$

is positive definite.

This implies the following.

Proposition 1.21. *If λ is a polarization of the abelian variety A, then the automorphism group of (A, λ) is finite.*

2 Abelian varieties over $\mathbb{C}$

In the present section we focus on the case $k = \mathbb{C}$. In the complex setting many concepts introduced in the precious section assume a less abstract flavor and hence are easier to visualize. Nevertheless, we are not deviating from our

purpose of calculating the abelian varieties defined over finite fields. Indeed most abelian varieties over a finite field $\mathbb{F}_q$, namely the ordinary ones, can be canonically lifted to the ring of Witt vectors $W(\mathbb{F}_q)$, which has characteristic zero. After fixing an isomorphism $\overline{\mathbb{Q}}_p \simeq \mathbb{C}$ we can extend the scalars and end up working with complex abelian varieties. This procedure is the core of the equivalence of categories defined in [Del69] which will be our main tool to study and compute the abelian varieties over $\mathbb{F}_q$, as we explain in more detail in Section 3.

Let A be an abelian variety over $\mathbb{C}$. Then $A(\mathbb{C})$ is a compact connected complex manifold with a group structure. If A has dimension g and we denote by $T_e(A(\mathbb{C}))$ the tangent space at e of $A(\mathbb{C})$, then there exists a unique homomorphism

$$\exp : T_e(A(\mathbb{C})) \to A(\mathbb{C}),$$

of complex manifolds such that for each $v \in T_e(A(\mathbb{C}))$ the map $z \mapsto \exp(zv)$ is a one-parameter subgroup $\varphi_v : \mathbb{C} \to A(\mathbb{C})$ corresponding to v. Moreover, the map exp is surjective and its kernel is a $\mathbb{Z}$-module L of full rank in $T_e(A(\mathbb{C}))$, that is, $\operatorname{rank}(L) = 2g$. Hence, $A(\mathbb{C})$ is isomorphic to the *complex torus* $\mathbb{C}^g/L$. But if $g > 1$ then the converse does not hold, that is, not every complex torus arises from an abelian variety.

Definition 2.1. *Let V be a complex vector space and let L be a full rank lattice in V. Consider a skew-symmetric form $L \times L \to \mathbb{Z}$ and its extension $E_{\mathbb{R}} : V \times V \to \mathbb{R}$. We call E a* Riemann form *on $X = V/L$ if:*

- *$E_{\mathbb{R}}(iv, iw) = E_{\mathbb{R}}(v, w)$ for every v and w in V, and*
- *the associated Hermitian form $H_E(v, w) := E_{\mathbb{R}}(iv, w) + iE_{\mathbb{R}}(v, w)$ is positive definite.*

We say that X is a polarizable torus *if it admits a Riemann form.*

A homomorphism of complex tori V/L and V'/L' is a $\mathbb{C}$-linear map $V \to V'$ that sends L into L'.

Theorem 2.2. *The functor $A \mapsto A(\mathbb{C})$ is an equivalence of categories from the category of abelian varieties over $\mathbb{C}$ to the category of polarizable tori.*

Let $X = V/L$ be a complex torus. Define the dual torus as $X^\vee = V^*/L^*$ where

$$V^* := \{\text{antilinear functionals } V \to \mathbb{C}\}$$

and

$$L^* := \{f \in V^* : \operatorname{Im}(f(L)) \subseteq \mathbb{Z}\}.$$

If A corresponds to X under the functor of Theorem 2.2, then the dual abelian variety $A^\vee$ will correspond to the dual torus $X^\vee$. A Riemann form E on X defines a homomorphism $\lambda_E : X \to X^\vee$ by $\lambda_E(v) = H_E(v,\cdot) : V \to V^*$. Then λ_E is an isogeny and it is in fact a polarization with degree equal to the size of the kernel. So the functor of Theorem 2.2 reduces the study of complex polarized abelian varieties to the study of polarized complex tori, which can be studied using linear algebra.

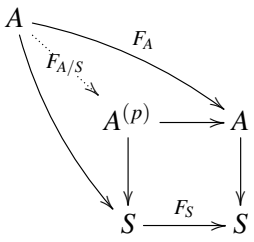
3 Abelian varieties in positive characteristic

In this section we focus on the case when k has characteristic equal to $p > 0$. The picture that we will obtain is much wilder compared to the situation over $\mathbb{C}$. For example, the statement of Theorem 2.2 does not hold. More precisely, it is not possible to functorially attach to an abelian variety of dimension g a free abelian group of rank $2g$ on the whole category of abelian varieties over k, as the next example indicates.

Example 3.1. *(Serre) Let E be a* supersingular *elliptic curve over $\overline{\mathbb{F}}_p$, that is an elliptic curve whose endomorphism algebra is a non-split quaternion algebra (see [Sil09, Theorem 3.1] for other equivalent definitions). Such algebras do not admit* 2*-dimensional $\mathbb{Q}$-representations.*

Nevertheless, over finite fields there are theorems analogous to Theorem 2.2, under some assumptions on the isogeny class in consideration, as we explain at the end of the section. See also Papers II and III of the thesis.

One of the peculiarities of working over a field of positive characteristic p is that the map $x \mapsto x^p$ is a ring homomorphism and hence induces a map on geometric objects defined over k. More precisely, if S is a scheme over $\mathbb{F}_p$ we define the *absolute Frobenius* of S to be the morphism $F_S : S \to S$ induced by the ring homomorphism $\mathcal{O}_S \to \mathcal{O}_S : x \to x^p$. Let A be a scheme over S. Define $A^{(p)}$ to be the fibered product $A \times_S S$ induced by the absolute Frobenius F_S. We define the *relative Frobenius* $F_{A/S}$ of A by



where F_A is the relative Frobenius induced by the $\mathbb{F}_p$-scheme structure of A and the vertical arrows are the projection $A^{(p)} \to S$ and the S-scheme structure map of A, respectively.

Example 3.2. *Let A be an affine scheme over $S = \mathrm{Spec}(\mathbb{F}_q)$ defined by a polynomial $\sum_I a_I X^I$, where I is a multi-index. Then $A^{(p)}$ is defined by $\sum_I a_I^p X^I$ and the relative Frobenius $F_{A/S}$ is the map $X_i \mapsto X_i^p$.*

If A is an abelian variety over a finite field $\mathbb{F}_{p^n}$ then the relative Frobenius sends zero to zero and so it is a homomorphism of group schemes. Moreover, we can identify $A^{(p^n)} \simeq A$ and we can define the *Frobenius* of A over $\mathbb{F}_{p^n}$ as

$$\pi_A = \left(A \xrightarrow{F_{A/S}} A^{(p)} \xrightarrow{F_{A^{(p)}/S}} A^{(p^2)} \xrightarrow{F_{A^{(p^2)}/S}} \ldots \to A^{(p^{n-1})} \xrightarrow{F_{A^{(p^{n-1})}/S}} A^{(p^n)} \simeq A. \right).$$

Proposition 3.3. *Let A be an abelian variety over k of dimension g, where k is field of characteristic $p > 0$. Then the relative Frobenius $F_{A/k}$ is an isogeny of degree p^g.*

By Proposition 1.8 there exists an isogeny $V_{A/k} : A^{(p)} \to A$ of degree p^g called the *relative Verschiebung* such that $V_{A/k} \circ F_{A/k} = [p]_A$ and $F_{A/k} \circ V_{A/k} = [p]_{A^{(p)}}$. As for the Frobenius, we can also define the *Verschiebung* as the n-th iterate of the relative Verschiebung.

3.1 Weil conjectures

Let V be a non-singular projective variety of dimension n over a finite field $\mathbb{F}_q$ with $q = p^d$, where p is any prime number. Observe that the number of points $V(\mathbb{F}_{q^m})$ of V defined over $\mathbb{F}_{q^m}$, which we will denote by N_m, is finite. We define the *Hasse-Weil zeta function* of V by

$$\zeta(V,T) = \exp\left(\sum_{m \geq 1} \frac{N_m}{m} T^m \right).$$

This function turns out to be a very important tool to study the variety V, since it encodes a lot of its arithmetic and geometric properties. For example, we can recover N_m by evaluating the following expression at $T = 0$:

$$\frac{1}{(m-1)!} \frac{d^m}{d^m T} \log(\zeta(V,T)).$$

Theorem 3.4. *(Weil conjectures) Let V be a non-singular projective variety of dimension n over a finite field $\mathbb{F}_q$.*

1. *(Rationality)*
$$\zeta(V,T) \in \mathbb{Q}(T);$$

2. *(Riemann hypothesis)*
   We can write

$$\zeta(V,T) = \frac{P_1(T)P_3(T)\dots P_{2n-1}(T)}{P_0(T)P_2(T)\dots P_{2n}(T)},$$

   where $P_i(T) \in \mathbb{Z}[T]$. Moreover we have that $P_0(T) = (1-T)$ and $P_{2n} = (1-q^nT)$ and for $1 \le i \le 2n-1$ the polynomial $P_i(T)$ factors (over $\mathbb{C}$) as $\prod_j (1-\alpha_{i,j}T)$, for some algebraic integers $\alpha_{i,j}$, with $|\alpha_{i,j}| = q^{i/2}$, that is, all the zeros of $P_i(T)$ lie on a circle;

3. *(Functional equation)*
   There is an integer χ called the Euler characteristic of V such that the zeta function satisfies the following equation:

$$\zeta(V, 1/q^nT) = \pm q^{\frac{n\chi}{2}} T^{\chi} \zeta(V,T),$$

   This implies that the numbers $\alpha_{i,j}$ are symmetric in the sense that in an appropriate ordering we have that the numbers $\alpha_{2n-i,1}, \alpha_{2n-i,2}, \dots$ are equal to $q^n/\alpha_{i,1}, q^n/\alpha_{i,2}, \dots$.

4. *(Betti numbers)*
   If V is the reduction modulo p of a non-singular variety Y defined over a number field, then the degree of each P_i is the i-th Betti number of the topological space $Y(\mathbb{C})$.

These conjectures were proposed by Weil in 1949 and proved by him for curves and abelian varieties. The rationality part was first proved by Dwork in 1960 with methods from p-adic functional analysis. A different proof was later given by Grothendieck and his collaborators using the ℓ-adic cohomology which also established the functional equation and the connection with the Betti numbers. Finally in 1974, Deligne proved the Riemann hypothesis.

3.2 The Tate module and the Frobenius endomorphism

Let A be an abelian variety over a perfect field k and let ℓ be a prime distinct from the characteristic of k. Then the multiplication by ℓ^m is a group homomorphism whose kernel $A[\ell^m]$ is a finite group scheme of rank $(\ell^m)^{2g}$, where g is the dimension of A. This implies that $A[\ell^m]$ is étale and hence it is completely described by its $\bar{k}$-points and the action of the absolute Galois group $\mathcal{G} = \mathrm{Gal}(\bar{k}/k)$.

The group schemes $A[\ell^m]$ form an inverse system under the multiplication by $\ell : A[\ell^{m+1}] \to A[\ell^m]$. We define the *$\ell$-Tate module* of A by

$$T_\ell A = \varprojlim A[\ell^m](\bar{k}).$$

It is a free $\mathbb{Z}_\ell$-module of rank $2g$ and $\mathcal{G}$ acts on it by $\mathbb{Z}_\ell$-linear maps. Moreover, we have an isomorphism of $\mathcal{G}$-modules $A[\ell^m](\overline{k}) \simeq T_\ell A/\ell^m T_\ell A$.

Consider a homomorphism of abelian varieties $\varphi : A \to B$. It sends $A[\ell^m]$ to $B[\ell^m]$ and hence it induces a morphism $\varphi_\ell : T_\ell A \to T_\ell B$. In particular this makes T_ℓ a functor from the category of abelian varieties over k to the category of $\mathbb{Z}_\ell[\mathcal{G}]$-modules.

Observe that $\mathrm{Hom}_{\mathbb{Z}_\ell[\mathcal{G}]}(T_\ell A, T_\ell B)$ has finite rank. An explicit formula for its rank depending on the factorizations of the characteristic polynomials of the maps induced by the Frobenius endomorphism of A and of B can be found in [Tat66].

Theorem 3.5 (Weil)**.** *Let A and B be two abelian varieties over a perfect field k and let ℓ be prime number distinct from the characteristic of k. The natural morphism*

$$\varphi : \mathrm{Hom}(A,B) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \to \mathrm{Hom}_{\mathbb{Z}_\ell[\mathcal{G}]}(T_\ell A, T_\ell B)$$

is injective. In particular, $\mathrm{Hom}(A,B)$ *is a free $\mathbb{Z}$-module of finite rank.*

Let A be an abelian variety over a finite field $\mathbb{F}_q$, with zeta-function

$$\zeta(A,T) = \frac{P_1(T)P_3(T)\dots P_{2g-1}(T)}{P_0(T)P_2(T)\dots P_{2g}(T)}.$$

The Frobenius π_A of A induces an endomorphism $T_\ell \pi_A$ of $T_\ell A$. Let h_A be its characteristic polynomial. It can be proven that $h_A = P_1$ and that P_r is the characteristic polynomial of the action of π_A on $\bigwedge^r T_\ell A$. In particular, $h_A \in \mathbb{Z}[T]$ and it does not depend on the prime $\ell \neq p$. The polynomial h_A will be called the *characteristic polynomial* of Frobenius π_A, or simply the characteristic polynomial of A.

Since the action of π_A on $T_\ell A$ is semisimple, we obtain by Theorem 3.5 that the $\mathbb{Q}$-algebra $\mathrm{End}^0(A)$ is a semisimple algebra of finite rank, which has center $\mathbb{Q}(\pi_A)$. If

$$A \sim B_1^{m_1} \times \dots \times B_r^{m_r},$$

as in Corollary 1.18, then

$$\mathrm{End}^0(A) = \prod \mathrm{End}^0(B_i^{m_i})$$

and for each i we have $\mathrm{End}^0(B_i^{m_i}) = M_{m_i}(\mathrm{End}^0(B_i))$. In particular $\mathbb{Q}(\pi_A)$ splits into a finite product of number fields, namely $\mathbb{Q}(\pi_A) = \prod \mathbb{Q}(\pi_{B_i})$.

Definition 3.6. *Let $q = p^n$ be a prime power. A* q-Weil number π *is an algebraic integer such that for every embedding $\psi : \mathbb{Q}(\pi) \to \mathbb{C}$ we have $|\psi(\pi)| = \sqrt{q}$. We say that two q-Weil numbers π and π' are conjugate if there exists a field isomorphism $\mathbb{Q}(\pi) \simeq \mathbb{Q}(\pi')$ (sending π to π'). Observe that this is equivalent to saying that the minimal polynomials of π and π' are the same.*

Theorem 3.7 (Weil)**.** *If A is a simple abelian variety over $\mathbb{F}_q$ then the Frobenius endomorphism π_A of $A/\mathbb{F}_q$ is a q-Weil number.*

This is a consequence of 1.20 and the next proposition.

Proposition 3.8. *For a simple abelian variety A over $\mathbb{F}_q$ we have:*

$$\pi_A \cdot \pi_A^\dagger = q.$$

3.3 Honda-Tate theory

The Frobenius endomorphism π_A of an abelian variety A defined over a finite field $\mathbb{F}_q$ is an invariant of the variety up to isogeny and the fact that it is an algebraic integer allows us to enumerate them, which leads to a complete classification. This will be the starting point for the computation of the isomorphism classes.

Theorem 3.9 (Tate)**.** *Let A and B be two abelian varieties over a finite field k, the morphism φ in Theorem 3.5 is then an isomorphism.*

Proof. See [Tat66, Main Theorem]. □

As important consequences, we have:

Theorem 3.10. *Let A and B be two abelian varieties over the finite field $\mathbb{F}_q$, where q is a prime power, with characteristic polynomials h_A and h_B, respectively. Then B is $\mathbb{F}_q$-isogenous to a subvariety of A if and only if h_B divides h_A. Moreover, the following are equivalent:*

- *A is $\mathbb{F}_q$-isogenous to B*
- *$h_A = h_B$*
- *the zeta-functions of A and B are the same*
- *A and B have the same number of points over $\mathbb{F}_{q^m}$ for every $m > 0$.*

Proof. See [Tat66, Theorem 3]. □

Consider the map Φ that sends a simple abelian variety A defined over $\mathbb{F}_q$ to its Frobenius π_A, considered as an algebraic integer. Observe that the characteristic polynomial h_A of π_A is a power of an irreducible polynomial, which will be the minimal polynomial of π_A over $\mathbb{Q}$. In view of Tate's Theorem 3.10, Φ induces an injective map between the isogeny classes of simple abelian varieties over $\mathbb{F}_q$ and the conjugacy classes of q-Weil numbers. Honda in [Hon68] proved that this is also surjective.

Theorem 3.11 (Honda-Tate)**.** *The map that sends a simple abelian variety A defined over $\mathbb{F}_q$ to the algebraic integer π_A defined by its Frobenius endomorphism induces a bijection between the isogeny classes of simple abelian varieties over $\mathbb{F}_q$ and conjugacy classes of q-Weil numbers.*

In particular we obtain that the isogeny class of an abelian variety A over $\mathbb{F}_q$ is completely determined by its *Weil support* $\{\pi_{B_1}, \ldots, \pi_{B_r}\}$ consisting of the conjugacy classes of Frobenius morphisms of the simple abelian varieties B_i's and positive integers m_i's such that

$$A \sim_{\mathbb{F}_q} B_1^{m_1} \times \ldots \times B_r^{m_r},$$

see Corollary 1.18.

This implies that in order to enumerate the abelian varieties defined over a finite field $\mathbb{F}_q$ up to isogeny of a given dimension g, it suffices to enumerate the q-Weil polynomials polynomials h of degree $2g$. Note that non all of such polynomials give rise to an isogeny class of varieties of dimension g, see Paper II for more details. Using Theorem 3.4 we can find bounds for the coefficients of such h, which shows that this is a finite problem. Refined algorithms to produce all such polynomials h can be found in [Hal10] and [HS12] for $g = 3$ and $g = 4$, respectively, and also [Ked08].

3.4 Categorical descriptions

Let $q = p^d$, where p is a prime number. We have seen that the abelian varieties over a finite field $\mathbb{F}_q$ can easily be enumerated up to isogeny, but in order to compute them up to isomorphism we need a more refined classification. As already mentioned at the beginning of the section, there is no hope to find a categorical equivalence in terms of lattices of full rank on the whole category of abelian varieties over $\mathbb{F}_q$, as we have in Theorem 2.2. Nevertheless, we can obtain similar functorial descriptions if we restrict ourselves to some subcategories of the category of abelian varieties over $\mathbb{F}_q$.

Definition 3.12. *Let A be an abelian variety over $\mathbb{F}_q$ with characteristic polynomial of Frobenius h_A. We say that A is* ordinary *if exactly half of the roots of h_A over $\mathbb{Q}_p$ are p-adic units.*

For other equivalent definitions we refer to [Del69, Section 2]. Denote by $\mathrm{AV}^{\mathrm{ord}}(q)$ the category of ordinary abelian varieties over $\mathbb{F}_q$. Consider the category $\mathcal{M}^{\mathrm{ord}}(q)$ consisting of pairs (T, F) where T is a finitely generated free $\mathbb{Z}$-module, say of rank $2g$, and F is a $\mathbb{Z}$-linear endomorphism of T such that

(a) $F \otimes_{\mathbb{Z}} \mathbb{Q}$ acts semisimply on $T \otimes_{\mathbb{Z}} \mathbb{Q}$ with eigenvalues with complex absolute value $\sqrt{q}$;

(b) half of the roots of the characteristic polynomial h of F (over $\mathbb{Q}_p$) are p-adic units;

(c) there exists $V : T \to T$ such that $F \circ V = q$.

A morphism in $\mathcal{M}^{\mathrm{ord}}(q)$ is given by a commutative diagram

$$\begin{array}{ccc} T & \xrightarrow{\varphi} & T' \\ {\scriptstyle F}\downarrow & & \downarrow{\scriptstyle F'} \\ T & \xrightarrow{\varphi} & T' \end{array}$$

Let W denote the ring of Witt vectors $W(\overline{\mathbb{F}}_q)$ and fix an embedding $\varepsilon : W \to \mathbb{C}$. Let A be in $\mathrm{AV}^{\mathrm{ord}}(q)$ and let $\tilde{A}$ be the *Serre-Tate canonical lift* of A to W. Put

$$T(A) = H_1(\tilde{A} \otimes_{\varepsilon} \mathbb{C}, \mathbb{Z}).$$

Observe that this construction is functorial in each step and hence the $\mathbb{Z}$-module $T(A)$ comes equipped with a morphism $F(A)$ which corresponds to the Frobenius endomorphism of A and that $\mathrm{Rank}\, T(A) = 2\dim(A)$.

Consider the functor

$$\begin{aligned} \mathcal{F}^{\mathrm{ord}} : \mathrm{AV}^{\mathrm{ord}}(q) &\to \mathcal{M}^{\mathrm{ord}}(q) \\ A &\mapsto (T(A), F(A)) \end{aligned}$$

for which we have the following theorem.

Theorem 3.13. *The functor $\mathcal{F}^{ord}$ induces an equivalence between $\mathrm{AV}^{ord}(q)$ and $\mathcal{M}^{ord}(q)$.*

Proof. See [Del69, Théorème]. □

Howe in [How95] describes how to use Theorem 3.13 to describe the dual of an abelian variety and polarizations in the category $\mathcal{M}^{\mathrm{ord}}(q)$. We refer also to Papers II and III for more details.

Deligne's result above has been extended to a much larger subcategory of abelian varieties defined over the prime field $\mathbb{F}_p$ by Centeleghe and Stix in [CS15]. More precisely consider the category $\mathcal{M}^{\mathrm{cs}}(p)$ consisting of pairs (T, F) as above. We set $q = p$ and we replace condition (b) by

(b') the characteristic polynomial h of F has no real roots.

Denote by $\mathrm{AV}^{\mathrm{cs}}(p)$ the category of abelian varieties over $\mathbb{F}_p$ whose characteristic polynomial of Frobenius does not have real roots. Then the following holds.

Theorem 3.14. *There is an anti-equivalence of categories*

$$\mathcal{F}^{cs} : \mathrm{AV}^{cs}(p) \to \mathcal{M}^{cs}(p)$$

Proof. See [CS15, Theorem 1]. □

The functor $\mathcal{F}^{\mathrm{cs}}$ from Theorem 3.14 does not rely on lifting the abelian varieties from $\mathbb{F}_p$ to characteristic zero, and it is not known what a polarization in $\mathrm{AV}^{\mathrm{cs}}(p)$ will correspond to in $\mathcal{M}^{\mathrm{cs}}(p)$.

Remark 3.15. *There are other functors from subcategories of the category of abelian varieties over a finite field to some category of finitely generated free $\mathbb{Z}$-modules, see for example the Appendix to [Lau02], [Kan11] and the recent pre-print [JKP+17]. We will not discuss these functors since we are not using them in our computations.*

4 Summary of results

Theorems 3.13 and 3.14 are the key results that we are are going to use in the papers that constitute the core of this thesis, where we describe algorithms to effectively compute the isomorphism classes of abelian varieties over a finite field $\mathbb{F}_q$, where q is a power of a prime p, in a given isogeny class determined by a q-Weil polynomial h which satisfies certain hypotheses. If the isogeny class is ordinary then we are also able to describe the polarizations and the group of automorphisms of the corresponding polarized abelian variety.

4.1 Paper I

In the first paper we give a survey of the theory of orders in finite étale $\mathbb{Q}$-algebras, that is, finite products of number fields, and of their fractional ideals. For such an order R in K we describe how to compute the *ideal class monoid* $\mathrm{ICM}(R)$ of R, that is the set of isomorphism classes of fractional R-ideals, which has the structure of a commutative monoid with the operation induced by ideal multiplication. There are algorithms to compute the invertible ideal classes (which form the Picard group $\mathrm{Pic}(R)$) that are well known, at least in the case when R is a integral domain. Not much is known about the non-invertible ideals which appear as soon as R is not the maximal order $\mathcal{O}_K$ of K. We first address the problem locally, by studying the so-called weak equivalence relation between fractional R-ideals and we produce an algorithm to compute representatives of the corresponding equivalence classes, denoted $\mathcal{W}(R)$. Then we reconstruct all the (global) isomorphism classes by considering the action of the Picard groups of the over-orders of R on the weak equivalence classes.

As an application we generalize a Theorem of Latimer and MacDuffee that allows us to describe the conjugacy classes of integral matrices with given minimal polynomial m and characteristic polynomial c. Under certain assumptions on m and c we can explicitely compute representatives of these matrices in terms of the ideal class monoid of the monogenic order $\mathbb{Z}[x]/(m)$.

A preliminary version of the results contained in Paper I was already in the licentiate thesis [Mar16]. More precisely, the algorithm to compute the isomorphism classes was described only in the case when K was an integral domain. We point out that if the generalization of the theory was fairly straightforward, then on the other hand the algorithmic part had to be done from scratch. Also, Examples 6.1 and 6.2 were already contained in [Mar16]. The code for the algorithms is available on the webpage of the author.

4.2 Paper II

The second paper is devoted to computing the isomorphism classes of abelian varieties over a finite field. Let $\mathrm{AV}(q)$ be the category of abelian varieties over a finite field $\mathbb{F}_q$, where q is a power of a prime number p. Let h be a q-Weil polynomial and let $\mathrm{AV}(h)$ be the full sub-category of $\mathrm{AV}(q)$ consisting of the abelian varieties in the isogeny class determined by h. Assuming that h is square-free and ordinary we prove that there exists an equivalence of categories between $\mathrm{AV}(h)$ and the category of fractional R-ideals (with R-linear morphisms), where R is the order $\mathbb{Z}[x,y]/(h(x),xy-q)$. In particular we deduce that the isomorphism classes are in bijection with $\mathrm{ICM}(R)$. An analogous result holds in the more general situation when h has no real roots but with the restriction that $q=p$. In the ordinary case we are also able to give a description of the polarizations of an abelian variety A in $\mathrm{AV}(h)$ and we produce an algorithm to compute the polarizations of a given degree up to isomorphism (of the polarized abelian variety). Given a principally polarized abelian variety (A,a) in $\mathrm{AV}(h)$ (with h ordinary) we are able to produce a period matrix associated to the complexification of the canonical lift of (A,a) to characteristic zero.

As for Paper I, a preliminary version of the results of Paper II was already in the licentiate thesis [Mar16]. More precisely, the algorithm to compute the isomorphism class was developed only for irreducible characteristic polynomials h and we were only able to compute principal polarizations. The generalization to the square-free case and to polarizations of higher degree is new. Also the algorithm to compute the period matrices is novel. Examples 7.3 and 7.4 were already contained in [Mar16].

An implementation of the algorithms is available on the webpage of the author.

4.3 Paper III

In the third paper we extend the description given in the second paper to abelian varieties isogenous to a power of an abelian variety. More precisely, let q be a power of a prime p and let $\mathrm{AV}(q)$ be the category of abelian varieties over $\mathbb{F}_q$. Define $\mathrm{AV}(h)$ as the full-subcategory of $\mathrm{AV}(q)$ consisting of the varieties in the isogeny class determined by h, where $h = g^r$ for a square-free ordinary q-Weil polynomial g or a square-free p-Weil polynomial g with no real roots. Put $R = \mathbb{Z}[x,y]/(g(x), xy - q)$ (with $q = p$ in the second case). We prove that there is an equivalence of categories between $\mathrm{AV}(q)$ and the category of torsion free R-modules M of rank r, that is $M \otimes K = K^r$, where $K = R \otimes_{\mathbb{Z}} \mathbb{Q}$.

Such modules are classified in terms of fractional R-ideals when the order R is Bass, that is when each over-order is Gorenstein, or equivalently when each fractional R-ideal is invertible in its multiplicator ring. In this situation we are able to compute the isomorphism classes of the abelian varieties in $\mathrm{AV}(h)$.

In the ordinary case we are also able to translate the notion of dual variety and of polarization to the module theoretic setting.

4.4 Paper IV

In this short note, we use the descriptions of Paper 2 and 3 of $\mathrm{AV}(q)$ to answer questions about base field extension. More precisely, if I is the fractional ideal corresponding to a simple ordinary abelian variety A over $\mathbb{F}_q$, we describe how to identify the module M corresponding to the variety $A_r = A \otimes \mathbb{F}_{q^r}$.

The results of this short note are presented separately since they are preliminary and with further work they could lead to an algorithmic test for finding absolutely indecomposable polarized abelian varieties, that is polarized abelian varieties that cannot be written as a product of polarized abelian varieties over any algebraic extension of the base field, and hence could be used to test whether an isomorphism class contains a Jacobian of a curve.

4.5 Computational remarks

Some steps in the algorithms presented in the papers are not efficient even if in practice they work well for most orders of rank up to 8 and hence isogeny classes of abelian varieties of dimension 4. Here we describe some of the computational issues that we have occasionally encountered. In order to compute $\mathrm{ICM}(R)$ we first need to know the over-orders of R which we compute by looking at the subgroup of the finite group $\mathcal{O}_K/R$, where $\mathcal{O}_K$ is the maximal order of $K = R \otimes \mathbb{Q}$. If the order R is "very singular" this group might be too

big to be handled from a computational point of view. Similarly, for a non-Gorenstein order R, in order to compute the weak equivalence classes of ideals I with $(I:I) = R$ we need to consider the subgroups of $H = T/(R:T)$, where T is an over-order of R such that the extension R^tT of the trace-dual ideal R^t of R is invertible (in T). Again, H might have a very big and complicated lattice of subgroups.

In order to compute the polarizations of an abelian variety A corresponding to a fractional R-ideal I in K, we need to compute a specific CM-type which detects the complex structure coming from characteristic p on the canonical lift of A to characteristic zero. Our method requires us to compute a Galois closure of K and such computation occasionally does not terminate on Magma [BCP97].

Finally, even if in Paper III we describe the polarizations of an abelian variety A corresponding to a module M we are not able to compute them (up to isomorphism) since this requires us to deal with a quotient of an infinite non-abelian group by the action $\mathrm{Aut}(A)$ which also is infinite and non-abelian.

References

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265. MR MR1484478 11, 30

[BFvdG14] Jonas Bergström, Carel Faber, and Gerard van der Geer, *Siegel modular forms of degree three and the cohomology of local systems*, Selecta Math. (N.S.) **20** (2014), no. 1, 83–124. MR 3147414 12

[CS86] Gary Cornell and Joseph H. Silverman (eds.), *Arithmetic geometry*, Springer-Verlag, New York, 1986. MR 861969 13

[CS15] Tommaso Giorgio Centeleghe and Jakob Stix, *Categories of abelian varieties over finite fields, I: Abelian varieties over* $\mathbb{F}_p$, Algebra Number Theory **9** (2015), no. 1, 225–265. MR 3317765 11, 26, 27

[Del69] Pierre Deligne, *Variétés abéliennes ordinaires sur un corps fini*, Invent. Math. **8** (1969), 238–243. MR 0254059 11, 19, 25, 26

[Hal10] Safia Haloui, *The characteristic polynomials of abelian varieties of dimensions 3 over finite fields*, J. Number Theory **130** (2010), no. 12, 2745–2752. MR 2684495 25

[Har77] Robin Hartshorne, *Algebraic geometry*, Springer-Verlag, New York-Heidelberg, 1977. MR 0463157 13

[Hon68] Taira Honda, *Isogeny classes of abelian varieties over finite fields*, J. Math. Soc. Japan **20** (1968), 83–95. MR 0229642 12, 24

[How95] Everett W. Howe, *Principally polarized ordinary abelian varieties over finite fields*, Trans. Amer. Math. Soc. **347** (1995), no. 7, 2361–2401. MR 1297531 11, 26

[HS12] Safia Haloui and Vijaykumar Singh, *The characteristic polynomials of abelian varieties of dimension 4 over finite fields*, Arithmetic, geometry, cryptography and coding theory, Contemp. Math., vol. 574, Amer. Math. Soc., Providence, RI, 2012, pp. 59–68. MR 2961400 25

[JKP+17] Bruce W. Jordan, Allan G. Keeton, Bjorn Poonen, Eric M. Rains, Nicholas Shepherd-Barron, and John T. Tate, *Abelian varieties isogenous to a power of an elliptic curve*, arXiv:1602.06237v2, 2017. 27

[Kan11] Ernst Kani, *Products of CM elliptic curves*, Collect. Math. **62** (2011), no. 3, 297–339. MR 2825715 27

[Ked08] Kiran S. Kedlaya, *Search techniques for root-unitary polynomials*, Computational arithmetic geometry, Contemp. Math., vol. 463, Amer. Math. Soc., Providence, RI, 2008, pp. 71–81. MR 2459990 25

[Lau02] Kristin Lauter, *The maximum or minimum number of rational points on genus three curves over finite fields*, Compositio Math. **134** (2002), no. 1, 87–111, With an appendix by Jean-Pierre Serre. MR 1931964 27

[Mar16] Stefano Marseglia, *Isomorphism classes of abelian varieties over finite fields*, Stockholm University, 2016. 12, 28

[Mum08] David Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, vol. 5, Hindustan Book Agency, New Delhi, 2008. MR 2514037 16

[Sil09] Joseph H. Silverman, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR 2514094 20

[Tat66] John Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1966), 134–144. MR 0206004 11, 23, 24